



FortiGate Firewall

FortiGate Essentials

By- Mohamed Marfadi

1	المقدمة
2	كلمة شكر وعرفان
3	مقدمة عن فورتى جيت
4	طريقة تنزيل وضبط اعدادات FortiGate vm
12	ضبط اعدادات كرت الشبكة على جهاز الكلاينت (Client)
18	طريقة عمل reset لعدد الأيام (14) لل VM
20	مشكله ظهور بان الايسنز (License) قد انتهى
20	طريقة عمل باك اب للإعدادات التابعه لل VM وكيفيه استعادتها
23	شرح مكونات وواجهات الفورتى جيت
24	طريقة تغيير باسورد الأدمن (admin) بواسطة CLI
24	إيقاف او اعاده التشغيل او تغيير الباسورد او للخروج من الفورتى ويب عبر GUI
25	شرح ال DASHBOARD
29	شرح القوائم
29	شرح استخدامات ومعلومات ال Widget
39	طريقة توصيل الانترنت لجهاز الفورتى جيت
44	متى احتاج الى عمل ترقيه - تحديث- لل Firmware التابع لجهاز الفورتى
44	طرق ترقيه النظام Upgrade firmware
45	عملية ال downgrade
45	Administration types & profiles
47	طريقة انشاء يوزر جديد بواسطة CLI

- 49 لحذف يوزر بواسطة CLI
- 52 ما هو FortiGuard ؟
- 53 SD-WAN=WAN Link Load Balancing SD-WAN
- 61 طريقة انشاء SD-WAN Rule جديده
- 62 جعل الـ https traffic يطلع عبر الـ wan 2
- 63 جعل الـ http traffic يطلع عبر الـ wan1
- 64 انشاء SLA باسم INTERNET حيث تقوم بفحص الخط الأفضل
- 66 طريقة اظهار ميزه جديده مثلا تريد اظهار الخاصية (features)
- 67 طريقة انشاء Rule policy جديده
- 70 شرح Schedule
- 70 طريقة انشاء schedule
- 73 تحديد أيام محدده ووقت محدد مره واحده فقط وينتهي
- 74 أنواع الـ actions في الـ policy
- 75 Traffic shapers
- 76 APPLICATION CONTROL
- 82 Web Filter
- 82 ما هو الـ fortiguard
- 82 ماهي فكره الـ Fortiguard
- 83 طريقة انشاء web filter profile
- 89 طريقة اغلاق موقع معين بالإضافة الى sub domain بواسطة الـ web filter
- 90 بعض التمارين والأمثلة حول الـ web filter واستخدام static URL filter

أساسيات فورتى جيت

98	Web category based filtering
101	Web category usage quota
105	Web Category Based Filter Overriding
107	Web Rating Override
109	Web Profile overrides
110	ADDRESS
112	Fortinet solution
113	Firewall
114	تسلسل واشكال الفايروول
116	Bandwidth ,Throughput ,Concurrent Sessions
118	FortiGate Series
119	موديلات فورتى جيت
119	Operating system OS key features 5 2
120	Home lab Design
121	FortiGate basics Registering FortiGate
121	طريقة عمل Registration لجهاز الفورتى جيت
122	ماهي ال features
126	ما هو Revisions في الفورتى جيت
129	NTP server(Network time protocol)
131	تصميم الشبكة
133	Advice administration

- 136 طريقة رفع مستوى الأمان عند الوصول الى جهاز الفورتني جيت
- 144 ما هو Trusted hosts
- 147 Interface ip address
- 153 Static route(default gateway)(static gateway)
- 156 Password recovery
- 158 طريقة عمل MAINTAINER MODE ↓ DISABLE
- 159 Password policy
- 162 كيف تفعيل DHCP server على الفورتني
- 165 بعض الأوامر (Cmd) التي يتم تطبيقها على اجهزه الكلاينت
- 168 طريقة تعديل الـ leased duration في الـ dhcp server
- 172 DNS(domain name service)
- 173 FortiGuard Concept
- 175 Fortiguard distribution network (FDN)
- 178 FortiExplorer
- 179 Fortigate firewall policy
- 180 ماهي انواع الـ objects الأساسية (الضرورية)
- 182 طريقة انشاء البوليسي
- 185 Firewall objects
- 193 شرح بعض اعمده الـ address list
- 201 ماهي أنواع الـ services ؟

206 ما هو الـ <i>service group</i>
208 <i>Schedule</i>
208 طريقة انشاء <i>schedule</i> جديد
214 طريقة انشاء <i>schedule group</i>
219 <i>Policy order</i>
224 <i>Managing devices</i>
225 كيف يقوم فورتى جيت بأداره الأجهزة؟
232 <i>Access control list (ACL)</i>
233 ما هو <i>Mac reservation</i>
243 <i>FortiClient</i>
245 طريقة تنزيل الفورتى كلاينت على الاجهزه
246 <i>Authentication</i>
247 ماهي طرق الـ authentication (التحقق من الهوية) في الفورتى جيت
248 <i>Local authentication</i>
256 <i>Max invalid authentication</i>
257 <i>Authentication timeout</i>
261 <i>Restricting number of concurrent user logons</i>
262 <i>Managing guests</i>
273 <i>FSSO(fortinet single sign on)</i>
279 الطريقة الأولى <i>Poll Active Directory server</i>
284 الطريقة الثانية لعمل الـ <i>integeration</i> بين الفورتى جيت والـ AD

302	Collector Agent	العمل عبر اختيار integration
303	Antivirus	
304		كيف تفرق بين قواعد بيانات الفيروسات على جهاز الفورتي جيت؟
304		كيف سيتم عمليه التحديث لل Antivirus DB؟
309		طريقة تفعيل ال antivirus على الفورتي جيت وعمل حمايه للشبكة من أي تهديدات ...
309		طريقة انشاء بروفایل جديد ل antivirus
311		طريقة اختيار البروفایل مخصص في البوليسي
312		Antivirus Mode
314		متى يتم استخدام flow base ومتى يتم استخدام proxy base؟
314		ماهي طريقة عمل مكافح الفيروسات في الفورتي
316		Antivirus Profile configuration
317		Web filtering
317		أسباب التحكم في Web filtering
318		Web filtering mode
319		ماهي الخيارات المتاحة على الفورتي جيت بخصوص web filtering
320		ماهي علاقه فورتي جار بالفورتي جيت
321		كيفيه التعامل مع ال fortiguard category في ال web filter
332		أنواع ال action
348		Web URL filtering
357		Web content filter
362		Application controller

363	Application control action
363	Traffic shape ما هو
370	Application control طريقة التحكم في التطبيقات عبر
371	category لمعرفة ماهي البرامج (signatures) التي بتكون مندرجه تحت الـ
373	Application and Filter Overrides
379	طريقة عمل حظر (ban) لجهاز معين
383	Email filter
387	ماهي الطرق التي يستخدمها الفورتى جيت لكي يساعدك لاكتشاف الاسباب ايميل؟
393	Logging and monitoring
395	VPN (Virtual private Network)
396	اشكال الاتصال الـ VPN او يسمى (VPN Tunnel designs)
398	أنواع بروتوكولات الـ VPN
398	VPN Encryption
400	التطبيق العملي لـ IPSec Client/server
413	IPSec SITE to SITE
416	vpn over SSL
435	VPN SITE TO SITE تمرين اخر حول
440	VPN SITE TO SITE DYNAMIC DNS (DDNS)
442	Network address
443	Traffic shaper
445	انواع الـ traffic shaper

أساسيات فورتني جيت

445	Traffic shaping policy	طريقة انشاء
447	Virtual IP	
448	Virtual ip	طريقة انشاء
450	Virtual group	
451	virtual group	طريقة انشاء
454	IPV4 DOS policy configuration	
457	DNS Filtering	
459	web filter And dns filter	الفرق بين ال
460		الخاتمة

المقدمة

بسم الله الرحمن الرحيم ونصلى ونسلم على أشرف المرسلين سيدنا محمد
صلى الله عليه وسلم رسولنا الكريم الذي علم الأمة ،
سوف نعرض لكم موضوع من أهم الموضوعات التي تواجهنا كمهندسي تقنيه
معلومات ،

وهذا الموضوع مهما تحدثت وكتبت لن اوفيه حقه ،ولكن سنحاول بقدر
الإمكان ان نعرض لكم أهم الجوانب والمعلومات الخاصة بالموضوع
" FortiGate UTM firewall " وندعو الله ان يوفقنا لهذا ..

كلمه شكر و عرفان

رسالة شكر وحب و عرفان إلى من بالحب غمروني وبجميل السجايا أدبوني إلى أبي وأمّي إلى من كان
حبهما يجري في عروق دمي إلى من كانت ابتسامتي تزيل شقاهم وسعادتي ترسم الابتسامة على
شفاهم إلى من أحببتهم حتى سارحهم في الوجدان إلى من أمرني ربي بطاعتهم والإحسان لهم أبي
وأمّي كلمات الحبّ عجزت عن وصف حبّي الكبير لعظمتكم حروف العشق عجزت عن نظم أجمل
القصائد والألحان فيكم أنتم قلبي، أنتم فرحي أنتم سرّ السعادة في قلبي أبي وأمّي حفظكم الله
وأبواقم لناظري أمّي أبي أنتم قلبي النَّابض حبكم يسري في شرايبيني كيف لا وأنتم أول من نظرتُ
إليهما أول أصوات سمعتها أول اسمين نطقت بها شفّاتي حبكما في قلبي كملء الأرض بل يطاول
عنان السّماء إلى شمعة دربي وبلسم جروحي إلى من سهروا اللّياالي من أجلي، من أجل راحتي ورسم
البسمة على شفّاتي إلى من إذا عشتُ الدهر كلّهُ لن أوفي حقهما إلى من أوصاني ربّي بطاعتهم دون
معصيته إلى سبب نجاحي وسعادتي في الدّنيا والآخرة إلى جنّتي شكراً أمّي الحنونّة أبي الغالي
حفظكم الله وعافاكم ..

شكرا لكل افراد اسرتي ...

واشكر كل أصدقائي وكل من وقفوا معي حتى بكلمه تشجيع ...

اسال الله ان يحفظ اليمن كاهه والحديده خاصه وان يعم الأمن والأمان في كل ارجاء اليمن .

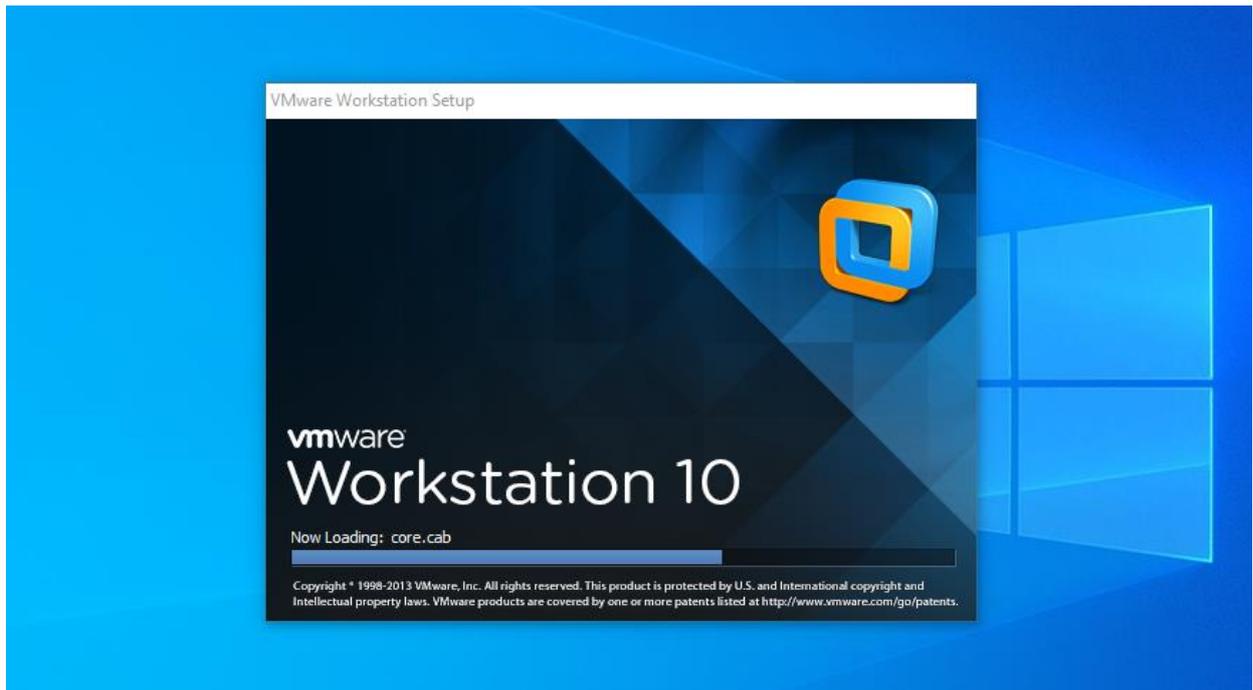
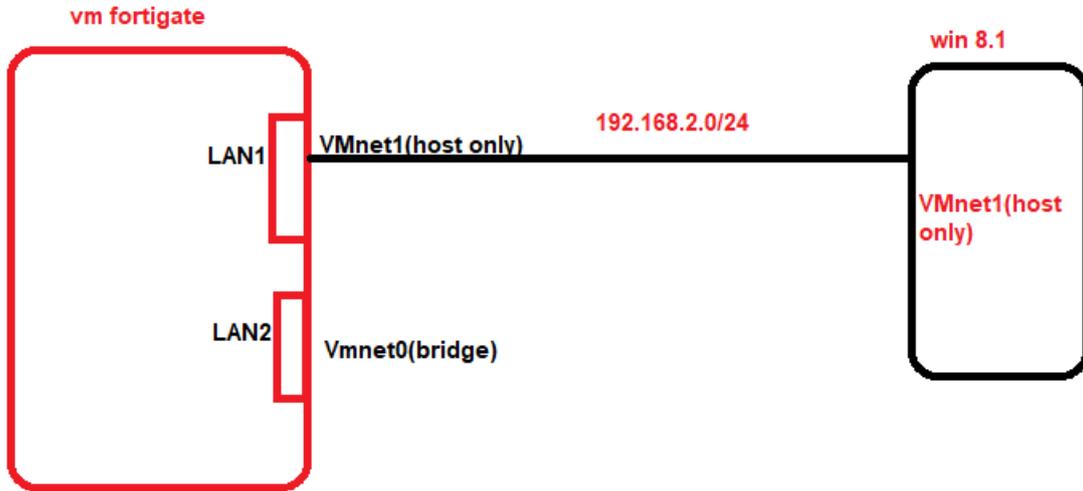
مقدمة عن فورتني جيت FortiGate

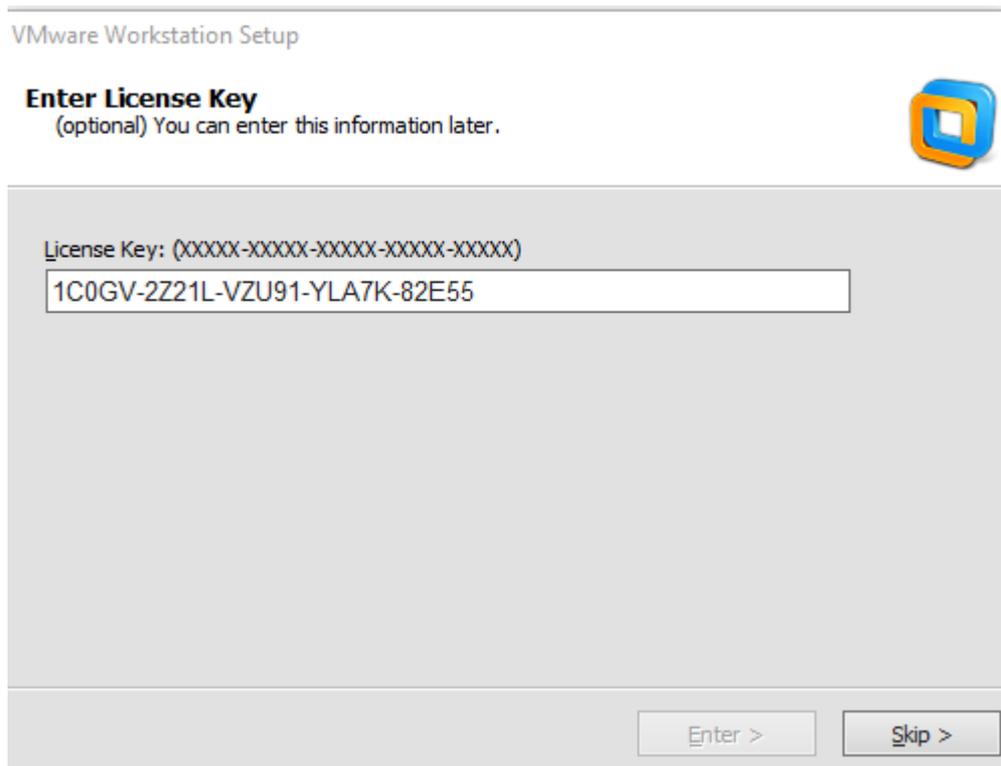
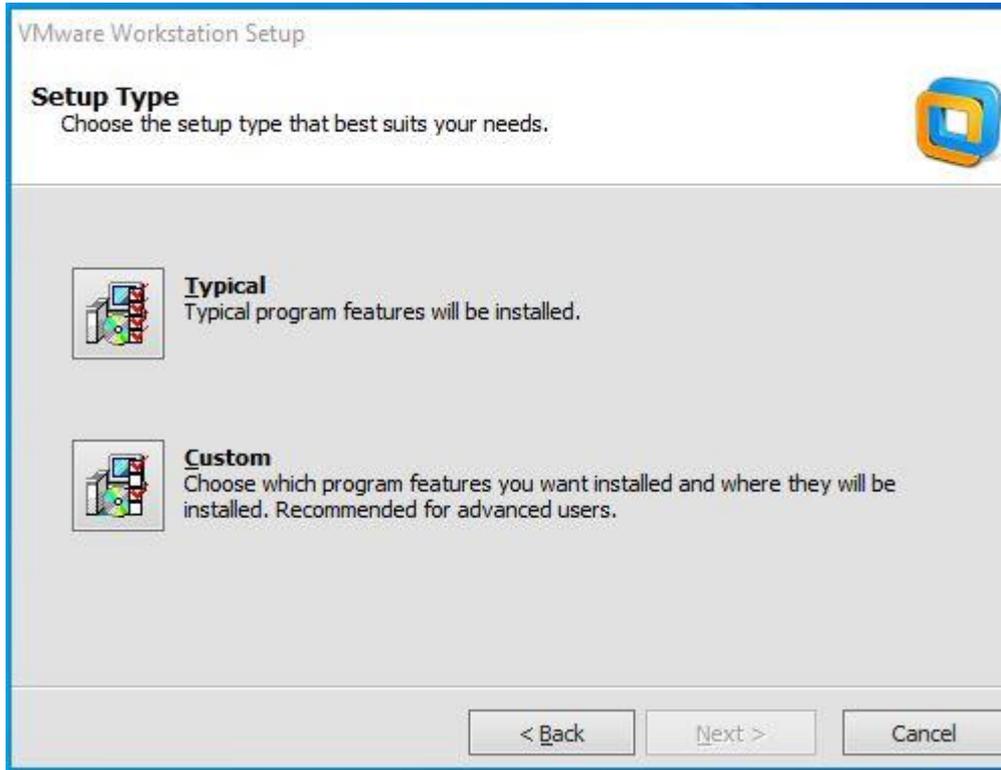
الفورتني جيت هو التطور الطبيعي للفايرول نظرا لانتشار الفيروسات والملفات الخبيثة فأصبحت الجدران النارية غير كافية لتأمين الشبكات ومن هنا ظهر مصطلح الـ UTM (Unified Threat Management)

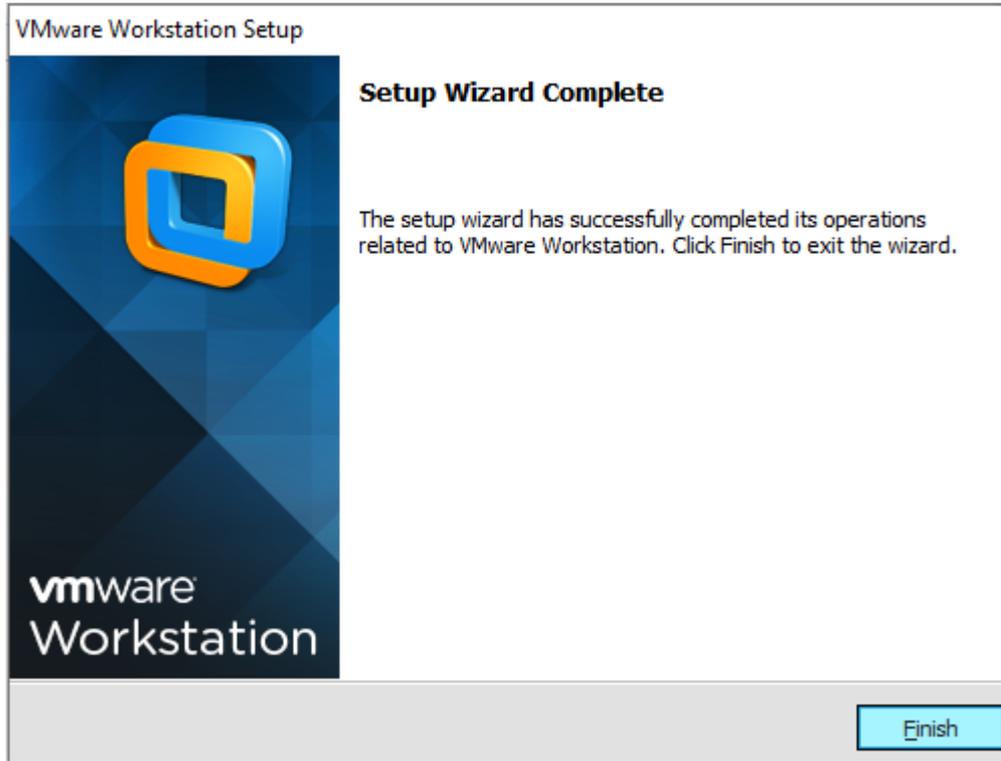
تعني إدارة التهديدات المجمععة او الموحدة بمعنى توفير أكثر من حماية للشبكة. حيث يقدم مجموعه واسعه من الوظائف الامنية في جهاز واحد يدعى FortiGate ويعمل هذا المنتج كأحد حلول UTM المعروفة وهي ان يعمل كـ , vpn , firewall , WAN acceleration , Web filtering , antivirus , antispan , والعديد من الوظائف التي لا غنى عنها لبناء شبكة عملاقة مؤمنة ،، هناك العديد من الموديلات الصغيرة والكبيرة لتغطية جميع الاحتياجات.



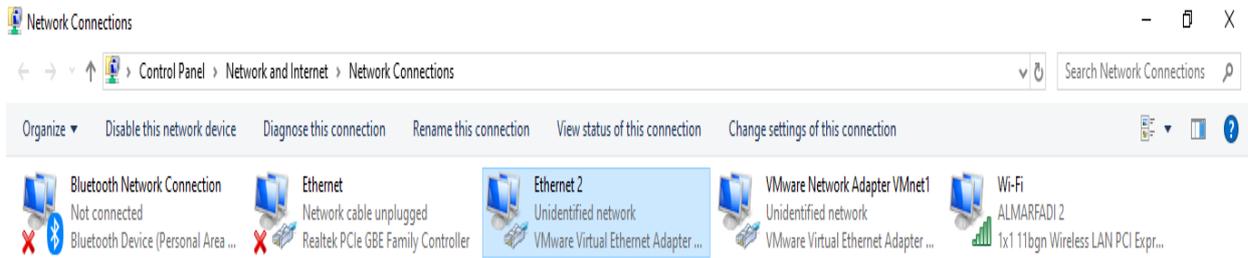
❖ طريقة تنزيل وضبط اعدادات الـ VM FortiGate :

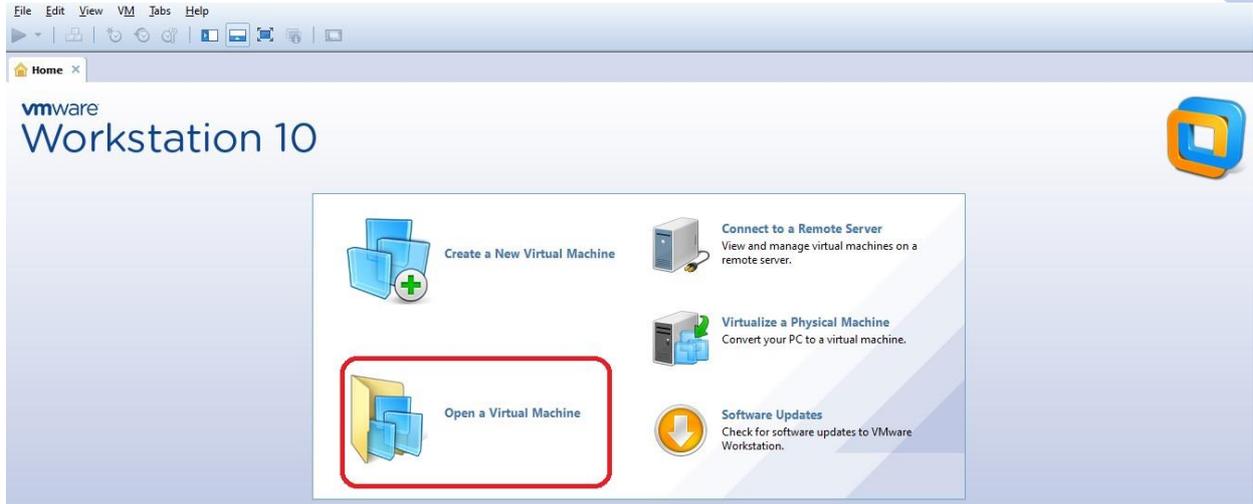




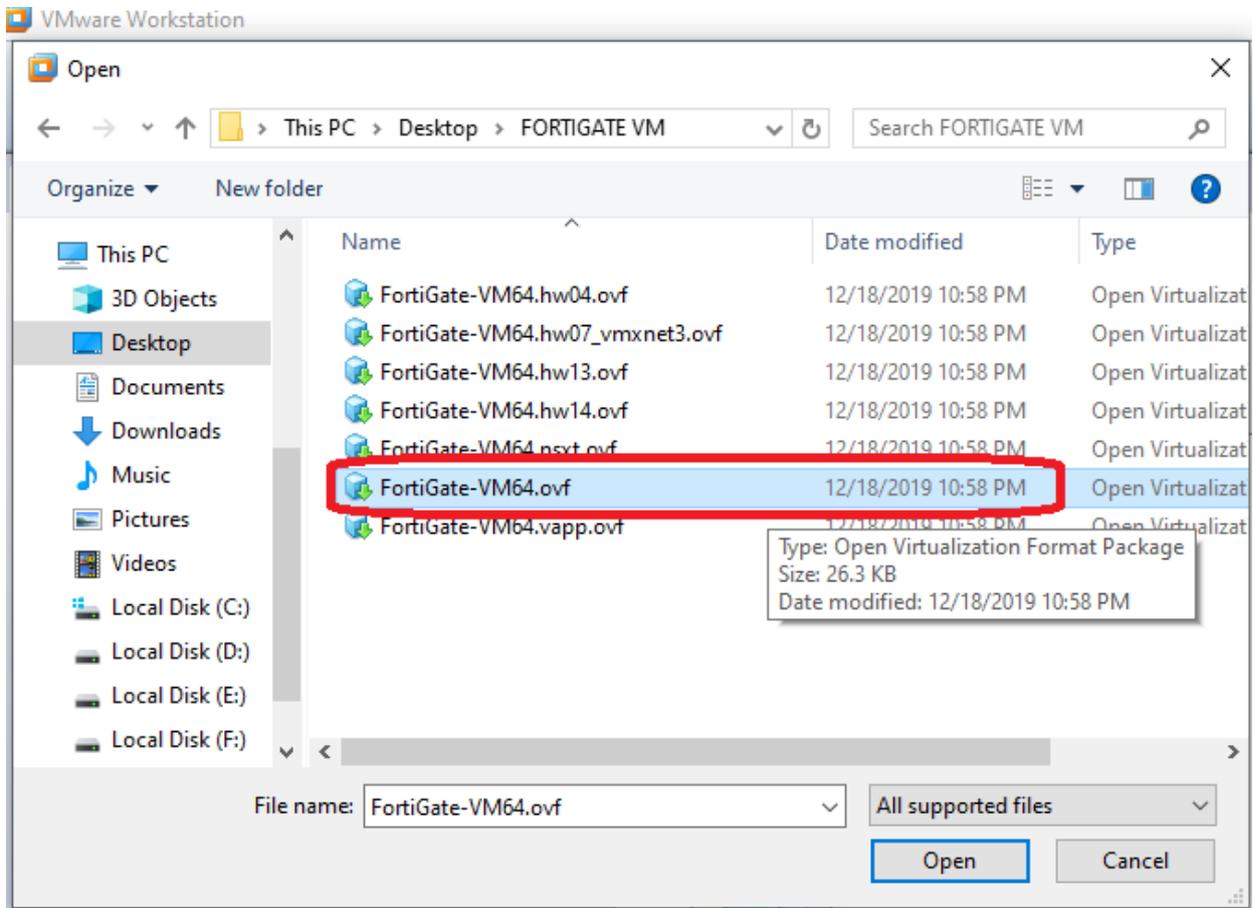


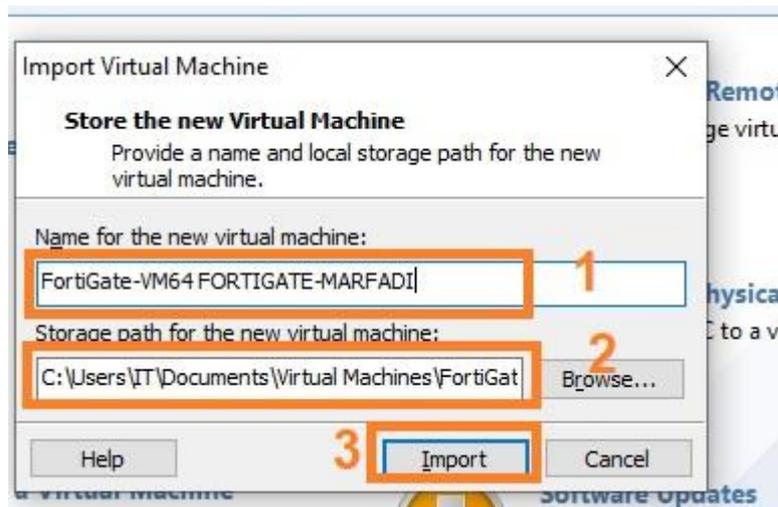
نلاحظ بالصورة ادناه بظهور كروت شبكة افتراضيه (وهميه) تابعه لـ vmware work station





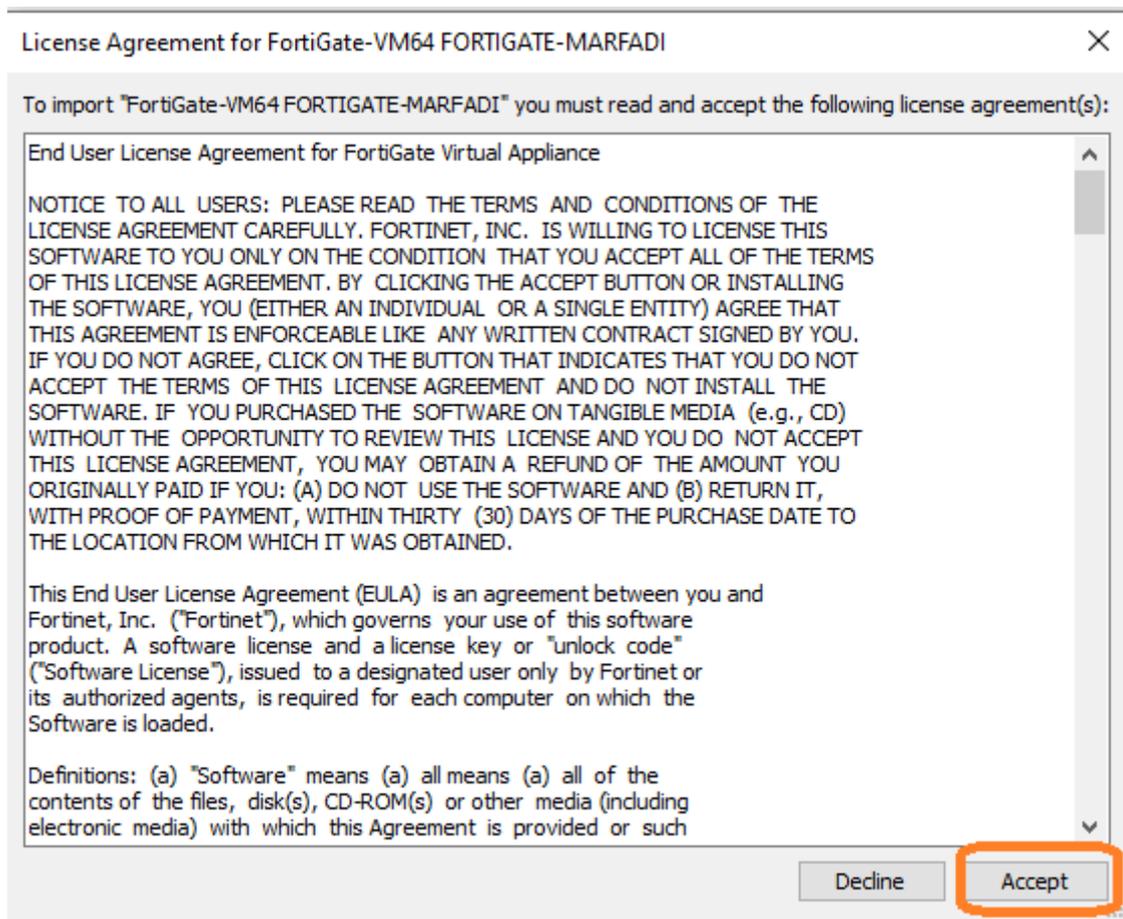
نقوم باختيار مكان fortigate vm والتي باسم FortiGate-VM64.ovf





نكتب اسم للvm مثلا FortiGate-VM64 FORTIGATE-MARFADI

ونحدد مكان حفظ نسخه الvm ثم نقوم بعمل استيراد ...

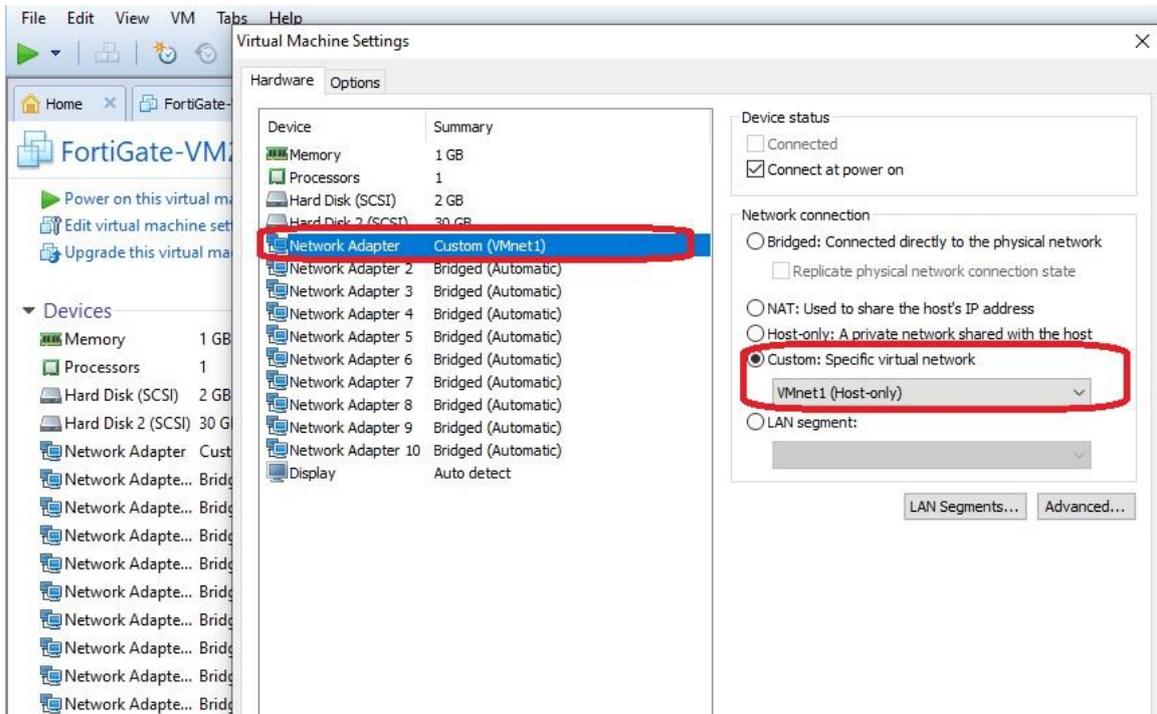


موافق...

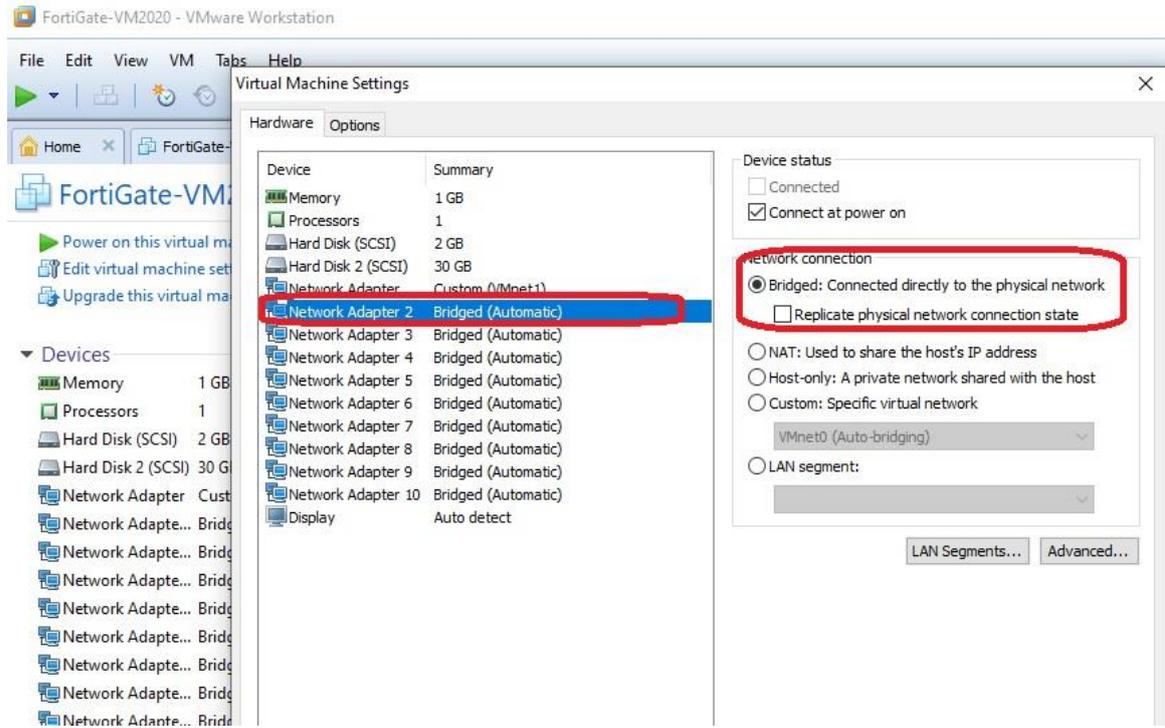


نلاحظ بالصورة أعلاه بان الرام 1 جيجا والهارد ..وعدد 8 كروت شبكة نوع Bridge

نقوم بتجهيز كروت الشبكة الوهمية التابعة لـ vm fortigate



كما بالصورة أعلاه تم ضبط كروت الشبكة كـ lan1 (host only) VMnet1



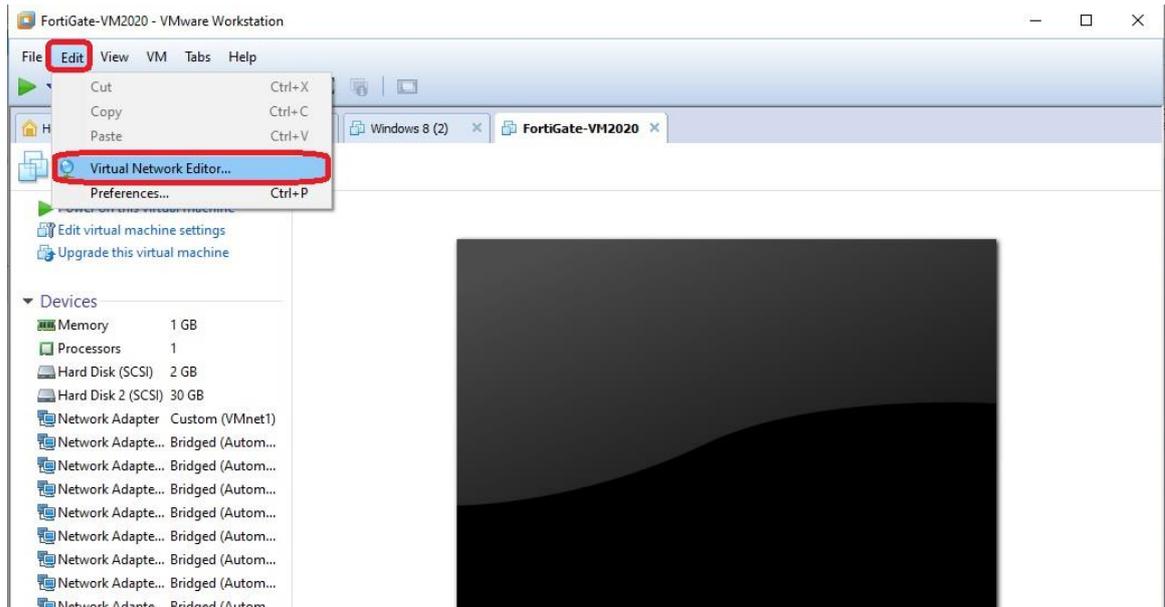
اما كرت الشبكة lan2 والذي وسوف يتم تغييره الى WAN سيتم ضبط إعداداته كما بالصورة أعلاه

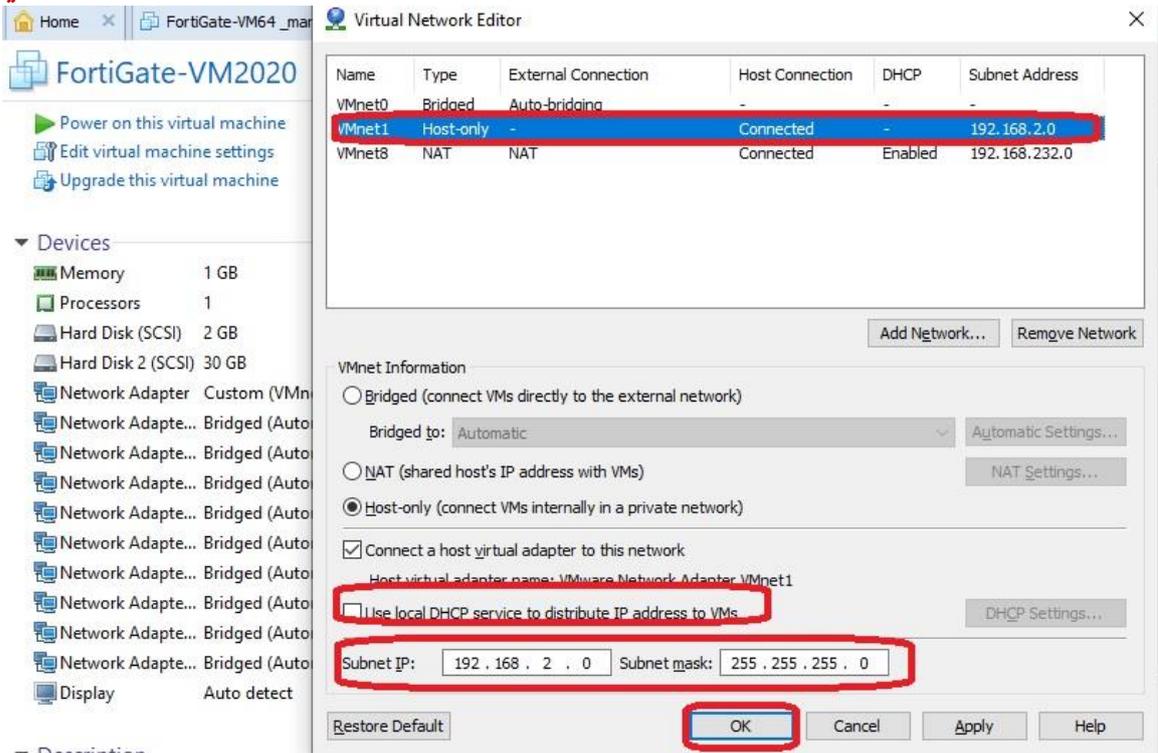
Bridge connected directory to the physical network

وذلك لكي يكون قادر على الوصول الى الروتر (المودم) لأنه سوف يكون موصل مع كرت الشبكة الوايرلس

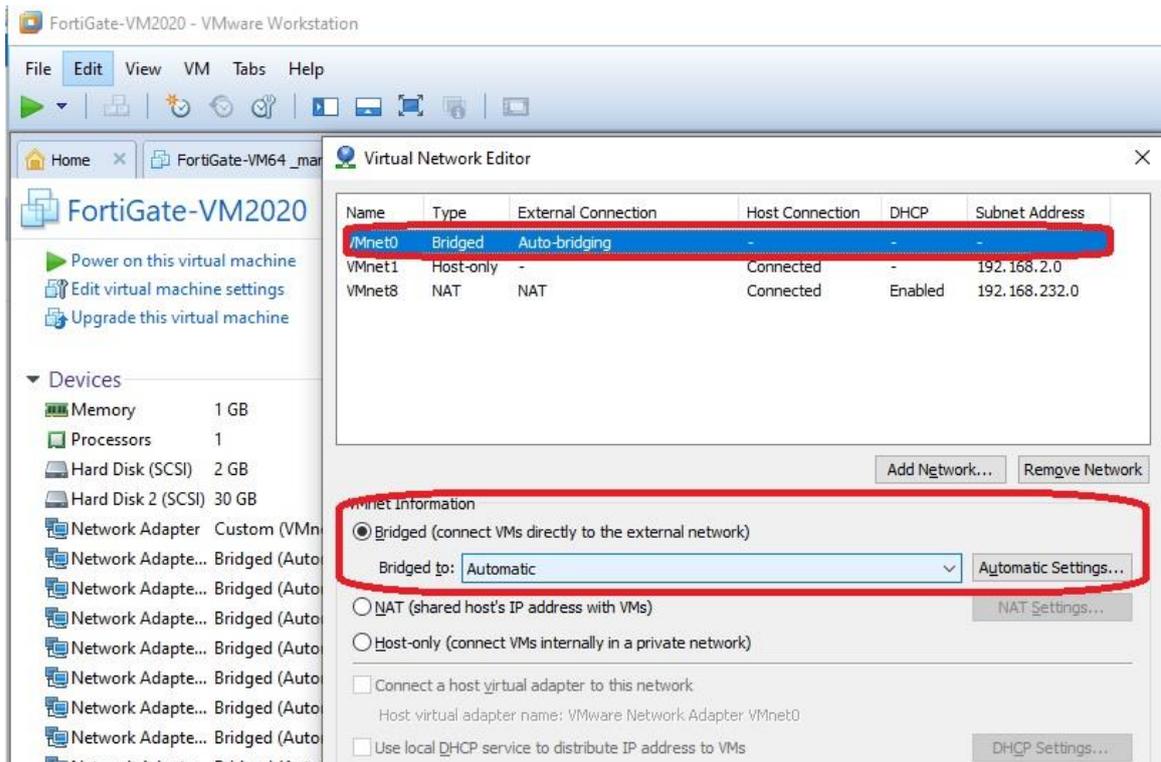
التابع للابتوب حيث سنقوم بجعل اعدادات كرت الشبكة الـ WAN بالايبي 192.168.1.60 .. ثم سوف

نقوم بضبط اعدادات كرت الشبكة الوهمي التابع لـ VMWARE كما بالخطوات التالية :





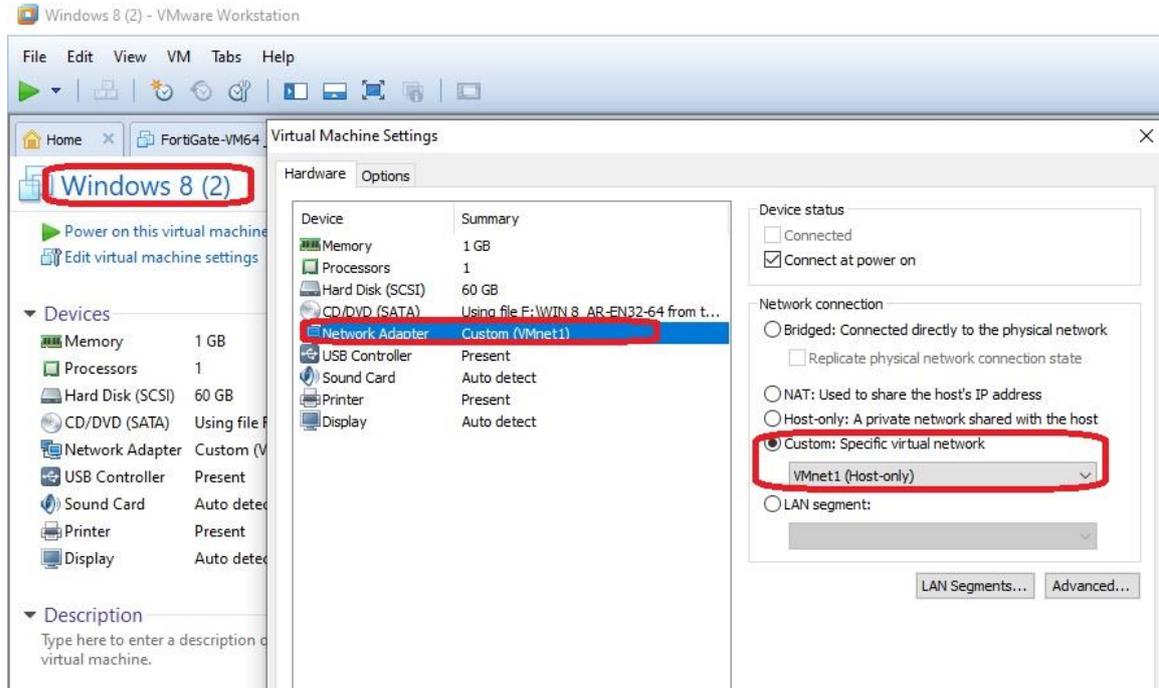
جعلنا كرت الشبكة الوهي (host only) Vnet1 من subnet 192.168.2.0 .



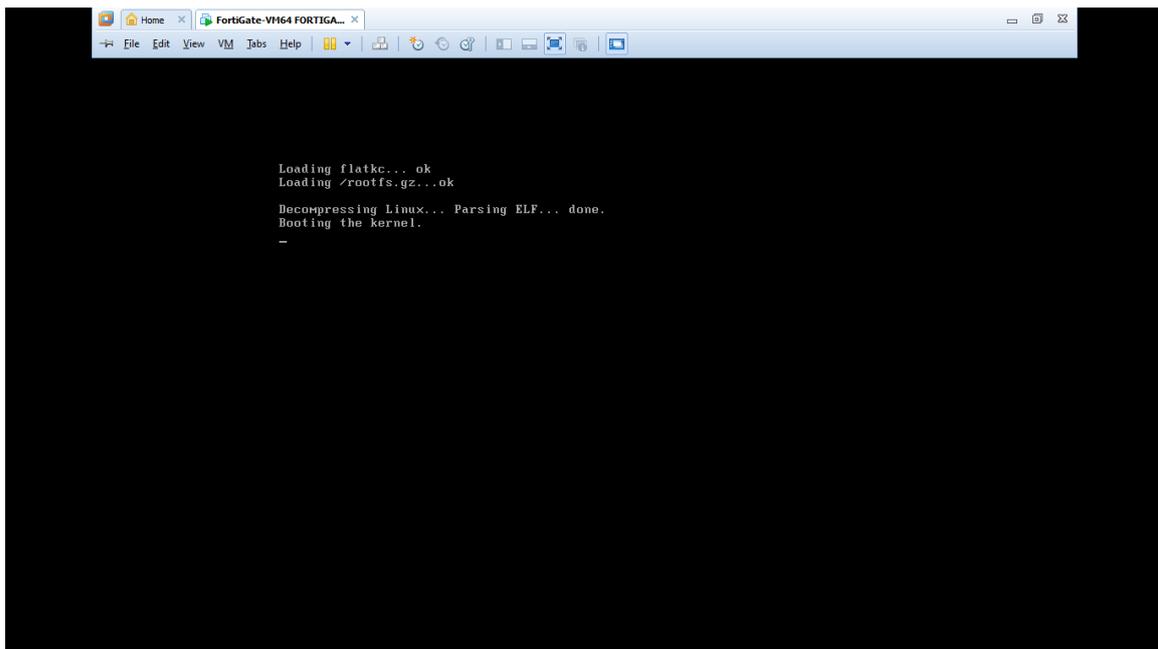
وأیضا ضبط الكرت vmnet0 بانه من نوع bridge

ضبط اعدادات كرت الشبكة على جهاز الكلاينت (Client):

يجب ضبط اعدادات كرت الشبكة لاجهزه الكلاينت كما بالصورة التالية حيث يتم توصيله بنفس السويتش التابع لكرت الشبكة lan1 التابع VM FortiGate



نقوم بتشغيل VM fortigate



جاااري التشغيل ...

```
Loading flatc... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Formatting shared data partition ... done!
Starting system maintenance...
Scanning /dev/sda1... (100%)
Scanning /dev/sda2... (100%)
Interface mapping (E1000)
Serial number is FGUMEUJ2LHXKZFB7

Disk usage changed, please wait for reboot...

Formatting the disk...
- unmounting /data2 : ok
Partitioning and formatting /dev/sdb label LOGUSEDXE49700DB ... _
```

```
Loading flatc... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Interface mapping (E1000)
Serial number is FGUMEUJ2LHXKZFB7

FortiGate-UM64 login: _
```

قم بإدخال اسم المستخدم admin والباسورد الافتراضي هو فارغ (blank)

```
Loading flatk... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Interface mapping (E1000)
Serial number is FG0MEUJ2LHXKZFB7

FortiGate-UM64 login: *ATTENTION*: Admin sessions removed because license regist
ration status changed to 'INVALID'

FortiGate-UM64 login: admin
Password: _
```

```
Loading flatk... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
Interface mapping (E1000)
Serial number is FG0MEUJ2LHXKZFB7

FortiGate-UM64 login: *ATTENTION*: Admin sessions removed because license regist
ration status changed to 'INVALID'

FortiGate-UM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:
FortiGate-UM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:*****
Confirm Password:*****_
```

تم تغيير الباسورد الافتراضي الى admin مثلا بدلا عن فالارغ (blank) ...

حيث الان لا يمكننا الوصول الى ال FortiGate vm عبر كرت الشبكة lan1 عبر الابتوب الحقيقي لأن كل جهاز في سويتش مختلف ..

لذا سيتم الوصول الى الفورتى جيت من على الجهاز الوهمي لويندوز 8.1 (الكلابنت)والذي هو أصلا موصل على نفس السويتش مع كرت الشبكة lan1 ل vm fortigate ..

كرت الشبكة الlan1 التابع للفورتى جيت موصل بنفس السويتش لجهاز الكلابنت عبر السويتش VMnet1 ونوعه Host only ..

لذا الان سوف نقوم بتجهيز كرت الشبكة الـ port1 والتابع لـ VM وذلك كما بالأوامر ادناه .

حيث عند كتابه الأوامر الخاصة بتجهيز كرت الشبكة 1 port بالايي 192.168.2.20

Config system interface

Edit port1

Set ip 192.168.2.20 255.255.255.0

فأنه تظهر رساله الخطأ (فقط على Vm FortiGate) كما بالصورة

"Can't change dynamic ip"

```
You are forced to change your password, please input a new password.
New Password:
FortiGate-UM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:*****
Confirm Password:*****
Welcome !

FortiGate-UM64 # cls
Unknown action 0

FortiGate-UM64 # clear
Unknown action 0

FortiGate-UM64 # config system interface
FortiGate-UM64 (interface) # edit port1
FortiGate-UM64 (port1) # set ip 192.168.1.20 255.255.255.0
Can't change dynamic IP

FortiGate-UM64 (port1) # ^\
FortiGate-UM64 (port1) # _
```

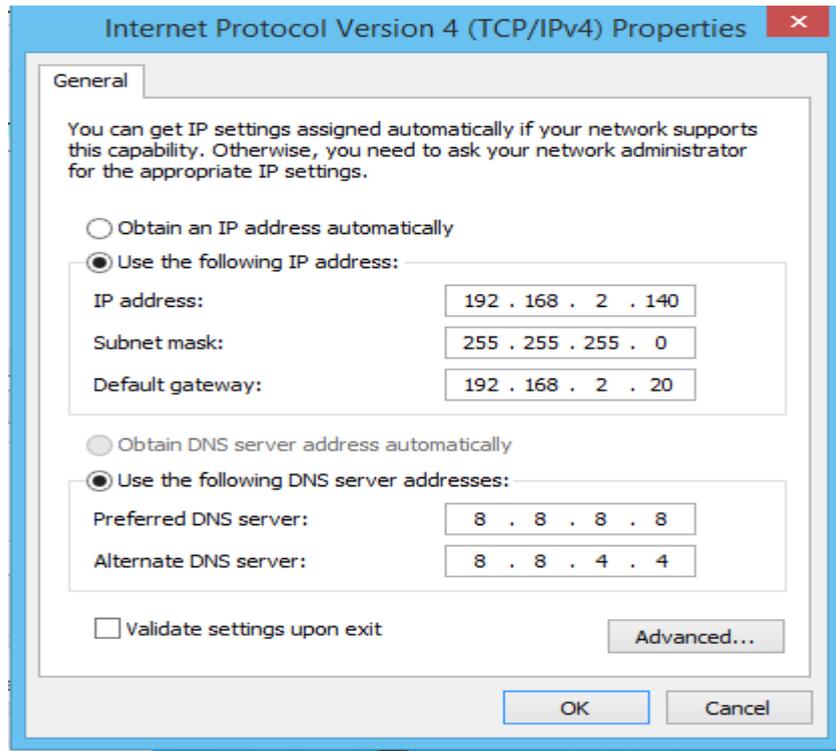
وذلك لأن كرت الشبكة بيوزع ايبهات أوتوماتيكية DHCP لذا سوف نقوم بتحول الكرت الى static كما بالأمر التالي :

Config system interface

Edit port1

Set mode static

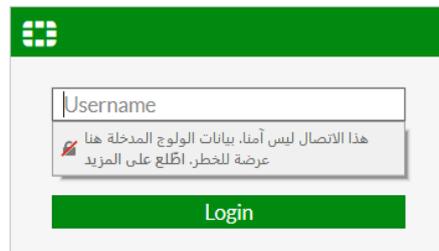
Set ip 192.168.2.20 255.255.255.0



ثم سنفتح الفورتى من خلاص الويب (192.168.2.20) بواسطة متصفح من على جهاز الكلاينت (win) (8.1)

ملاحظة: lan1:192.168.2.20

سنقوم بالدخول الى الفورتى عبر الويب وذلك من جهاز الكلاينت 8.1 عبر الايبي 192.168.2.20 كما بالصورة ادناه ...

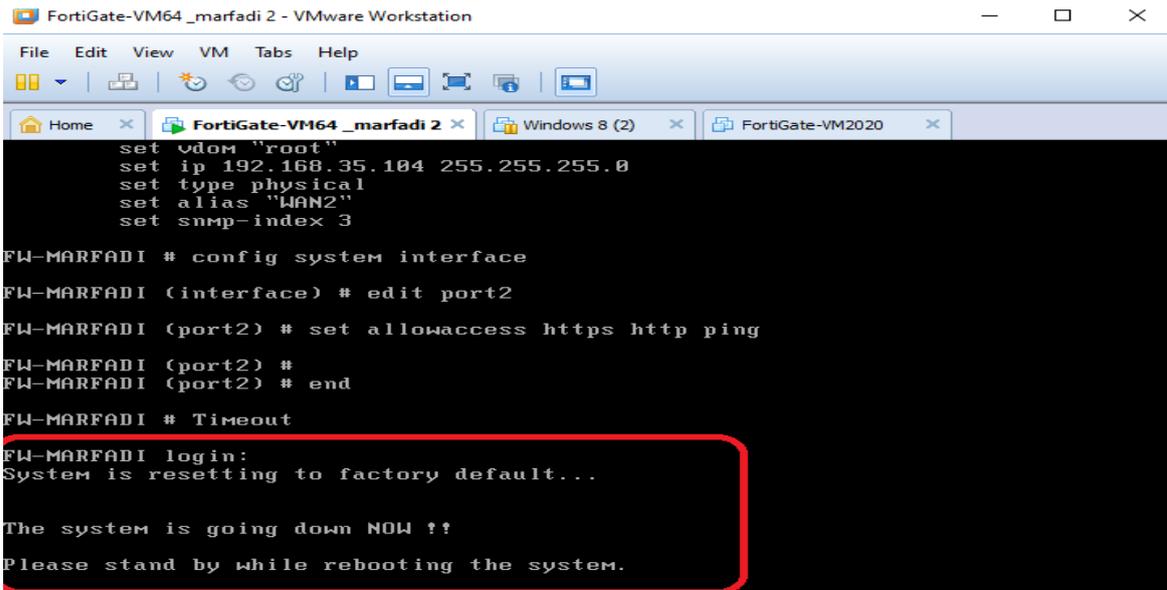
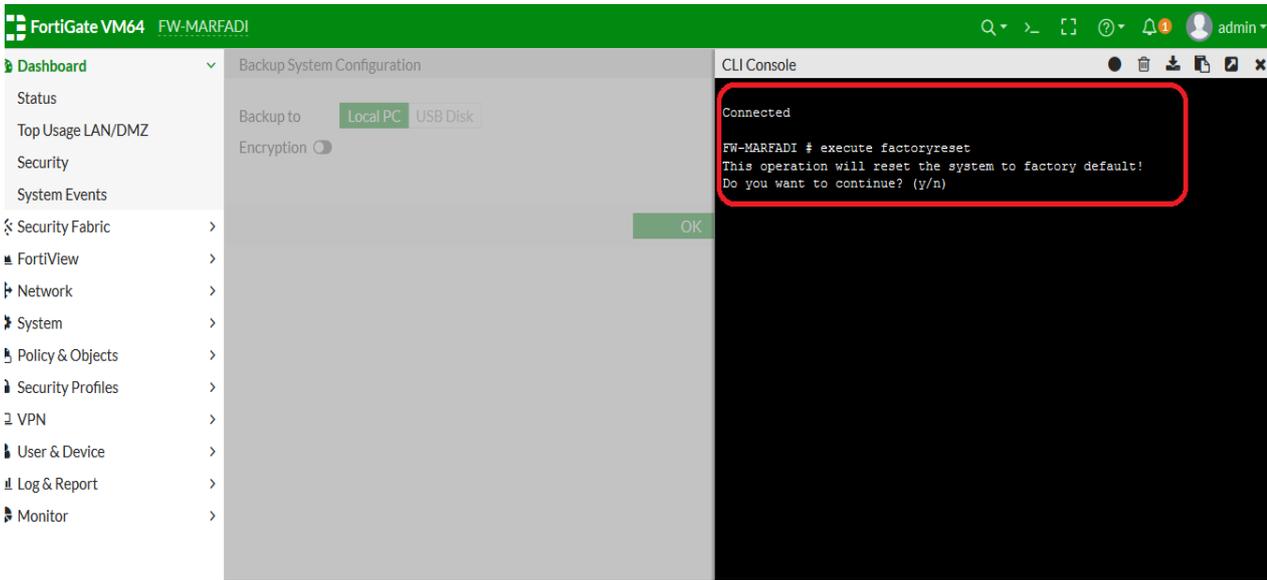


❖ طريقة عمل reset لعدد الأيام (14) للـ VM :

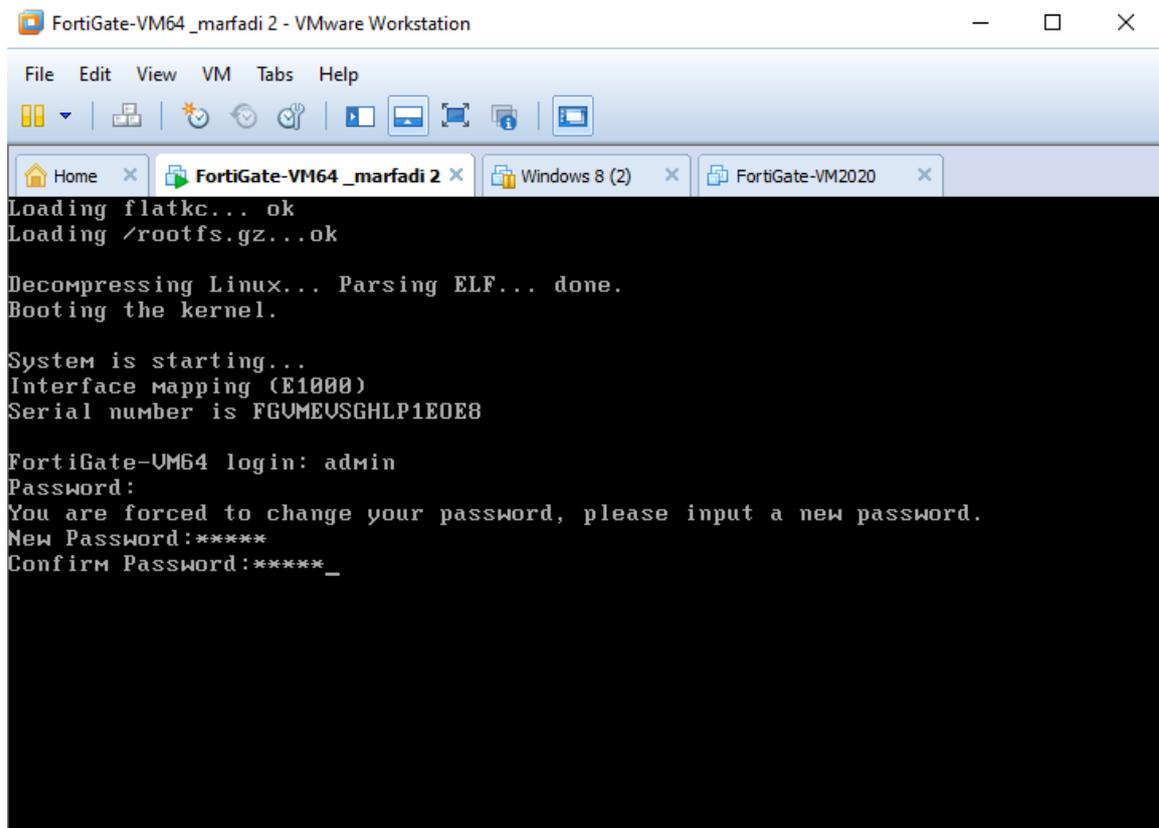
الفترة التجريبية لـ fortigate vm هي 14 يوم، لذا قبل ما تنتهي الفترة التجريبية فأنت تقوم بأخذ باك اب للفورتى جيت كما سيتم الشرح لاحقا ثم عمل VM Reset كما بالخطوات التالية :

1- اخذ نسخه باك اب من الاعدادات (سيتم شرحه لاحقا)

2- عمل reset للـ vm بكتابه الامر كما بالصورة ادناه



يتم حاليا عمل استعادته اعدادات المصنع (Reset)



```
FortiGate-VM64 _marfadi 2 - VMware Workstation
File Edit View VM Tabs Help
Loading flatkc... ok
Loading /rootfs.gz... ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
System is starting...
Interface mapping (E1000)
Serial number is FGUMEUSGHL1E0E8
FortiGate-VM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:*****
Confirm Password:*****_
```

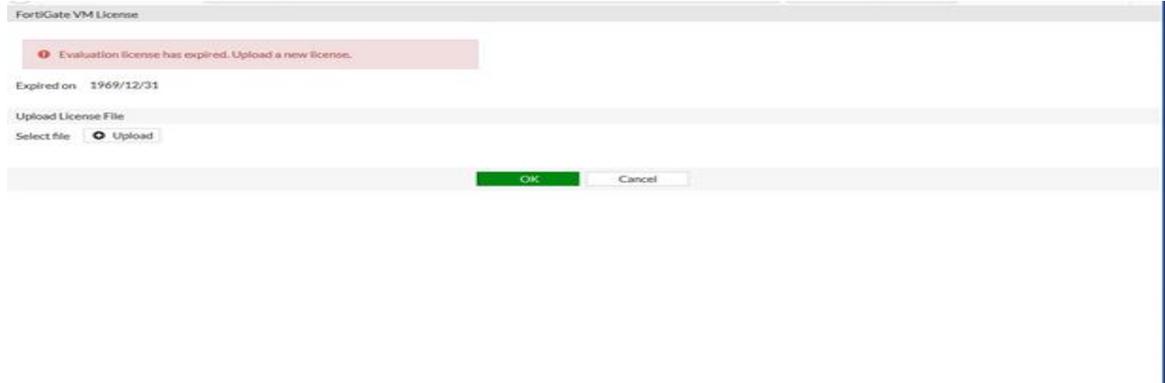
ضبط الإعدادات من باسورد وأيضا ضبط اعدادات كروت الشبكة مره أخرى كما تم شرحه سابقا وذلك بدلا من ان تقوم بحذف الvm وتقم بتنزيله مره أخرى ...

LAN1=PORT1=192.168.2.20

LAN2=WAN=192.168.1.60

WIN 8.1=192.168.2.140

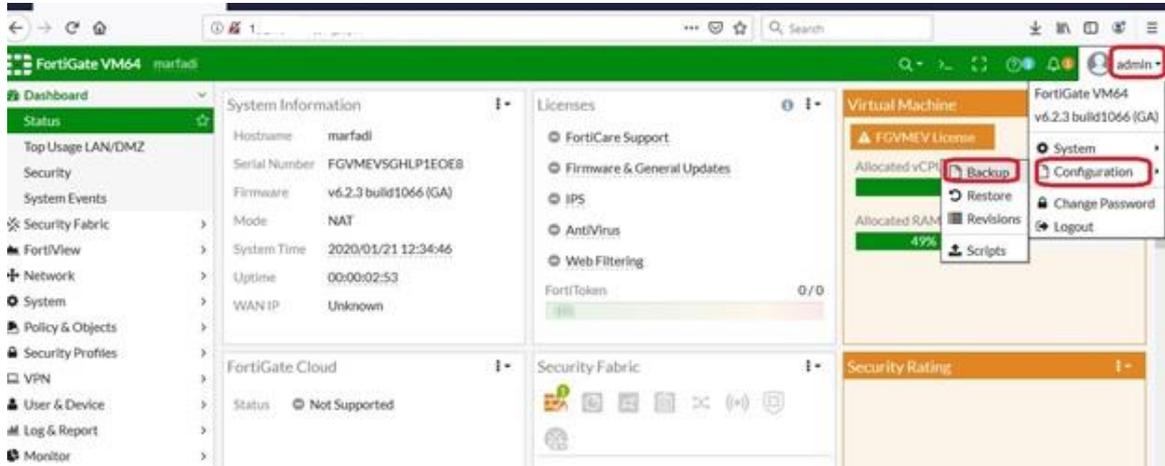
❖ مشكلة ظهور بان الأيسنر (License) قد انتهى كما بالصورة ادناه بالرغم اني لم استخدمه الا لساعه فقط ..

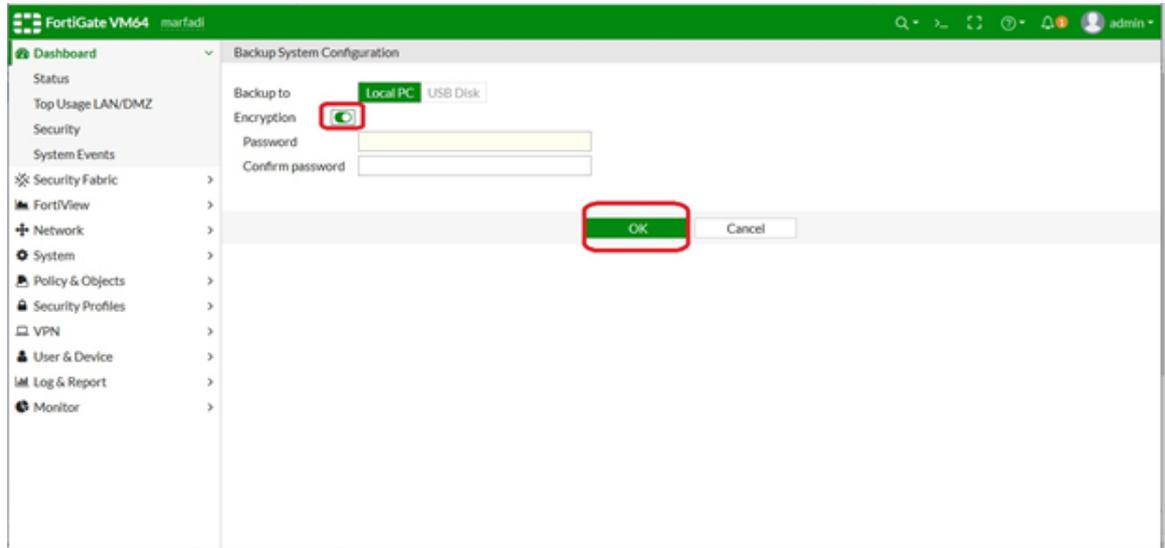
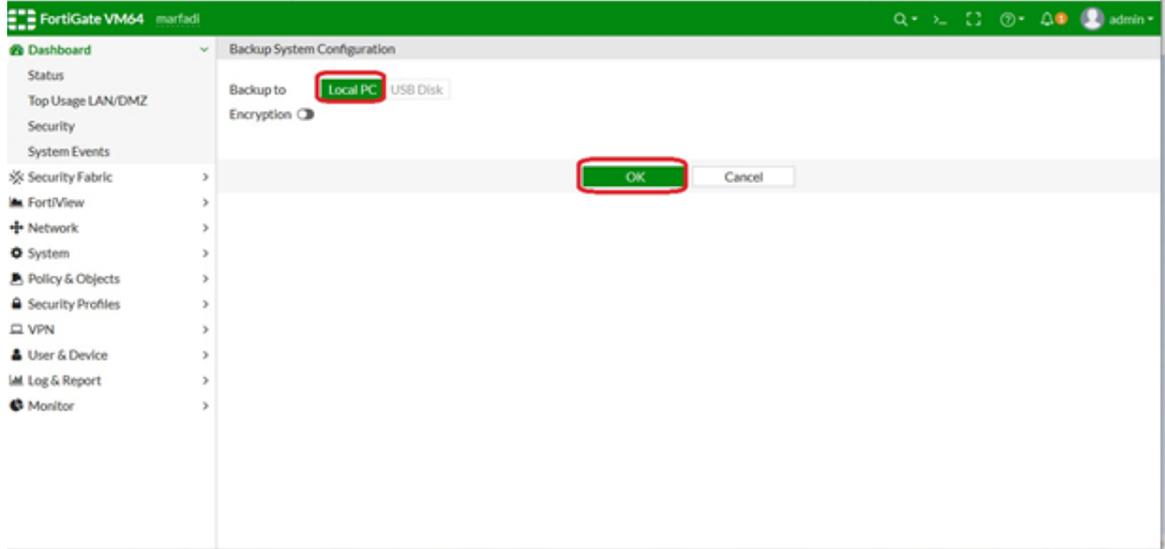
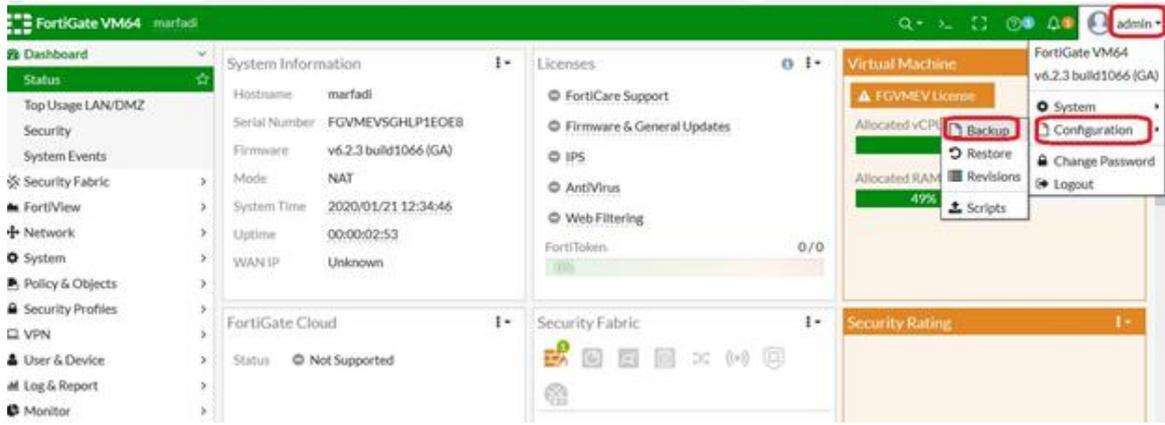


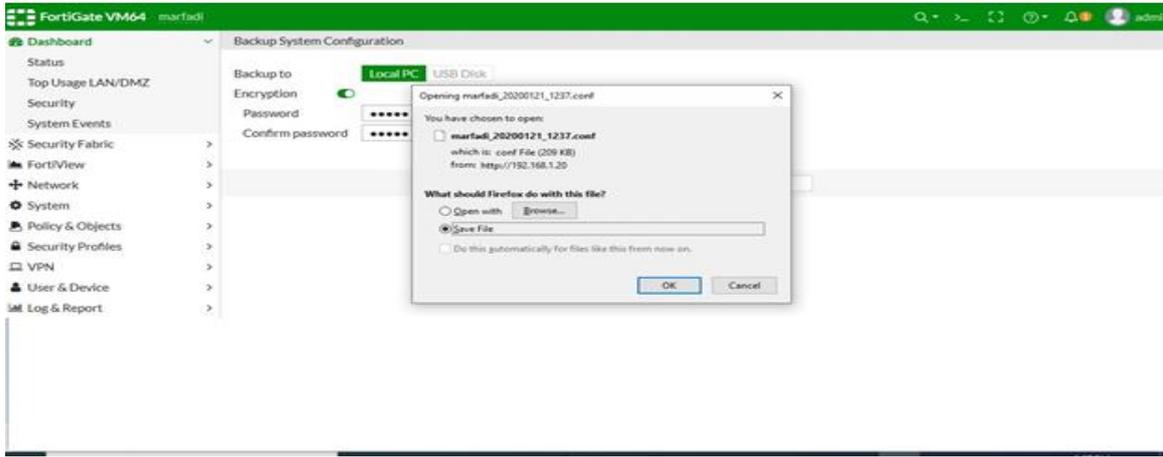
E

فقتم بتزير الVM واعدادها مره أخرى....واشتغلت واعطت لي 14 يوم تجريبي..

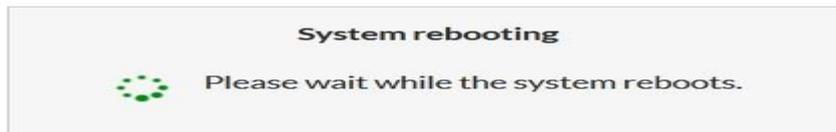
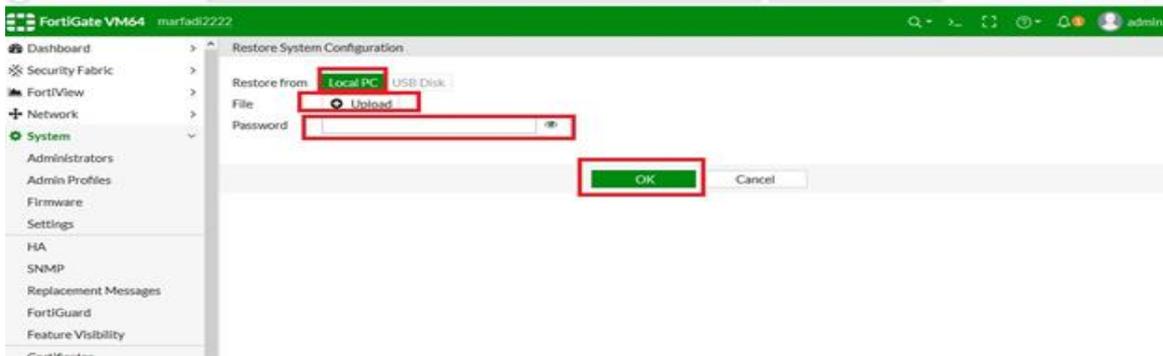
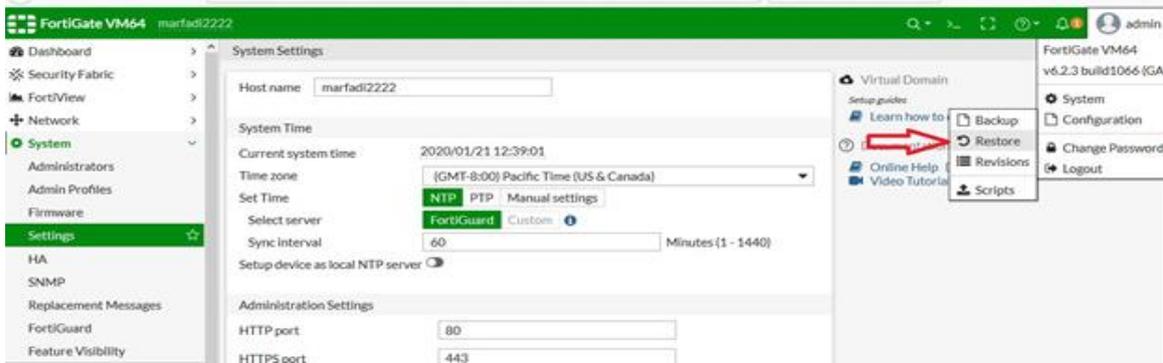
❖ طريقة عمل بانك اب للإعدادات التابعه للـVM وكيفيه استعادتها :





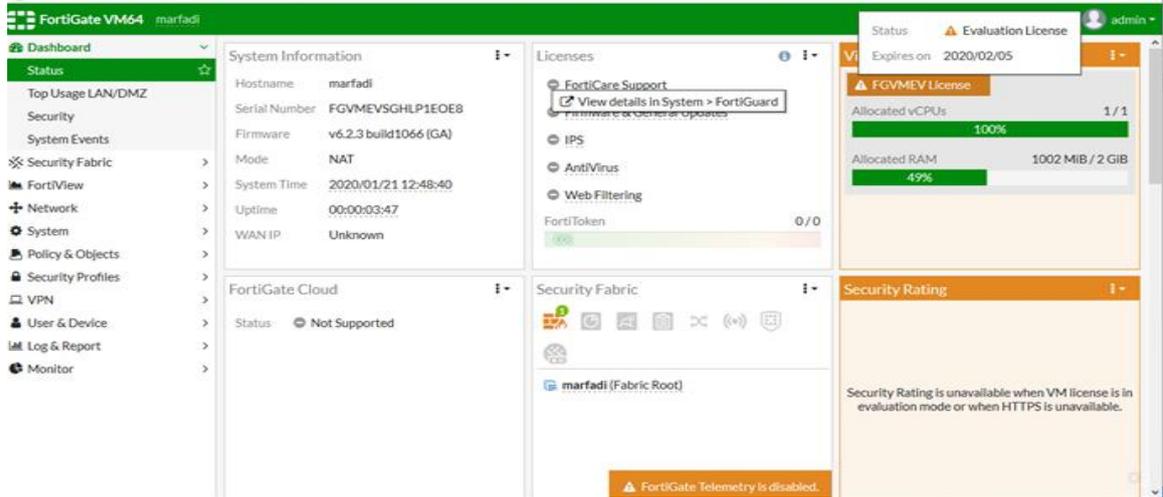


للاستعادة ...

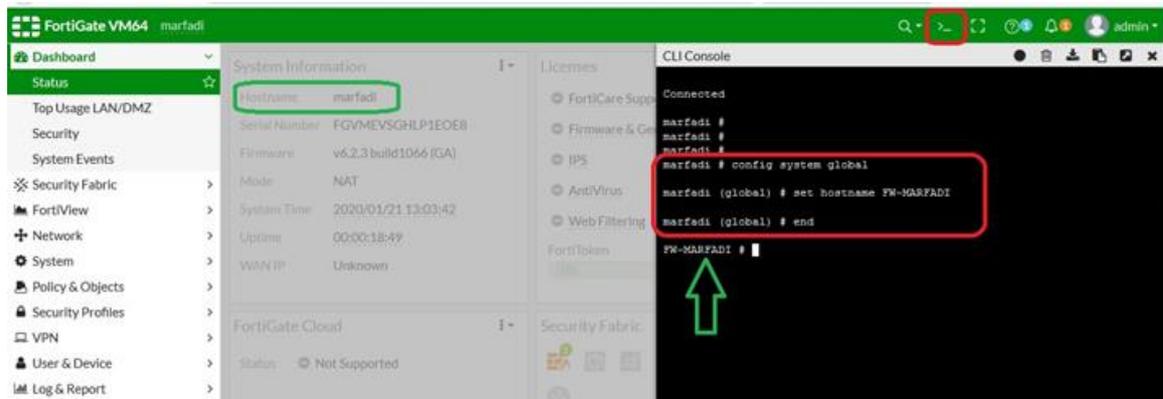


شرح مكونات وواجهات الفورتى جيت :

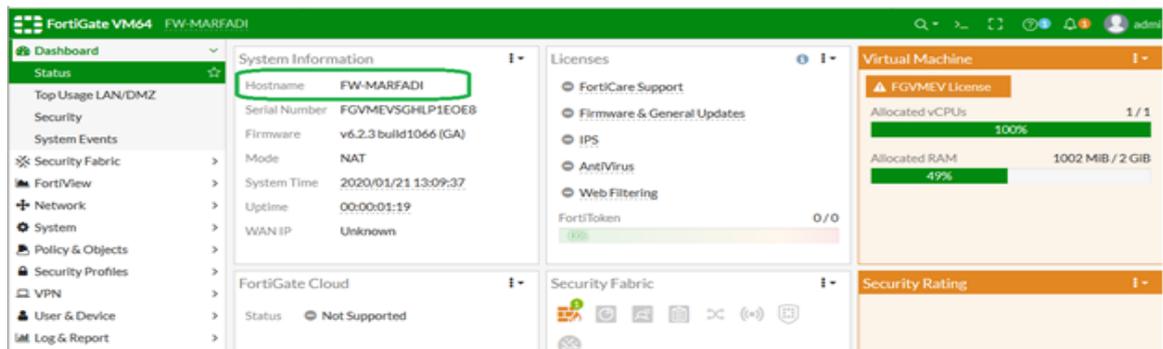
ال Dashboard توضح لنا معلومات حول النظام مثل اسم الجهاز والسيريال وإصدار الفريم وير والتاريخ والوقت للجهاز الفايروول ومتى تاريخ انتهاء الايسز نزل لكل خدمه.



طريقة تغيير اسم الجهاز بواسطة الأوامر:



بعد تعديل اسم الجهاز واعاده التشغيل



❖ طريقة تغيير باسورد الأدمن (admin) بواسطة CLI

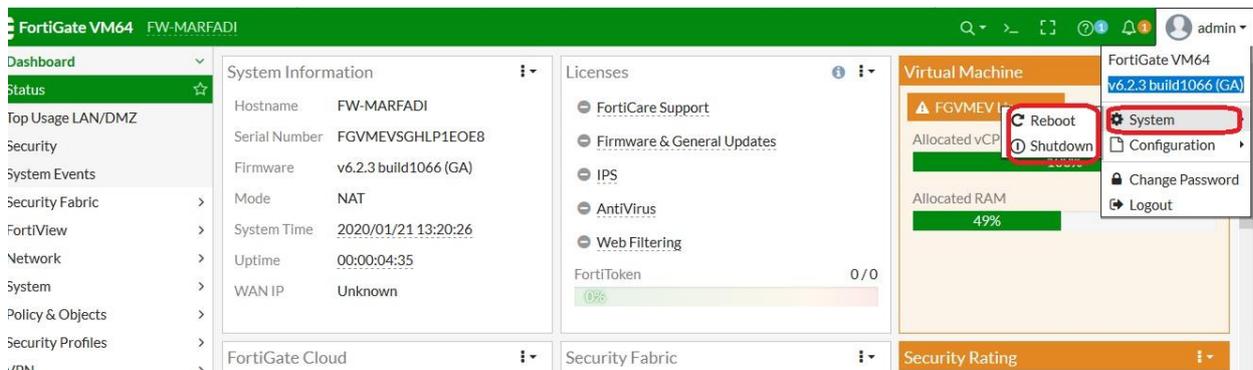
```
CLI Console
Connected
FW-MARFADI # config system admin
FW-MARFADI (admin) # edit admin
FW-MARFADI (admin) # set password 123
```

حيث يجب ان تقوم بكتابه الامر end بعد الأوامر أعلاه لكي يتمكن من حفظ التغييرات..

حيث اصبح الباسورد لليوزر admin هو 123 .

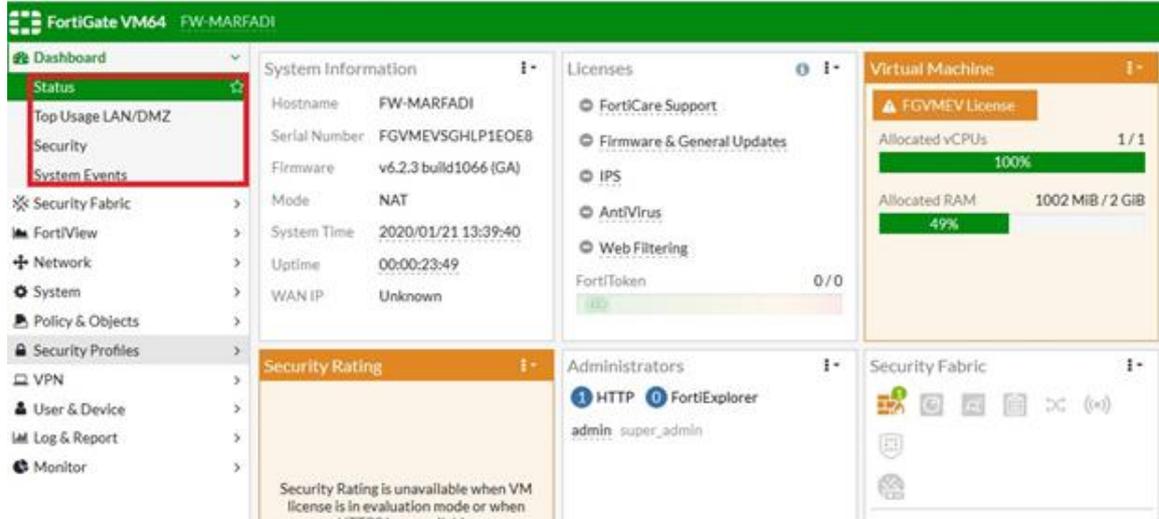
إيقاف او اعاده التشغيل او تغيير الباسورد او للخروج من الفورتني ويب ،

عبر GUI كما بالصورة ادناه ..

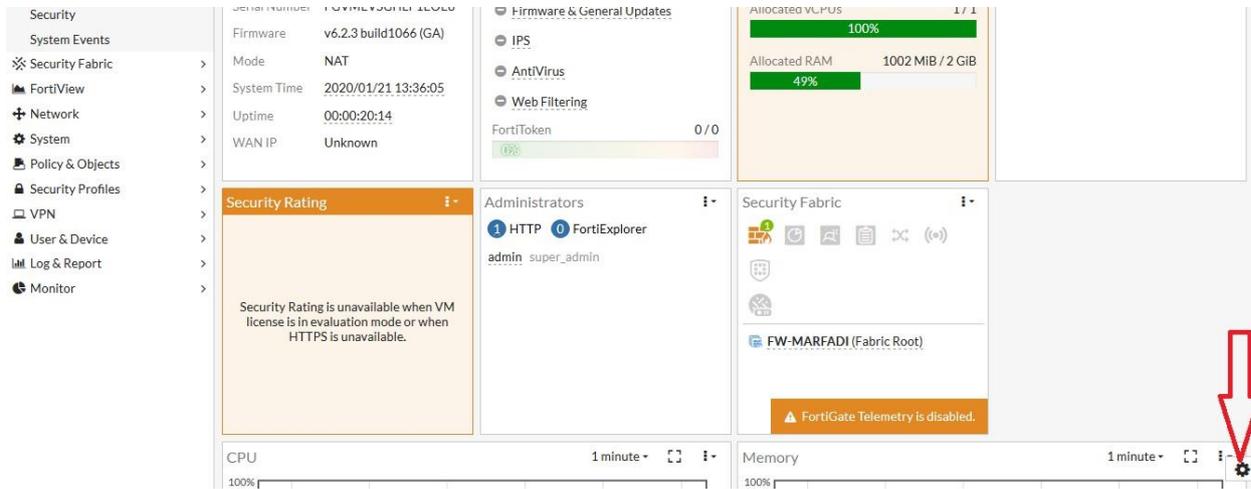


شرح ال DASHBOARD :

هي القوائم الموجودة على يسار الشاشة والمشار إليها بالمرجع الأحمر حيث يمكن إضافه أي قائمة وتسميها حسب ما تريد وتضيف اليها نوافذ (Widget)..



مثلا سوف نقوم بأضافه Dashboard باسم IMPORTANT وسوف نظيف اليها نوافذ محدده



أساسيات فورتني جيت

Mode: NAT
System Time: 2020/01/21 13:43:43
Uptime: 00:00:27:52
WAN IP: Unknown

Allocated RAM: 1002 MIB / 2 GIB
49%

Security Rating: Security Rating is unavailable when VM license is in evaluation mode or when HTTPS is unavailable.

Administrators: 1 HTTP 0 FortiExplorer
admin super_admin

Security Fabric: FW-MARFADI (Fabric Root)
FortiGate Telemetry is disabled.

+ Add Dashboard
Edit Dashboard
Reset Dashboards
+ Add Widget

CPU: 100% 1 minute
Memory: 100% 1 minute

FortiGate VM64 FW-MARFADI

Dashboard
Status
Top Usage LAN/DMZ
Security
System Events
IMPORTANT
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor

No widgets

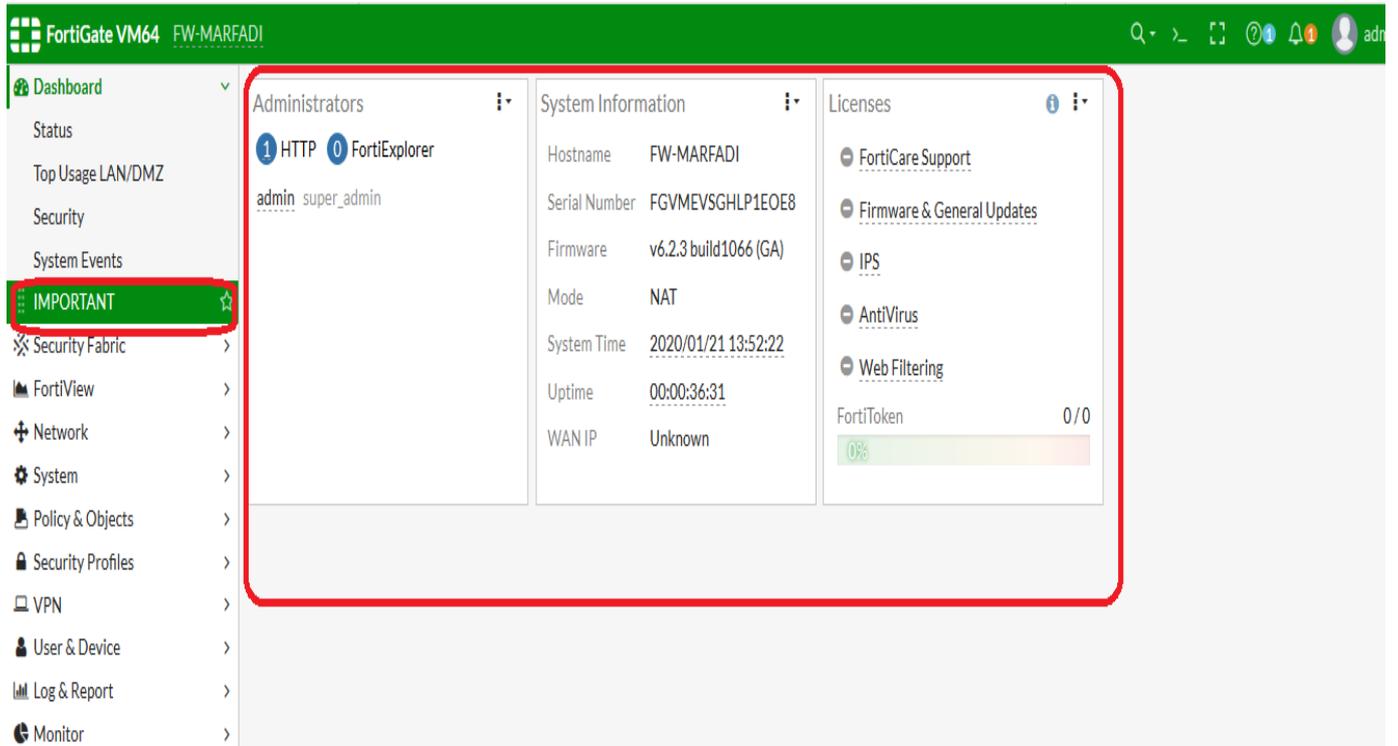
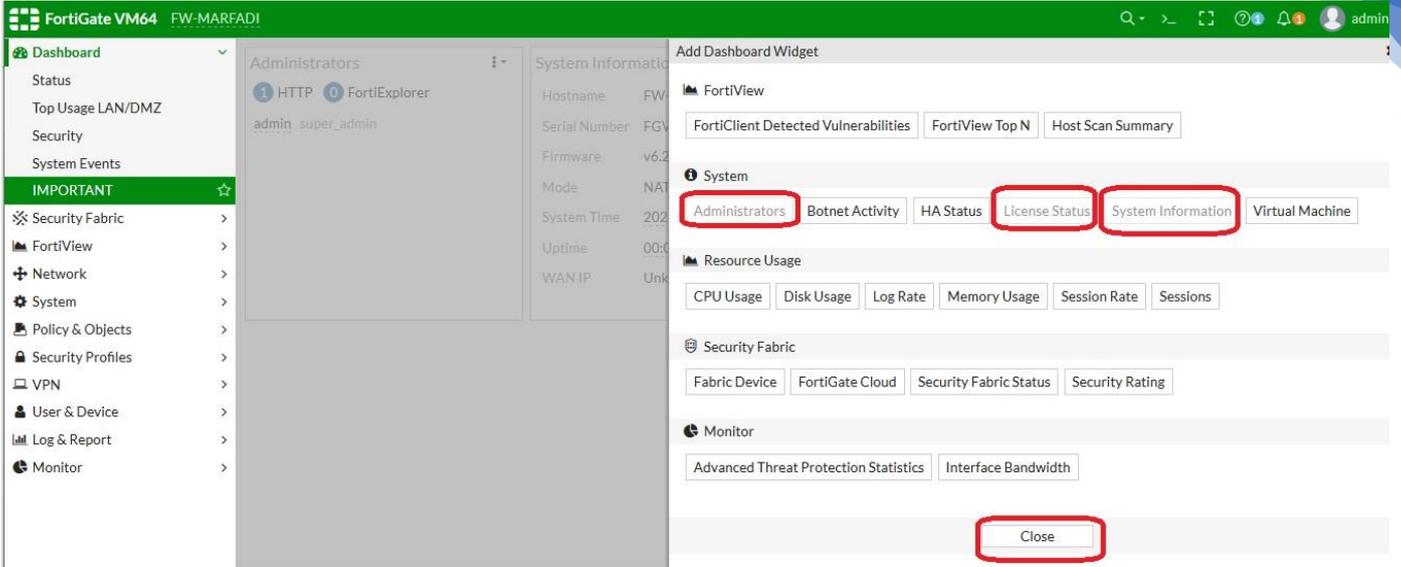
الآن سوف نقوم بإضافة نافذه جديده للـ DASHBOARD المسماة IMPORTANT

Security
System Events
IMPORTANT
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor

No widgets

+ Add Dashboard
Edit Dashboard
Delete Dashboard
Reset Dashboards
+ Add Widget

حيث سنضيف نوافذ كما بالصورة ادناه



وللتحكم من حيث حذف او تصغير او تكبير حجم النافذه على ال DASHBOAARD نتبع الخطوات كما بالصور ادناه ...

The screenshot displays the FortiGate VM64 dashboard for device FW-MARFADI. The interface includes a left-hand navigation menu with categories like Dashboard, Status, Top Usage LAN/DMZ, Security, System Events, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, Log & Report, and Monitor. The main content area is divided into several widgets:

- System Information:** Shows Hostname (FW-MARFADI), Serial Number (FGVMEVSGHLP1E0E8), Firmware (v6.2.3 build1066 (GA)), Mode (NAT), System Time (2020/01/21 13:29:50), Uptime (00:00:13:59), and WAN IP (Unknown).
- Licenses:** Lists FortiCare Support, Firmware & General Updates, IPS, AntiVirus, and Web Filtering. FortiToken is 0/0.
- Virtual Machine:** Shows FGVMEV License (Not Supported), Allocated vCPUs (1/1, 100%), and Allocated RAM (1002 MiB / 2 GiB, 49%).
- FortiGate Cloud:** Status is Not Supported.
- Security Rating:** A warning message states: "Security Rating is unavailable when VM license is in evaluation mode or when HTTPS is unavailable."
- Administrators:** Lists HTTP and FortiExplorer, with users admin and super_admin.
- Security Fabric:** Shows FW-MARFADI (Fabric Root) and a warning: "FortiGate Telemetry is disabled."
- CPU:** A line graph showing usage over time, with a current usage of 2%.
- Memory:** A line graph showing usage over time, with a current usage of 73%.
- Sessions:** A line graph showing the number of sessions over time, with a current count of 9.

This screenshot shows the same dashboard as above, but with a context menu open over the System Information widget. The menu options are:

- Resize
- Remove

 A red arrow points to the menu icon in the top right corner of the System Information widget. The Security Rating widget now displays the message: "Security Rating is unavailable when VM license is in evaluation mode or when HTTPS is unavailable."

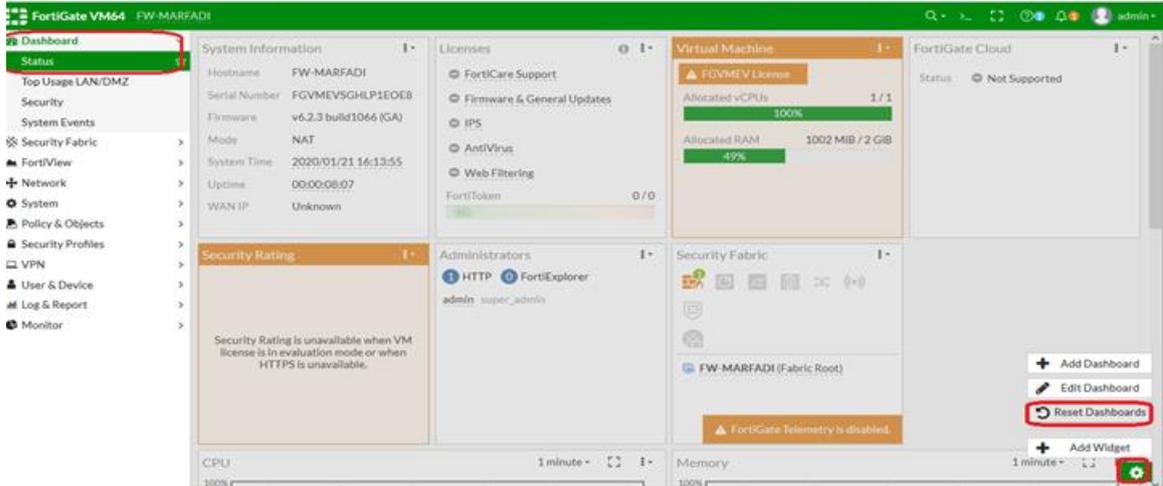
This is another view of the dashboard, showing the context menu options (Resize and Remove) over the System Information widget. The layout and data are consistent with the previous screenshots.

حيث يمكنك تعديل حجم او حذف أي نافذة (Widget) من الـ Dashboard .

ملاحظات :

أساسيات فورتى جيت

- ممكن نقل النوافذ (Widget) من مكان الى اخر بواسطة السحب والافلات .
- لا يمكن حذف ال Main Dashboard .
- في حالة قمت بتعديلات على ال Dashboard وتريد استعادتها كما كانت افتراضيا فأنا ننقر على الرمز العجمله ثم Reset Dashboard ثم OK



❖ شرح القوائم :

١- Dashboard :

هي عباره عن لوحه التحكم ، حيث بشكل افتراضي يتم انشاء Main dashboard وتحتوي على نوافذ (Widget) حيث كل نافذه تعرض معلومات مختلفه عن الأخرى مثل System information ,license ,forti cloud ,adinsitrators ,security fabric ,current usage , ويمكن أضافه dashboard او widget كما تم شرحه سابقا ...

شرح استخدامات ومعلومات ال Widget :

A- System information :

مثل hostname ، firmware ، Mode ، system time&date ،

B- License :

مثل لايسنر fortiguard ,anti spam ,Antivirus,Web filtering,IPS,

في حالة كنت مشترك في هذه الخدمة فانك عند تفعيلها فانه متاح لك امكانيه فتح واستعراض أي تقرير من أي مكان بالعالم وليس فقط من على جهاز الفورتني نفسه حيث كل التقارير تكون على سيرفر في الكلاود.

-D : Administrators Widget

يعرض لك معلومات عن اليوزرات الذي ياكسسو(يوصلوا) الى جهاز الفورتني مثل يوزر admin او Marfadi ويعرض لك البروفايل الخاص بهم ونوع الوصول هل هو https او http او ssh وهكذا ...

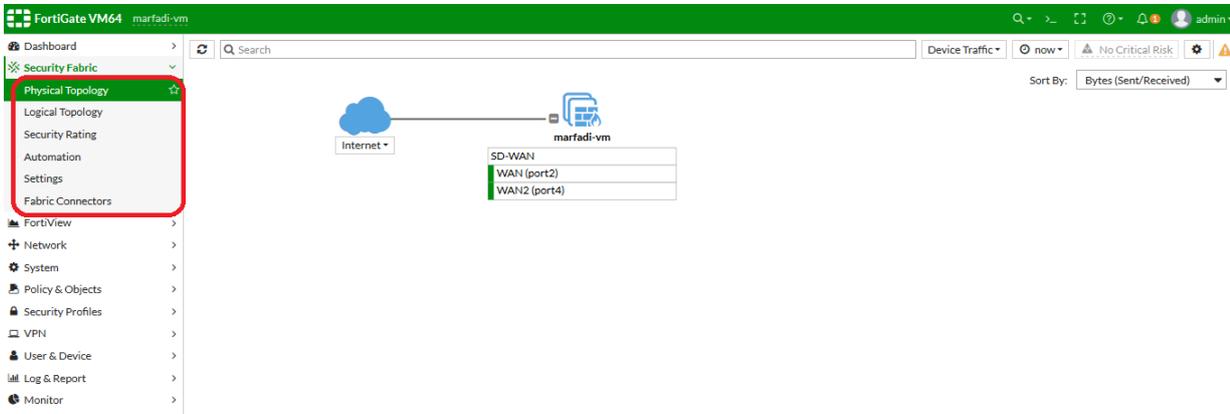
- ٢ : Security fabric

هي عباره عن خاصية عرض فقط (View) لكل الاجهزه التابعه لشركه فورتني من معلومات حول الشبكة وعرض تفاصيل عن الشبكة ومتابعة ال logs والترافيك ... الخ

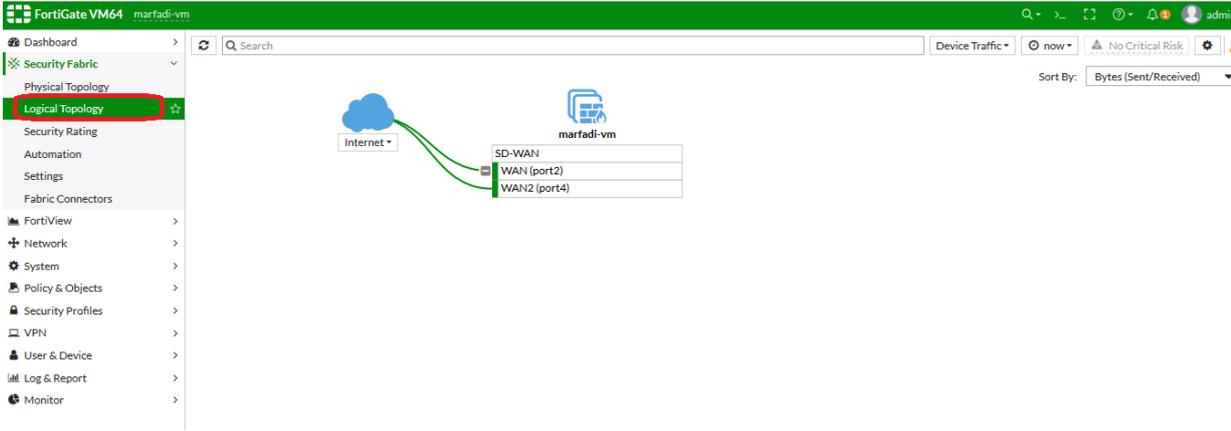
في الشركات الكبيرة يوجد لديهم اكثر من جهاز حمايه (فايروول) في الشركة مثلا ممكن يكون لديهم جهاز -fortianalyzer-forimail

حيث على الأقل يجب ان يكون لديك fortigate و fortianalyzer لكي تفعل (تعمل) هذه الخاصية ، توجد طريقتين للعرض :

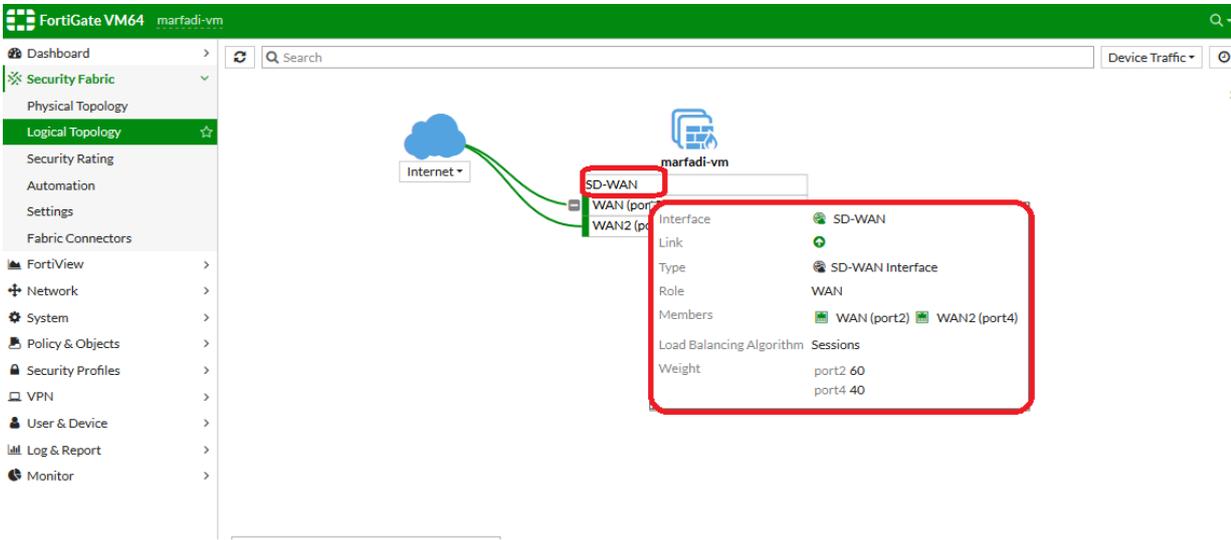
- ١ Physical topology



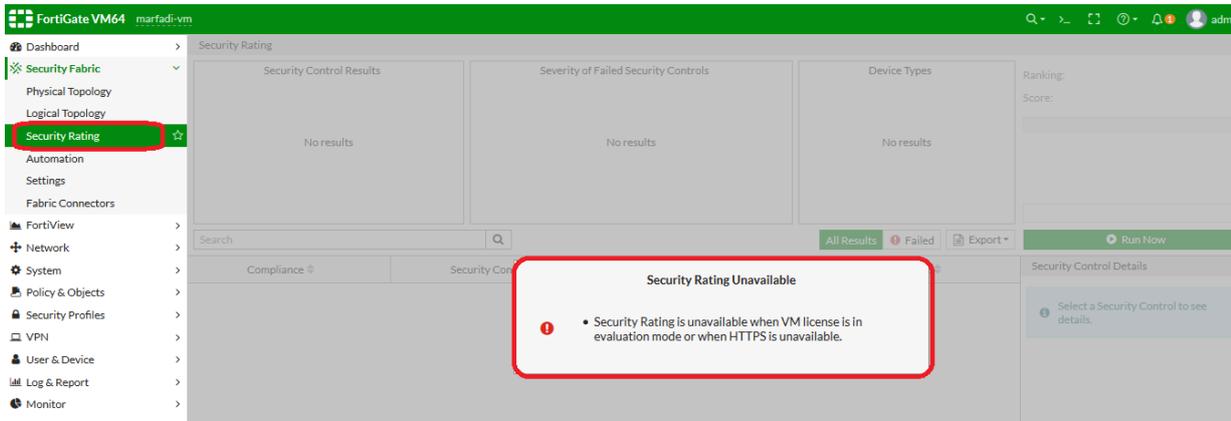
يمكنك بواسطته ان تظهر Topology للفورتني جيت كما بالصورة أعلاه ...



حيث بمجرد تمرير مؤشر الماوس على العناصر يوضح لك مثلا الايبيات والinterface...



: Security Rating -3



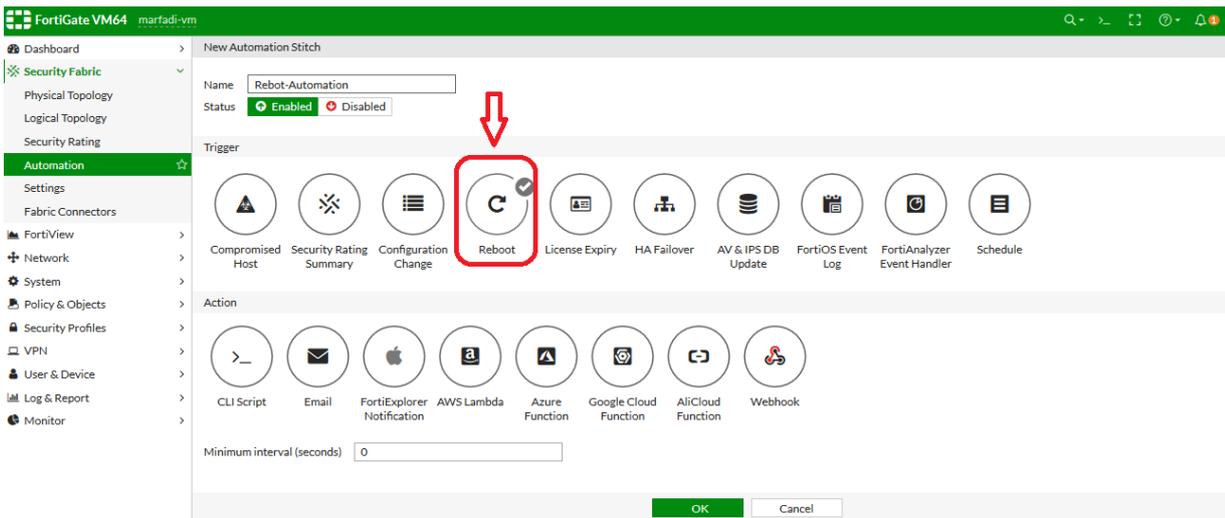
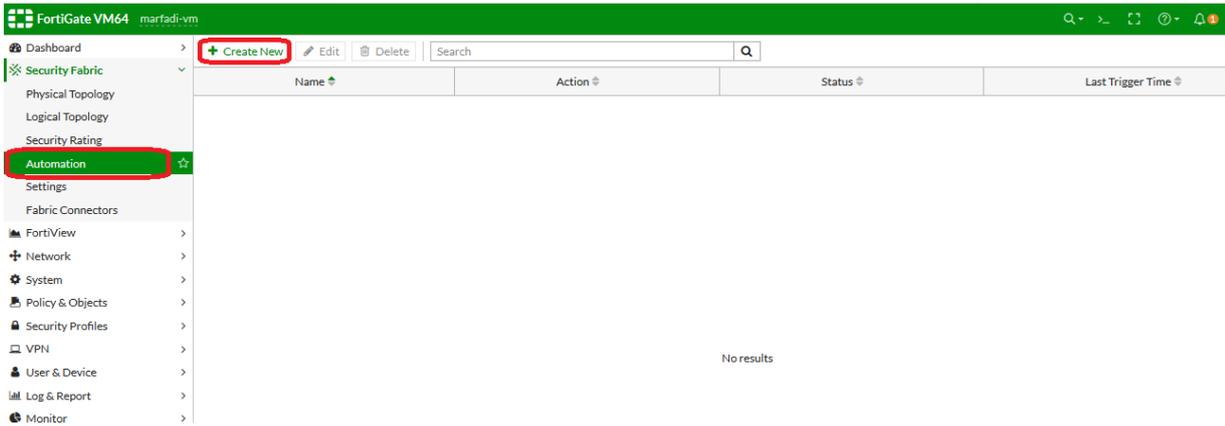
غير متاح في VM ولكن فعليا يتم استخدامه كآليه فحص للأجهزة التابعه لفورتى نت مثلا FortiAnalyzer وغيرها ...

: Automation -4

فكره الAutomation قائمه على Trigger (حدث) فأما يحدث (true) واما لا يحدث (False) فلو كان true قم بعمل action معين .

حيث لو لاحظ الفورتى جيت شي معين انا بحدده فقم بعمل action

مثال لو قمت بعمل اعاده تشغيل لجهاز الفورتى جيت فقم بإرسال أوامر عبر cli



كما بالصورة أعلاه قمنا بالنقر على الحدث Reboot

فنقوم للفورتى جيت في حالة حصل اعاده تشغيل للفورتى جيت قم بعمل ال action كما بالصورة التالية وليكن CLI Scripts مثلا عمل ping 8.8.8.8

أساسيات فورتى جيت

Name: Rebot-Automation
Status: Enabled

Trigger: Reboot

Action: CLI Script (highlighted)

Minimum interval (seconds): 0

CLI Script
1st Action Name: CLI Script
Script: CLI Script

Name: Reboot
Status: Enabled

Trigger: Reboot

Action: CLI Script

Minimum interval (seconds): 0

CLI Script
1st Action Name: ping_order
Script: execute ping 8.8.8.8

مثلا اريد اعمل Ban او حضر لجهاز بمجرد حصل له Hacked

Name: Ban-Compromised
Status: Enabled

Trigger: Compromised Host (highlighted)

Threat level threshold: Medium

Action: IP Ban (highlighted)

Minimum interval (seconds): 5

بعد حصول المشكلة ب5 ثواني قم بعمل BAN للجهاز هذا ..

-٣ FortiView :

هو نظام مراقبة للشبكة الخاصة بك مثل الLOGS وعمل فلتر بحسب الايبي او فلتر بحسب برنامج معين او فلتر بحسب يوزر معين والخ حيث قائمه الMonitor تعرض لك معلومات real time ف نفس الوقت وحقيقه عن تفاصيل مثل من اخذ dhcp او اي حالة ال VPN وهكذا تختلف عن ال fortiview اللي يعرض لك احداث مسجله مش شرط تكون real time .

-٤ Networks :

يقوم بعرض معلومات عن كروت الشبكة وتندرج تحت هذه القائمة :

-١ Interfaces :

يعرض معلومات عن كل المنافذ (ports) للفورتى مثل lan و Wan

-٢ DNS :

يوضح الDNS المستخدم هل هو التابع لفورتى مثلا او التابع لجوجل مثل 8.8.8.8 او 8.8.4.4 او غيرها ..

-٣ Packet capture :

يستخدم لعمل مراقبه لجهاز معين مثلا جهاز صاحب الايبي 192.168.20.140 عند الخروج الى الانترنت عبر المنفذ WAN حيث يتم حفظها في ملف من نوع Cab حيث يمكن فتح هذا الملف ببرنامج متخصص بمتابعة المشاكل :

```
Network>packet capture>create New>enable filter>
```

```
Max pacjet to save:4000 (by default)
```

```
Host(s):192.168.20.40 ممكن تعمل مدى ايبهات
```

```
Port(s):443 httpsمراقبه الترافيك التابع
```

```
OK
```

أي ان الايبي 192.168.20.140 اذا استخدم HTTPS مثل فتح موقع معين فان ذلك سيتم حفظه داخل الملف لعمل متابعه وتحليل للمشاكل ..

٤- **SD-WAN**: اسمها أيضا WAN LOAD BALANCED تستخدم لعمل load balance لعدد 2 خطوط مثلا في حالة توقف احدى خطوط الانترنت فأن الخط الاخر يعمل بشكل اوتوماتيكي ..

٥- **Static route**

تعمل Route بحيث تقول لو وصل اليك احد من ال internal واراد ان يخرج الى external (الانترنت)خرجه من ال interface مثلا WAN كذا ...

Network >Static Route>Create New>

Destination:0.0.0.0/0.0.0.0

Device:port2(WAN)

Gateway :192.168.1.1

حيث 192.168.1.1 هو ابي الروتر..

٥- **System**

١- Administrator : يظهر لك يوزر باسم admin وهو الافتراضي حيث له الحق بالوصول الى الفورتى جيت من أي جهاز Trusted Hosts 0/0.0.0.0 حيث ان البروفايل الخاص به نوعه Super_admin

٢- Admin profiles : هو البروفايل الي له الحق بالوصول الى الفورتى جيت حيث بشكل افتراضي super_admin و prof_admin ويمكنك ان تقوم بتخصيص بروفايل وتحدد نوع صلاحية الوصول بحسب ما تريد.

٣- Firmware : يعرض لك الإصدار الحالي لـ OS الخاص بجهاز الفورتى ويمكن عمل Upload

للـ Firmware وأيضا يعرض لك الإصدارات المتاحة ويمكن عمل ترقيته (upgrade) او انزال (downgrade) من هنا.

٤- Settings : ممكن تعديل اسم الجهاز من Hostname ، وايضا يعرض لك الوقت والتاريخ الحالي ويمكنك تغيير المنطقة الزمنية لجهاز الفورتى ،

يمكنك أيضا تعديل رقم البورت الافتراضي http=80 الى أي رقم تريده وايضا https:443 ..

ويمكنك أيضا تعديل الثيم theme للواجهة من ألوان ولغة العرض وايضا لتعديل وقت انتهاء الجلسة لصفحة الدخول (login) وذلك بتعديل قيمته idle timeout:2 حيث سيتم اغلاق الـ login بعد مرور دقيقتين بدون ان تستخدم GUI .

٥- HA : في حالة وجود جهاز فورتى جيت وحيد بالشركة فأن النمط هو Mode=standalone اما في

حالة وجود اكثر من جهاز فورتى في الشركة فان النمط (Mode) ممكن ان يكون active-active او active-passive أي يستخدم كنوع من الباك اب بحيث لو تعطل او توقف احدى اجهزه الفورتى فأن الاخر يعمل بشكل تلقائي بدون توقف للشبكة .

٦- SNMP : احدى بروتوكولات المراقبة حيث يقوم بمراقبه حالة جهاز الفورتى ويرسل كل شي الى سيرفر يسمى SNMP server .

٧- Replacement Messages : هي عبارته عن الرسائل التي تظهر لك كأدمن للفورتى او كيوزر في

حالات مختلفة مثل فتح مواقع محجوبه او خطأ في الولوج الى الفورتى جيت ... الخ

ويمكنك تعديل الرسائل كما تريد ..

٨- FortiGuard : في هذه القائمة تظهر لك حالة ال licenses الخاصة بجهاز الفورتى مثل Web filter، Antispam، Antivirus، IPS وايضا متابعه حالة التحديث لهم ..

٩- Certificate : لوقمت بتفعيل خاصيه SSL Inspection فيجب عليك ان تقوم بإنشاء شهاده ..

٦- Policy&Objects :

١- ipv4 policy : هذه القائمة التي من خلالها يمكنك انشاء او تعديل policy (Rule) ، ،

٢- ipv4 Dos policy : هذه القائمة من خلالها تستطيع عمل policy لحماية الشبكة من هجوم المخترقون من نوع Dos attack حيث يتم تطبيق هذه البوليسى على منفذ الWAN لأن الهجوم لا يأتي الا عبر

Incoming interface :wan

٣- Address : لإنشاء عناوين للأجهزة .

٤- Internet service database : تحتوي على معلومات بجميع الخدمات المتاحة على الانترنت مثل DNS التابع لجوجل ..

٥- Schedule : ممكن تحديد وقت معين حيث يتم استخدامها مع البوليسى.

٦- Traffic shaper : تسمح لك بتحديد max bandwidth او limit bandwidth لجهاز معين لكي لا يستهلك الانترنت بالشبكة ..

٧- Security profiles : تستخدم لحماية الشبكة من الهجمات .

١- Antivirus : عمل سكان للترافيك الداخلى او الخارج من الشبكة .

- ٢- Web filter : تستخدم لتحديد الوصول للمواقع (سماح او منع).
- ٣- Application filter : تتحكم بالترافيك الذي داخل او خارج بواسطة التطبيقات وليس عن طريق البورت .
- ٤- Intrusion prevention : تسمى أيضا ب IPs تستخدم لحماية الشبكة من عمليه الهاك (HACK)
- ٥- SSL/SSg inspections : في حالة تفعيل ssl/ssh inspect فانه يتم عمل deep inspections للترافيك من نوع HTTPS .

: SSL INSPECTION

عندما نقوم مثلا بعمل Block لموقع الفيسبوك عبر ال Web filter فان الفورتى جيت يواجه مشكله وهي ان لو اليوزر فتح موقع الفيسبوك بجلسه مشفره أي عبر https فأن الفورتى جيت لا يعرف ما بداخل هذه الجلسة الا لو قمت بتفعيل خاصيه ssl inspection ..

حيث افضل طريقة هي Deep ssl inspection من حيث الفحص وبنفس الوقت تكون بطئ نوعا ما ..

-٨ : User&Device

- ١- User definition : اليوزر لكي يصل للشبكة سواء انترنت او غيرها يجب ان يكون لديه يوزر اكاونت وكلمه سر ولذا يتم انشاء local user .
 - ٢- User groups : يتم انشاء جروب لكي يتم أضافه اليوزرات اليها وبذلك يسهل عمليه تطبيق البوليسي عليهم جميعا بدلا من تطبيق بوليسي على مستوى اليوزر .
 - ٣- Device Inventory : تجميع معلومات عن الأجهزة الموجودة بالشبكة
 - ٤- Single sign-on : تسمى SSO حيث عن تفعيل هذه الخاصية (دمجها مع ال active directory) فأن اليوزر لا يحتاج الى ادخال يوزرنيم وباسورد اكثر من مره بل يكفي ان يدخل اليوزرنيم والباسورد عن عمل login بجهازه مره واحده فقط ،
- اما ان لم تكن هذه الخاصية مفعله فأن اليوزر سوف يضطر الى ادخال اليوزر نيم والباسورد الخاص بالدخول الى الويندوز بالإضافة لليوزرنيم والباسورد الخاص بالفورتى الذي تم انشاءه مسبقا من قائمه User definition للوصول الى الانترنت .

٩- **WiFi & switch controller**: في حالة وجود fortiAP بالشبكة وتريد عمل له ادارته وتحكم كامل بواسطة الفورتى... حيث fotiAP هو عبارة عن اكسس بوينت ولكن خاص بشركه فورتى نت

١٠- **Log & Reports**

١١- **Monitor**

❖ **طريقة توصيل الانترنت لجهاز الفورتى جيت :**

يجب ان يكون جهاز الفورتى جيت موصلا بالإنترنت لكي يتمكن من عمل registration وأيضا عمل update لكلا من Antivirus DB و IPs DB و Antispam DB و Web filtering DB... الخ

وايضا لأنه سيكون هو الجيتواي (Gateway) للأجهزة الموجودة بالشبكة

وايضا لو اردت عمل update ل firmware الخاص بك .

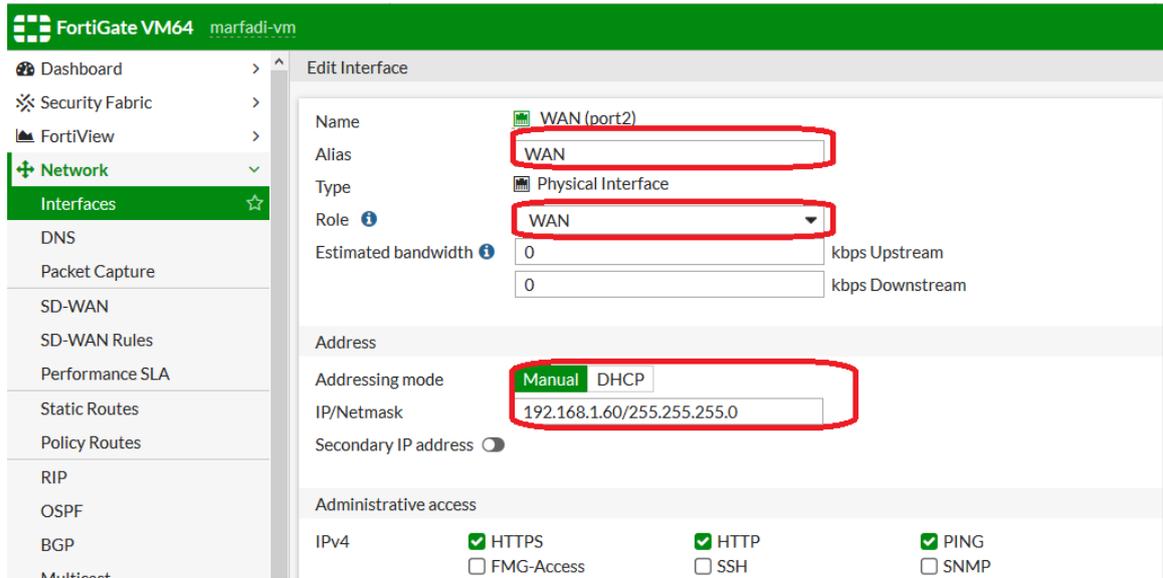
وللقيام بذلك يجب ان تقوم بالخطوات التالية :

١- اظافه ايبي ل WAN PORT

٢- اظافه DNS

٣- عمل static route بحيث أي احد يريد ان يصل الى الانترنت يجب ان يخرج عبر المنفذ WAN

الخطوة الأولى :



Network>Interfaces>port2>Edit>alias(Write WAN)>Role=WAN>

Addressing mode :manual or DHCP

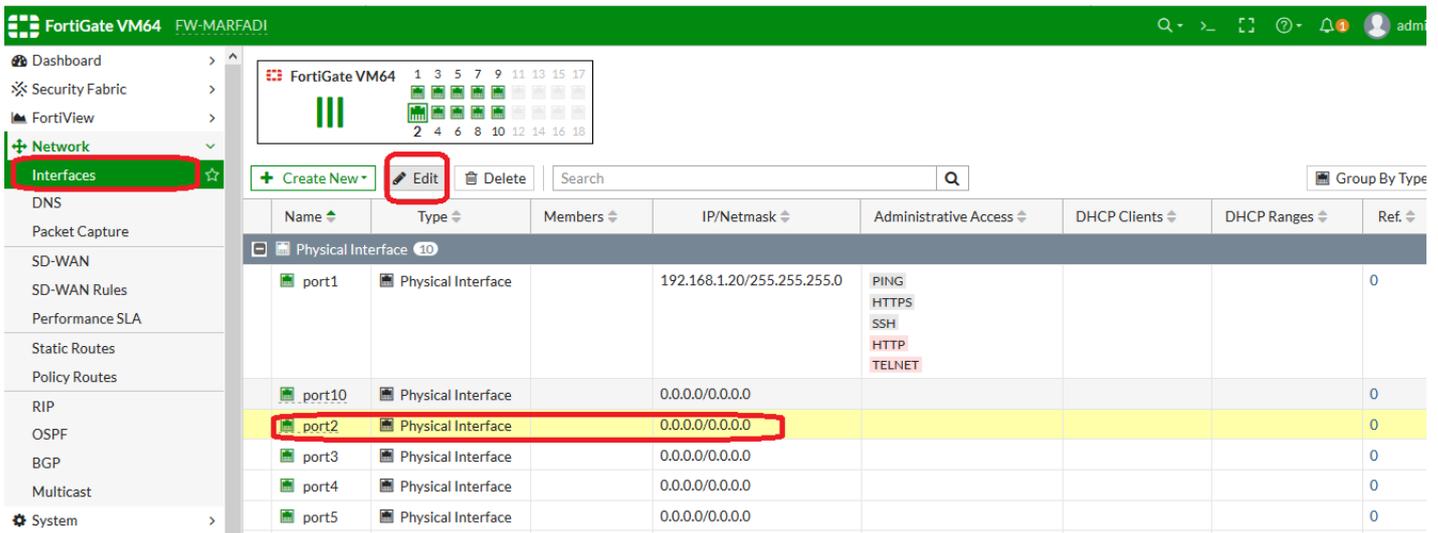
حيث manual سوف تقوم بكتابه 255.255.255.0/192.168.1.60

ولو اخترت DHCP فإنه سوف يأخذ بشكل اوتو من الروتر..

حيث من الممكن تحديد طريقة الوصول الى المنفذ ال WAN بأكثر من طريقة مثل HTTPS و HTTP ووالخ ولكن كنوع من السيكيورتي يتم فقط السماح بالوصول الى البورت عبر PING .

حيث بعد ذلك يمكن من الابتوب الشخصي (Host) ان تعمل

Ping 192.168.1.60 وهو ايي بورت ال WAN



Edit Interface

Name: port2
 Alias: WAN
 Type: Physical Interface
 Role: WAN
 Estimated bandwidth: 0 kbps Upstream / 0 kbps Downstream

Addressing mode: Manual **DHCP**
 Retrieve default gateway from server:
 Distance: 5
 Override internal DNS:

Administrative access:

IPv4: HTTPS, PING, FMG-Access
 SSH, SNMP, FTM
 RADIUS Accounting, Security Fabric Connection

ثم OK .

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
Physical Interface 10							
port1	Physical Interface		192.168.1.20/255.255.255.0	PING HTTPS SSH HTTP TELNET			0
port10	Physical Interface		0.0.0.0/0.0.0.0				0
port3	Physical Interface		0.0.0.0/0.0.0.0				0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
port9	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (port2)	Physical Interface		192.168.1.105/255.255.255.0	PING			0

تلاحظ بان المنفذ WAN حصل على ايبى 192.168.1.105 وكما هو ظاهر بان ال ping مفتوح ...

نحن سوف نجعل كرت lan2=wan ايبى static

Name	Type	Members	IP/Netmask	Administrative Access
port10	Physical Interface		0.0.0.0/0.0.0.0	SSH HTTP TELNET
port3	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	
port5	Physical Interface		0.0.0.0/0.0.0.0	
port6	Physical Interface		0.0.0.0/0.0.0.0	
port7	Physical Interface		0.0.0.0/0.0.0.0	
port8	Physical Interface		0.0.0.0/0.0.0.0	
port9	Physical Interface		0.0.0.0/0.0.0.0	
WAN (port2)	Physical Interface		192.168.1.60/255.255.255.0	PING HTTPS HTTP

حيث يمكنك بعد ذلك ان تدخل الى اعدادات الفورتى جيت عبر الويب من نفس الـ (Host) وذلك بكتابه ابي wan وهو 192.168.1.60 في متصفح الانترنت وبهذا يكون قد قلت استهلاك الـ resources للابتوب عند العمل والتطبيق والتعلم ، حيث ليس هناك داعي الدخول الى اعدادات الفورتى جيت عبر جهاز الكلاينت ..

الخطوة الثانية :

ضبط اعدادات DNS لجهاز الفورتى جيت كما بالخطوات التالية :

Network > DNS > Specify > 8.8.8.8 8.8.4.4

>apply

FortiGate VM64 FW-MARFADI

DNS Settings

DNS Servers: Use FortiGuard Servers **Specify**

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Local Domain Name: [Empty]

DNS over TLS: Disable Enable Enforce

Dynamically Obtained DNS Servers

Interface	DNS Server
WAN (port2)	82.114.160.45 82.114.160.46

DNS Servers

208.91.112.53	10,830 ms
208.91.112.52	10,630 ms

Acquired DNS Servers

82.114.160.45	4,950 ms
82.114.160.46	20 ms

DNS Filter Servers

111.108.191.92	Unreachable
45.75.200.89	Unreachable

Setup guides

- DNS local domain list
- Using FortiGate as a DNS server
- FortiGuard DDNS

Documentation

Network>static route>create New>

Destination:subnet 0.0.0.0/0.0.0.0 أي يمكنك الخروج الى أي شبكة

Gateway:192.168.1.1 ايبي المودم

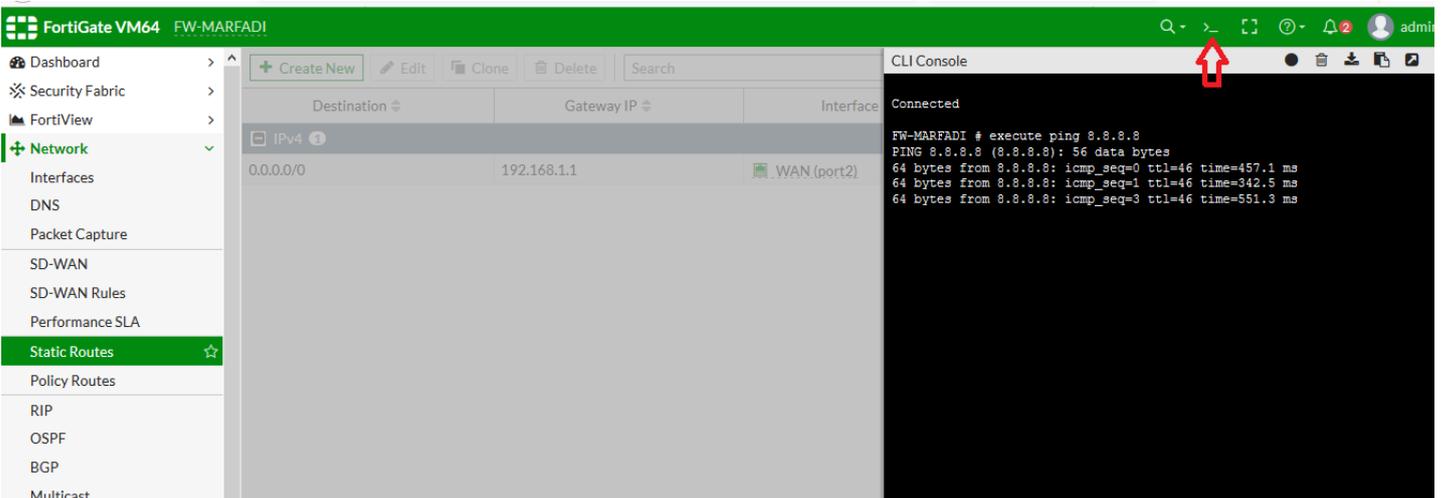
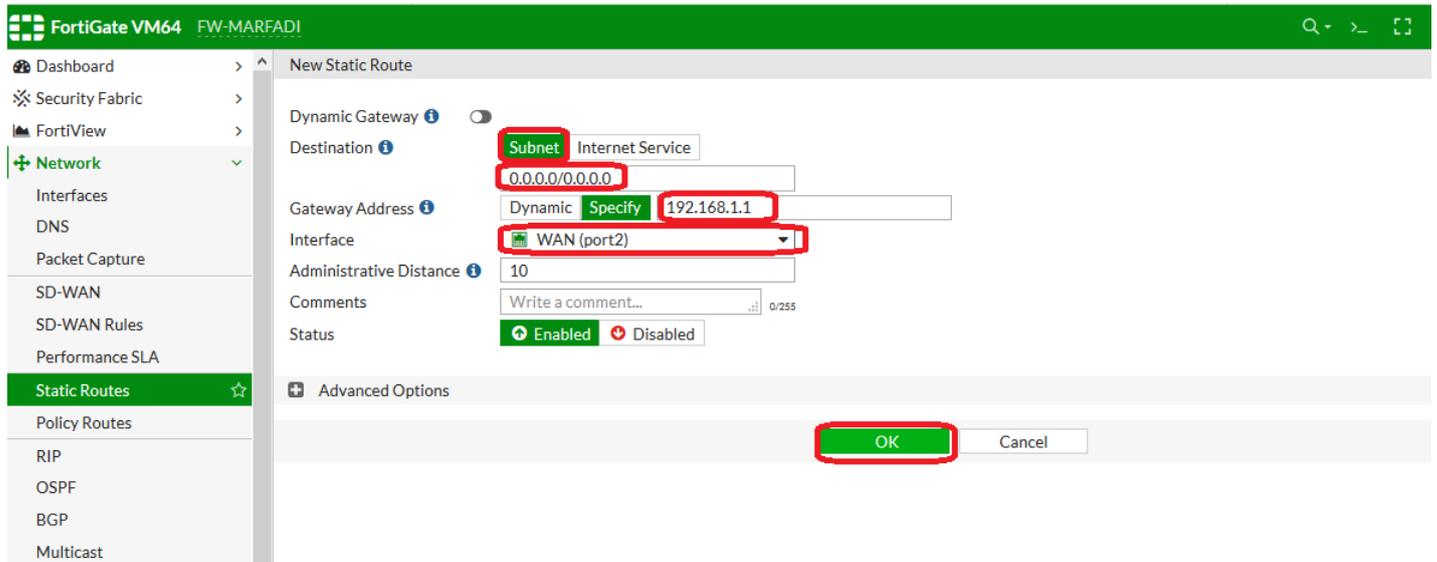
Interface :port2(WAN)

OK

ثم نقوم بالدخول الى CLI عبر GUI ثم نكتب الامر

Execute ping 8.8.8.8

فتلاحظ بان الانترنت اصبح متاح لجهاز الفورتى جيت الآن ..



❖ متى احتاج الى عمل ترقية - تحديث - لل Firmware التابع لجهاز الفورتى:

- ١- أضافه مميزات جديده للإصدار الجديد
- ٢- تحسين وحل مشكله في ميزه معينه في الإصدار الجديد
- ٣- بسبب أضافه bugs لحل بعض الثغرات بالإصدار القديم

قبل عميه ال Upgrade (ترقيه) يجب ان تقوم بالتالي :

- ١- يجب ان يكون لديك باك اب لل Current configuration حيث لو حصل أي مشكله اثناء عمليه الترقية نقوم بالاستعادة
- ٢- يجب ان تتأكد من وجود نسخه current firmware حيث لو حدث مشكله اثناء الاستعادة فانك ستقوم بإعادة تثبيت النسخة ومن ثم عمل استعادته ل configuration التي قمت بها في الخطوة رقم 1
- ٣- يجب ان يكون لديك Upgrade path لأنه لا يمكن ان تقوم بعمل ترقية من اصدار 5.0 الى 6.00 مباشرة بل يجب ان تقوم بالترقية بالتدرج بحسب upgrade path مثلا من 5.0 الى 5.6 والخ الى ان تصل الى الإصدار المطلوب 6.0

❖ طرق ترقية النظام Upgrade firmware :

- ١- بواسطة الfortiGuard أي ان نقوم بتنزيل الإصدار الحديث من الانترنت مباشرة بواسطة شركة فورتى جيت
- ٢- بواسطة local device (أي ان تكون نسخه ال OS في جهازك
ثم نقوم بالخطوات التالية

System >upload firmware >select file>choose the file of OS>Backup config and upgrade >

ثم سيتم اعاده التشغيل مرتين ...

ثم نتأكد من نجاح عمليه الترقية وكذلك من ان الاعدادات لازالت سليمة وذلك بالدخول الى

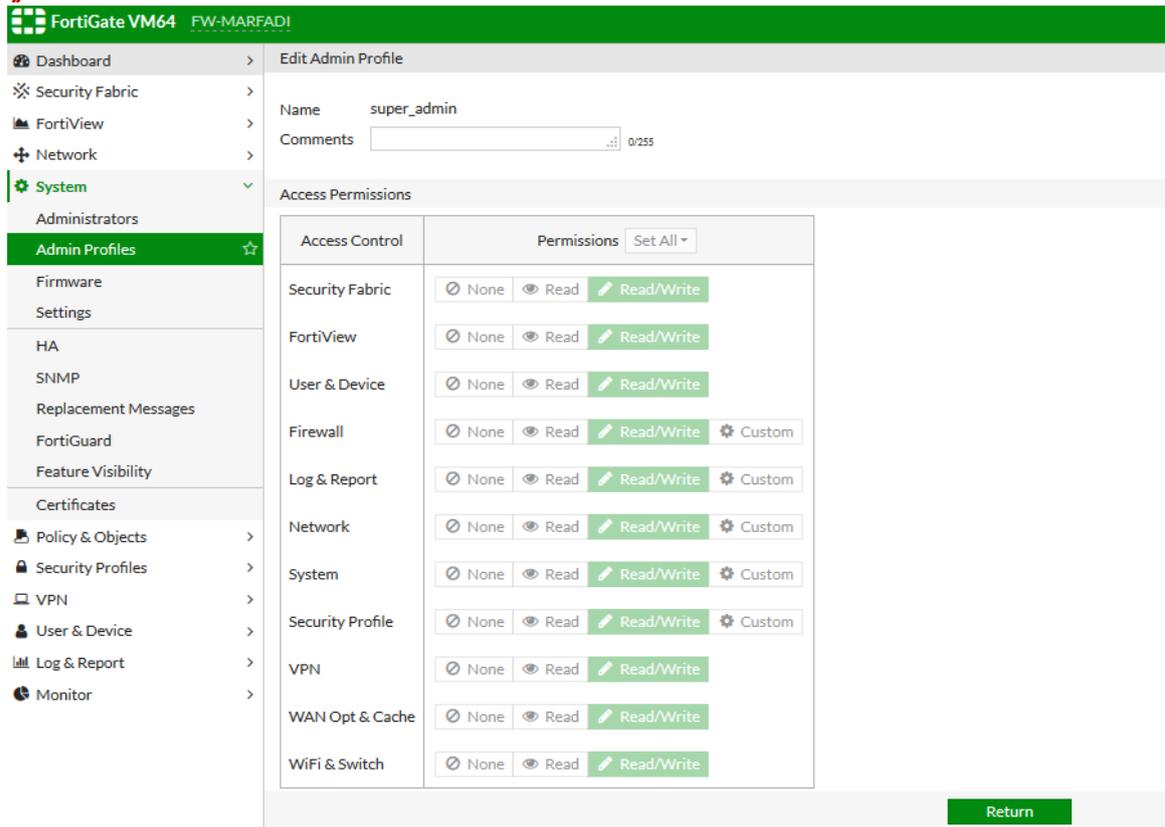
Main>firmware >

The screenshot shows the FortiGate VM64 web interface. The top navigation bar includes 'Dashboard', 'Security Fabric', 'FortiView', 'Network', 'System', 'Firmware', 'Settings', 'Policy & Objects', 'Security Profiles', 'VPN', 'User & Device', 'Log & Report', and 'Monitor'. The 'Firmware' section is active, displaying 'Firmware Management' with the current version 'FortiOS v6.2.3 build1066 (GA)'. Under 'Upload Firmware', there is a 'Select file' dropdown with a 'Browse' button highlighted by a red box. Below this, there is a 'FortiGuard Firmware' section with 'Latest' and 'All available' tabs. A yellow warning message states 'No firmware available from FortiGuard'.

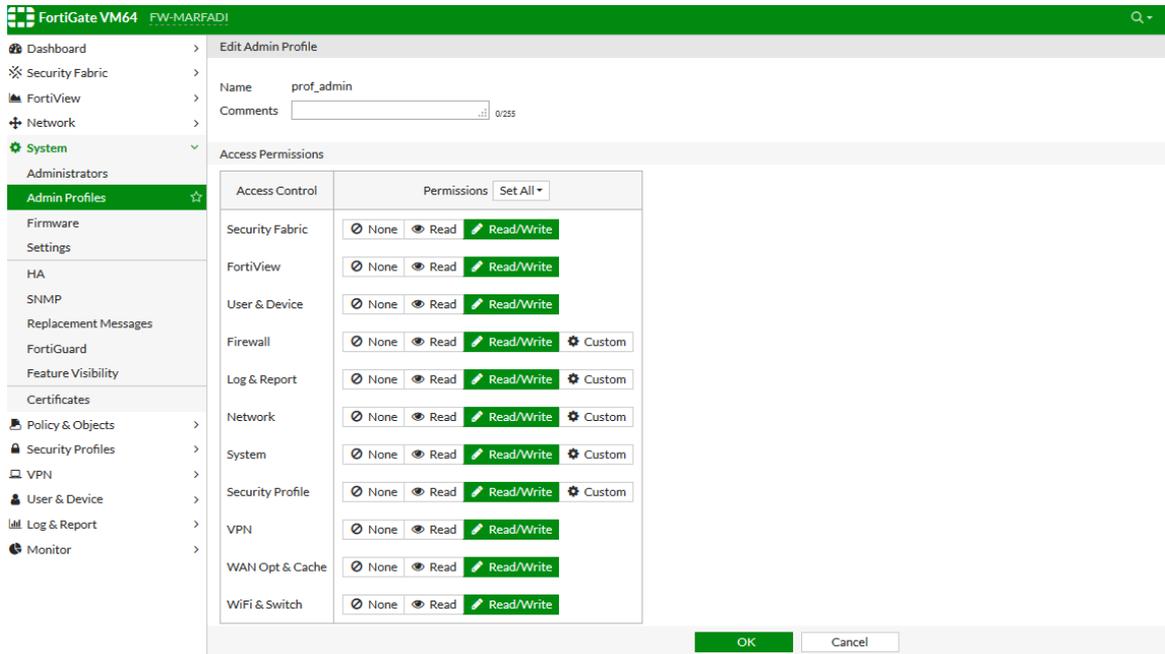
: Administration types & profiles

Admin profiles: من خلاله تحدد اليوزر الذي سوف يعمل login على الفورتى جيت يعمل ماذا! ويشوف ماذا!!! ويتحكم بماذا ...

البروفايالات الافتراضية هما super admin و prof admin



نلاحظ بان البروفايل أعلاه من نوع super_admin غير قابل للتعديل..



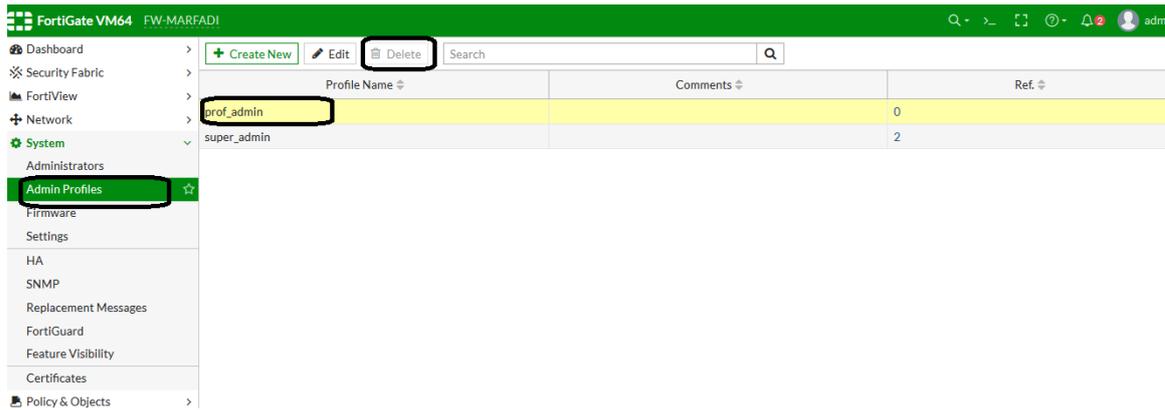
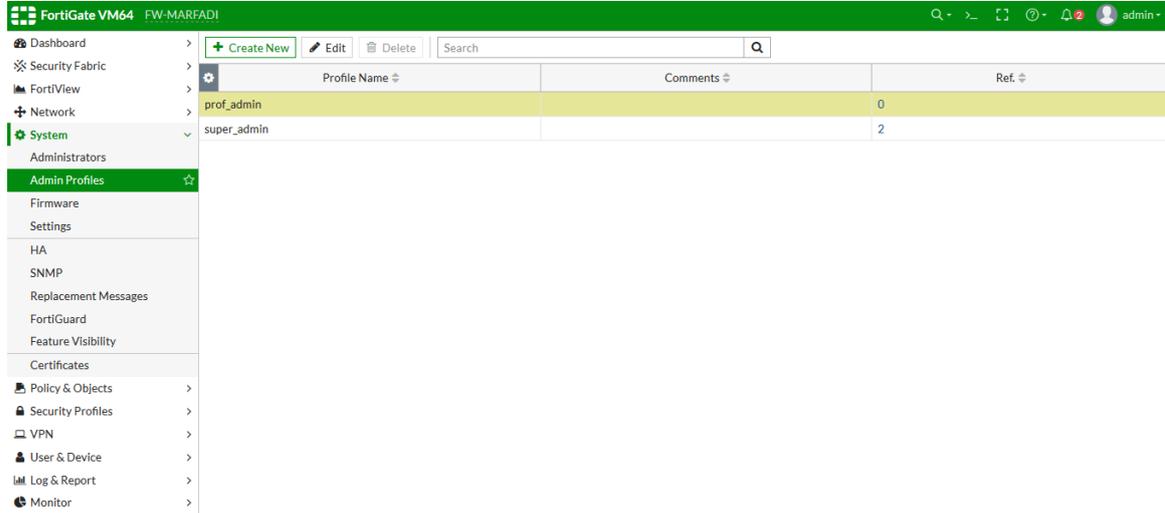
نلاحظ من الصورة أعلاه بأن البروفايل prof_admin قابل للتعديل ..

Super admin : له full access على كل مكونات الفورتني جيت مثل delete و create لـ other

administrator ويعمل بالكاب واستعادته وأيضا ترقية او تنزيل لنسخه الـ firmware ..

لا يمكنك ان تقوم بعمل تعديل او حذف على super_admin profile ،

يفضل انشاء يوزر جديد وتعديل الاسم الى admin الى أي اسم اخر كنوع من السيكيوريتي او حذف اليوزر admin بعد انشاء يوزر اخر نوع super_admin .



كما تلاحظ بالصورة أعلاه فانه لا يمكن حذف البروفايل ولكنك يمكن تعديله ...

❖ طريقة انشاء يوزر جديد بواسطة CLI :

```
#config system admin
```

```
#edit marfadi
```

```
#set password 123
```

```
#set accprofile prof_admin or super_admin
```

```
#end
```

The screenshot shows the FortiGate VM64 Admin Console interface. The main panel displays the 'Edit Admin Profile' configuration for 'prof_admin'. The 'Access Permissions' table is as follows:

Access Control	Permissions	Set All
Security Fabric	None, Read, Read/Write	
FortiView	None, Read, Read/Write	
User & Device	None, Read, Read/Write	
Firewall	None, Read, Read/Write, Custom	
Log & Report	None, Read, Read/Write, Custom	
Network	None, Read, Read/Write, Custom	
System	None, Read, Read/Write, Custom	

The CLI Console on the right shows the following commands and output:

```

Connected
FW-MARFADI # config system admin
FW-MARFADI (admin) # edit marfadi
new entry 'marfadi' added
FW-MARFADI (marfadi) # set password 123
FW-MARFADI (marfadi) # set accprofile prof_admin
FW-MARFADI (marfadi) # end
FW-MARFADI #
    
```

تم انشاء يوزر باسم marfadi وباسورد 123 وانشاء بروفايل نوع prof_admin او super_admin بحسب ما تريد ..

ثم حفظ الاعدادات ...

The screenshot shows a login form with the following fields and buttons:

- Username field: marfadi
- Password field: [masked]
- Login button

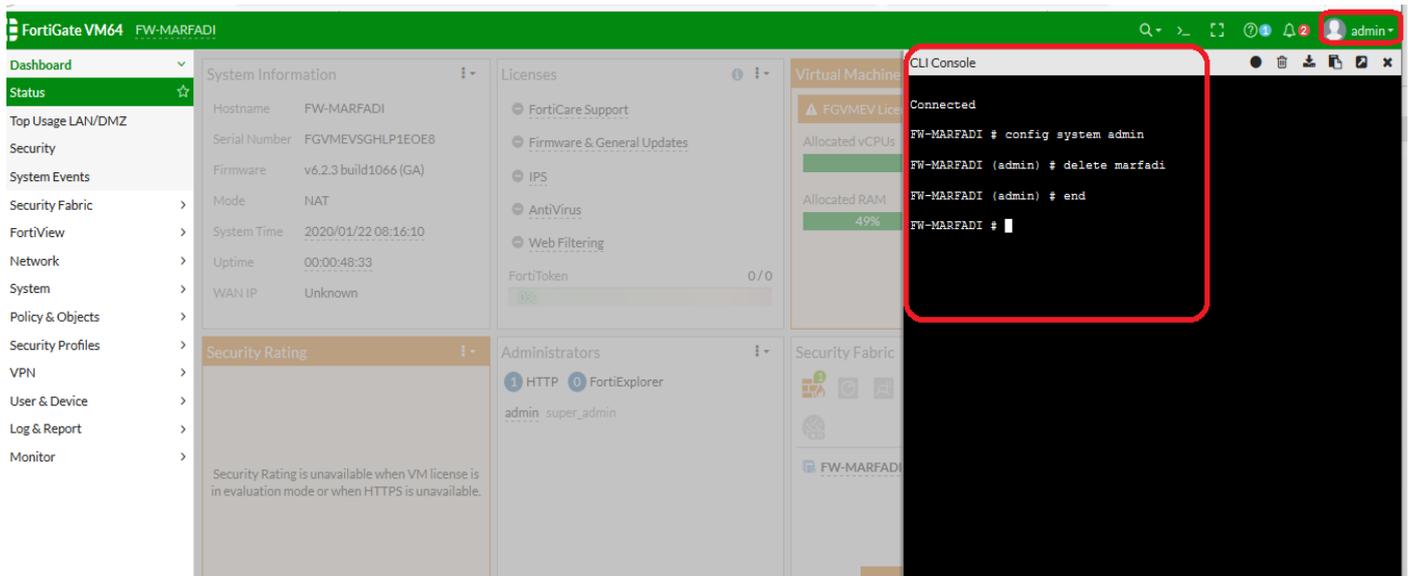
The screenshot shows the FortiGate VM64 Admin Console dashboard. The left sidebar is highlighted with a red box. The main content area displays the following information:

- System Information:** Hostname: FW-MARFADI, Serial Number: FGVMEVSGHLP1EOE8, Firmware: v6.2.3 build1066 (GA), Mode: NAT, System Time: 2020/01/22 08:13:01, Uptime: 00:00:45:24, WAN IP: Unknown.
- Licenses:** FortiCare Support, Firmware & General Updates, IPS, AntiVirus, Web Filtering, FortiToken: 0/0.
- Virtual Machine:** FGVMEV License, Allocated vCPUs: 1/1 (100%), Allocated RAM: 1002 MIB / 2 GIB (49%).
- FortiGate Cloud:** Status: Not Supported.
- Administrators:** HTTP, FortiExplorer, marfadi, prof_admin.

#config system admin

#delete marfadi

End



كما بالصورة أعلاه اليوزر admin له الحق ان يحذف اليوزر marfadi ..

Prof_admin : يتم إنشاءه بشكل افتراضي وهو نفس super admin لكنه يمكن عمل تعديل على

العناصر مثل firewall و log&report و network ووالخ

حيث ممكن نعملها none او read او write او custom للعناصر وأيضا لا يمكنك حذف البروفايل

المسمى prof_admin .

حيث ال prof_admin لا يمكن عمل تغيير للباسورد ..

وأيضا اليوزر من نوع prof_admin لا يمكنه انشاء يوزر من نوع super_admin .

The top screenshot shows the 'Admin Profiles' table in the FortiGate VM64 web interface. The table has columns for Profile Name, Comments, and Ref. The 'prof_admin' profile is highlighted in yellow, and the 'super_admin' profile is listed below it with a reference count of 2. The 'Edit' button for 'prof_admin' is circled in red.

Profile Name	Comments	Ref
prof_admin		0
super_admin		2

The bottom screenshot shows the 'System > Administrators' page. The 'admin' user is listed with the 'super_admin' profile assigned to it. The 'admin' user name and the 'super_admin' profile name are both circled in red.

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
admin		super_admin	Local	Disabled

تلاحظ بالصورة أعلاه بأن اليوزر المسمى admin من نوع super_admin profile

طريقة انشاء custom profile أي نقوم بتخصيص مجموعة محددة من العناصر التي من حق اليوزرات التي في هذا الجروب (البروفایل) ان تصل اليها ..

مثل سوف انشى بروفایل باسم Yasser Ossimi

System > admin profile > create New >

ثم سنحدد العناصر التي ممكن الوصول اليها فقط كما بالصورة ادناه ..

FortiGate VM64 FW-MARFADI

- Dashboard >
- Security Fabric >
- FortiView >
- Network >
- System >**
 - Administrators
 - Admin Profiles ☆**
 - Firmware
 - Settings
 - HA
 - SNMP
 - Replacement Messages
 - FortiGuard
 - Feature Visibility
 - Certificates
- Policy & Objects >
- Security Profiles >
- VPN >
- User & Device >
- Log & Report >
- Monitor >

New Admin Profile

Name: Yasser Ossimi

Comments: 0/255

Access Permissions

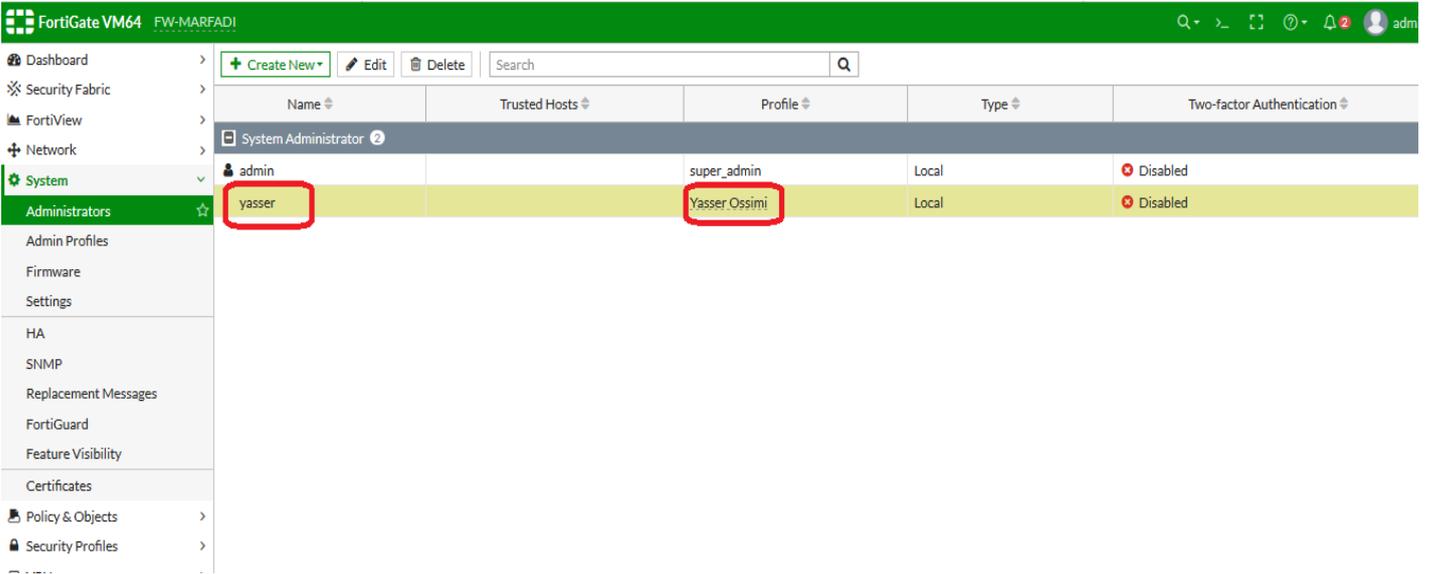
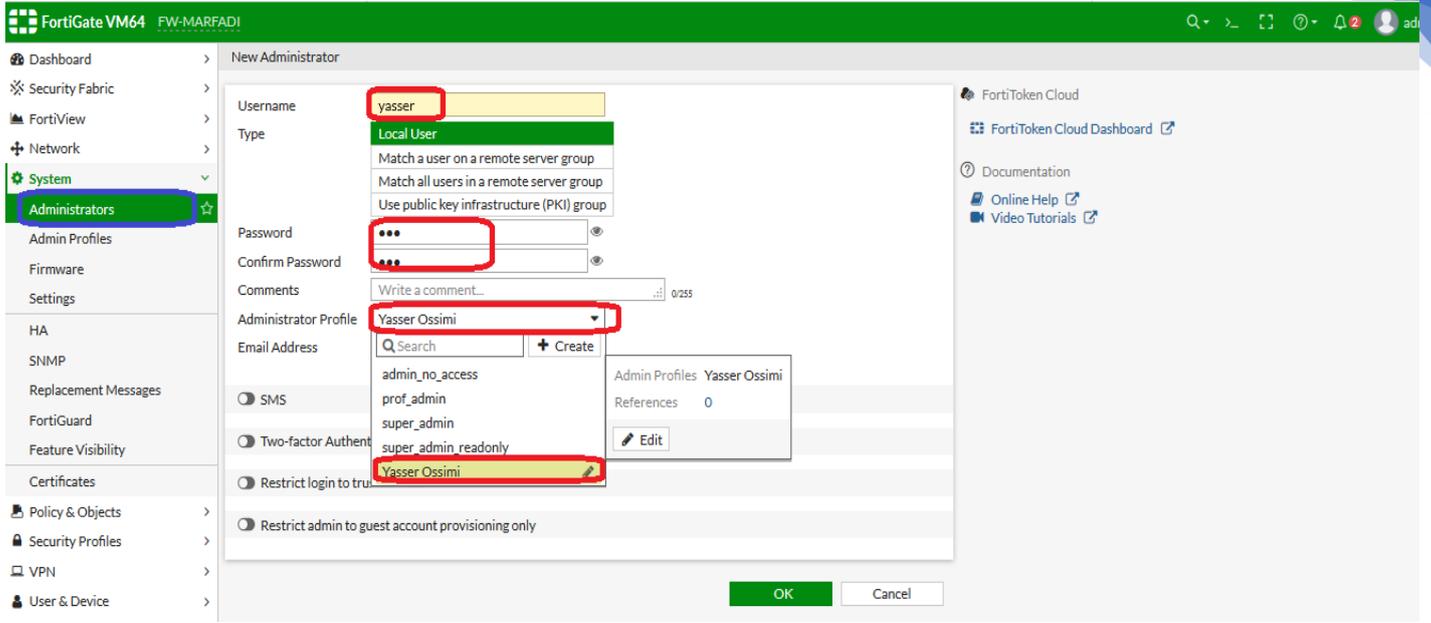
Access Control	Permissions
Security Fabric	None Read Read/Write
FortiView	None Read Read/Write
User & Device	None Read Read/Write
Firewall	None Read Read/Write Custom
Log & Report	None Read Read/Write Custom
Network	None Read Read/Write Custom
System	None Read Read/Write Custom
Security Profile	None Read Read/Write Custom
VPN	None Read Read/Write
WAN Opt & Cache	None Read Read/Write
WiFi & Switch	None Read Read/Write

ثم OK ...

الآن سوف نقوم بإنشاء يوزر باسم Yasser وسوف يكون نوع البروفايل الخاص به هو Yasser ossimi

حيث هذه المرة سيتم إنشاء اليوزر عن طريق الGUI كما بالصورة أدناه

System>administrators>Create New>administrator>



نلاحظ بأنه تم انشاء يوزر باسم Yasser تابع للبروفایل الذي تم تخصيصه سابقا باسم Yasser Ossimi

❖ ما هو FortiGuard ؟

هو خدمه في الكلاود يتم الوصول اليه عن طريق الانترنت ،

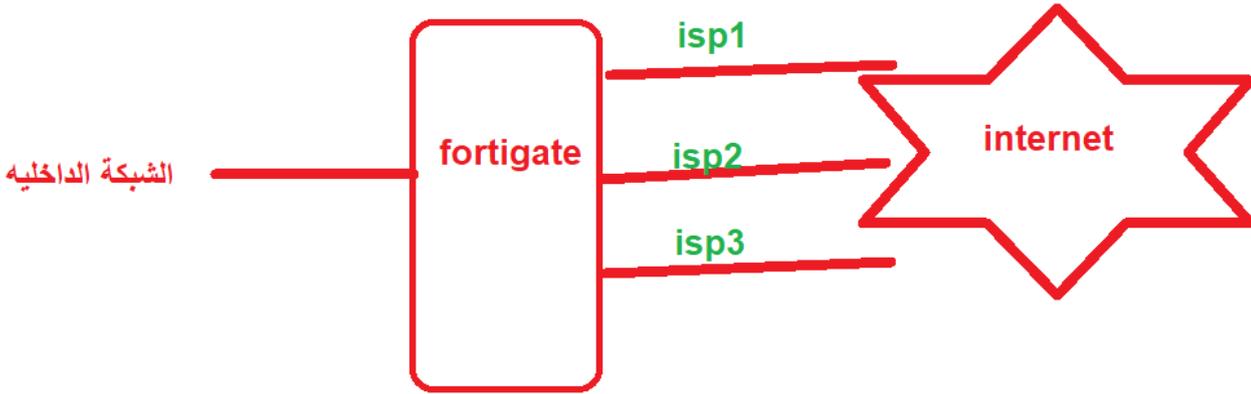
يتم تحديث كل من Antivirus، Antispam، IPs، Web filter، Application control.. الخ الموجود في

جهاز الفورتى جيت عبر FortiGuard ..

حيث أي فايروس جديد يتم عمل update وتنزيله الى جهاز الفورتى جيت وأيضا أي هجمات جديد يتم

تنزيل update جديد لها وهكذا ..

لذا يجب ان تكون مشترك (license) مع FortiGuard



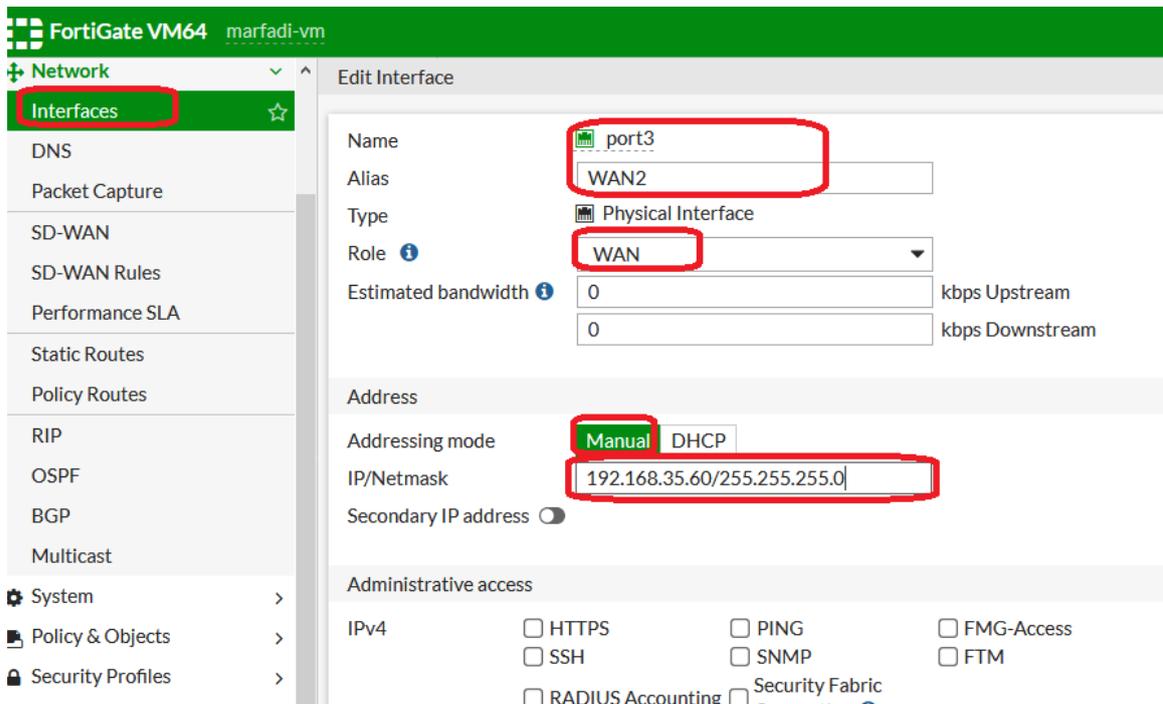
تحويل اكثر من physical interfaces الى logical interface واحد فقط ...

Network>SD-WAN>status:enable>create New>interfaces:

ثم نقوم بتحديد كروت الشبكة المراد دمجها (load balance)

لنفترض بان لدينا 2 خطوط انترنت موصله على كروت الشبكة WAN و WAN2 ثم نحدد خوارزميه لتوزيع الانترنت للمستخدمين.

أولا نقوم بضبط اعداد كرت wan2 كما بالصورة ادناه



FortiGate VM64 marfadi-vm

SD-WAN New SD-WAN Member

Name SD-WAN
Type SD-WAN
Status Enable Disable

Interface WAN (port2)
Gateway 192.168.1.1
Cost 0

Enable Disable

FortiGate VM64 marfadi-vm

SD-WAN New SD-WAN Member

Name SD-WAN
Type SD-WAN
Status Enable Disable

Interface WAN2 (port3)
Gateway 192.168.35.1
Cost 0

Enable Disable

FortiGate VM64 marfadi-vm

SD-WAN

Name SD-WAN
Type SD-WAN Interface
Status Enable Disable

SD-WAN Interface Members

Interfaces	Gateway	Cost
WAN (port2)	192.168.1.1	0
WAN2 (port3)	192.168.35.1	0

SD-WAN Usage

Bandwidth Volume **Sessions**

ثم نلاحظ بانہ تم انشاء logical interface باسم SD-WAN كما بالصورة ادناه ...

The screenshot shows the FortiView Network Interfaces page. A table lists various interfaces:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	D
port10	Physical Interface		0.0.0.0/0.0.0.0			
port4	Physical Interface		0.0.0.0/0.0.0.0			
port5	Physical Interface		0.0.0.0/0.0.0.0			
port6	Physical Interface		0.0.0.0/0.0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0.0			
port9	Physical Interface		0.0.0.0/0.0.0.0			
SD-WAN	SD-WAN Interface	WAN (port2) WAN2 (port3)	0.0.0.0/0.0.0.0			
WAN (port2)	Physical Interface		192.168.1.60/255.255.255.0	PING HTTPS HTTP		

The screenshot shows the FortiView Network Interfaces page with a different configuration for the SD-WAN interface:

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
port10	Physical Interface		0.0.0.0/0.0.0.0			
port5	Physical Interface		0.0.0.0/0.0.0.0			
port6	Physical Interface		0.0.0.0/0.0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0.0			
port9	Physical Interface		0.0.0.0/0.0.0.0			
WAN2 (port3)	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS HTTP		
SD-WAN	SD-WAN Interface	WAN (port2) WAN2 (port4)	0.0.0.0/0.0.0.0			
WAN (port2)	Physical Interface		192.168.1.60/255.255.255.0	PING HTTPS HTTP FMG-Access		
WAN2 (port4)	Physical Interface		192.168.35.1/255.255.255.0			

The screenshot shows the SD-WAN configuration page. The SD-WAN interface is named "SD-WAN" and is currently disabled. The "SD-WAN Interface Members" table is as follows:

Interfaces	Gateway	Cost
WAN (port2)	192.168.1.60	.
WAN2 (port4)	192.168.35.1	.

Below the table, there are two pie charts showing SD-WAN Usage:

- Upstream:** port2: 5.7 kbps, port4: 0 kbps (indicated by a red circle).
- Downstream:** port2: 6.8 kbps, port4: 0 kbps (indicated by a red circle).

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_AWS	http://aws.amazon.com/				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
sla1	8.8.8.8	WAN (port2): 1.00% WAN2 (port4):	WAN (port2): 119.48ms WAN2 (port4):	WAN (port2): 28.45ms WAN2 (port4):	5	5

Performance SLA : يتم من خلاله انشاء monitoring profile مثلا SLA1

مثلا سوف أقول للفورتى جيت بأن قوم بعمل ping 8.8.8.8 و ping 8.8.4.4

حيث عبر الخيار Participants تقوم بتحديد من اين سيقوم بعملية ال ping هل من خلال الخط wan1 مثلا او عبر wan2 او عن طريق الاثنين .

مثلا سوف أقوم بعملية ال ping عبر wan1

سوف نقوم بإنشاء SLA كما بالصورة ادناه باسم SLA1

وسيتم الفحص (ping) 8.8.8.8 و 8.8.4.4 عبر الخط wan1

حيث سيتم عملية ارسال الفحص (ping) الى 8.8.8.8 و 8.8.4.4 كل 500 ملي ثانية - أي كل نصف ثانية قم بعمل ارسال echo request -

أساسيات فورتى جيت

١ - حيث سيتم عملية ارسال الفحص (ping) الى 8.8.8.8 و 8.8.4.4 كل 500 ملي ثانية - أي كل نصف ثانية قم بعمل ارسال echo request -

٢ - فلوتم ارسال 5 echo request الى 8.8.4.4 , 8.8.8.8 ولم تستلم أي رد (echo reply)

فأعتبر بأن الخط wan1 في حالة down ففي هذه الحالة فان wan1 لن يدخل في عملية الload balance (SDWAN) مع ملاحظة بأنه سيتم ارسال echo request في هذا الفترة كل 500 ثانية ولن يتوقف عن عملية الارسال بالرغم ان الخط down .

٣- بعد ان اصبح الخط wan1=down فبأي وقت لو حصل echo reply لعدد 5 مرات فاجعل wan1=up

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_AWS	http://aws.amazon.com/				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
sla1	8.8.8.8 8.8.	WAN (port2): 0.00%	WAN (port2): 93.86ms	WAN (port2): 5.11ms	5	5

انشاء monitoring profile للخط wan2 عبر البروفایل sal2

أساسيات فورتني جيت

The screenshot shows the configuration for a new Performance SLA named 'sla2'. The configuration includes the following details:

- Name:** sla2
- Protocol:** Ping
- Server:** 4.4.2.2
- Participants:** WAN2 (port4)
- Enable probe packets:** Checked
- SLA Targets:** Add Target button
- Link Status:**
 - Check interval: 800 ms
 - Failures before inactive: 5
 - Restore link after: 4 check(s)
- Actions when Inactive:** Update static route (checked)

ملاحظة: لا يمكن فحص نفس السيرفر مثلا ان تجعل عليه ال ping لـ sla1 و sla2

على نفس ابي 8.8.8.8 و 8.8.4.4 لذا تم تغييرهم ..

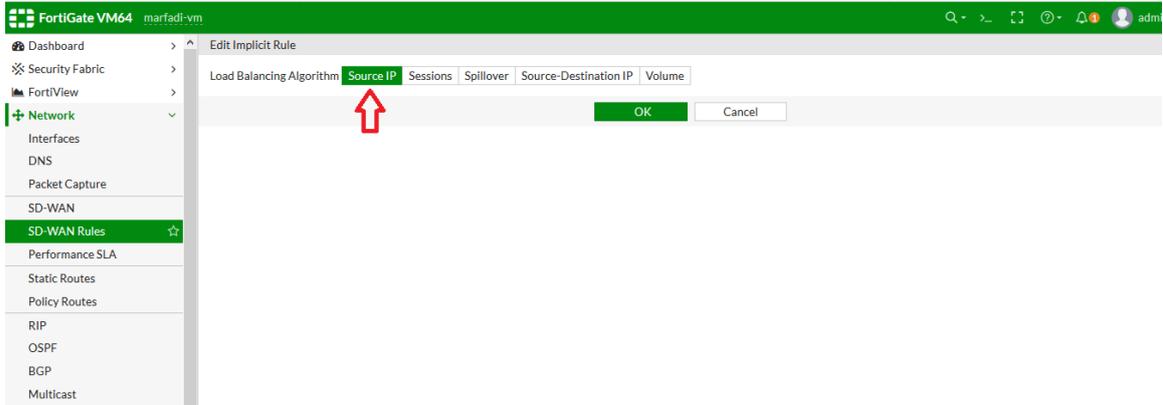
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_AWS	http://aws.amazon.com/				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
sla1	8.8.8.8 8.8.4.4	WAN (port2): 0.00%	WAN (port2): 91.39ms	WAN (port2): 3.67ms	5	5
sla2	4.4.2.2 1.1.1.1	WAN2 (port4):	WAN2 (port4):	WAN2 (port4):	5	4

عملية ال sd-wan سيتم تطبيقها عبر SD-Wan rules بحيث لو تركتها بشكل افتراضي كما بالصورة ادناه

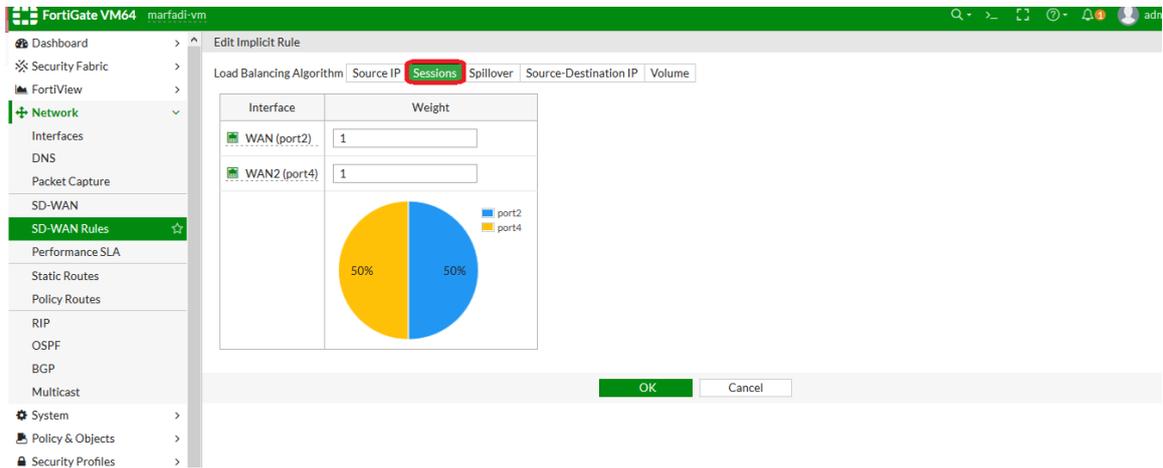
The screenshot shows the configuration for an SD-WAN rule named 'sd-wan'. The rule is currently inactive (greyed out). The configuration includes the following details:

- Name:** sd-wan
- Source:** all
- Destination:** all
- Criteria:** Source IP
- Members:** any

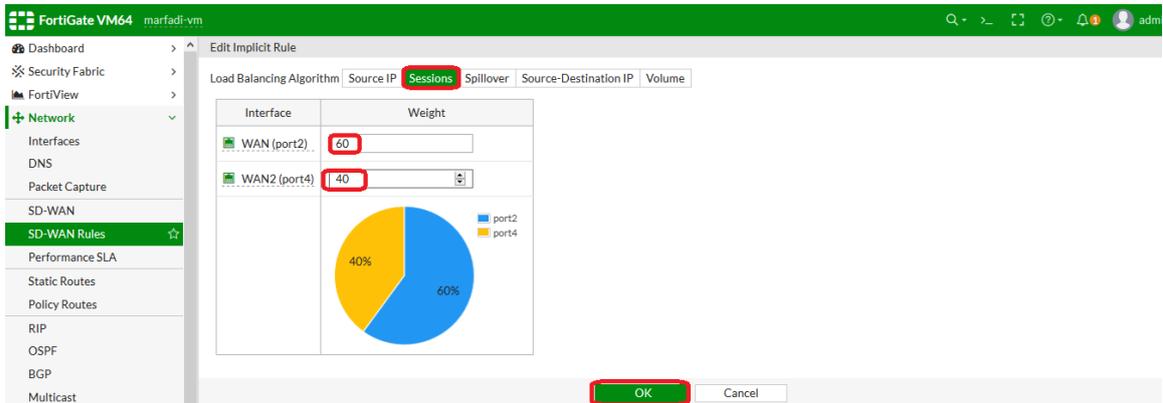
أي انني لم أقوم بإنشاء Rule فأن الرول الافتراضية هي حيث عند النقر عليها مرتين تظهر لك criteria المطبقة هي Source IP حيث يمكنك تغييرها ..



مثلا يمكنك تغييرها الى Sessions :



حيث يمكنني تغيير النسبة مثلا لـ WAN1 60% و لـ WAN2 40%



مثلا لو كان لدينا 1000 جلسه (Sessions) فأن الفورتى جيت سوف يقوم بتوزيعها بنسبه 60% عبر WAN1 و 40% عبر WAN2 .

اما النوع الاخر المسمى Source-Destination IP :

لوال source ip وال destination ip يكونوا ثابتين على نفس ال interface يتم إخراجة عبر نفس ال interface

اما لوال source رايح على destination مختلف فإنه يتم اخرجة عبر interface اخر

From 192.168.1.20 to 8.8.8.8 >>>WAN1

From 192.168.1.40 to 8.8.8.8 >>>WAN2

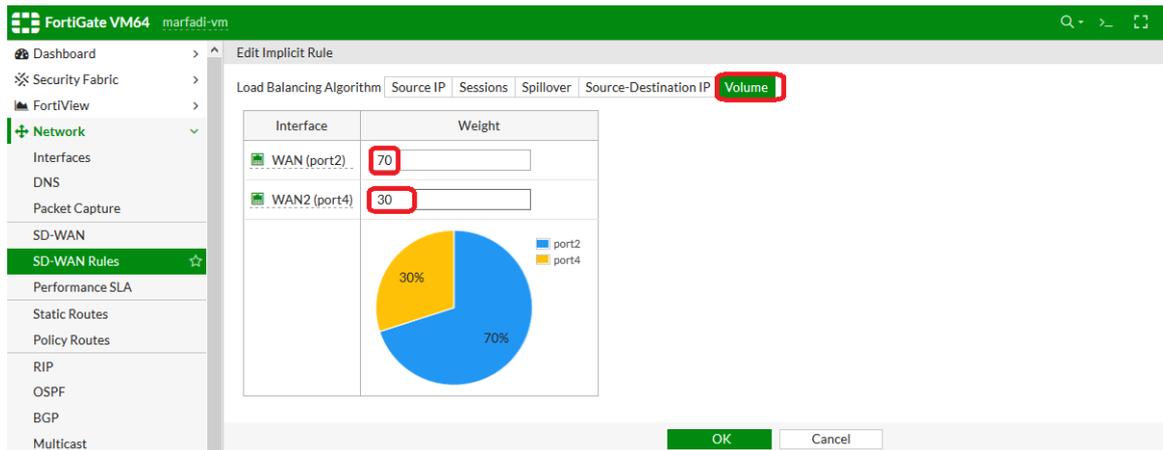
From 192.168.1.50 to 8.8.8.8 >>>WAN1

From 192.168.1.60 to 8.8.8.8 >>>WAN2

وهكذا....

From 192.168.1.20 to 4.2.2.2 >>>WAN2

النوع الثالث : Volume

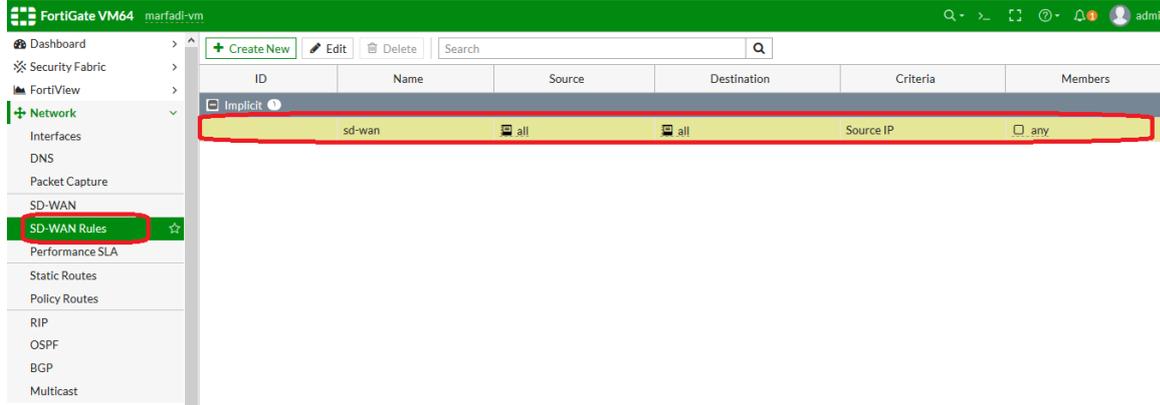


هذا النوع من الخوارزميات تعتمد على كميته ال bytes

فلوا كانت لدينا packets بحجم مثلا 1000 بايت فإن 70% منها سوف تكون عبر WAN1 و 30% البقيه ستكون عبر WAN2

أساسيات فورتني جيت

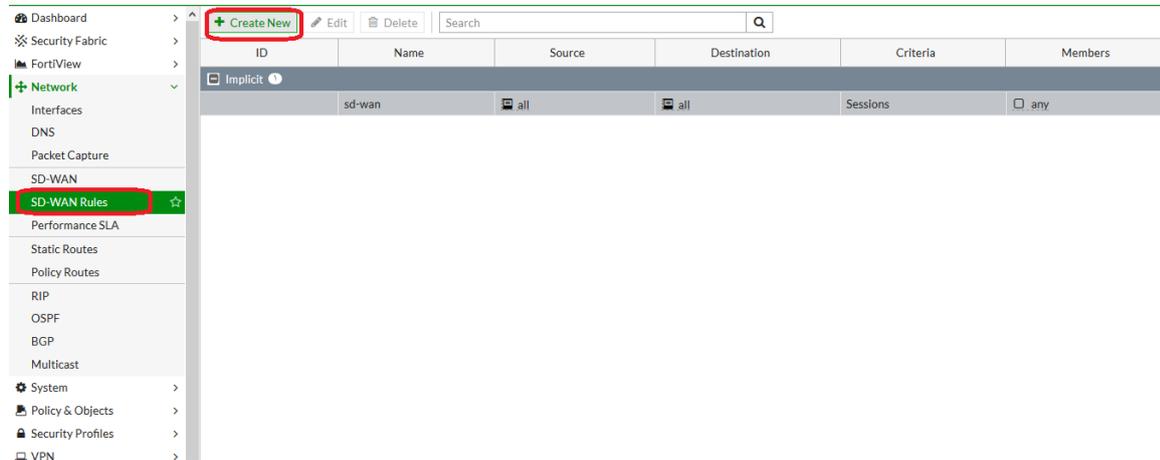
فلو لم نقم بإنشاء أي SD-WAN Rule وتركناها افتراضية فان أي ترافيك سوف يتم تطبيق ال rule الافتراضية كما بالصورة أدناه وسيتم تطبيق الcriteria بحسب ما تم اختياره ..



❖ طريقة انشاء SD-WAN Rule جديده كما بالتالي :

✓ جعل ال ICMP traffic يطلع عبر ال WAN1 :

أي ان أي عمليه ping اريدها تطلع عبر ال wan1 بالتحديد .



أساسيات فورتى جيت

The screenshot shows the configuration for an SD-WAN rule named 'ICMP_TRAFFIC'. The 'Source' section is set to 'all'. The 'Destination' section is also set to 'all'. Under 'Protocol number', 'Specify' is selected and the value '1' is entered, which is highlighted with a red arrow. The 'Outgoing Interfaces' section shows 'Manual' selected as the strategy and 'WAN (port2)' selected as the interface preference. The status is set to 'Enable'.

ملاحظة: ICMP protocol number هو 1 حيث يمكنك البحث في جوجل عن ارقام protocol numbers .

ID	Name	Source	Destination	Criteria	Members
1	ICMP_TRAFFIC	all	all		WAN (port2)
	Implicit	sd-wan	all	Sessions	any

❖ جعل الـ https traffic يطلع عبر الـ wan 2 :

The screenshot shows the configuration for an SD-WAN rule named 'HTTPS_Traffic'. The 'Source' section is set to 'all'. The 'Destination' section is also set to 'all'. Under 'Protocol number', 'TCP' is selected and the value '443' is entered in the 'Port range' field. The 'Outgoing Interfaces' section shows 'Manual' selected as the strategy and 'WAN2 (port4)' selected as the interface preference. The status is set to 'Enable'.

❖ جعل الـ http traffic يطالع عبر الـ wan 1 :

The screenshot shows the configuration for a Priority Rule named "HTTP_Traffic". The configuration is as follows:

- Name:** HTTP_Traffic
- Source:** Source address is set to "all".
- Destination:** Address is set to "all".
- Protocol number:** TCP (selected), with a port range of 80 - 80.
- Outgoing Interfaces:** Strategy is set to "Manual" and Interface preference is set to "WAN (port2)".

The screenshot shows the SD-WAN Rules table in FortiGate. The table has the following columns: ID, Name, Source, Destination, Criteria, and Members. The rules are as follows:

ID	Name	Source	Destination	Criteria	Members
1	ICMP_TRAFFIC	all	all		WAN (port2)
2	HTTPS_Traffic	all	all		WAN2 (port4)
3	HTTP_Traffic	all	all		WAN (port2)
sd-wan	sd-wan	all	all	Sessions	any

❖ إنشاء SLA باسم INTERNET حيث تقوم بفحص الخط الأفضل للخروج منه

The screenshot shows the FortiView Performance SLA configuration page. The left sidebar contains a navigation menu with categories like Security Fabric, FortiView, Network, System, and Monitor. The main configuration area is titled 'INTERNET' and includes the following fields:

- Name: INTERNET
- Protocol: Ping
- Server: 8.8.8.8
- Participants: WAN (port2), WAN2 (port4)
- Enable probe packets:
- SLA Targets: Target 1 with Latency threshold (5 ms), Jitter threshold (5 ms), and Packet Loss threshold (0 %).
- Link Status: Check interval (500 ms), Failures before inactive (5), Restore link after (5 check(s)).
- Actions when Inactive: Update static route (enabled).

تمت عملية إنشاء SLA كما بالصورة ادناه حيث يتم عمل check على جوجل 8.8.8.8 ويطلع من اقل خط منهم ...

حيث سيتم تنفيذ sla على الخطين wan1, wan2 عن طريق البينج على جوجل وبيتم تحديد احسن خط على حسب الأرقام الموجودة

ال latency: يحسب التأخير في الخطين wan1, wan2 والتأخير الأقل سيتم اختياره على انه افضل خط .

حيث ال latency هي الوقت الذي يقطعه الباكيت (ping) من المصدر الى الهدف (8.8.8.8) .

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=88ms TTL=117
Reply from 8.8.8.8: bytes=32 time=89ms TTL=117
```

أي 88 نفسها ..

jitters : يحسب الفرق في الوقت بين الباكت الأول والثاني والاقبل فارق بيتم اختياره كأفضل خط .

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=88ms TTL=117
Reply from 8.8.8.8: bytes=32 time=89ms TTL=117
```

Jitters=89-88=1

packet loss: هذا يقصد به الفقد في البيانات حيث ممكن يكون احدي الخطوط يفقد بيانات اثناء الارسال والاستقبال وهذه مهمه في استخدام التلفونات والمكالمات حيث يسبب تقطع في الصوت حيث الخط الذي فيه فقط في البيانات لن يقوم sd-wan باختياره وسيختار الخط الاخر.

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
Default_AWS	http://aws.amazon.com/				5	10
Default_FortiGuard	http://fortiguard.com/				5	10
Default_Gmail	gmail.com				5	10
Default_Google Search	http://www.google.com/				5	10
Default_Office_365	http://www.office.com/				5	10
INTERNET	8.8.8.8	WAN (port2): 0.00% WAN2 (port4): 0	WAN (port2): 115.50ms WAN2 (port4): 0	WAN (port2): 44.20ms WAN2 (port4): 0	5	5
sla2	4.4.2.2 1.1.1.1	WAN2 (port4): 0	WAN2 (port4): 0	WAN2 (port4): 0	5	4

الآن سنقوم بعمل Rule لتحديد ال interface الأفضل للخروج منه بحسب

SLA=INTERNET التي قمنا بإنشائها سابقا

أساسيات فورتى جيت

Priority Rule

Name: Voice_Traffic

Source

Source address: all

User group: +

Destination

Address: all

Protocol number: TCP UDP ANY Specify 0

Internet Service: +

Application: +

Outgoing Interfaces

Strategy: Manual Best Quality Lowest Cost (SLA) Maximize Bandwidth (SLA)

Interface preference: WAN (port2) WAN2 (port4)

Measured SLA: INTERNET

Quality criteria: Latency

Status: Enable Disable

ID	Name	Source	Destination	Criteria	Members
1	ICMP_Traffic	all	all		WAN (port2)
2	HTTPS_Traffic	all	all		WAN2 (port4)
3	HTTP_Traffic	all	all		WAN (port2)
1	Voice_Traffic	all	all	Latency	WAN (port2) WAN2 (port4)
Implicit					
	sd-wan	all	all	Sessions	any

❖ طريقة اظهار ميزه جديده مثلا تريد اظهار الخاصية (features)

Multiple interface policies والتي تتيح لك تحديد اكثر من incoming interface او outgoing interface عند عمل policy وذلك بالخطوات التالية :

System > features visibility > Multiple interface policies :enable .

أساسيات فورتى جيت

The screenshot shows the FortiGate configuration interface. On the left, the 'System' menu is highlighted with a red box. Below it, 'Feature Visibility' is also highlighted with a red box. In the main configuration area, the 'Multiple Interface Policies' option is checked and highlighted with a red box. At the bottom, the 'Apply' button is highlighted with a red box.

نلاحظ عند تفعيل الخاصية أعلاه باننا قادرين على اختيار أكثر من كرت عند انشاء الرول بعكس لو كانت الخاصية غير مفعلة فأننا نستطيع فقط أضافه (اختيار) كرت واحد فقط كما بالصورة ادناه ..

The screenshot shows the 'New Policy' configuration screen in FortiGate. The 'Incoming Interface' field is set to 'port1' and 'port4', both highlighted with red boxes. The 'Outgoing Interface' field is set to 'WAN (port2)' and 'WAN2 (port3)', both highlighted with red boxes. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Flow-based'. The 'Firewall / Network Options' section is visible at the bottom.

❖ طريقة انشاء Rule policy جديد :

Policy & object > ipv4 policy > Create New > Name: اسم الرول

Incoming interface: port1, outgoing interface: wan1,

Source: يوزر او عنوان كمبيوتر او جروب معين في الدومين

،subnet،ip : Address

User : ممكن يكون يوزر عادي على الفورتني جيت او يوزر على الدومين (AD)

Device: ربط جهاز بواسطة الماك ادرس

Destination :all الى أي مكان

اسم الرول (البوليسي)
البورت الدخل
البورت الخرج
المصدر: مثلا جهاز معين او يوزر معين
او جروب او مجموعه ضمن الAD
الهدف: الى اي مكان

كما بالصورة أعلاه سيتم تطبيق رول (سياسه) اسمها full_access وطبق على منفذ الدخل

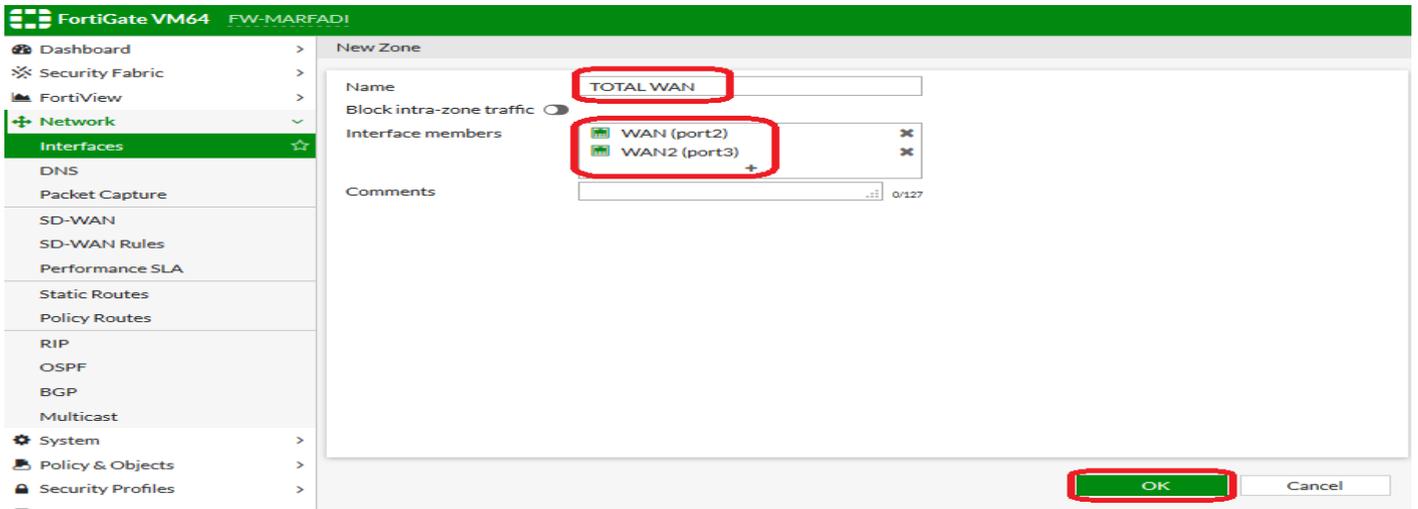
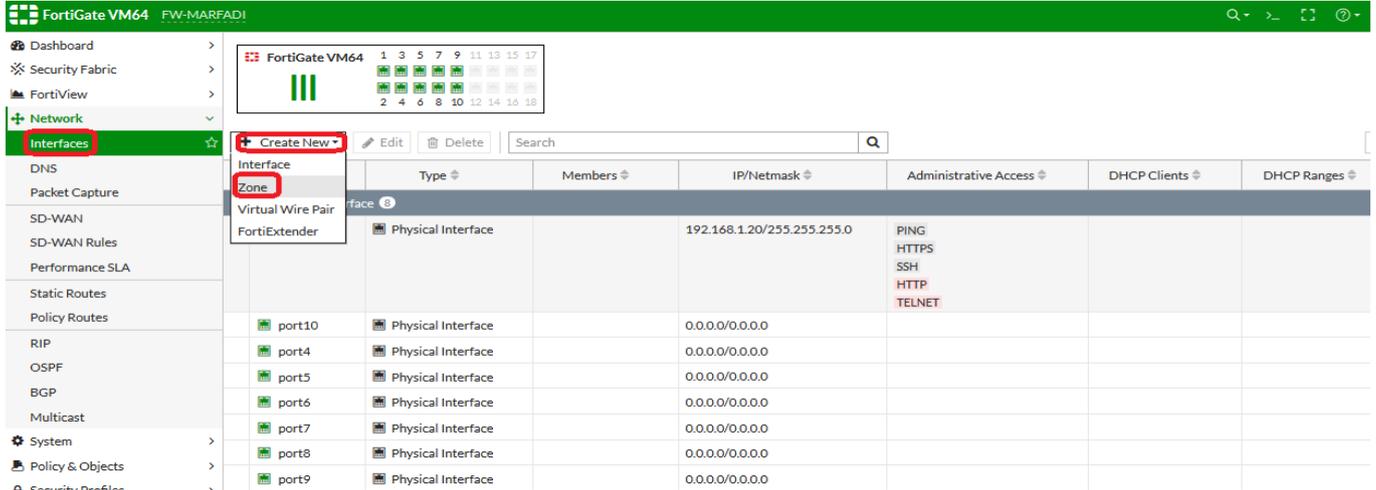
Port1 والخارج عبر wan(port2) ويطبق فقط على جهاز الكمبيوتر المسمى pc1 وهذا تم انشاءه مسبقا

،والى أي مكان (all) ..

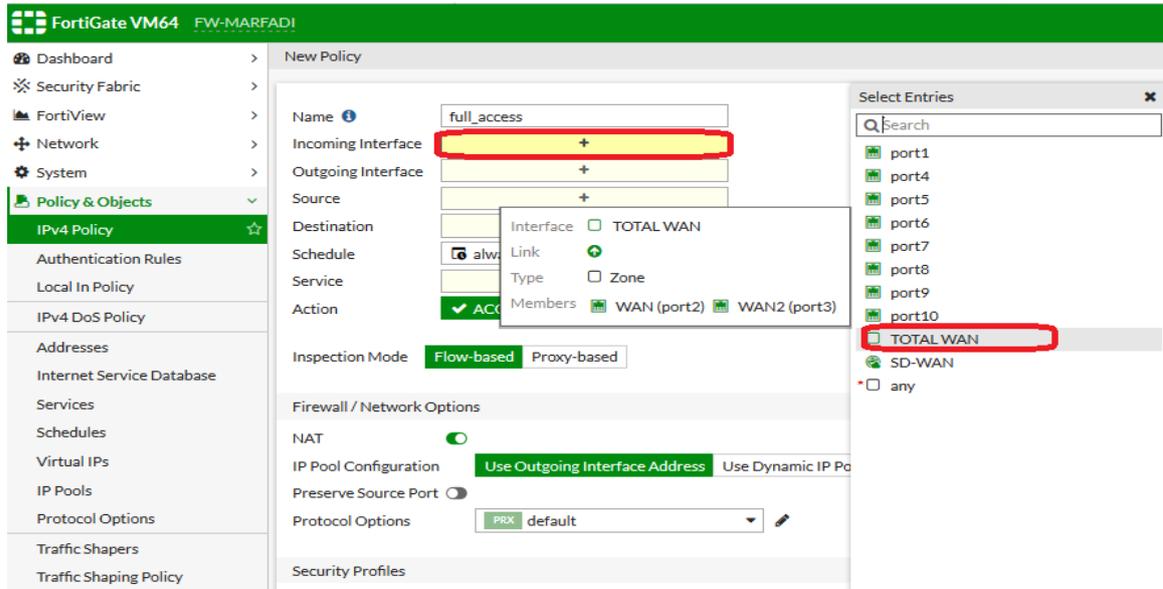
طريقة جمع (دمج) اكثر من منفذ (interface) لكي يصبحوا logical interface واحد وذلك بواسطة ال zone :

Network>interface>Create New>Zone>Name: أي اسم تريد:

>Interface member : نختار المنافذ المراد دمجها :>OK



حيث سوف يصبح لدينا كرت وهي باسم TOTAL WAN كما بالصورة ادناه



ملاحظة: لا يمكن حذف ال zone اذا كانت مستخدمه في أي رول ،لذا لو تريد حذف ال zone المسماة TOTAL WAN يجب أولا حذفه من البوليسي أعلاه...

شرح Schedule:

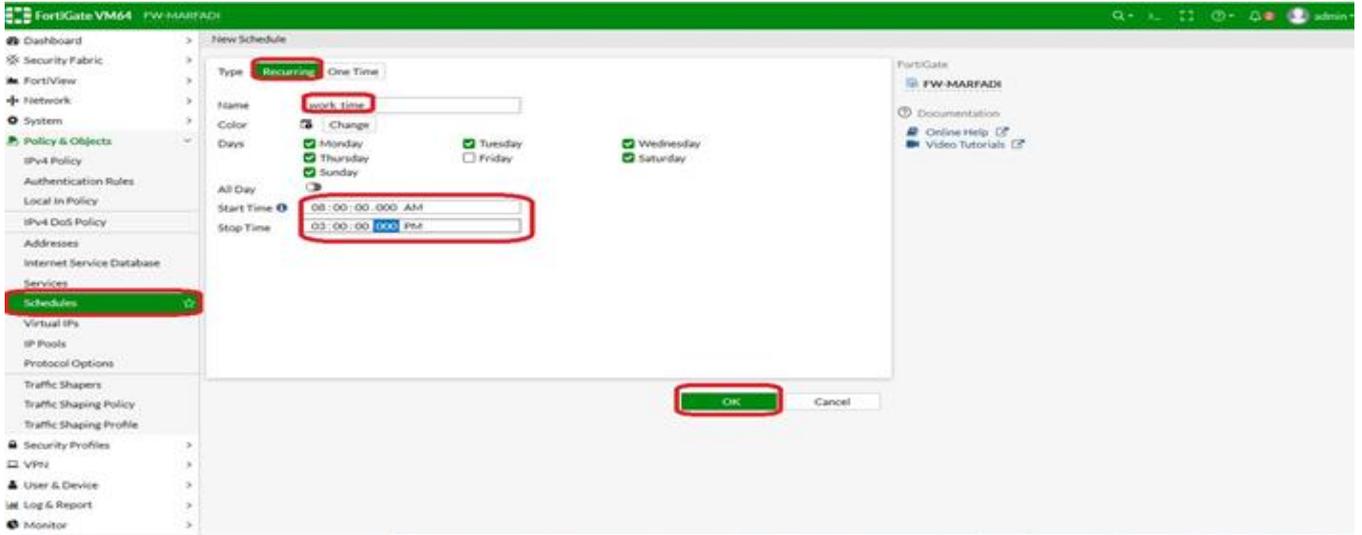
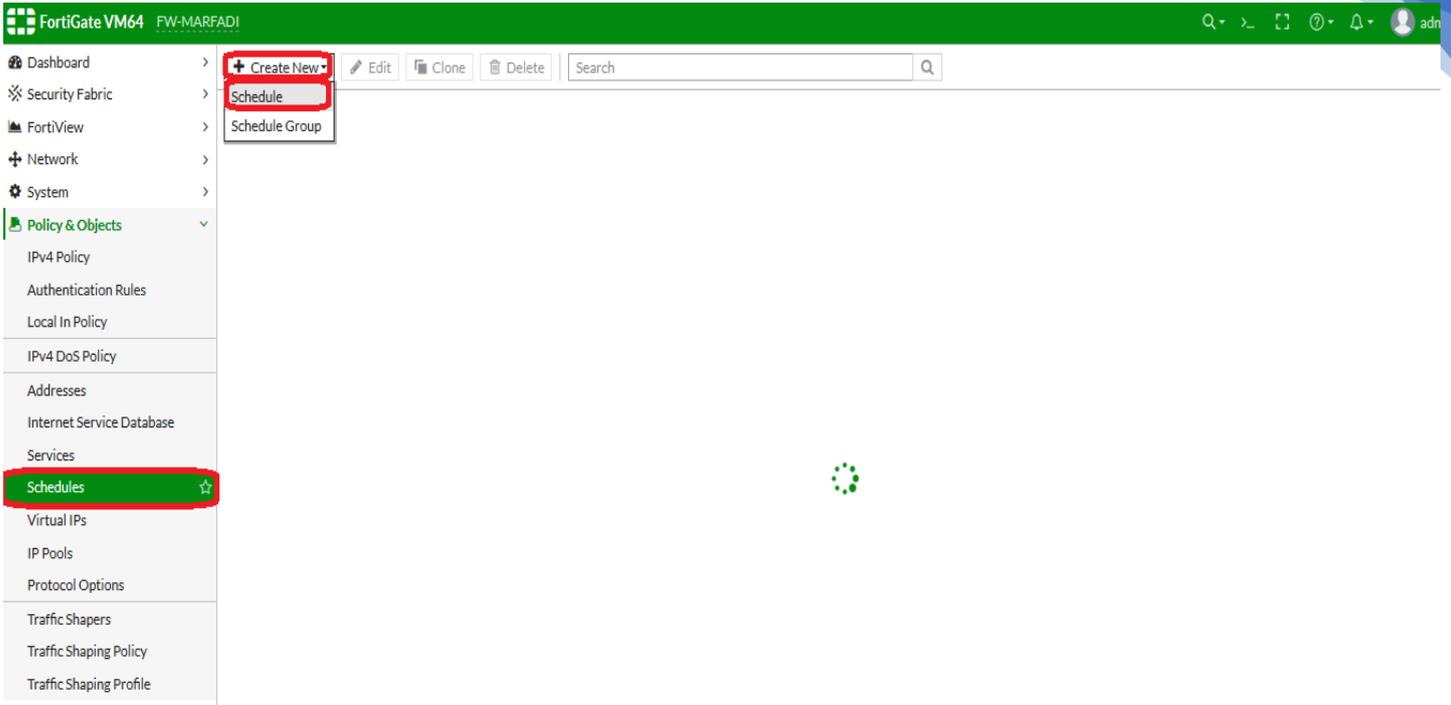
أنواع ال schedule:

- ١- Onetime schedule : يتم تنفيذها مره واحده فقط ثم تلتغي .
- ٢- Recurring schedule : يتم تنفيذها بشكل مستمر

❖ طريقة انشاء schedule :

Policy&objects>schedules>Create New>schedule >type: Recurring

>Name: اسم تريده >Days: المطلوبه



نحدد START TIME و Stop Time ...

تم تحديد اسم لـ schedule باسم Work_time وتم تحديد أيام العمل والوقت .

- عملية تكرار schedule معين :

أساسيات فورتى جيت

Name	Days/Members	Start	End	Ref.
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	4
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0
work_time	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	2

مثلا اريد انسخ نفس الاعدادات والاقوات لـ work_time وانشائها في schedule جديده مثلا باسم time2

حيث الخيار Clone يقوم بنسخ كل العنصر وبكل مواصفاته ...

Please enter the desired name for the clone:

Name:

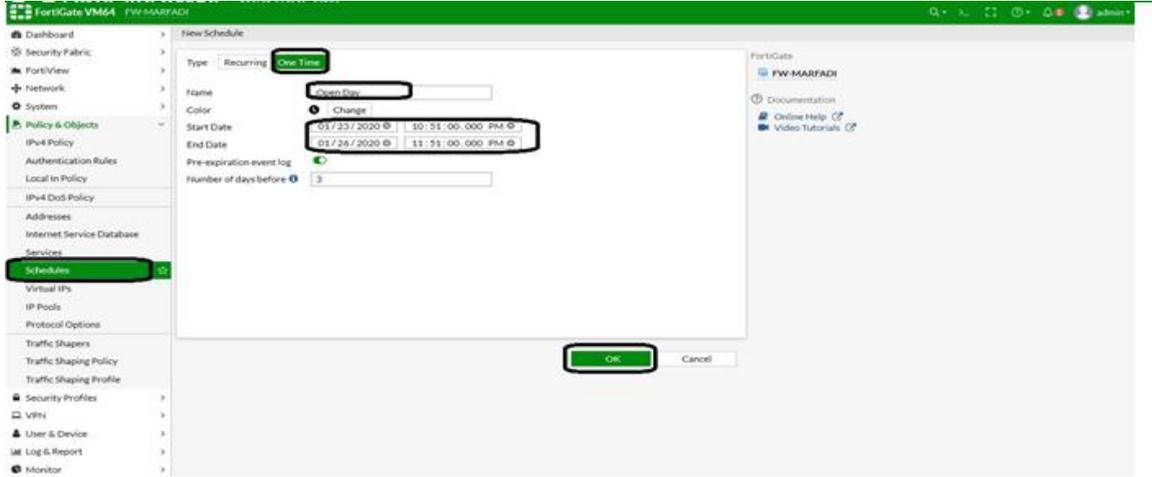
فقط قمنا بكتابه اسم الـ schedule الجديد باسم time2 ونلاحظ بان الأوقات والأيام كما في الـ work_time كما بالصورة ادناه

Name	Days/Members	Start	End	Ref.
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	4
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0
time2	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	0
work_time	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	2

*** **

❖ تحديد أيام محددة وقت محدد مرة واحدة فقط وينتهي ...

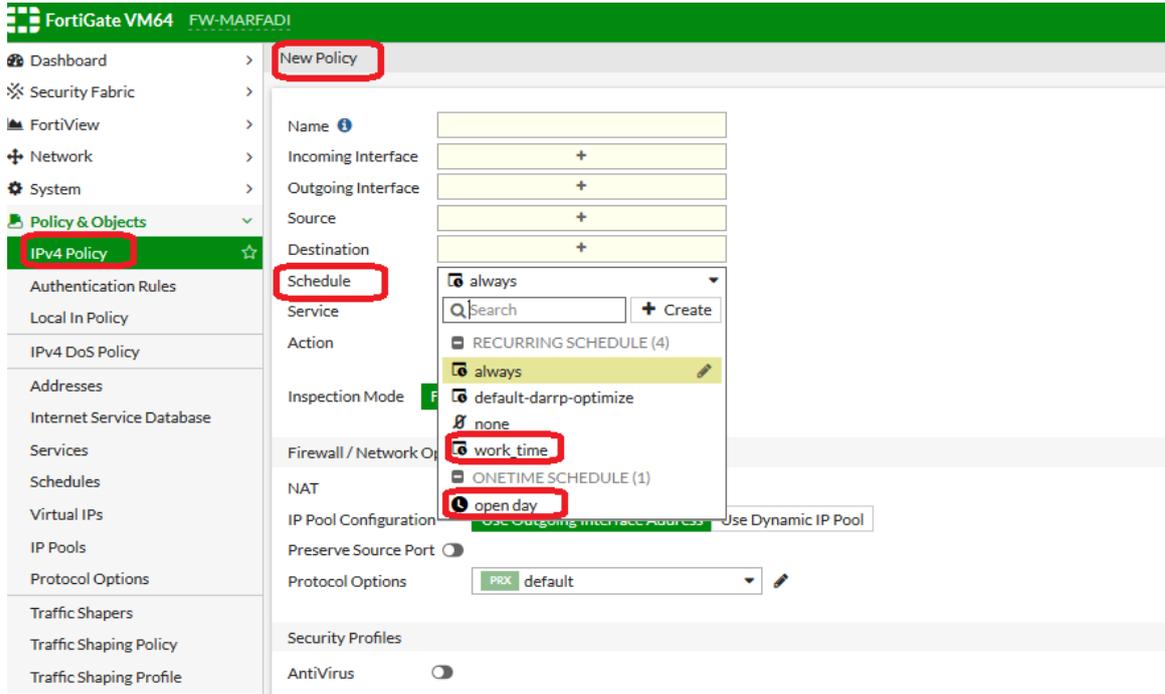
- ❖ Policy&objects>schedules>Create New>schedule >type: Onetime>
- ❖ >Name: اسم تريده>start time: بداية الوقت: بداية التاريخ : start date > أي اسم تريده>
- ❖ >stop time: نهاية الوقت: >stop date > نهاية التاريخ



Name	Days/Members	Start	End	Ref.
Recurring				
always	Sunday Monday Tuesday Wednesday +3	13:00:00	13:00:00	0
default-darrrp-optimize	Sunday Monday Tuesday Wednesday +3	14:00:00	14:30:00	1
none	None	13:00:00	13:00:00	0
work_time	Sunday Monday Tuesday Wednesday +3	21:00:00	04:00:00	0
One Time				
open day		2020/01/23 11:59:00	2020/01/26 12:59:00	0

كما تلاحظ بالصورة أعلاه يبين بأنه تم انشاء schedule عدد 2 باسم

Work_time و Open day ويمكن استخدامهم اثناء انشاء الرول (البولييسي) كما بالصورة ادناه ..



❖ أنواع الـ actions في الـ policy :

- ١- Accept : الموافقة وتمرير الباكث (الترافيك)
- ٢- Deny : منع مرور الباكث

حيث في الإصدارات القديمة يوجد نوع ثالث وهو learn

- ٣- Learn : يستخدم لمعرفة حركة الترافيك (الباكث) في الشبكة ، حيث بعد ما أقوم بتطبيق البوليسي المناسبة ، ممكن ان تقوم بمراقبه ماذا يفعل الموظفون بالشركة حيث

Learn=accept بالإضافة الى تسجيل كل ال logs على شكل تقارير ويتم معرفة ال logs عن طريق التالي :

Log&reports>learning report>

The screenshot shows the FortiGate VM64 FW-MARFADI interface. The left sidebar contains a navigation menu with 'Policy & Objects' expanded and 'IPv4 Policy' selected. The main area displays the 'New Policy' configuration page. The 'Action' field is set to 'ACCEPT' and 'DENY' is disabled. The 'Inspection Mode' is set to 'Flow-based'. The 'Firewall / Network Options' section shows 'NAT' is enabled, 'IP Pool Configuration' is set to 'Use Outgoing Interface Address', and 'Protocol Options' is set to 'PRX default'.

: Traffic shapers ❖

هو عبارة عن عملية تحديد الـ Bandwidth .

أنواع الـ traffic shapers :

١- Per-ip traffic shaper

تحديد مثلا 5 ميغا لكل جهاز او ايتي حيث يكون سرعه هذا الجهاز هو 5 ميغا .

٢- Shared traffic shaper

تحديد مثلا 5 ميغا للأجهزة كاملا يتم تقاسمها جميعا أي ان سرعتهم جميعا هي 5 ميغا .

نحدد النوع المناسب : type > Create New > traffic shapers > Policy & object

>

أساسيات فورتني جيت

Dashboard >
Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
IPv4 Policy
Authentication Rules
Local In Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers *
Traffic Shaping Policy
Traffic Shaping Profile

New Traffic Shaper

Type: Shared Per IP Shaper
Name:

Quality of Service

Traffic priority: High
Bandwidth unit: Mbps
Maximum bandwidth: 1 Mbps
Guaranteed bandwidth:
DSCP:

OK Cancel

FortiGate VM64 FW-MARFADI

Dashboard >
Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
IPv4 Policy
Authentication Rules
Local In Policy
IPv4 DoS Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers *
Traffic Shaping Policy
Traffic Shaping Profile

New Traffic Shaper

Type: Shared Per IP Shaper
Name: 300 KB

Quality of Service

Bandwidth unit: kbps
Maximum bandwidth: 300 kbps
Max concurrent connections:
Forward DSCP:
Reverse DSCP:

OK Cancel

تم تحديد 300 كيلو لكل ابي (جهاز) كما بالصورة اعلاه....

APPLICATION CONTROL ❖

هو عبارة عن عملية تحكم ومراقبه لكل التطبيقات التي سيتم تشغيلها على الشق ابيكه
مثلا (فيسوك، يوتيوب، جوجل...) حيث عن طريق APP CONTROL ممكن اقلل من استهلاك الانترنت او
من الثغرات المتواجدة في تلك التطبيقات .

1- Categories: تحتوي على قوائم (تصنيفات) مقسمة بحسب النوع ..

حيث كمجموعة برامج (تطبيقات) يتم وضعها في التصنيف الخاص به مثلا تطبيقات الألعاب تكون مصنفة تحت games category ، وتطبيقات البروكسي والvpn تحت التصنيف proxy category حيث ممكن ان تقوم لهذا التصنيف ال action المناسب اما allow او Monitor او Block او quarantine و View signature ...

The screenshot shows the 'New Application Sensor' configuration page in FortiGate. The left sidebar contains navigation options: Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles (highlighted), AntiVirus, Web Filter, DNS Filter, Application Control (highlighted), Intrusion Prevention, SSL/SSH Inspection, Web Rating Overrides, Web Profile Overrides, Custom Signatures, VPN, User & Device, Log & Report, and Monitor. The main content area is titled 'New Application Sensor' and includes fields for Name, Comments, and a Categories dropdown menu. The Categories dropdown is expanded, showing a list of application categories with their respective counts and icons. The categories are: Business (179, 6), Collaboration (293, 6), Game (124), Mobile (3), P2P (85), Remote.Access (91), Storage.Backup (296, 16), Video/Audio (206, 13), Web.Client (18), Cloud.IT (31), Email (87, 12), General.Interest (241, 9), Network.Service (332), Proxy (106), Social.Media (150, 31), Update (48), VoIP (31), and Unknown Applications. Below the Categories list, there is a 'Network Protocol Enforcement' section with a toggle switch. At the bottom, there is an 'Application and Filter Overrides' section with a table containing columns for Priority, Details, Type, and Action, and buttons for Create New, Edit, and Delete.

حيث يمكنك اختيار التصنيف المناسب للبروفایل المراد إنشاؤه ...

أساسيات فورتني جيت

كما بالصورة أعلاه يمكنك اختيار action المناسب للتصنيف ... فإذا اردت مثلا معرفة على ماذا يحتوي هذا التصنيف فتقوم باختيار الخيار View Signatures وسوف تظهر لك البرامج التي تنتهي لهذا التصنيف ..

Name	Category	Technology	Popularity	Risk
Access.Remote.PC	Remote.Access	Client-Server	☆☆☆☆	██████
Airdroid	Remote.Access	Client-Server	☆☆☆☆	██████
Alpemix	Remote.Access	Client-Server	☆☆☆☆	██████
Ammyy.Admin	Remote.Access	Client-Server	☆☆☆☆	██████
AnyDesk	Remote.Access	Client-Server	☆☆☆☆	██████
Anyplace.Control	Remote.Access	Client-Server	☆☆☆☆	██████
Apple.Remote.Desktop	Remote.Access	Network-Protocol Client-Server	☆☆☆☆	██████
Back.Orifice	Remote.Access	Client-Server	☆☆☆☆	██████
BeAnywhere.Support.Express	Remote.Access	Client-Server Peer-to-Peer	☆☆☆☆	██████
Bomgar.Jump.Client	Remote.Access	Client-Server	☆☆☆☆	██████
Chrome.Remote.Desktop	Remote.Access	Client-Server	☆☆☆☆	██████
Citrix.ICA.FileTransfer	Remote.Access	Network-Protocol Client-Server	☆☆☆☆	██████
Citrix.ICA.Print	Remote.Access	Network-Protocol Client-Server	☆☆☆☆	██████
Citrix.Receiver	Remote.Access	Client-Server	☆☆☆☆	██████

حيث ممكن البحث عن برنامج معين لتعرف هل ينتهي لهذا التصنيف وذلك عبر كتابه البرنامج في خانه search ثم ال Enter لتظهر النتائج ...

٢- Application overrides : ممكن بواسطته ان اسمح او اسمح لتطبيقات معينه بعكس الخيار

الأول الذي لا يمكنني ان اختار تطبيقات معينه بتصنيف معين ..

حيث تختار Create New ثم application tab ثم تقوم باختيار التطبيق او التطبيقات المطلوبة ثم ننقر على الزر Add selected ...

Name	Category	Technology	Popularity	Risk
1loun	Video/Audio	Client-Server	★★★★★	██████
1und1_Mail	Email	Browser-Based	★★★★★	██████
2Safe	Storage.Backup	Browser-Based	★★★☆☆	██████
2Safe_File.Download	Storage.Backup	Browser-Based	★★★☆☆	██████
2Safe_File.Upload	Storage.Backup	Browser-Based	★★★☆☆	██████
2ch	Social.Media	Browser-Based	★★★★★	██████
2ch_Post	Social.Media	Browser-Based	★★★★★	██████
2shared_File.Download	Storage.Backup	Browser-Based	★★★★★	██████
2shared_File.Upload	Storage.Backup	Browser-Based	★★★★★	██████
3PC	Network.Service	Network-Protocol	★★★★★	██████
4Sync	Storage.Backup	Browser-Based Client-Server	★★★★★	██████
4Sync_File.Upload	Storage.Backup	Browser-Based Client-Server	★★★★★	██████

FortiGate VM64 FW-MARFAD!

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > Application Control

New Application Sensor

- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)
- VoIP (31)
- Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New Edit Delete

Priority	Details	Type	Action
1	... Psiphon3 ... Teamviewer ... Teamviewer_CallReceive ... Teamviewer_CallRequest ... AnyDesk	Application	Block

Options

Block applications detected on non-default ports

Allow and Log DNS Traffic

نلاحظ كما بالصورة أعلاه تم اختيار تطبيقات معينه مثل Psiphon3 و TeamViewer و anydesk والaction هو Block ..

٣- Filter overrides: انشاء تصنيف (category) يكون فيها جميع أنواع التطبيقات التي تكون خطورتها عليه .

ملاحظة :

في حالة قمت بتطبيق (تفعيل) الثلاثة الأنواع أعلاه في بروفایل واحد فإنه يتم أولاً تطبيق حسب الأولوية

١- Application overrides

٢- Filter overrides

٣- Categories

مثال لو قمنا بالسماح لتطبيق ال Anydesk في الخيار Categories

وبنفس البروفایل قمت بمنع التطبيق نفسه في الخيار Application overrides فإنه سوف يتم تطبيق

المنع لهذا التطبيق لأن الأولوية لـ application override عن Categories .

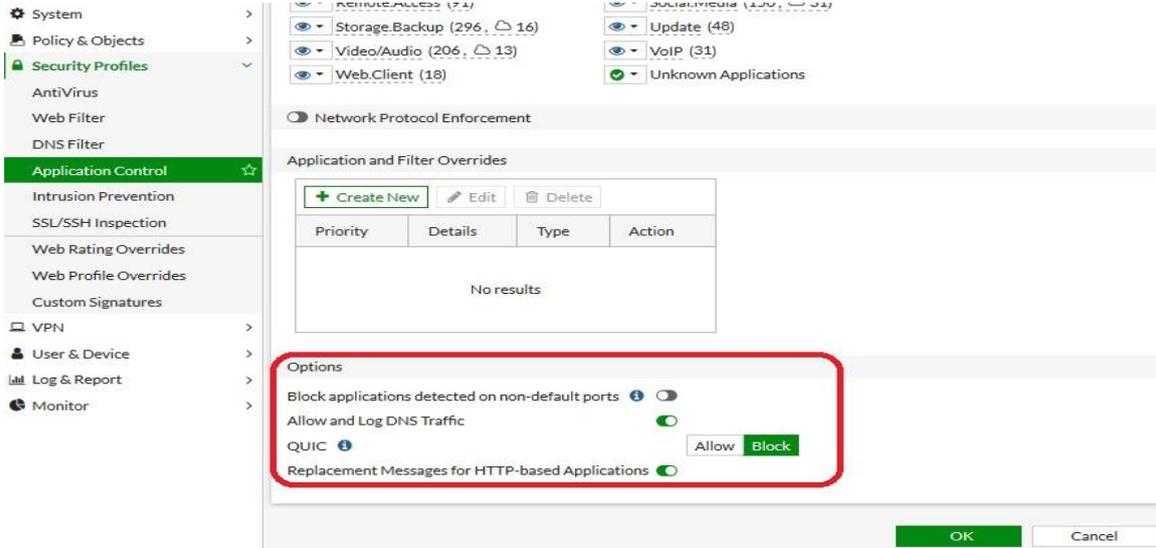
الACTION :

- ١- Allow : السماح لهذا النوع من التطبيقات
- ٢- Monitor : السماح لهذا التطبيق مع توليد logs
- ٣- Block منع التطبيق مع توليد logs
- ٤- Quarantine : منع ولكن مرتبط بزمن محدد ..اي ان اليوزر الذي سيحاول فتح تطبيق معين فأن فورتى جيت سوف يقوم بعمل ban (حظر) لهذا الايبي حيث بعدها لن يستطيع هذا الايبي ان يطلع انترنت لمدة معينه يتم تحديدها مسبقا ..
- ٥- View Signature : معرفة التوقيع لهذا التنصيف

هناك بعض الخيارات :

- ١- Allow and log DNS traffic :
ينصح بتفعيله في بداية مرحلة التعلم (learning) لمعرفة التطبيقات المستخدمة ولكن ينصح بإيقافها بعد ذلك لأنها تعمل على اهدار المعالج .
- ٢- Replacement messages for Http-based application :
عند تفعيلها سيتم اظهار رساله عند اليوزر عندما يحاول فتح تطبيق غير مسموح به بأن التطبيق مغلق (Blocked).

أساسيات فورتى جيت



Web Filter ❖

هي عملية تحكم ومراقبه مواقع الانترنت التي يحاول المستخدم الوصول اليها وحمايه الشبكة المحلية من المواقع الغير موثوقة

❖ ما هو الـ fortiguard :

هي عبارة عن اشتراك يتم ما بين الفورتى جيت و الفورتى جارد تيم من خلاله تم تقسيم URL الى مجموعات ، بحيث تتم عملية التقسيم عندما يقوم صاحب الموقع بإنشاء موقعه فإنه ملزم بأن يقوم بتصنيف الموقع هل سياسي اورياضي او... الخ أيضا توجد خوارزميات في الفورتى جارد تعمل على تصنيف الURL على حسب محتوى الموقع نفسه ...

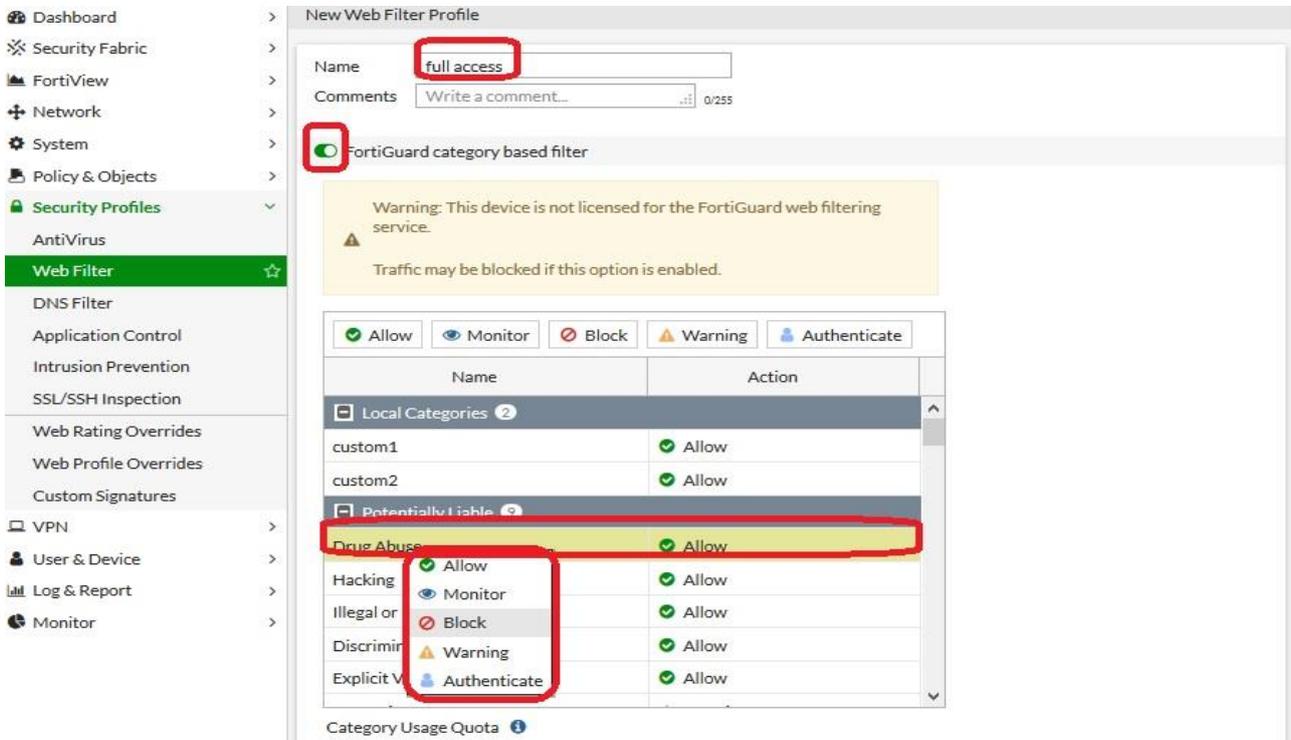
❖ ماهي فكره الـ Fortiguard ؟

عندما اليوزر يطلب موقع مثل www.facebook.com فإن جهاز الفورتى جيت يرسل طلب الى الفورتى جارد لمعرفة تصنيف هذا الموقع وبعد ذلك يتم تخزينه (cache) على جهاز الفورتى جيت .. بحيث لو قام يوزر اخر بطلب نفس الموقع فلا يحتاج الى عمل طلب الى الفورتى جارد .. حيث بعد ما يحصل جهاز الفورتى على تصنيف الموقع فإنه يعمل له action المناسب ...

Security profile>web filter>+>Name:نختار اسم مناسب

>fortiguard category based filter:enabled

حيث نحدد التصنيف (category) ثم بالزر الأيمن عليها ثم نختار ال action المناسب لهذا التصنيف هل block او allow او monitor ..



ملاحظة: في تصنيف اسمه local categories ويوجد بداخله نوعين (تصنيفين) هما Custom 1 و Custom 2 حيث ممكن تخصيص مواقع وأضافته اليها ..

حيث تستطيع أضافه أي مواقع اليها مثلا موقع www.bab.com وذلك بالخطوات التالية

Security profile >web rating overrides >create New>

[URL:www.bab.com](http://www.bab.com)

أساسيات فورتى جيت

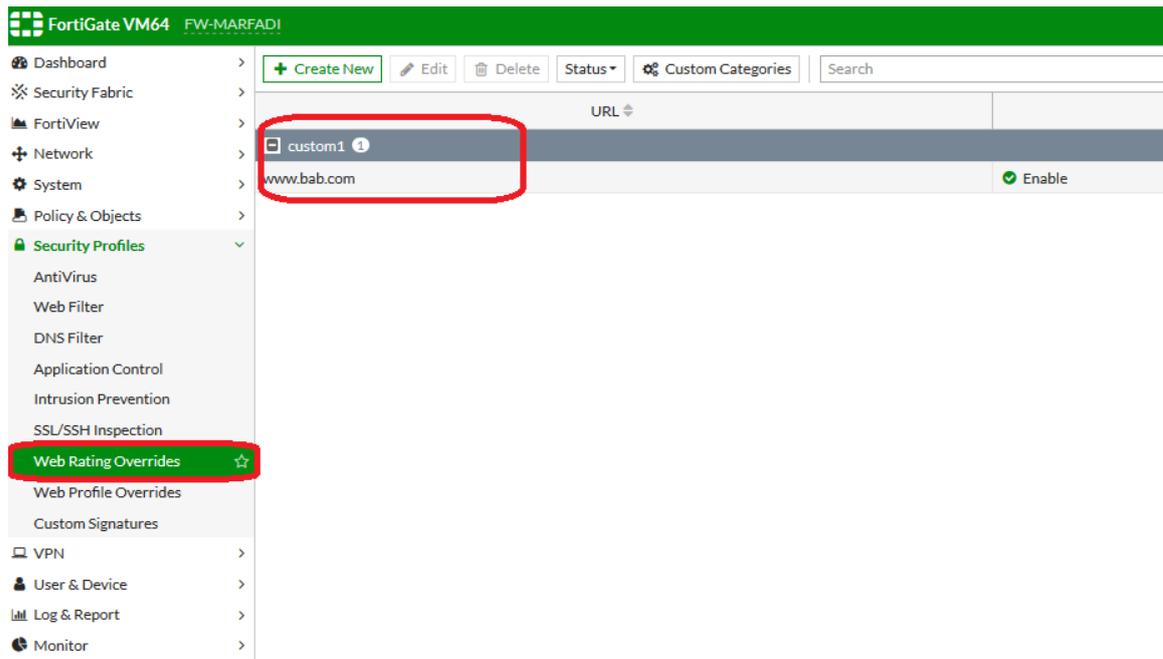
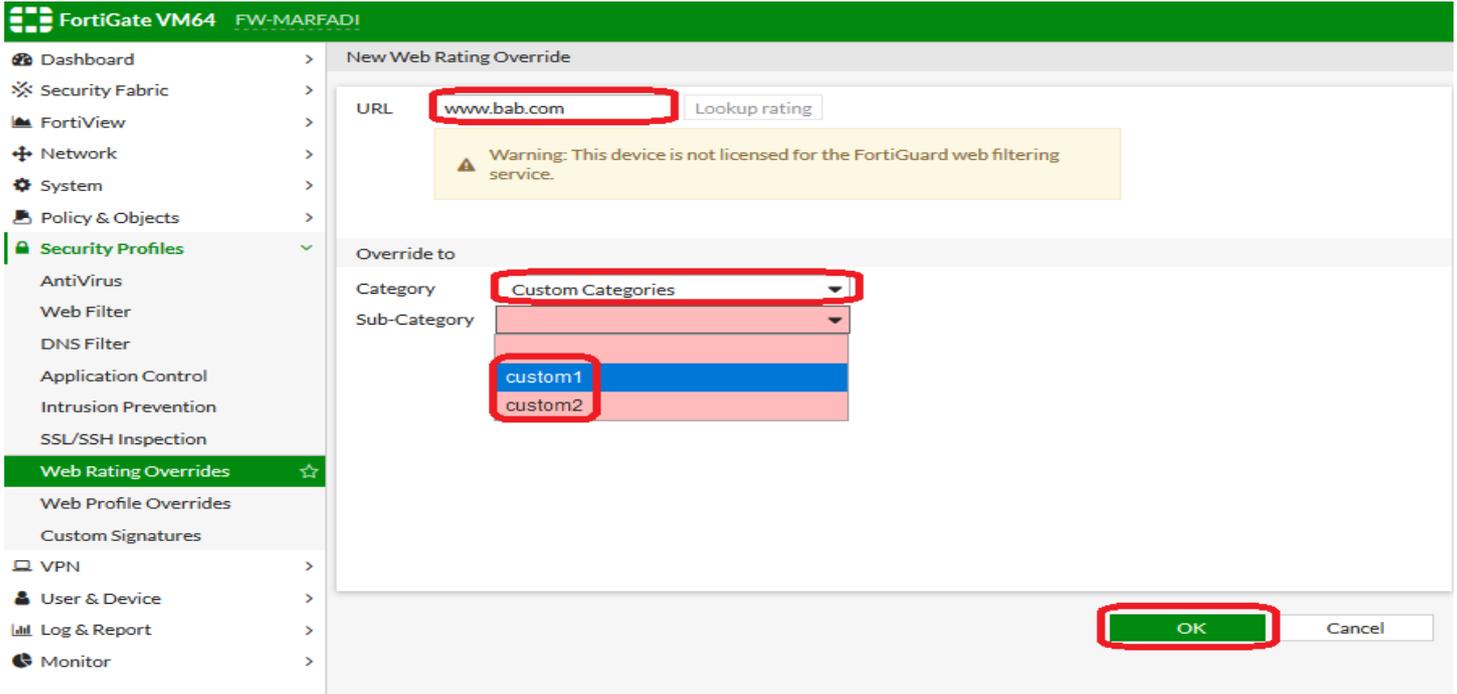
Override to :

Category: custom category

Sub category: custom 1

ok

كما بالصورة ادناه



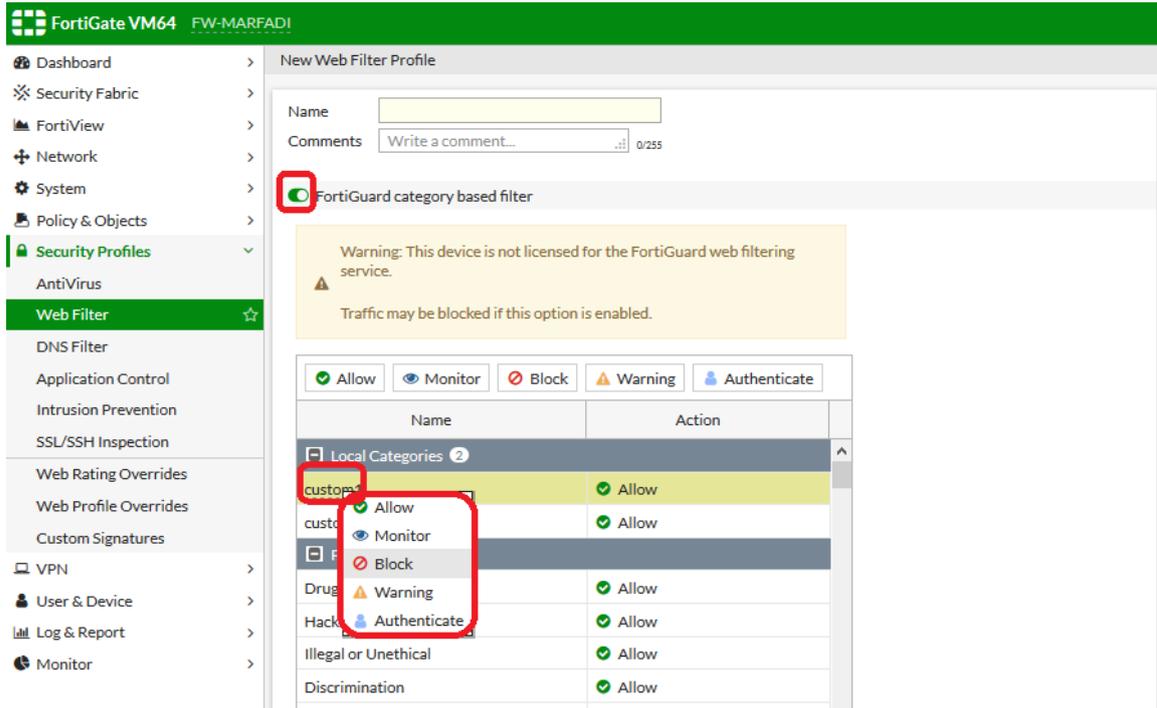
ثم نذهب الى

Web filter>+>fortiguard category based filter =enable>

Local categories>نختار custom 1

حيث ننقر بالزر الأيمن على custom 1 ونختار نوع الـ action المراد تطبيقه على التصنيف custom 1 وبذلك سوف يتم تطبيق الـ action على قائمه الـ URL الموجودة في الـ custom 1..

الفكره: تقوم بتحديد المواقع المراد السماح لها في custom 1
والمواقع المراد منعها في الـ custom 2



Static URL filter

Security profile>web filter>URL filter:enable>Create New>

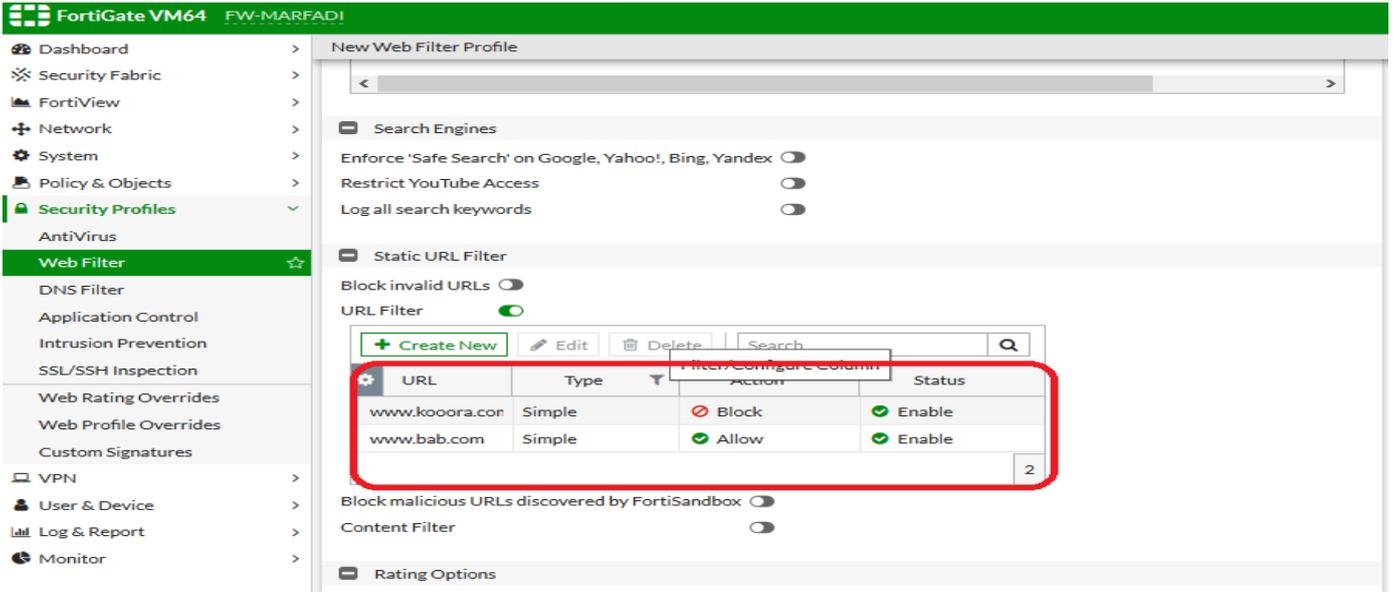
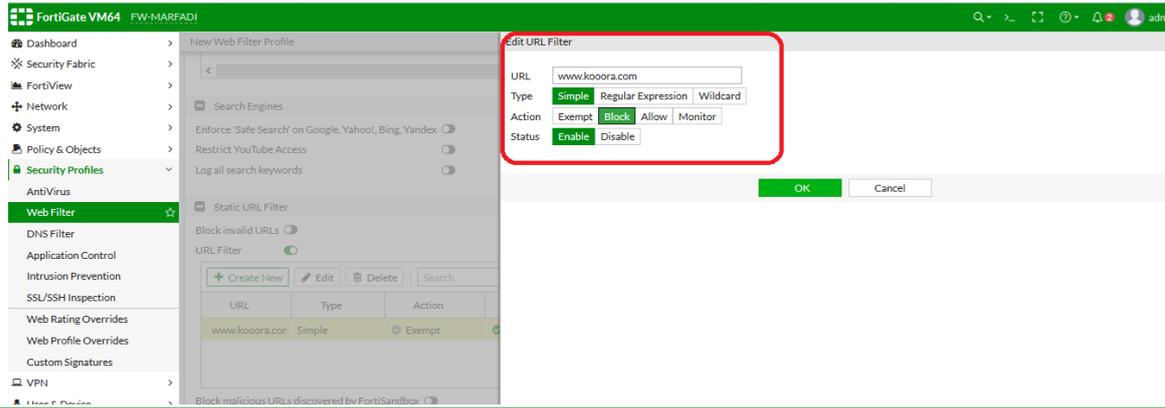
URL: www.kooora.com

Type:simple

Action:block

Status:enable

OK

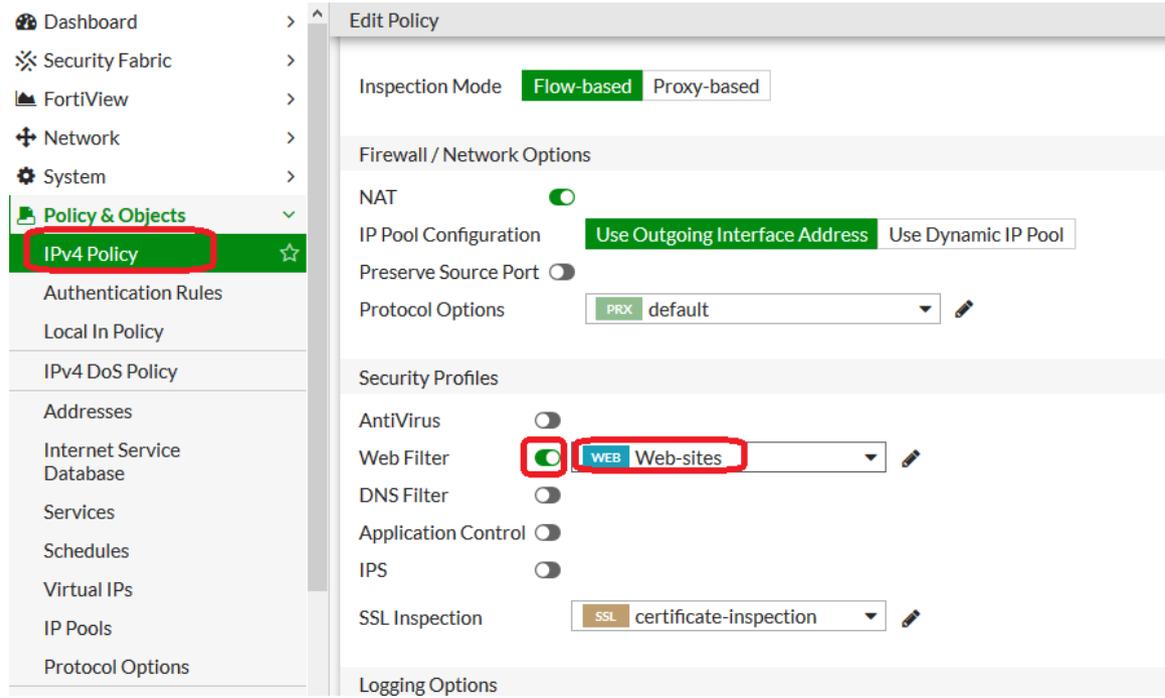


حيث ممكن أضافه اكثر من موقع بنفس القائمة حتى وان كانت بـ action مختلفة ..

وكما بالصورة ادناه في البوليسي (الرول) تم اختيار الـ web filter المسمى Web-sites والتي تم انشاءها

كما بالصورة أعلاه ...

أساسيات فورتني جيت



الآن سوف نجرب نفتح الموقع المسمى www.kooora.com على جهاز الكلاينت والذي تم اغلاقه كما هو موضح بالصورة أعلاه ..

content filter

يتم عمل ال action بحسب المحتوى لهذا الموقع وذلك كالتالي

```
security profiles>web filter>content filter:enable
```

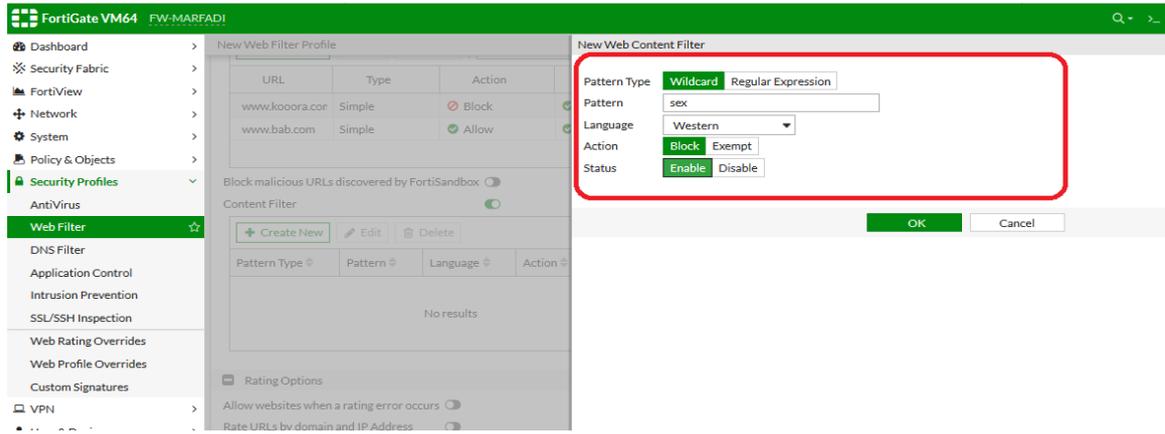
```
>create New>Pattern Type:Wildcard
```

```
>patern :sex
```

```
>action:Block
```

```
Status:enable
```

```
OK
```



ملاحظة هامه :

الأولوية تكون حسب الترتيب التالي :

- 1- Static URI filter
- 2- Fortiguard filter
- 3- Web content filter

يعني في حالة تعارض الثلاث التصنيفات أعلاه فإن الأولوية بحسب الترتيب أعلاه ...

في حالة اردت ان تطبق الى web filter على المواقع https فإنه يجب تفعيل خاصيه ssl-certificate inspection=deep inspection عند انشاء policy .

❖ طريقة اغلاق موقع معين بالإضافة الى sub domain بواسطة ال web filter

Security profiles>web filter>+>static URL filter >url filter >+>create

new>URL:*facebook.com

Action:block

Ok

طهور رساله insecure connection عند فتح موقع https وذلك بسبب الشهادة ولتفادي هذه الرساله
نقوم بالخطوات التالية

Security profiles>ssl/ssh inspection>download certificate>

ثم من المتصفح في اجهزه الكلاينت نقوم باستيراد الشهادة

Option>privact&security>certificate>view certificates?authorities >import>trusted this

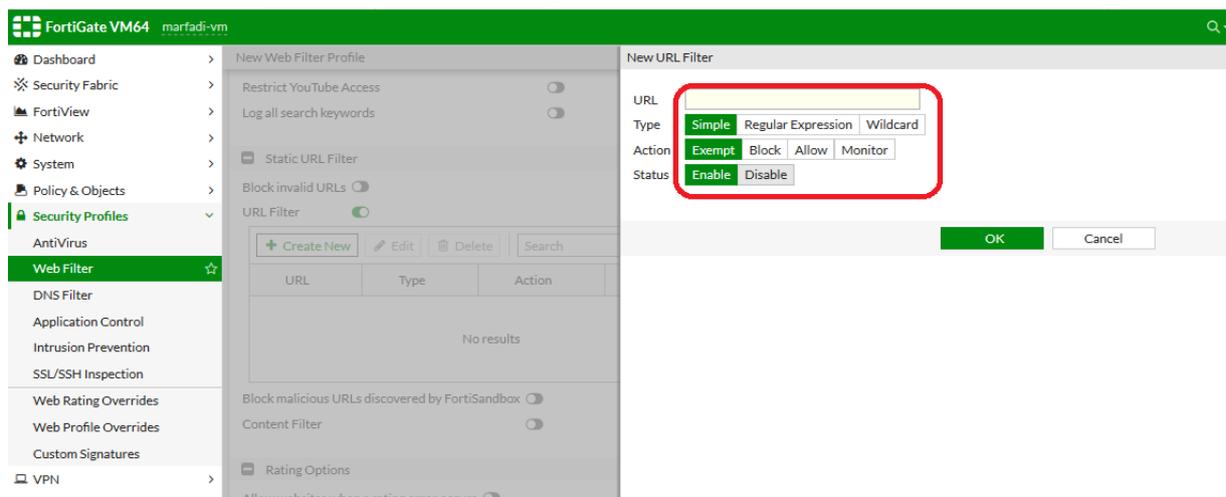
CA to identify websites>ok

حيث بعدها نغلق المتصفح ونفتحه فأذا فتحت موقع https لن تظهر لك مجددا.

اغلق الفيسبوك واليوتيوب عن قسم تقنيه المعلومات والسماح لباقي المواقع بشرط عمل تسجيل لـ logs للمواقع :

The screenshot shows the FortiGate Web Filter configuration interface. The left sidebar has 'Web Filter' selected. The main panel shows the configuration for a filter named 'IT_DEP'. The 'File Filter' section is enabled, and the 'Static URL Filter' section is also enabled, with the 'URL Filter' toggle switch highlighted in red.

The screenshot shows the 'New Web Filter Profile' configuration page. The 'Static URL Filter' section is expanded, and the 'URL Filter' toggle switch is highlighted in red.



كما بالصورة أعلاه فإن URL ممكن كتابتها بأحدى الصيغ التالية :
Simple: سوف يقوم بتنفيذ مثلا `action=block` على الموقع الذي يحتوي على نفس الصيغة بالضبط (حرفيا) مثلا www.facebook.com فلو المستخدم حاول يدخل على الموقع فلو قام اليوزر بالدخول على `login.facebook.com` فان موقع فيسبوك سوف يشتغل معه طبيعي وهذا النوع غير محبيب .

Regular Expression: مثلا لو كان الurl مكتوب `facebook.com` فإن أي رابط يحتوي على `facebook.com` سوف يتم تطبيق `action` عليه فمثلا لو اليوزر كتب `Login.facebook.com` فإنه أيضا سوف ينطبق عليه `action` وهكذا ..

ملاحظة: هذا النوع لا يمكن استخدام الرموز مثلا `*.facebook.com`.

: Wildcard

مثلا لو كتبت في url الموقع `*facebook.com` فإن اليوزر لو حاول يدخل على أي رابط يحتوي على `facebook.com` فإنه سوف يطبق عليه `action` .
 كمان ممكن ان تستخدم الطريقة `*facebook*` فإن أي موقع الرابط له بيحتوي على `facebook` سوف يتم تطبيق `action` عليه ..

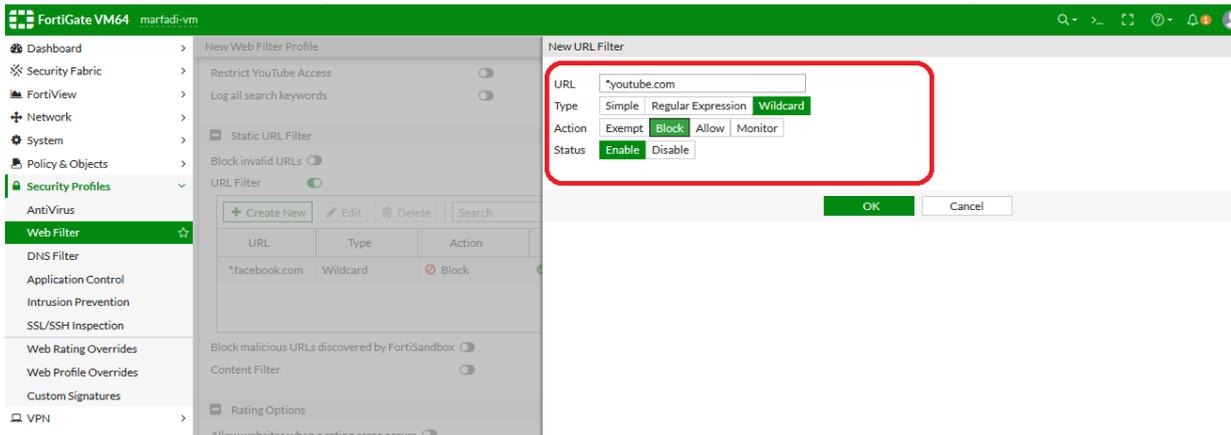
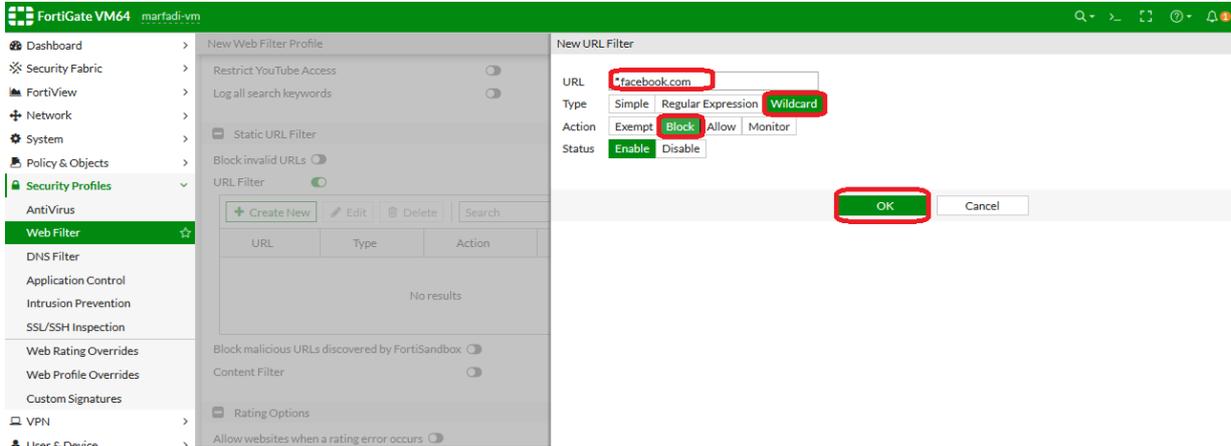
أنواع ال `action` :

Exempt: يعتبر مثل الـ allow أي السماح للترافيك

Allow : السماح للترافيك ولكن يتم تمرير الترافيك الى بروكسي سيرفر اخر...

Monitor : السماح مع عمل log للترافيك .

Block : امنع الترافيك ..



أساسيات فورتني جيت

Dashboard >
Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
Security Profiles >
AntiVirus >
Web Filter >
DNS Filter >
Application Control >
Intrusion Prevention >
SSL/SSH Inspection >
Web Rating Overrides >
Web Profile Overrides >
Custom Signatures >
VPN >
User & Device >
Log & Report >
Monitor >

New Web Filter Profile

Restrict YouTube Access
Log all search keywords

Static URL Filter

Block invalid URLs
URL Filter

URL	Type	Action	Status
*facebook.com	Wildcard	Block	Enable
*youtube.com	Wildcard	Block	Enable

Block malicious URLs discovered by FortiSandbox
Content Filter

Rating Options

Allow websites when a rating error occurs
Rate URLs by domain and IP Address
Rate images by URL

Blocked images will be replaced with blanks

كما بالصورة أعلاه تم انشاء web filter security profile باسم IT_DEP يقوم باغلاق الفيسبوك واليوتيوب ..

Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
Security Profiles >
AntiVirus >
Web Filter >
DNS Filter >
Application Control >
Intrusion Prevention >
SSL/SSH Inspection >
Web Rating Overrides >
Web Profile Overrides >
Custom Signatures >
VPN >
User & Device >
Log & Report >
Monitor >

Search Engines

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex
Restrict YouTube Access
Log all search keywords

Static URL Filter

Block invalid URLs
URL Filter

URL	Type	Action	Status
*facebook.com	Wildcard	Block	Enable
*youtube.com	Wildcard	Block	Enable

Block malicious URLs discovered by FortiSandbox
Content Filter

Rating Options

Allow websites when a rating error occurs

أساسيات فورتني جيت

في الصورة أعلاه في حالة تفعيل الخيار Block invalid URL فان عند فتح أي موقع غير صحيح سوف يعمل له block او أي موقع يعتمد على الشهادة وفيها warning فإنه سيتم عمل لها Block حيث يعتبر هذا الموقع invalid ويقوم بعمل منع للموقع.

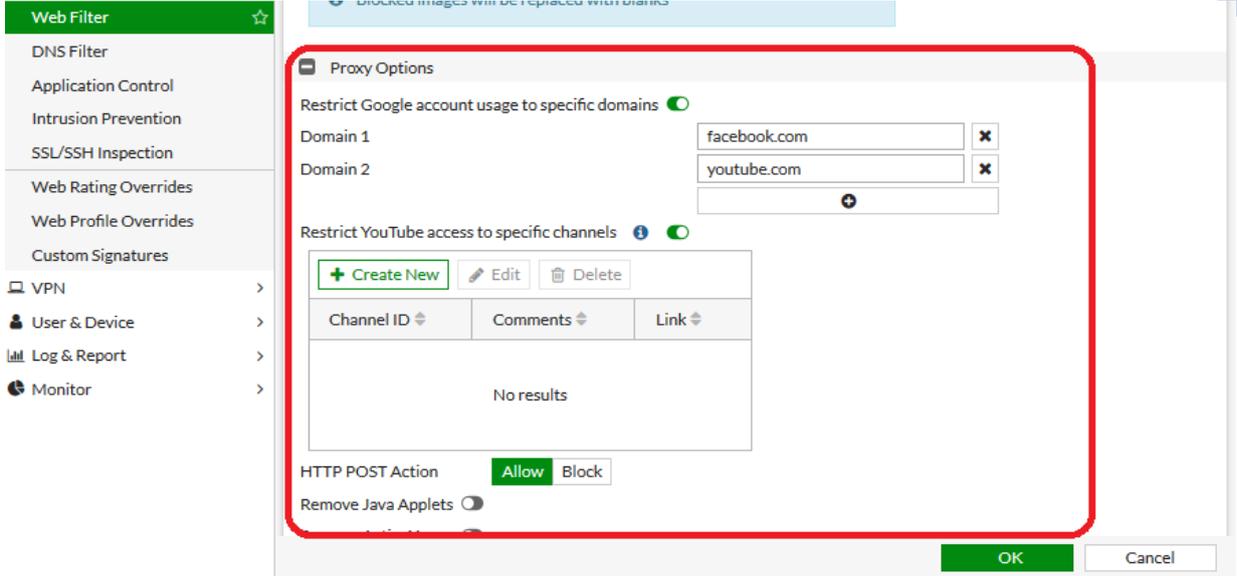
URL	Type	Action	Status
*.facebook.com	Wildcard	Block	Enable
*.youtube.com	Wildcard	Block	Enable

Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex: تجبر بان عمليه البحث الامن في محركات البحث جوجل وياهو وبينج وياندكس ..

Restrict YouTube Access: فلو الخيار كان **Strict** فهذا يعني يتم فقط فتح الفيديوهات التعليميه فقط في اليوتيوب.

moderate: يشغل جميع الفيديوهات ماعدا فيديوهات العري والporn وغيرها .

Log all search keywords: عمل تسجيل للlogs لكلمات البحث على اليوتيوب .



Restrict Google account usage to specific domains: تقيد حسابات جوجل بحيث يمكن

تستخدمها فقط في الشركة في التسجيل بـ فيسبوك ويوتيوب كما بالصورة أعلاه ..

Restrict YouTube access to specific channels: ممكن تحديد قنوات محده على اليوتيوب فقط

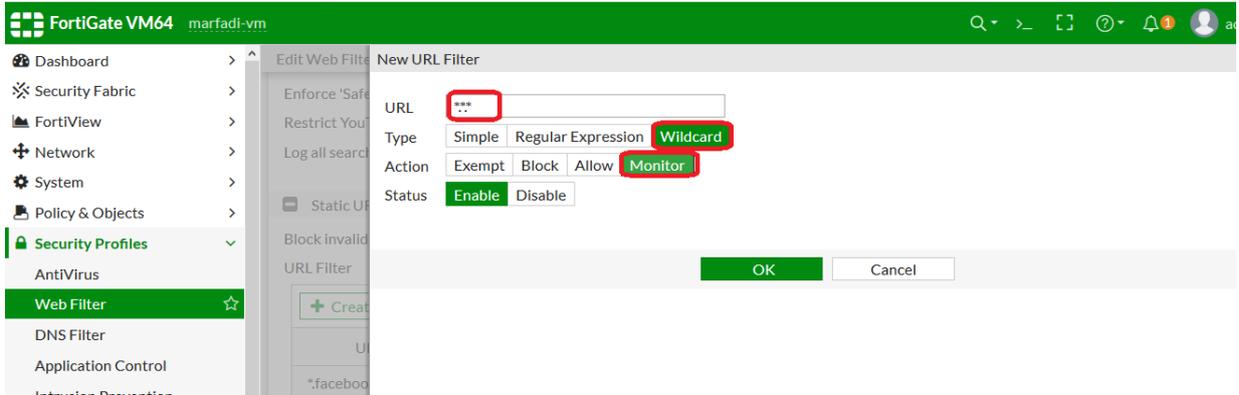
للسماح فيها مثلا نسخ رابط القناة



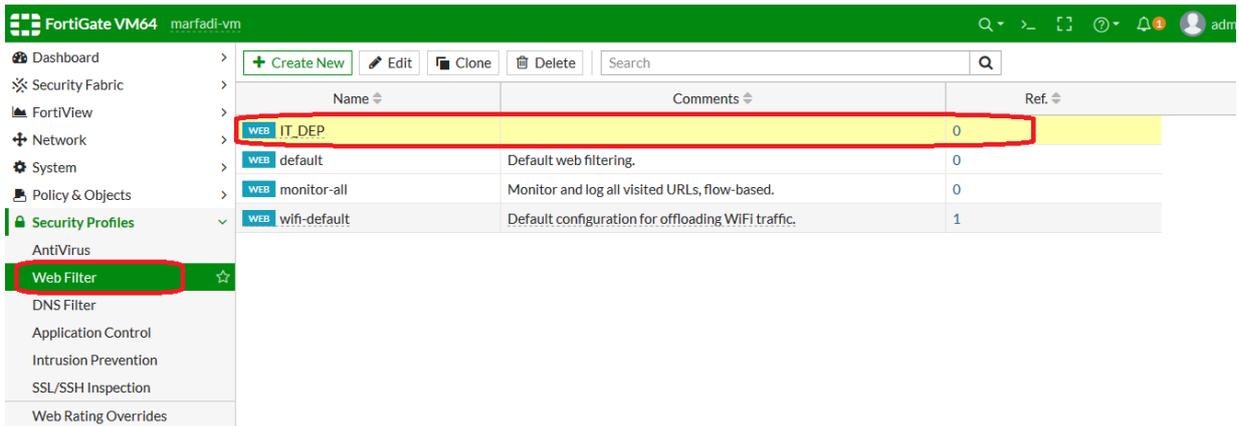
The screenshot shows the FortiGate VM64 configuration interface. The left sidebar contains the navigation menu with 'Web Filter' selected. The main area displays the 'New YouTube Channel Filter' dialog box, which is open over the 'Web Filter' configuration page. In the dialog, the 'Channel ID' field is highlighted with a red box and contains the value 'UCWzXbcIzEvSbQb4wQ6_em4A'. The 'Comments' field is empty. The 'Web Filter' configuration page shows the 'Proxy Options' section with 'Restrict YouTube access to specific channels' enabled. Below this, a table lists the restricted channels, with the same Channel ID 'UCWzXbcIzEvSb...' highlighted in a red box. The 'HTTP POST Action' is set to 'Allow'.

سيتم السماح لهذه القناة بالتحديد ...

❖ لو اريد مراقبه وتسجيل الـ logs أي موقع يتم تصفحه وذلك كما بالصورة ادناه

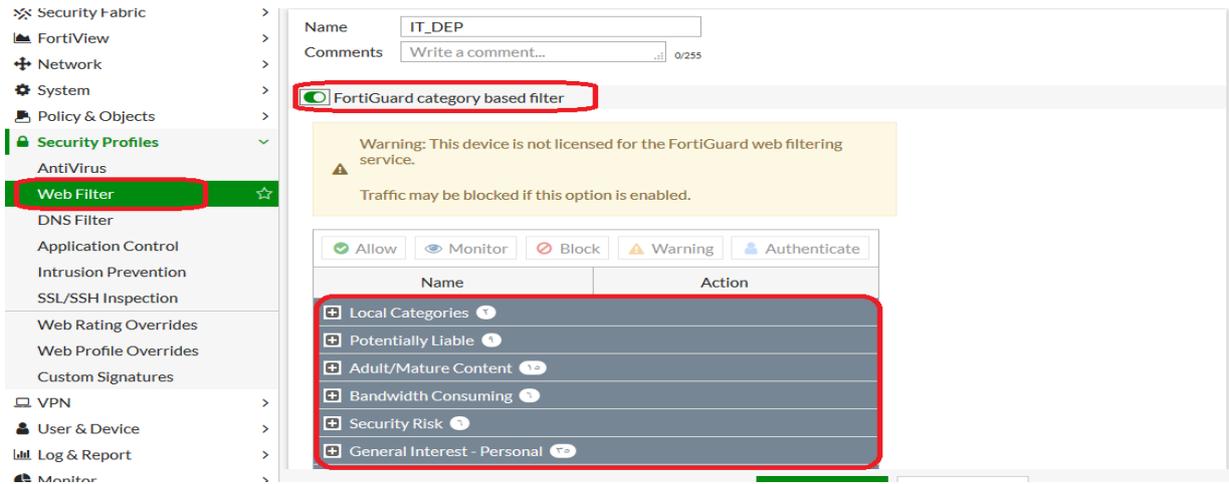


ولا يفضل عمل مثل هذا لأنه يسبب حمل شديد على جهاز الفورتى جيت ...



كما بالصورة أعلاه تم انشاء الـ web filter security profile باسم IT_DEP .

الـ category based filter تستخدم لتطبيق action معين على تصنيف معين من المواقع (مثلا تريد اغلاق كل مواقع الرياضة)، فبدلا من استخدام كتابه كل موقع على حده كما بالطريقة السابقة في Static URI filter فهذا صعب جدا .
فبواسطة الـ web category based يتم فقط اختيار التصنيف (category) المطلوب تطبيق الـ action عليه



ملاحظة : الـ FortiGuard category based filter لا يعمل على النسخة الـ VM التجريبية ويجب شراء الـ license كما بالرسالة التحذيرية الموضحة أعلاه

"Warning: This device is not licensed for the FortiGuard web filtering service.

Traffic may be blocked if this option is enabled.

"

حيث الفورتى جيت مقسم الـ category الى قسمين :

١- Main category :القائمة الرئيسية مثلا Adult/Mature content

٢- Sub category :القائمة الفرعية حيث تحتوي كما بالصورة ادناه على 15 تصنيف فرعي ...

أساسيات فورتى جيت

Name	Action
Adult/Mature Content	Warning
Alternative Beliefs	Warning
Abortion	Warning
Other Adult Materials	Warning
Advocacy Organizations	Warning
Gambling	Warning
Nudity and Risque	Warning
Pornography	Warning
Dating	Warning

فيمكنك اغلاق مثلا مواقع القمار المسي **Gambling**.

Name	Action
Adult/Mature Content	Warning
Alternative Beliefs	Warning
Abortion	Warning
Other Adult Materials	Warning
Advocacy Organizations	Warning
Gambling	Block
Nudity and Risque	Warning
Pornography	Warning
Dating	Warning

فلوتريد اختيار كل ال sub category للتصنيف الرئيسي المسي **Adult/Mature**

فأنك تقوم بعمل تحديد الكل بالنقر على **Alt+A** ثم تختار ال action المناسبه كما بالصورة ادناه

Name	Action
Adult/Mature Content	Warning
Alternative Beliefs	Warning
Abortion	Warning
Other Adult Materials	Warning
Advocacy Organizations	Warning
Gambling	Warning
Nudity and Risque	Warning
Pornography	Warning
Dating	Warning

أساسيات فورتني جيت

- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
- AntiVirus
- Web Filter ☆
- DNS Filter
- Application Control
- Intrusion Prevention
- SSL/SSH Inspection
- Web Rating Overrides
- Web Profile Overrides
- Custom Signatures
- VPN >
- User & Device >
- Log & Report >
- Monitor >

Allow Monitor Block Warning Authenticate

Name	Action
Adult/Mature Content 15	
Alternative Beliefs	Block
Abortion	Block
Other Adult Materials	Block
Advocacy Organizations	Block
Gambling	Block
Nudity and Risque	Block
Pornography	Block
Dating	Block

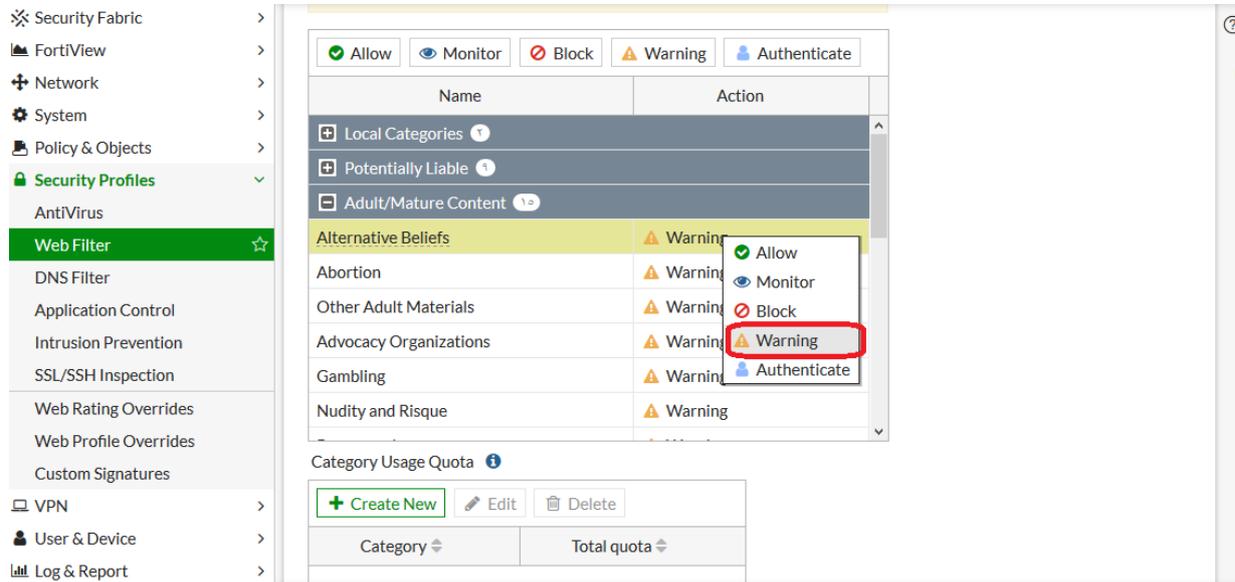
Category Usage Quota ⓘ

+ Create New Edit Delete

Category	Total quota
----------	-------------

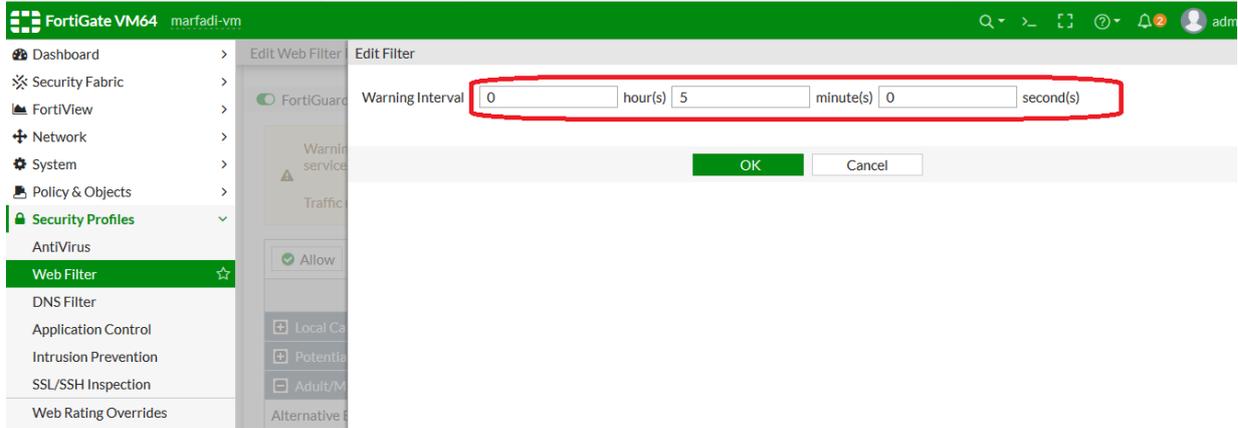
OK Cancel

: Web category usage quota



ال Warning action يقصد به عمل تحذير لليوزر الذي يدخل للمواقع مثلًا Gambling ويكون دخول الموقع على مسؤوليه المستخدم .

حيث بمجرد النقر على الزر warning تظهر لك الرسالة التالية



حيث ستظهر رساله التحذير مدتها 5 دقائق ...

ال Authenticate action :

حيث يظهر للمستخدم يوزرنييم وباسورد للدخول للموقع مثلًا عند دخول اليوزر لأي موقع ضمن التصنيف sex education .

أساسيات فورتى جيت

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow Monitor Block Warning Authenticate

Name	Action
Dating	Warning
Weapons (Sales)	Warning
Marijuana	Warning
Sex Education	Warning
Alcohol	Warning
Tobacco	Warning
Lingerie and	Warning
Sports Hunt	Warning

OK Cancel

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow Monitor Block Warning Authenticate

Name	Action
Dating	Warning
Weapons (Sales)	Warning
Marijuana	Warning
Sex Education	Authenticate
Alcohol	Warning
Tobacco	Warning
Lingerie and Swimsuit	Warning
Sports Hunting and War Games	Warning

FortiGate VM64 marfadi-vm

Edit Web Filter Edit Filter

FortiGuard

Warning Interval 0 hour(s) 5 minute(s) 0 second(s)

Selected User Groups FSSO-GROUP-IT

OK Cancel

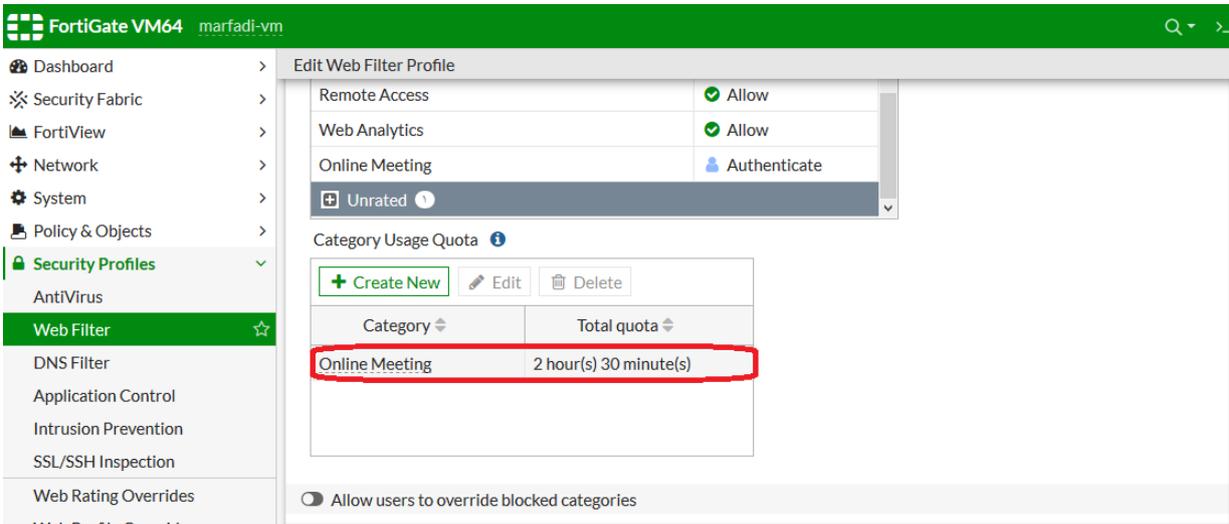
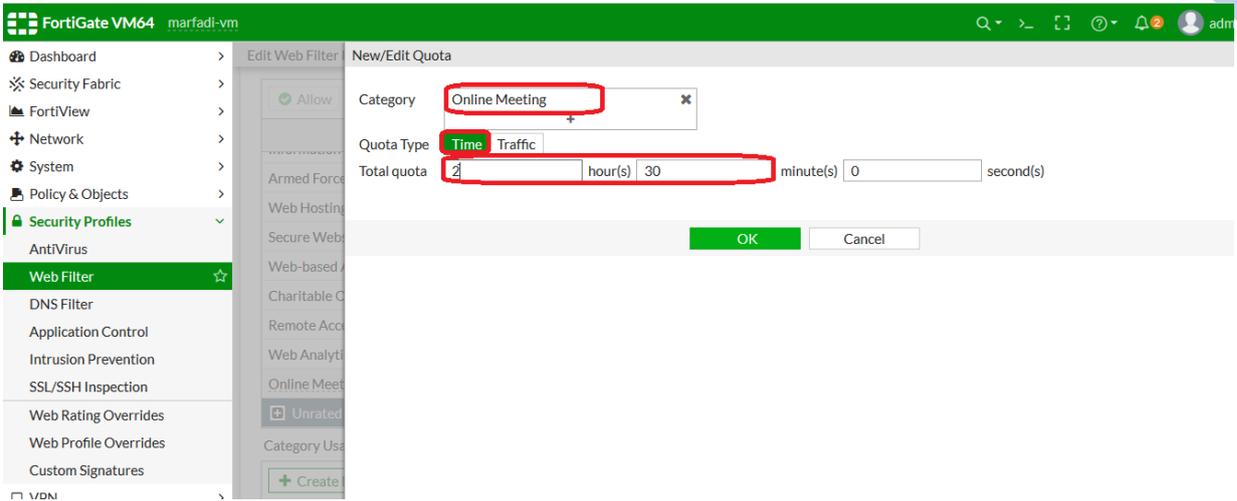
حيث تم أضافه جروب الـ IT فيجب على اليوزر المراد فتح أي موقع تنتهي لـ sex education ان يكون ضمن الـ IT group حيث يجب ان يقوم بإدخال يوزرنيم وباسورد لأي حساب ضمن الـ IT group.

أساسيات فورتى جيت

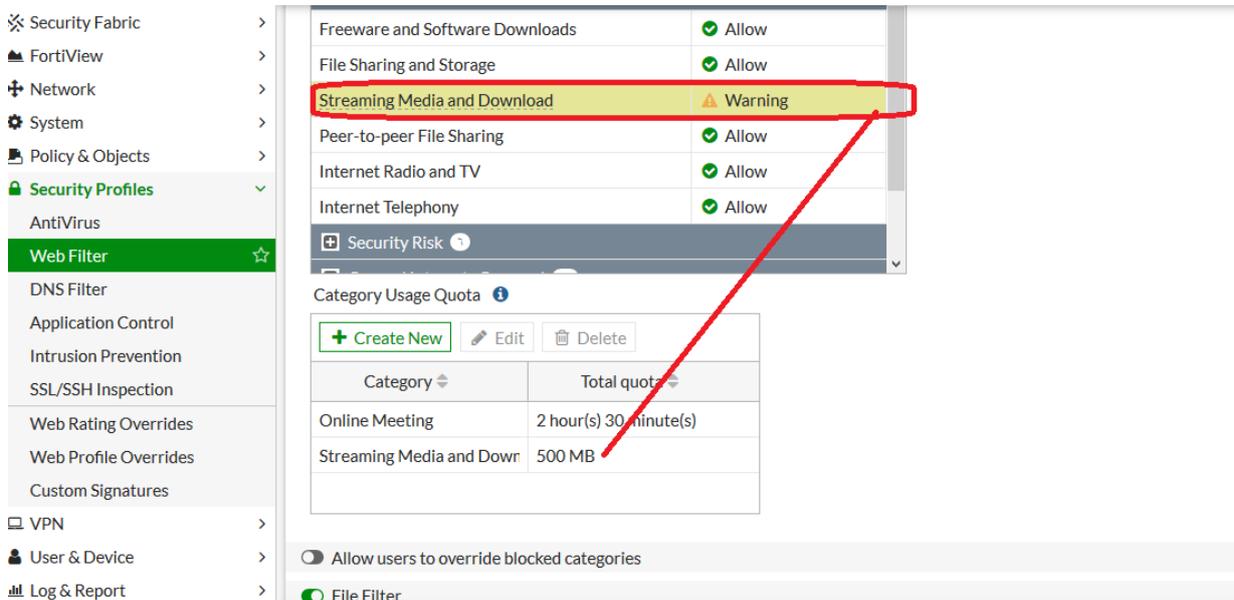
الآن سنقوم بعمل Quota لتصنيف معين وليكن الـ online meeting بحيث نحدد مثلاً ساعه ونصف فقط وبعدها يتم الخروج من الموقع ..

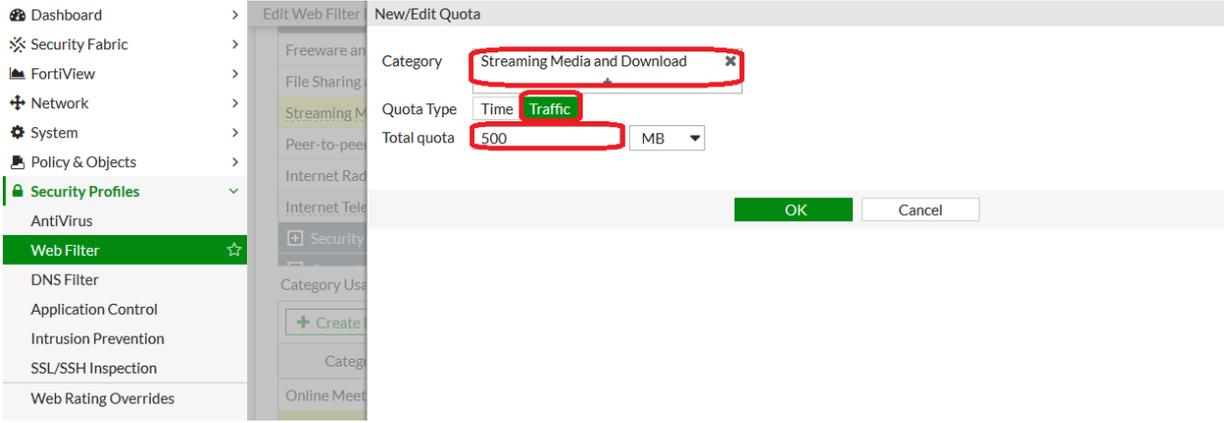
حيث لا يمكن عمل quota الا للتصنيفات المعمول لها Monitor او Authenticate او Warning في الـ FortiGuard web category filter ...

حيث يتم استخدام مواقع التصنيف Online meeting لمدة ساعتين ونصف ومن ثم ظهور رساله الـ authenticate



أيضا اريد ان اسمح ان يتم فتح مواقع ال streaming media and download 500 ميغا فقط ..

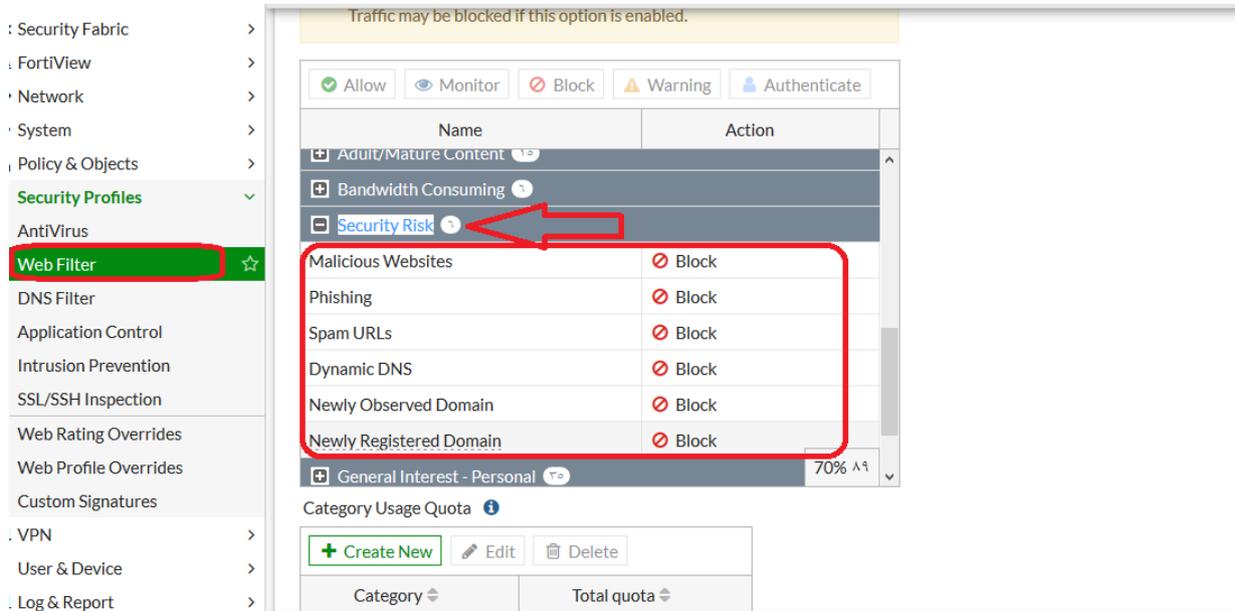




: Web Category Based Filter Overriding

تعمل override (تجاوز) لأي تصنيف معمول لها block في الFortiGuard web category لـ group معين.

مثلا اريد انا اسمح لجروب اسمه IT_Managers بأن يتجاوز غلق مواقع الSecurity Risk الذي تم اغلاقه في الFortiGuard web category، وبهذا اليوزرات التي تحت الجروب IT_Managers سوف يسمح لهم بالوصول الى المواقع المدرجه تحت التصنيف Security Risk .



نلاحظ بأنه تم عمل تجاوز -override- لهذا البروفایل للجروب المسماة IT_Managers بحيث يتم تطبيق الـ profile اخر مثلا اسمه allow-all على اليوزرات التي تندرج تحت الجروب IT_Managers...

Name	Action
Local Categories	
Potentially Liable	
Adult/Mature Content	
Bandwidth Consuming	
Security Risk	
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block

Allow users to override blocked categories

Groups that can override: IT_Managers

Profile Name: WEB allow-all

Switch applies to: User User Groups IP Ask

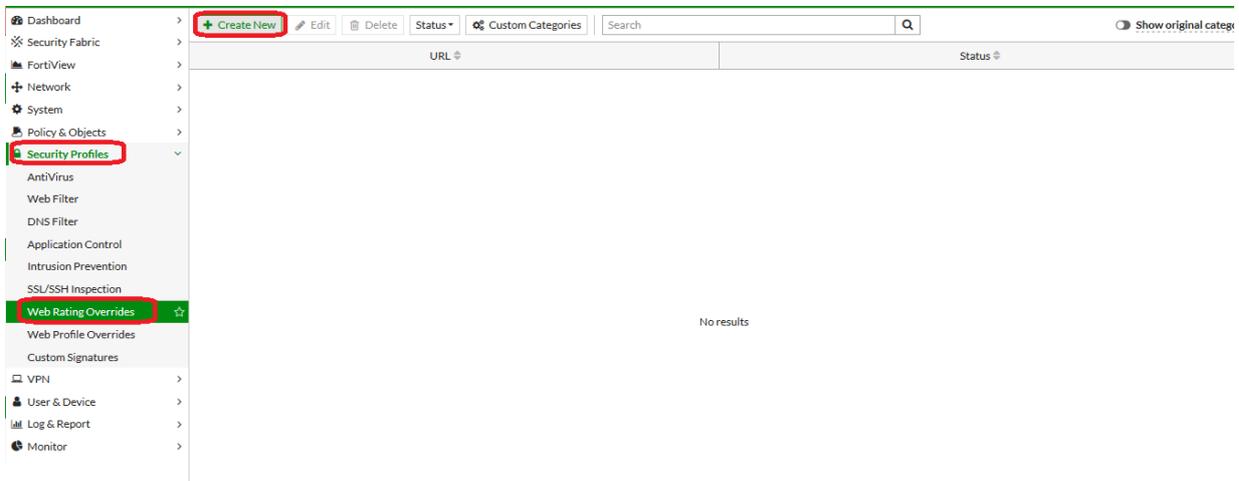
The original user or group must be specified as the 'Source' in firewall policies using this profile

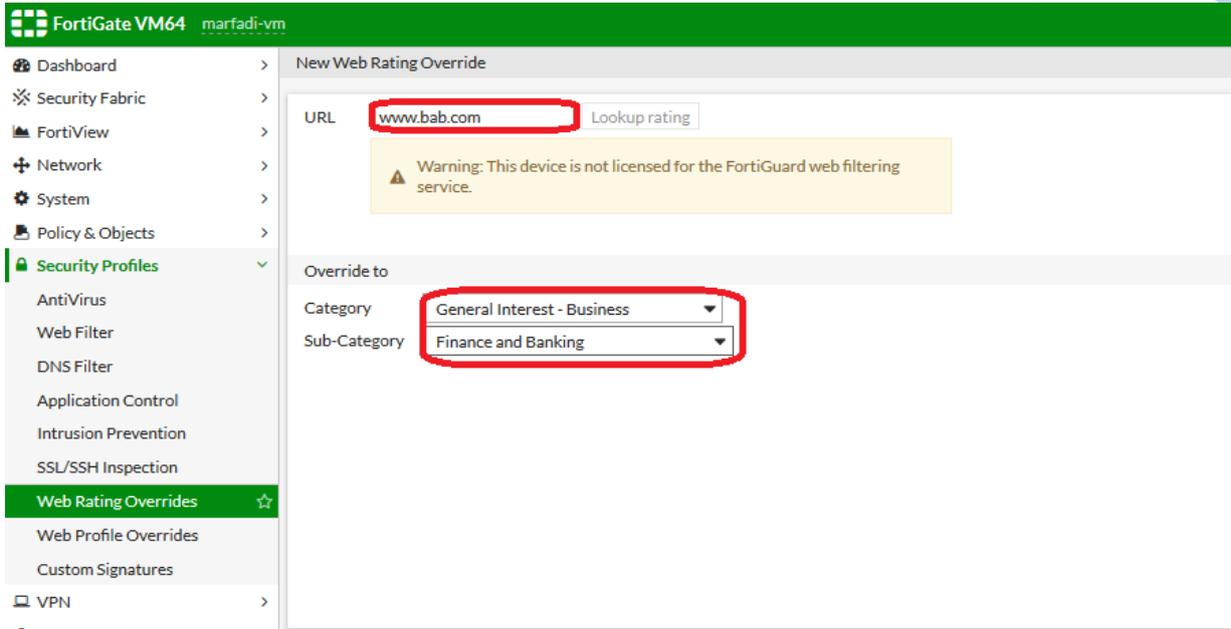
Switch Duration: Predefined Ask

0 day(s) 0 hour(s) 15 minute(s)

: Web Rating Override

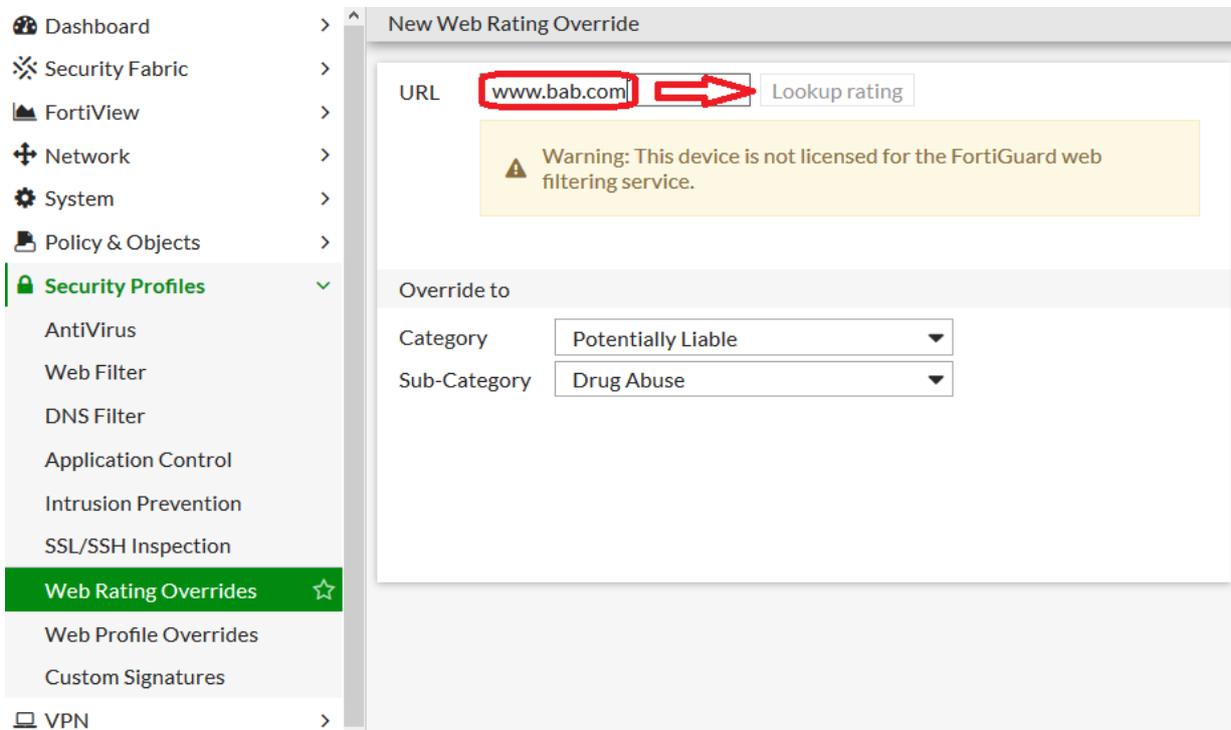
في حالة كان لدينا موقع مثلا www.bab.com ونفترض بأن الموقع ليس له تصنيف معين او الفورتني جيت غير قادر على معرفة الcategory التي يندرج تحتها .
او ان هذا الموقع موجود في category وتريد نقله الى category أخرى فأن بواسطة ال Web Rating Override يمكن عمل ذلك .





تم تصنيف موقع www.bab.com بأنه ينتهي إلى General Interest-Business تحت التصنيف الفرعي المسى Finance and banking .

حيث أي موقع تريد معرفة إلى أي تصنيف ينتهي نقوم بالخطوات التالية :



بالنقر على الزر Lookup rating سيتم معرفة التصنيف للموقع www.bab.com ولكن نظرا لأننا نعمل ب FortiGate VM ولا تحتوي على FortiGuard web filtering license فأننا غير قادرين على الاستفادة من هذه الخاصية ..

: Web Profile overrides

يستخدم في حالة وجود يوزر او جروب معين او ايبي معين مطبق عليه web filter profile معين وتريد في وقت معين ان يتطبق عليه web filter profile اخر...

Initiator	Scope	Original Profile	New Profile	Status	Expires
Admin generated					
admin	marfadi	WEB IT_DEP	WEB allow-all	Enable	2020/08/23 15:55:00

كما بالصور أعلاه يتبين بأن اليوزر المسى marfadi الذي بالأصل ضمن الجروب الـ IT_Managers والذي في الأصل مطبق عليها web filter profile =IT_Dep ولكن سيتم تطبيق الـ web filter profile =allow-all في هذه الفترة الى تاريخ 2020-08-23 الساعة 15:55:00 .

:ADDRESS

طريقة انشاء عنوان بحسب الماك ادرس للجهاز

The image shows two screenshots from the FortiGate VM64 management interface. The top screenshot displays the 'Addresses' table, and the bottom screenshot shows the 'New Address' configuration dialog.

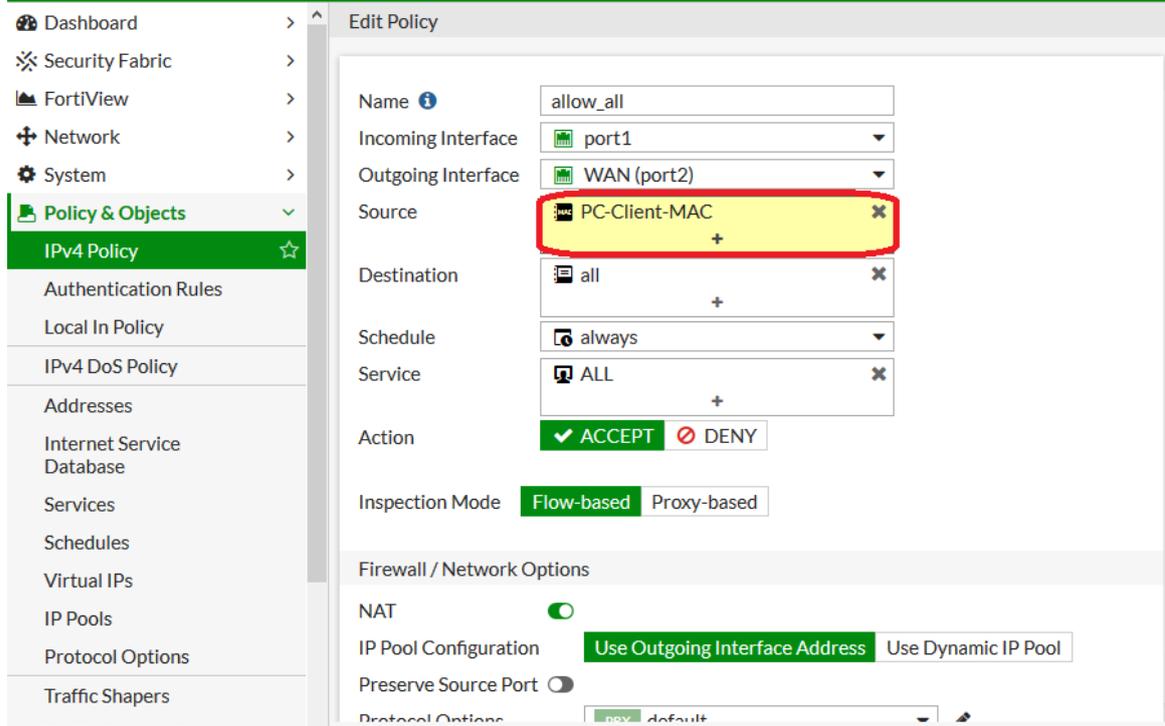
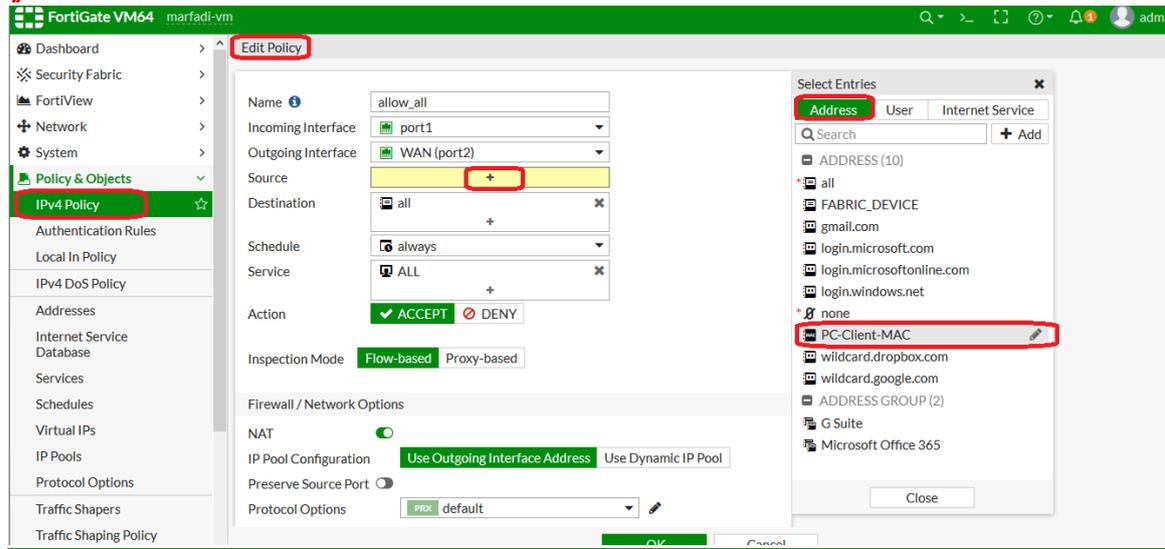
Addresses Table:

Name	Type	Details	Interface	Visibility	Re
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
all	Subnet	0.0.0.0/0		Visible	2
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
wildcard.dropbox.com	FQDN	*.dropbox.com		Visible	0
wildcard.google.com	FQDN	*.google.com		Visible	1

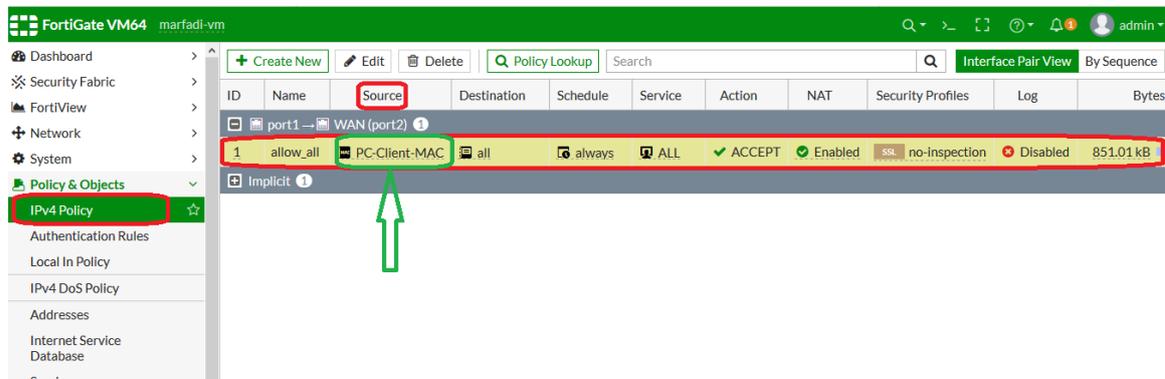
New Address Configuration:

- Name: PC-Client-MAC
- Color: Change
- Type: Device (MAC Address)
- MAC Address Scope: Single Address
- MAC Address: 00:0c:29:ff:72:33
- Interface: any
- Show in address list:
- Comments: Write a comment... (0/255)

Buttons: OK, Cancel



تم تحديد هذا العنوان للجهاز بحسب الماك ادرس



بحسب الصورة أعلاه تم انشاء الرول (البولييسي) باسم allow_all حيث المصدر عنوان باسم PC-Client-MAC وهو عنوان الماك ادرس للجهاز الكلاينت (win 8.1).

Fortinet solution ❖

الفورتي جيت :هو ال UTM او الفايروول او الجهاز الرئيسي بالشبكة حيث يوجد منه نوعين

- ١- هاردوير يسمى appliance
- ٢- سوفتوير vm حيث ممكن تشتغل عليه على VMware او ESXI وكلاهما يقدموا نفس المميزات او الخدمات

حيث يستخدم الفورتي جيت:

- ١- حمايه الترافيك من الهجمات
- ٢- حمايه من الفايروسات والWORMS
- ٣- حمايه من الاسبام
- ٤- يعمل ك Bandwidth management
- ٥- يعمل ك fail over و redundancy

حيث يستطيع العمل مع AD

ماهي اجهزه الفورتي نت :

- ١- Fortigate
- ٢- Fortimail وينقسم الى نوعين :
- ١- Security filter أي يتم أضافه هذه الميزة الى سيرفر المييل الخاص بك مثل سيرفر ال exchange server
- ٢- Mail server : يعمل ك mail server مثله مثل ال exchange server ويعتبر اقوى ..
- ٣- Fortimanager :عبارة عن جهاز يعمل لك تحكم بكل اجهزه الفورتي التي عندك بالشبكة حتى 5000 جهاز تحكم كامل بالسياسات والاعدادات واداره التحديثات ويعمل أيضا مع الجهاز fortianalyzer

أساسيات فورتى جيت

- ٤- Fortianalyzer : جهاز يقوم بعمل تحليل الترافيك بشكل كامل وأيضا البروتوكولات التي تمر بالشبكة ويعطيك تقارير تفصيليه وبشكل رسومات عن الشبكة وال logs حيث يعمل دمج كامل مع جهاز ال fortimanager .
- ٥- fortiDatabase :عباره عن جهاز يوفر لك حمايه من الهجمات الخاصة ب database (قواعد البيانات)
- ٦- fortiWeb :عباره عن حل للشركات المتوسطة والكبيرة فقط حيث يستخدم لحمايه التطبيقات من هجمات SQL injection و attack Dos مثل لو كان لديك تطبيق على الكلاود وتريد حمايته
- ٧- Forticlient :برنامج مثله مثل مكافح الكاسبرالذي بينزل على الجهاز الخاص بك (End point) حيث الفورتى كلاينت يعمل ك antivirus و web filter و فايروول ومن مميزاته بانه مجاني ولو عندك جهاز فورتى جيت فأنتك ممكن ان تستفيد من ميزات إضافية ..
- ٨- Fortiswitch :هو عبارة عن جهاز مثله مثل سويتشات سيسكو وغيرها
- ٩- fortiAP : عبارة عن جهاز يعتبر من الحلول القوية والرائعة في ادارته والتحكم بالوايرلس ..

❖ Firewall :

الفرق بين ال Firewall و Next Generation firewall و UTM

الفايروول :عبره عن مبدا يقوم بتحقيق الأمان للشبكات من خلال التحكم ب incoming or outgoing traffic من خلال قواعد (rules) معموله على هذا الجهاز مسبقا .

حيث الفايروول يوجد منه نوعين

1- هارديوير: يعتبر اقوى من السوفتوير واكثر ثبات و يحقق مبدا الأمان

مثل جهاز fortigate firewall من شركه فورتى نت ،

عائله Netscreen firewall من شركه جونيبر

منتج ASA firewall من شركه سيسكو

و أيضا منتج اسمه paloalto firewall

حيث كل واحد مهم له مزايا ونقاط ضعف حيث تختار المنتج المناسب لك للمتطلبات التي تحتاجها وايضا

الدعم الفني ..

-2 سافتوير: مثل Zonealarm من شركة شيك بوينت و pfsense من شركة كومودو

Forefront من شركة مايكروسوفت مثل TMG والايضا

➤ تسلسل واشكال الفايرووول :

❑ Firewall & UTM & Next Generation Firewall concepts

Firewall	Concept
Transparent Firewalls Layer 2	<ul style="list-style-type: none"> ✓ These firewalls do not have IP address except for management interface ✓ No NAT in this mode ✓ Inspect traffic flow based based on pre-configured rule
First Generation Traditional Firewall or packet filters Layer 3	<ul style="list-style-type: none"> ✓ Static packet-filter firewalls are first generation devices that examine data packets at OSI layer 3 , based on pre-configured rules ✓ Includes : Packet filter – NAT – VPN
Second Generation Circuit-level Layer 4	<ul style="list-style-type: none"> ✓ These second-generation firewalls validate that a packet is either a connection request or part of a connection between two peers at the Transport layer

Firewall	Concept
Next Generation NGFW or Application-layer Layer 7	<ul style="list-style-type: none"> ✓ The goal of next generation firewalls is to include more layers of the OSI model up to layer 8 (today) , previously it was at layer 7 ✓ Application layer firewall also called application layer proxies offers the highest of level security by examining traffic at all seven layers of the OSI model ✓ Includes : Web & App filter – IPS – bandwidth management
UTM Unified threat management	<ul style="list-style-type: none"> ✓ UTM product able to perform multiple security functions within one single appliance, Start in 2005 Includes : App firewall – GW-AV – GW-spam - DLP Multi link management content filtering – Load Balancing

كما بالصور أعلاه

-1 : Transparent firewall layer 2

يشتغل على الطبقة الثانية فقط لا غير .

لا يحتوي على ايبي الا ايبي الذي عن طريقة بنعمل ادارته وتحكم للفايروول

لا يعمل nating

يعمل فحص للترافيك باستخدام flow based ويمررها على الرول التي قمت بإعداداتها على الفايروول

مسبقا .

-2 First generation او يسمى traditional firewall واحيانا يسمى packet filter لأنه يعمل على الطبقة الثالثة ..

يتعامل مع الIP الا انه في network layer يستطيع عمل فلتر على مستوى الباكيت وأيضا يستطيع عمل NATING و VPN (ربط بين الشبكة الداخلية وشبكة أخرى)

-3 Second generation: يعمل في الطبقة الرابعة وهي (transport layer) حيث يعتبر الجيل الثاني من الفايروول (لا يقصد بها next generation) لأن ال next generation حاجه اعلى من ال second generation . حيث تم الانتقال من الطبقة الثانية الى الطبقة الرابعة .

-4 Next generation: يسمى اختصارا NGFW حيث في هذا النوع تم التعامل مع الطبقة السابعة (Application layer) حيث بدأ التعامل مع على مستوى التطبيقات وظهر معنا أيضا IPS و bandwidth management و web filter و application filter ..ومن عيوبه هو البطئ مقلنه بالأنواع السابقة لأنه كلما حققت حمايه وامان زياده فانه يكون على حساب السرعة.

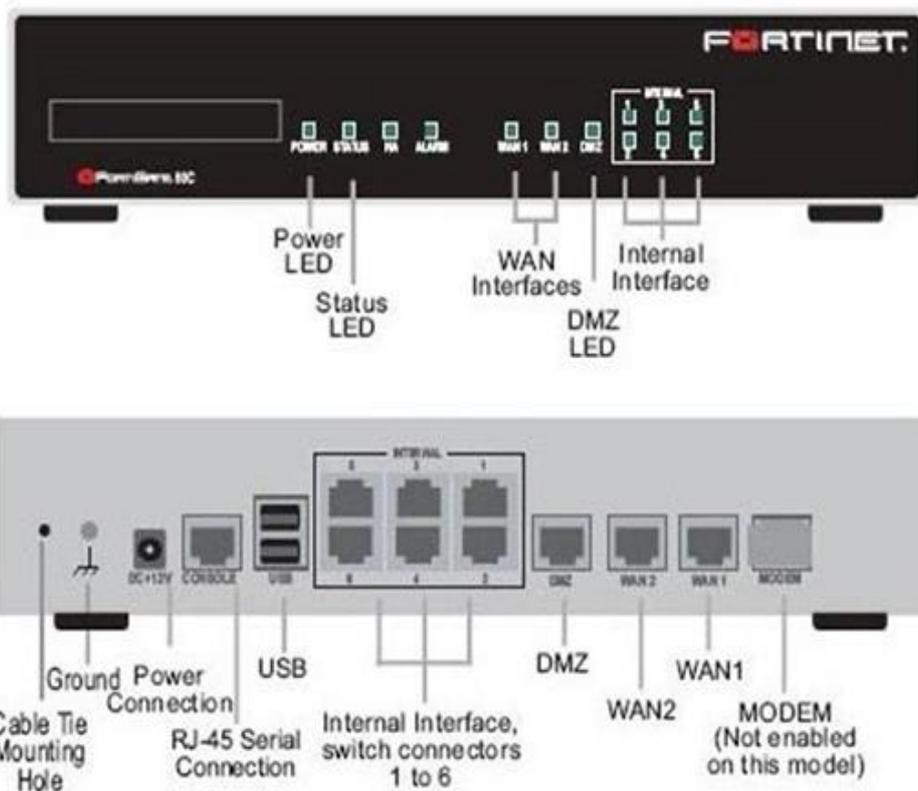
-5 UTM(Unified threat management) : عبوره عن جهاز لديه القدرة على تأدية عدة مهام (خصائص) من خلال جهاز واحد حيث يتعدى فايروول و next generation firewall و يحقق لك ال load balancing و (PLD) data leak prevention و gateway و Antivirus و gateway Antivirus و app firewall وهذا هو النوع الي سوف نشرحه ونتعامل معه حيث هذا الجهاز يحقق لك كل نقاط الحماية في الشبكة من خلال جهاز واحد فقط وهو UTM .

Bandwidth ,Throughput ,Concurrent Sessions

مصطلحات مهمة :

- 1 Bandwidth : هو أقصى عدد للباكت تمر داخل القناة (اي القدرة الاستيعابية لهذه القناة) ..
- 2 Throughput : هو عدد الباكث التي يمر حاليا عندما الجهاز يتعامل (يتصل) مع جهاز اخر ...
- 3 Concurrent sessions : هي عبارة عم عدد ال connections (sessions) الذي يستطيع فيه الفايروول التعامل معها بنفس الوقت .
حيث عند فتح صفحة انترنت تعتبر جلسته او session او فتحت برنامج سكايب يعتبر جلسته وهكذا ...





كما باصوره أعلاه لأحدى منتجات الفايروول فورتني جيت ..

- 6 منافذ شبكة (Lan)
- 2 منافذ wan تستطيع توصيل فيها 2 خطوط انترنت ..
- والمنفذ DMZ تستطيع توصيل السيرفرات التي سوف يتم الوصول اليها عبر الانترنت (سيرفرات موجودة بالشبكة الداخليه ولكنك سوف تسمح بالوصول اليها من خارج الشبكة عبر الانترنت).
- منفذ USB يستخدم لأخذ نسخه باك اب من الاعدادات الخاصة بالجهاز او لو اردت أضافه firmware جديد للجهاز .
- Console port :يستخدم لعمل الاعدادات لجهاز الفورتني ويستخدم ذلك عندما تقوم بشراء جهاز فايروول جديد .

- 1 Entry level : تستخدم للشركات والاعمال الصغيرة .
- 2 MID RANGE : تستخدم للشركات الكبيرة .
- 3 HIGH-END : يستخدم لشركات مزودي الخدمة (ISP) وهو اقوى الأنواع
- 4 Virtual appliances : يتم تزييلها على احدى منتجات الانظمة الوهمية ومن ثم يعمل كفايروول .

يتم تحديد موديل معين للشراء وذلك بحسب احتياجاتك في العمل وذلك بعد ما تقرا موصفات الموديل وأيضا يجب ان تحدد احتياجاتك انت مثلا كم لديك خطوط انترنت وكم سرعتهم وماهي الخصائص او المميزات التي سوف تحتاجها بالشركة عندك. هل ستحتاج vpn ام لا! وان كان نعم كم عدد الناس الذين سوف يعملوا معاك vpn

Operating system OS key features 5 2

ماهي مميزات الfortiOS او نظام التشغيل لجهاز الفورتى جيت

❑ FortiOS operating system key features

- ✓ Firewall
- ✓ Network Services and Support
- ✓ VPN
- ✓ WAN Optimization, Web Cache and Explicit Proxy^
- ✓ User & Device Identity Control
- ✓ Integrated Token Server
- ✓ SSL Inspection
- ✓ Data Leak Prevention (DLP)
- ✓ Endpoint Control
- ✓ Vulnerability Scanning
- ✓ Wireless and Switch Controller
- ✓ Anti-Malware / Advanced Threat Protection
- ✓ Application Control
- ✓ High Availability
- ✓ Web Filtering
- ✓ Administration, Monitoring & Diagnostics
- ✓ Log & Reporting

حيث أي جهاز فورتى جيت يكون في نفس المميزات (الخصائص) أعلاه تقريبا ...

أي جهاز فورتني جيت فايروول (حقيقي وليس وهمي) يكون الايبي الافتراضي له هو 192.168.1.99 ويمكنك الوصول اليه عبر الPING و HTTP و HTTPS وذلك عبر أي منفذ lan في الجهاز ... حيث المنفذ lan1 يكون مفعّل عليه DHCP أي بمجرد توصيل كابل الشبكة للـ port1 الى الـ port الخاص بك فإن كرت الشبكة في الـ port سوف يأخذ ايبي من نفس الـ رينج 192.168.1.0 . بعكس لو قمت بتوصيل الكابل بين الـ port و 2,3,... فإنه يجب عليك ان تكتب ايبي لكرت الشبكة للـ port من نفس الـ رينج 192.168.1.0 بشكل يدوي .. اليوزر نيم الافتراضي يكون admin والباسورد (لا يوجد باسورد)

الأشياء (المميزات) التي توجد بالفايروول معتمده بشكل رئيسي على الترخيص (لايسنز) مثل

- 1 Antivirus
- 2 Antispam
- 3 Web filter
- 4 Ips

وهذه الأشياء يجب ان تشتريها وتجدها سنويا من شركة فورتني جيت ..

لكي تتمكن من تزيل الـ vm fortigate يجب ان يكون لديك حساب على

<https://support.fortinet.com>

ولن تتمكن من انشاء حساب الا لو كنت مشتري جهاز من شركة فورتني جيت..

حيث عن طريق الرابط أعلاه يمكنك عمل تسجيل لجهاز الفورتني جيت التابع لك او عمل تجديد للترخيص للجهاز (أيضا يمكنك عمل هذا أيضا من خلال صفحة الويب التابع لجهاز الفورتني جيت نفسه) وأيضا يمكنك تزيل الـ firmware الجديد او قطع ticket للتواصل مع شركة فورتني في حالة مواجهه مشكله ما او عمل chatting معهم ..

FortiGate basics Registering FortiGate

عند شراء جهاز جديد يجب ان تعمل له تسجيل في موقع الدعم الخاص بفورتى نت وذلك لكي تقوم بتفعيل الجهاز الخاص بك وبهذا تسمح لجهاز الفورتى جيت الخاص بك بأن يستلم التحديثات من الفورتى جلد (fortiguard) الخاصة بIPS وAV وAntispam و web filtering و application control . وأيضا لكي تتمكن من عمل upgrade OS للجهاز..
ولكي تقوم بالتسجيل يجب ان يكون جهاز الفورتى جيت موصل بالإنترنت .

❖ طريقة عمل Registration لجهاز الفورتى جيت :

القوائم الرئيسية للفورتى جيت :

1- System : هي الاعدادات الرئيسية للفورتى جيت

2- Policy&objects :

الpolicy هي السلاح الخاص بك في الفورتى جيت الذي يتم استخدامه لتطبيق كل الرولات على الشبكة الخاصة بك او على المستخدمين .

الobjects هي اللي بيتطبق عليها البوليسي مثل address –services-schedule-traffic shaper وغيرها ..

3- Security profiles :

هي الاعدادات الأمنية مثل الويب فلتر او IPS

4- User& devises :

خاص بالمستخدمين والأجهزة التي سيتعامل معها الفورتى جيت.

5- Logs&reports :عبلره عن التقارير والlogs على أي شي يحصل لدي في الشبكة .

ما هو operation mode:هي طريقة عمل جهاز الفورتى جيت، حيث الفورتى جيت يعمل في mode 2 هما

1- NAT mode

The screenshot shows the FortiGate VM64 GUI for a device named 'marfadi-vm'. The left sidebar contains a navigation menu with 'Status' highlighted. The main content area is divided into several sections: 'System Information' (with fields for Hostname, Serial Number, Firmware, Mode, System Time, Uptime, and WAN IP), 'Licenses' (with expandable sections for FortiCare Support, Firmware & General Updates, IPS, AntiVirus, and Web Filtering), 'FortiGate Cloud' (showing 'Not Supported'), and 'Security Fabric' (with various security-related icons).

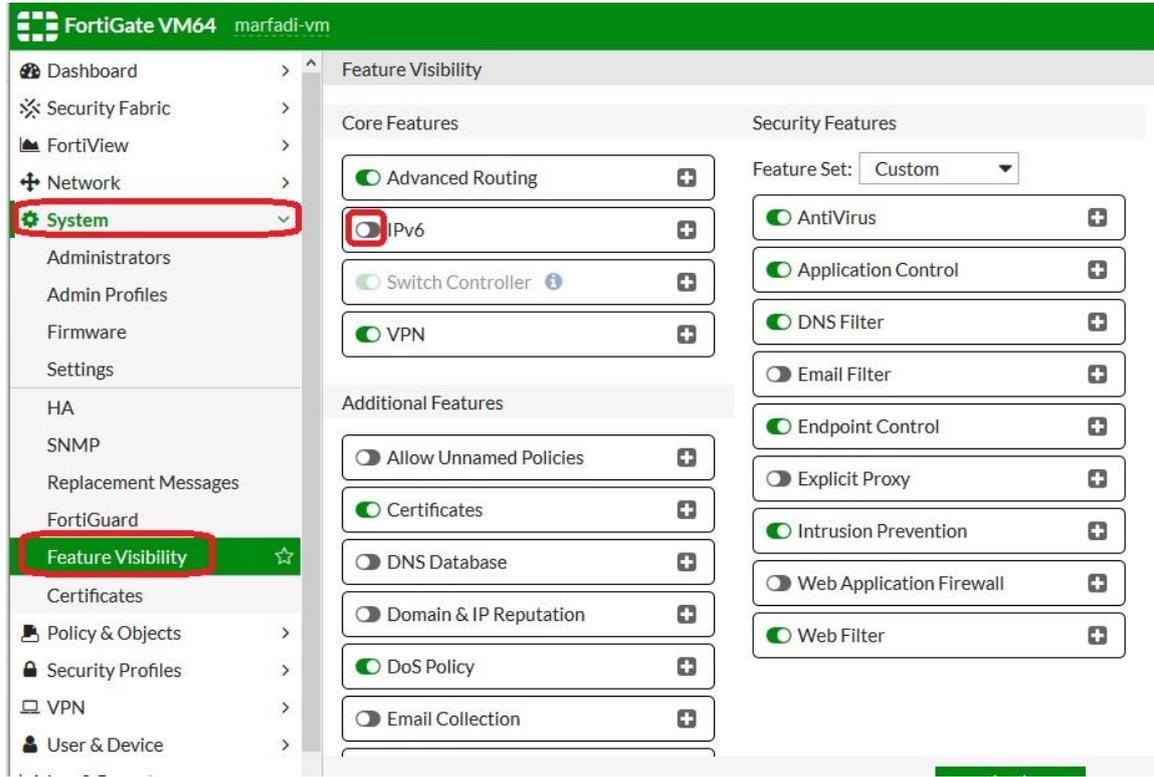
ملاحظة:

جهاز الفورتى جيت لا يحتوي على زر لإيقاف التشغيل أو إعادة التشغيل بل يمكنك ذلك من CLI أو من GUI.

ماهي ال features :

هي الوظائف التي اجعل جهاز الفورتى جيت يلعبها مثلا VPN و AV و IPS و IPV6.... الخ

بعض الوظائف لا تحتاجها في الشبكة عندك مثل IPv6 فالأفضل إيقاف هذه الوظيفة (features) لكي نقلل من استهلاك مصادر الجهاز (Ram, HDD, CPU) وتزويد عمره الافتراضي فالأفضل تعمل لها OFF ..



كما بالصورة أعلاه فإن جهاز الفورتني جيت لا يدعم IPv6 .

حيث الـ features مقسمه الى جزئين :

-1 Core Features : هي الخصائص الخاصة بالشبكة ليس لها علاقة بـ security مثل advanced

routing و IPv6 و VPN حيث استطيع تشغيلها بدون ترخيص (license).

-2 Security features : هي الخصائص الخاصة بالحماية مثل AV,application control,ips,web

filter,email filter وهذه الخصائص لا تعمل الا بترخيص

ويمكن تعديل الخصائص من features set واختير المناسب لك مثلا UTM full حيث سيقوم بتشغيل

كل الخائص (features)

أساسيات فورتني جيت

The screenshot shows the FortiGate web interface. On the left, the 'System' menu is highlighted, and 'Feature Visibility' is selected. The main content area is titled 'Feature Visibility' and is divided into 'Core Features' and 'Security Features'. The 'Feature Set' dropdown menu is open, showing options: Custom, NGFW, ATP, NGFW + ATP, UTM, Full UTM (highlighted), WF, and Custom. The 'Full UTM' option is selected.

The screenshot shows the FortiGate web interface with the 'Feature Set' dropdown menu set to 'Full UTM'. The 'Security Features' section is expanded, showing a list of features with toggle switches: AntiVirus, Application Control, DNS Filter, Email Filter, Endpoint Control, Explicit Proxy, Intrusion Prevention, Web Application Firewall, and Web Filter. An 'Apply' button is visible at the bottom right.

تم تحديد كل security features كما بالصورة أعلاه..

أساسيات فورتى جيت

The screenshot shows the FortiGate Feature Visibility page. The left sidebar is expanded to 'System' > 'Feature Visibility'. The main content area is divided into 'Core Features', 'Additional Features', and 'Security Features'. The 'Feature Set' dropdown is set to 'NGFW'. In the 'Security Features' section, 'Application Control' and 'Intrusion Prevention' are highlighted with red boxes. The 'Feature Set' dropdown is also highlighted with a red box.

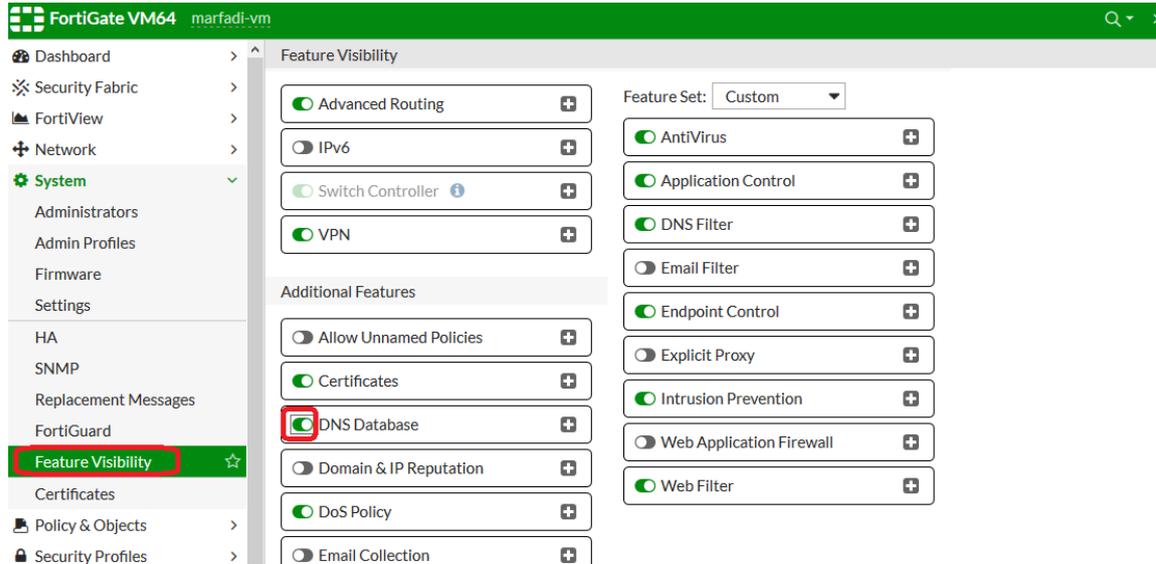
عند اختيار features set=NGFW .

ولدينا خيار يسمى ADVANCE THREAT PROTECTION=ATP

The screenshot shows the FortiGate Feature Visibility page with the 'Feature Set' dropdown set to 'ATP'. The 'Feature Set' dropdown is highlighted with a red box. In the 'Security Features' section, 'AntiVirus', 'Endpoint Control', and 'Web Filter' are highlighted with red boxes. The 'Feature Visibility' option in the left sidebar is also highlighted with a red box.

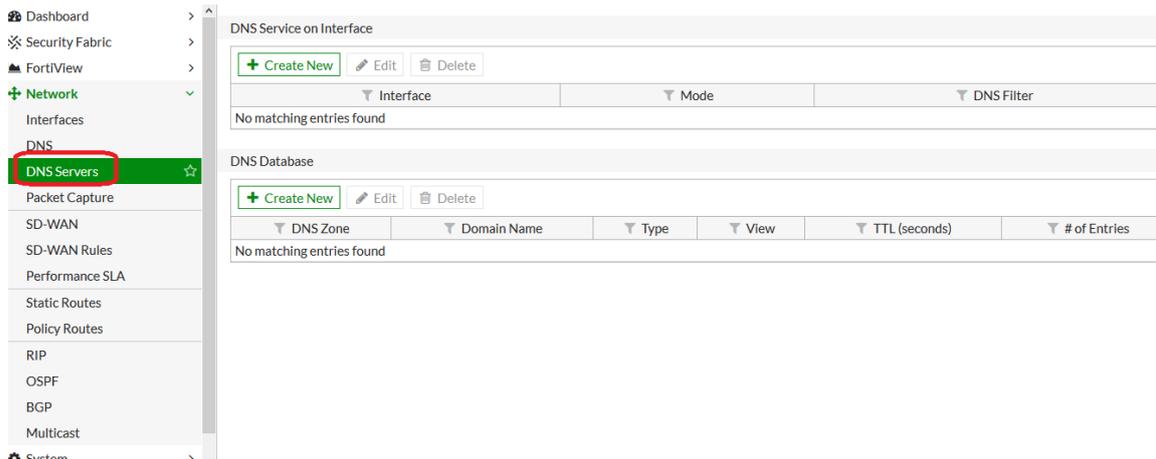
حيث هنا قمنا فقط بتفعيل الخاصية ولكننا لم نقوم بعد بتطبيقها على أي احد بالشبكة (أي تطبيقها كروول على اليوزرات او الاجهزه).

فلو تريد مثلا جعل جهاز الفورتى جيت يعمل ك dns server فأننا نقوم بتفعيل الخاصية DNS Database وليس فقط dns forwarder .



فبمجرد تفعيل DNS Database فإنه تظهر لك قائمه باسم

DNS SERVER كما بالصورة ادناه

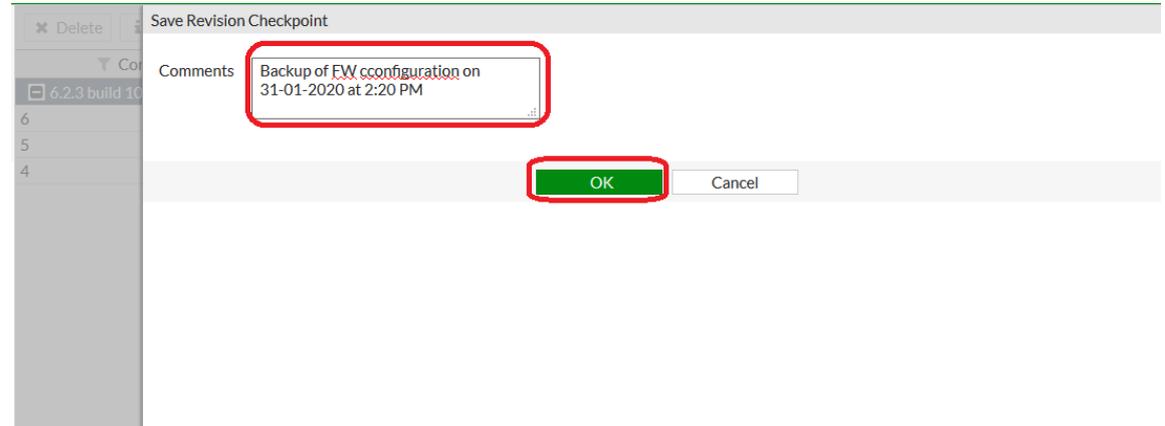
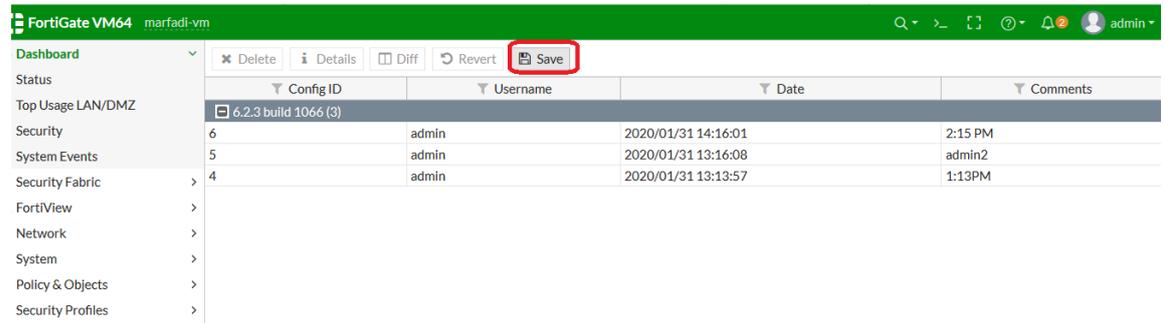
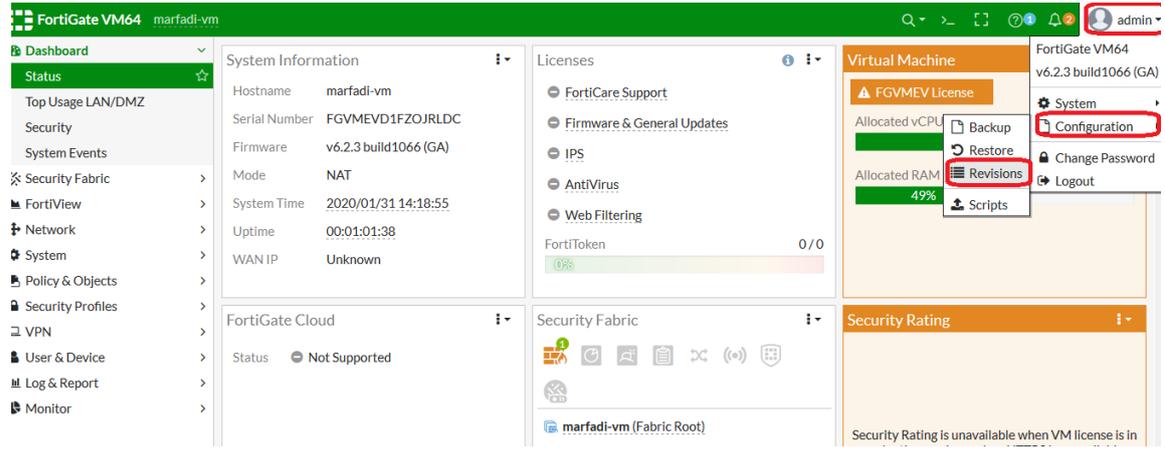


ما هو Revisions في الفورتى جيت :

هي عباره عن عمليه باك اب ولكن بدون ما اقوم بحفظ نسخه الباك اب (configuration file) في مكان معين ..

حيث بمجرد ما اعمل revisions كأنى عملت checkpoint او نسخه احتياطيه للإعدادات وحفظتها على نفس جهاز الفورتى جيت..

واستطيع لرجاها باي وقت ...



حيث كما بالصورة أعلاه تم عمل نسخه باك اب للإعدادات وتم حفظها على جهاز الفورتى جيت نفسه

...

الآن سنقوم بعملية الاستعادة لـ checkpoint كما بالصورة التالية

FortiGate VM64 marfadi-vm

Dashboard

Status

Top Usage LAN/DMZ

Security

System Events

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

User & Device

Log & Report

Monitor

Config ID	Username	Date	Comments
6.2.3 build 1066 (4)			
7	admin	2020/01/31 14:22:44	Backup of FW cconfiguration on 31-01-2020 at 2:20 PM
6	admin	2020/01/31 14:16:01	2:15 PM
5	admin	2020/01/31 13:16:08	admin2
4	admin	2020/01/31 13:13:57	1:13PM

FortiGate VM64 marfadi-vm

Dashboard

Status

Top Usage LAN/DMZ

Security

System Events

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

User & Device

Log & Report

Monitor

Config ID	Username	Date	Comments
6.2.3 build 1066 (4)			
7	admin	2020/01/31 14:22:44	Backup of FW cconfiguration on 31-01-2020 at 2:20 PM
6	admin	2020/01/31 14:16:01	2:15 PM
5	admin	2020/01/31 13:16:08	admin2
4	admin	2020/01/31 13:13:57	1:13PM

FortiGate VM64 marfadi-vm

Dashboard

Status

Top Usage LAN/DMZ

Security

System Events

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

User & Device

Log & Report

Config ID	Username	Date	Comments
6.2.3 build 1066 (4)			
7	admin	2020/01/31 14:22:44	Backup of F
6	admin	2020/01/31 14:16:01	2:15 PM
5	admin	2020/01/31 13:16:08	admin2
4	admin	2020/01/31 13:13:57	1:13PM

Confirm

Reverting to a system configuration revision will cause the device to reboot. Are you sure you want to continue?

OK Cancel

سيتم استرجاع النسخة بالاعدادات التي كانت عليها في تلك اللحظة بعد اعاده تشغيل الجهاز ..

والأفضل كما انك تأخذ نسخه باك اب العادية بالإضافة الى طريقة revisions بحيث لو تعطل جهاز الفورتى جيت فأنك لن تستطيع بإخذ باك اب من داخل الجهاز نفسه الخاصة ب revision ...

NTP server(Network time protocol)❖

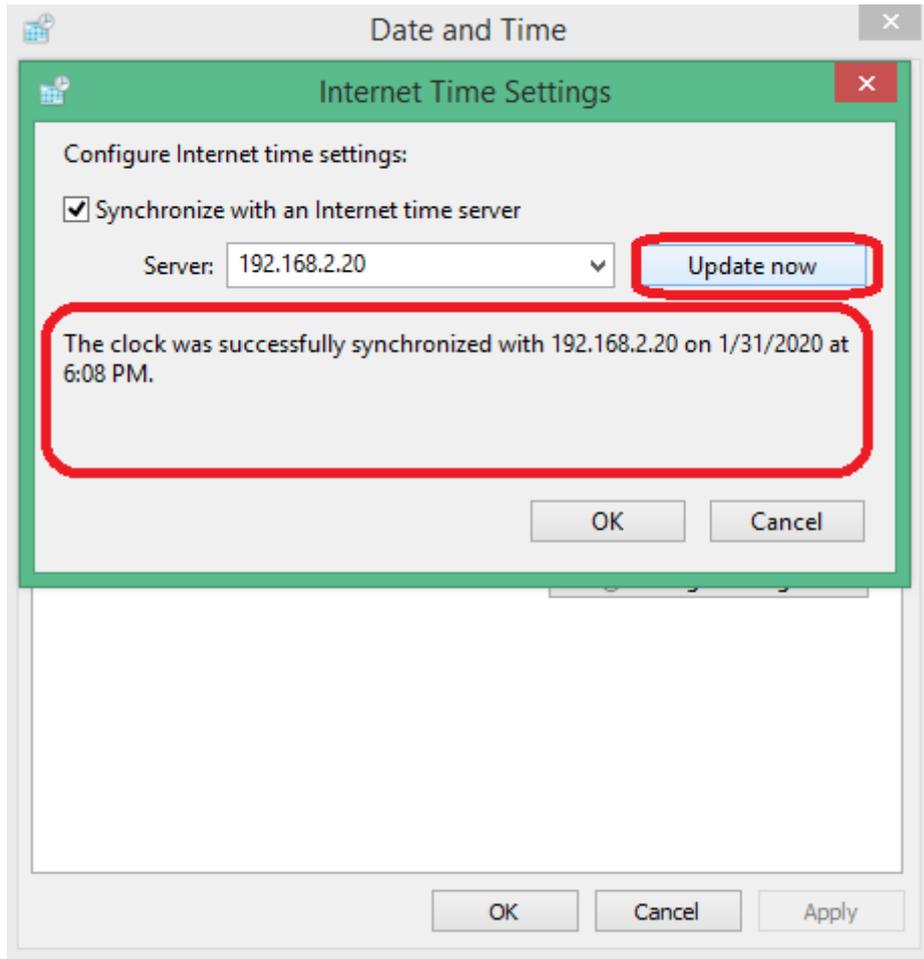
حيث سنجعل جهاز الفورتى جيت يعمل ك NTP server أي جعل الاجهزه تأخذ الوقت والتاريخ من جهاز الفورتى جيت ..

نقوم أولاً بالتأكد بأن الوقت والتاريخ والمنطقة الزمنية على الفورتى جيت مضبوطة حيث سيتم عمل مزامنه للوقت والتاريخ بين جهاز الفورتى وسيرفر fortiguard ntp server كل 60 دقيقة.

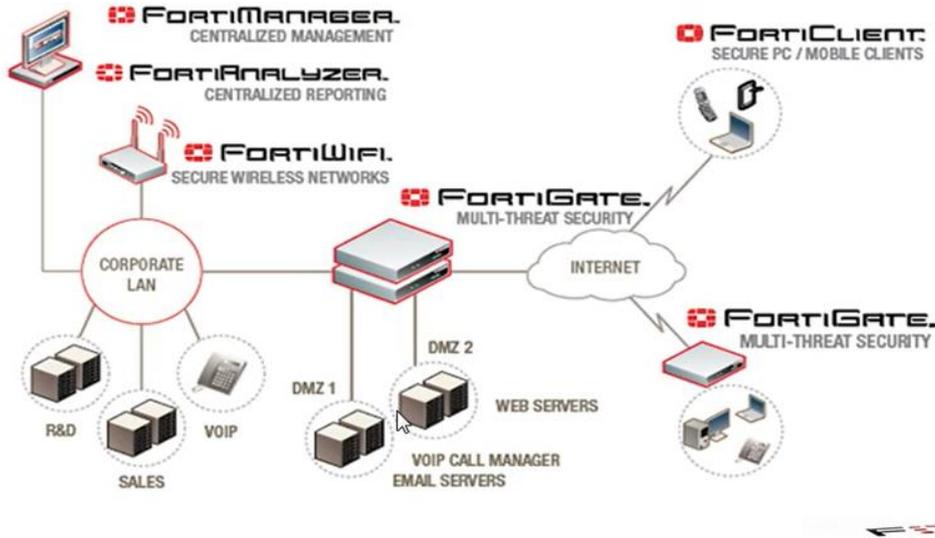
حيث سيتم تفعيل ntp server على المنفذ port1 وهو المنفذ الذي موصول عليه الشبكة المحلية للأجهزة بالشبكة وسيتم توزيع الوقت والتاريخ للأجهزة المتوصله بالمنفذ port1

تم الحفظ بالإعدادات كما بالصورة أعلاه ...

ثم من على اجهزه الشبكة نقوم بتعديل الاعدادات لديهم بأن ال ntp server هو عبره عن ايبي 192.168.2.20 وهو للفورتي جيت.



FortiGate Network Design



الفورتى جيت سوف يكون Edge الحافه (حافه الشبكة).

كما بالصورة أعلاه فأن الفورتى جيت يكون في المنتصف أي بين الانترنت والشبكة الداخلية لذا يسمى edge لأنه هو اللي يحمي الشبكة الداخليه من الهجمات القادمة من الانترنت..

هناك طرفين واحد امام الفورتى جيت(الانترنت) والطرف الاخر خلف الفورتى جيت وهو الشبكة الداخليه(LAN).

في اجهزه تكون في المنتصف تسمى DMZ او الشبكة المعزولة ..

حيث DMZ هي شبكة معزولة ومرتبطة بالفورتى جيت لكنها ليست LAN ولا هي internet هي ما بين الاثنين .

حيث DMZ مكان بيتم وضع السيرفرات التي على الشبكة المحلية ولكنك تريدها ان تكون متاحه للناس ان يصلوا اليها من برع الشبكة (أي من خلال الانترنت)

أساسيات فورتى جيت

حيث هي مرتبطة بـ lan لأنها موجودة أصلا في الشبكة المحلية ومرتبطة بالإنترنت لأن أي احد يريد ان يصل اليها عبر الانترنت ممكن أيضا ان يستفيد من خدمات هذه السيرفرات ..

مثل خدمه Web server او mail server .

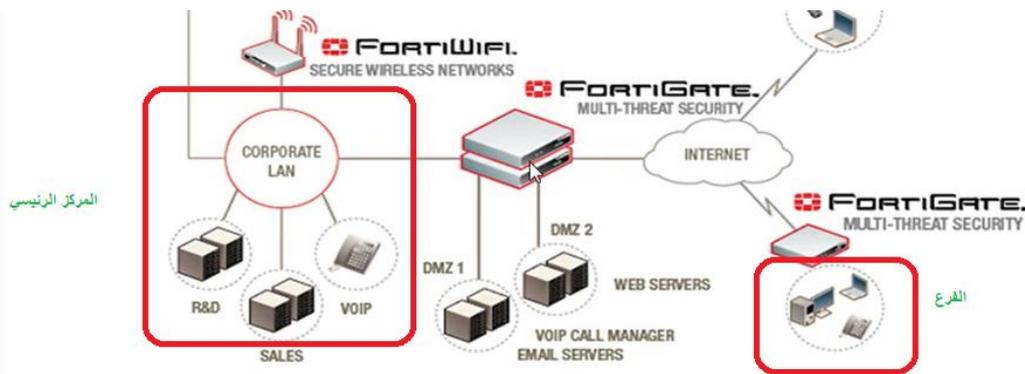
أي شي خلف الفورتى جيت يسمى LAN مهما كان اسمه سواء سيرفرات او اكسس بوينت او اجهزه عاديه او سويتشات .. الخ وجميعها سوف تكون تحت سيطرة الفورتى جيت .

ملاحظة:

السيرفرات التي ستوفرها على الانترنت مهما كانت الخدمة المقدمه يجب ان تكون خلف الفايرول وفي DMZ لكي تحمي تلك السيرفرات.

سيناريو اخر للتصميم الشبكة للربط بين الفروع :

نفترض لديك مركز رئيسي وفرع اخر في مكان اخر وكل فرع يوجد لديه انترنت وايضا يحتوي على جهز فورتى جيت .

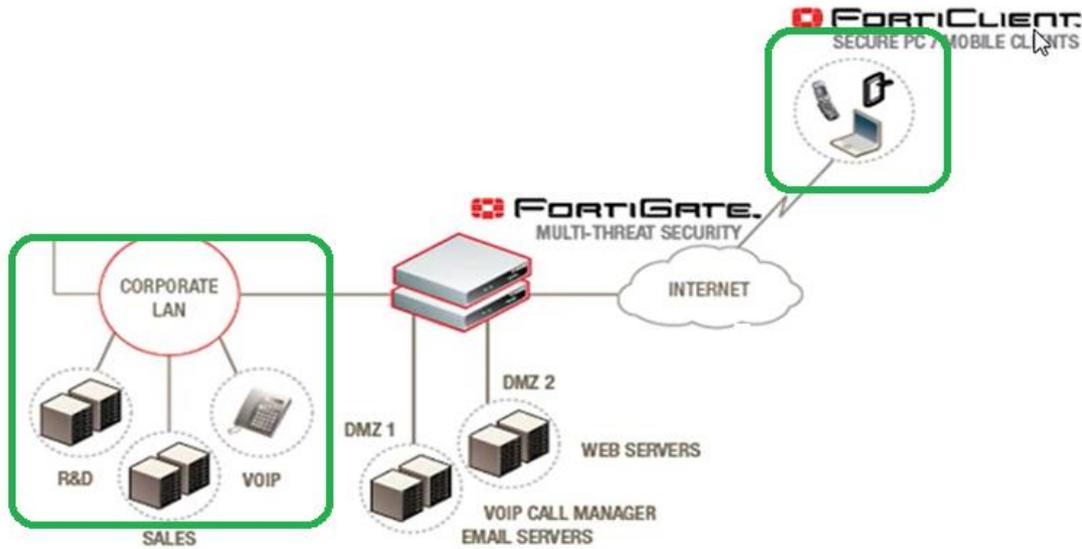


حيث الفرعين متوصلين مع بعض عبر الانترنت عن طريق VPN.

حيث يصبح الفرعين متوصلين مع بعض وكانهم شبكة واحده ..

أساسيات فورتيجيت

وأيضاً لو لدي جهاز موبايل او لابتوب موجود في دولة أخرى حيث تستطيع ان اتحكم بهذا الجهاز عبر الفورتيجيت الموجود بالمركز الرئيسي عبر برنامج يسمى كلاينت ايند بوينت يتم نزوله على الابتوب او الموبايل..



Advice administration

طرق التعامل مع جهاز الفورتيجيت والتحكم فيه من اعدادات وغيرها ..

1- Web GUI(http,https) :يجب ان يكون لديك متصفح انترنت تدخل من خلاله بالايبي التابع

للفورتيجيت.

2- CLI(console,Telnet,ssh,GUI widget) :هنا يتم التعامل مع جهاز الفورتيجيت بالاوامر

command line باحدى الطرق التالية :

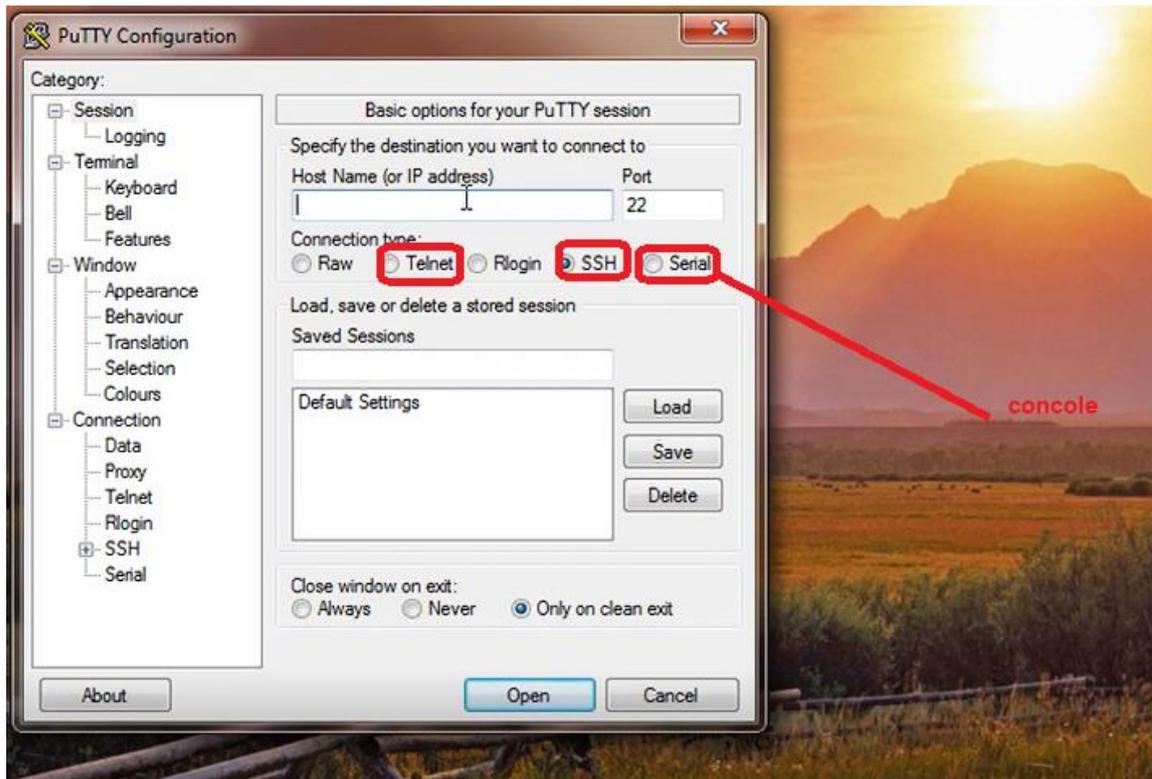
A – console : توصيل كيبيل كونسول للابتوب وبواسطة برنامج مثل putty وتوصيل للفورتيجيت بدون

ماحتاج الى ايبي الفورتيجيت (حتى لو مش عارف الايبي للجهاز يتم استخدام هذه الطريقة).



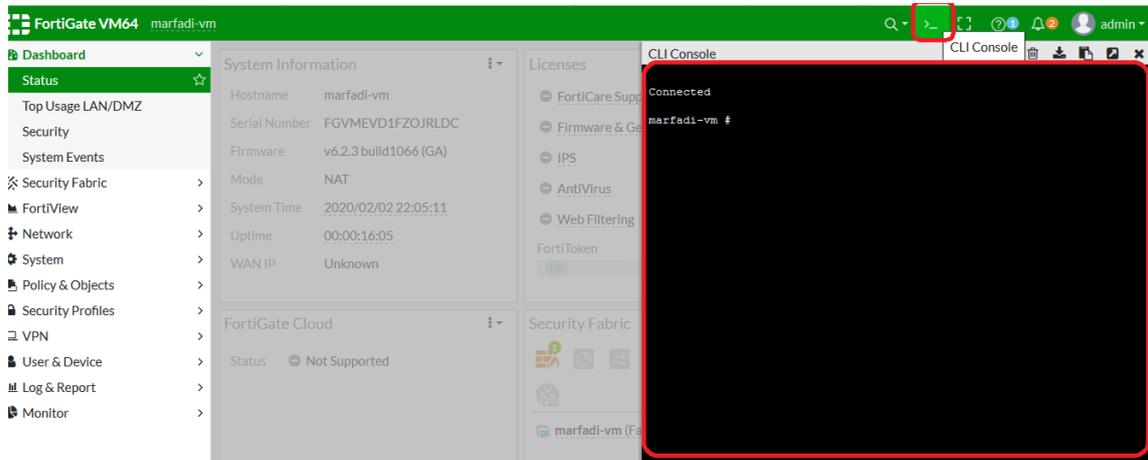
B-telnet: يتم الدخول الى الفورتى جيت عبر برنامج مثل putty بواسطة ايبى الفورتى جيت من أي مكان بالشبكة .

C-SSH: يتم الدخول الى الفورتى جيت عبر برنامج مثل putty بواسطة ايبى الفورتى جيت من أي مكان بالشبكة حيث يعتبر نفس الtelnet ولكنة اكثر امانا لأنه مشفر .

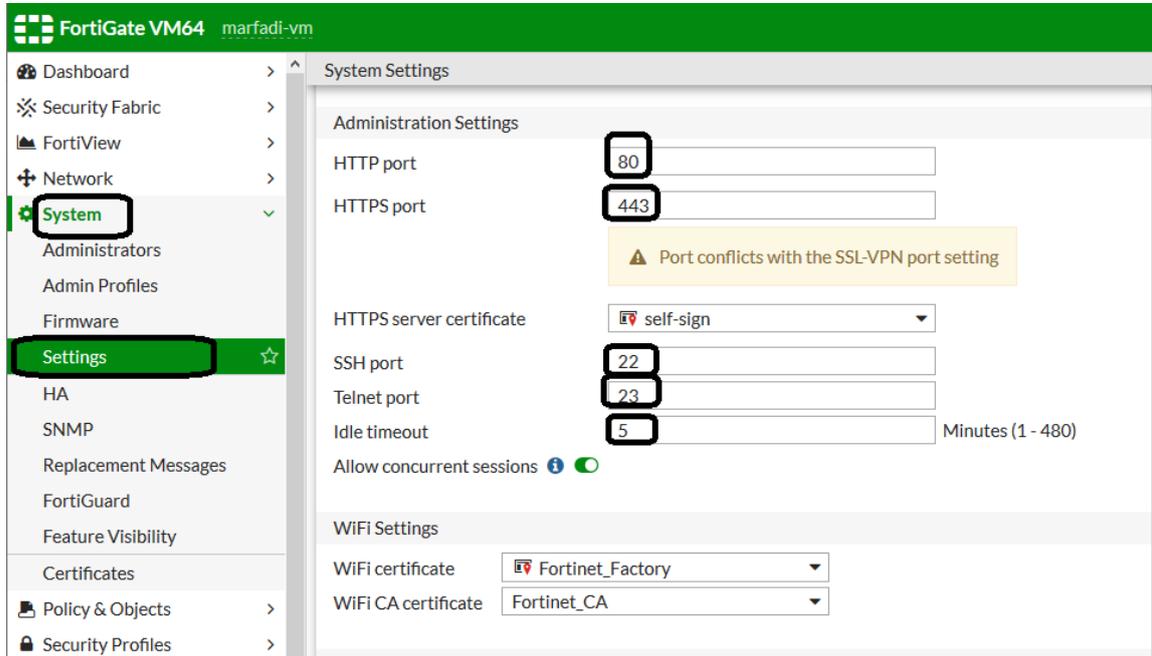




ملاحظة: لا يمكنك الوصول الى الفورتى جيت سواء ssh او telnet عبر برنامج ال putty الا بعد عمل الامر
Set allowaccess ssh telnet
لكرت الشبكة الخاص بالفورتى المراد الوصول اليه ..
GUI Widget – D :شاشه سوداء مثل CMD يتم الوصول اليها من GUI كما بالصورة ادناه .



❖ طريقة رفع مستوى الأمان عند الوصول الى جهاز الفورتى جيت ..



حيث البورتات الافتراضية حسب الصورة أعلاه فالأفضل تغيير ارقام البورتات مثلا https:443 ويتم تحويله الى 4433 مثلا

ولذا عند الدخول الى الفورتى جيت يجب ان تقوم بكتابه البورت كما التالي:

192.168.2.20:4433

وهكذا ..

خيل idle timeout =5: هذه الخاصية بتجر الفورتى جيت على عمل logout بعد مرور 5 دقائق وبعدها تجر اليوزر بإدخال اليوزرنيم والباسورد مره أخرى كنوع من الأمان .

Device administration

Administrator: الأشخاص الذي لهم صلاحيات للدخول للفورتى جيت والتعامل معه وعمل اداره

للجهاز وأنواع ال administrator هي:

أساسيات فورتى جيت

- 1 Full admin (super admin): هو الذي له صلاحيات على كل الفورتى جيت بدون أي تقييد
- 2 Prof admin : هو نوع من administrator الذي لديه صلاحيات عالية جدا ضمن بيئته اسمها (SVD) single virtual domain
- 3 Custom profile: الوصول الى صلاحيات محددته حيث أقوم بتحديدتها انا له.



Admin profile : هي الاعدادت التي أقوم بإعدادها لأحدى administrator أعلاه لكي يصل اليها ..

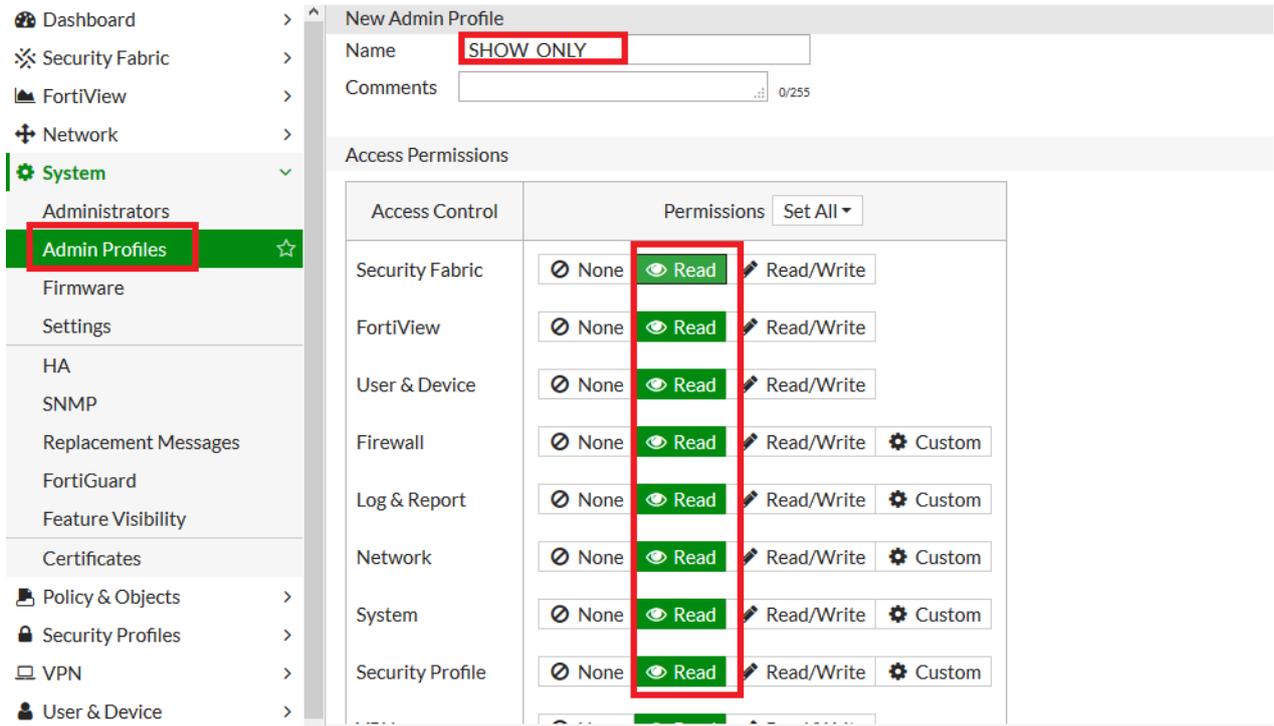
Permission : هي الصلاحيات (read,write,none) التي سيتم تحديدها للadministrator .

طريقة انشاء administrator جديد :

The screenshot shows the 'New Administrator' configuration page in the FortiGate web interface. The left sidebar has 'Administrators' highlighted. The main form fields are: Username: 'hosam', Type: 'Local User', Password: masked with dots, Confirm Password: masked with dots, Comments: 'Write a comment...', Administrator Profile: 'super_admin' (selected from a dropdown menu), Email Address: empty. There are 'OK' and 'Cancel' buttons at the bottom.

اسم administrator هو hosam ونوعه local user وتم تحديد الباسورد له وأيضا يجب ان تحدد administrator profile لهذا اليوزر بإحدى الأنواع كما ذكرناها أعلاه ..

حيث لو تريد ان تقوم بتخصيص custom profile فيجب عليك انشاء أولا custom profile وذلك بحسب الصورة ادناه



حيث اسم البروفايل هو show_only وله صلاحيات القراءة فقط على كل الأشياء (الأشياء) التي سوف تتعامل معها كما بالصورة أعلاه ..

حيث صلاحيه ال none معناها بأن هذه الشاشة لن تظهر نهائيا لليوزر.

و read: للقراءة فقط ولا يمكنك التعديل عليها ،

و read/write: يمكنك التعديل على الشاشات ..

Profile Name	Comments	Ref.
SHOW_ONLY		0
prof_admin		0
super_admin		2

يوجد لدينا الان 3 بروفيلات كما بالصورة اعلاه ...

الآن يمكننا تحديد البروفايل المناسب مثلا show_only لليوزر hosam كما بالصورة ادناه

New Administrator

Username: hosam

Type: Local User

Password: [Redacted]

Confirm Password: [Redacted]

Comments: Write a comment... 0/255

Administrator Profile: SHOW_ONLY

Email Address: [Redacted]

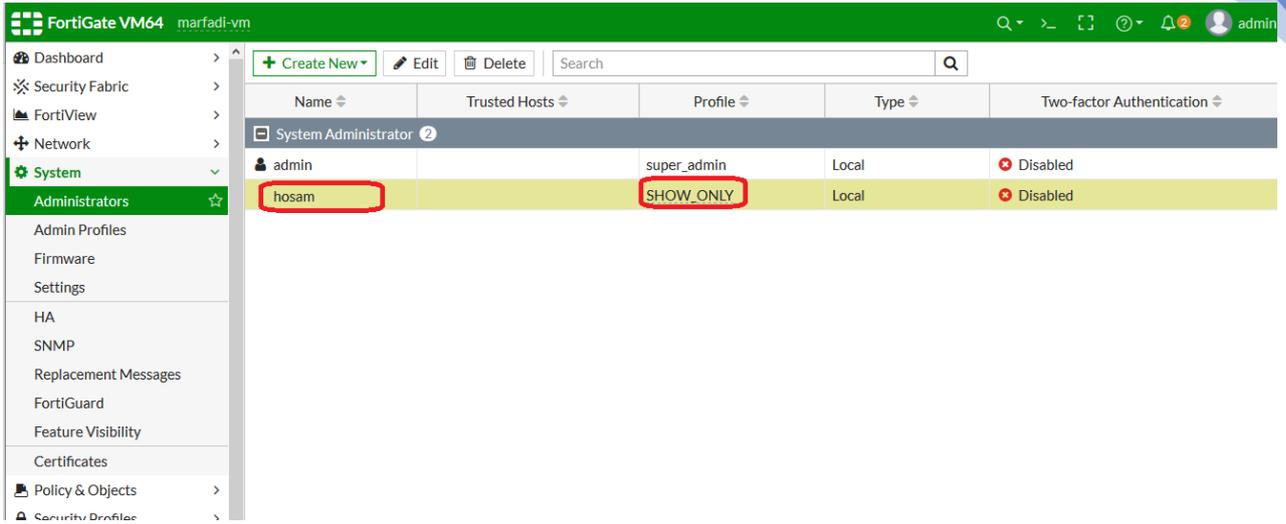
SMS

Two-factor Authentication

Restrict login to trusted hosts

Restrict admin to guest account provisioning only

OK Cancel

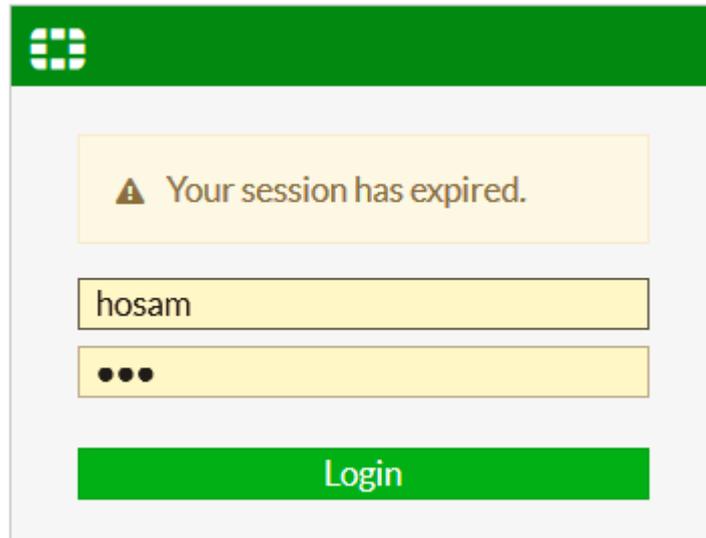


The screenshot shows the FortiGate VM64 administrators page. The left sidebar contains navigation options: Dashboard, Security Fabric, FortiView, Network, System, Administrators (selected), Admin Profiles, Firmware, Settings, HA, SNMP, Replacement Messages, FortiGuard, Feature Visibility, Certificates, Policy & Objects, and Security Profiles. The main content area displays a table of administrators. The table has columns for Name, Trusted Hosts, Profile, Type, and Two-factor Authentication. Two administrators are listed: 'admin' with profile 'super_admin' and 'hosam' with profile 'SHOW_ONLY'. Both are of type 'Local' and have two-factor authentication 'Disabled'. The 'hosam' row is highlighted in yellow, and both the name 'hosam' and the profile 'SHOW_ONLY' are circled in red.

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
admin		super_admin	Local	Disabled
hosam		SHOW_ONLY	Local	Disabled

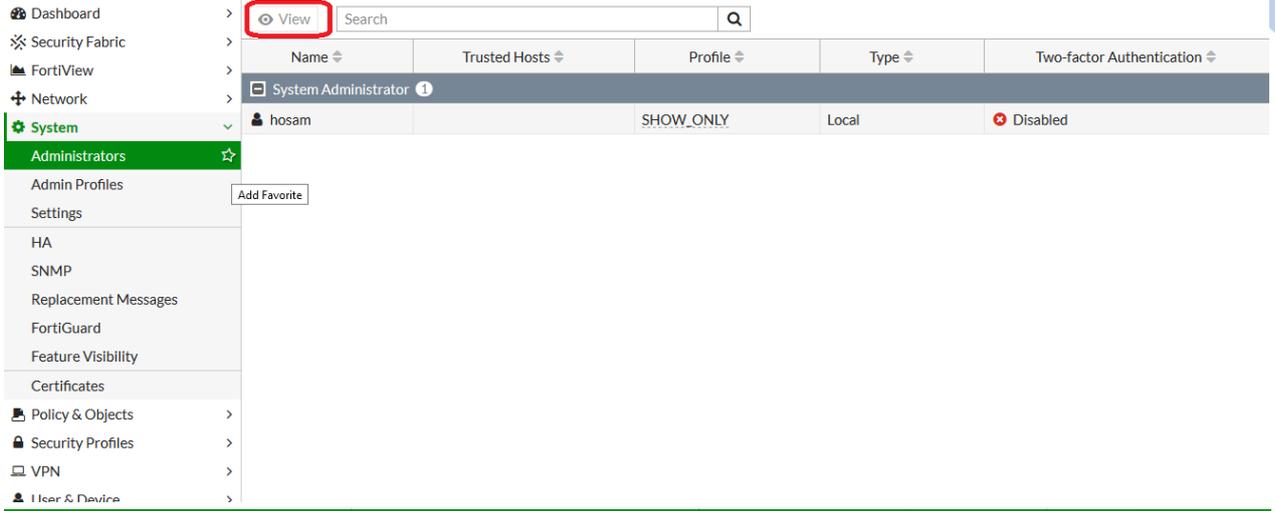
كما بالصورة أعلاه يوجد لدينا 2 يوزرات ..

الآن سوف ندخل للفورتى جيت من خلال اليوزر الذي أنشأناه سابقا



The screenshot shows the FortiGate login page. At the top, there is a green header with the FortiGate logo. Below the header, there is a yellow warning box with a triangle icon and the text 'Your session has expired.'. Underneath the warning box, there are two input fields: the first contains the username 'hosam' and the second contains three dots representing a password. At the bottom of the login area, there is a green button labeled 'Login'.

أساسيات فورتى جيت



Dashboard > View Search

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator 1				
hosam		SHOW_ONLY	Local	Disabled

Administrators

Admin Profiles

Settings

HA

SNMP

Replacement Messages

FortiGuard

Feature Visibility

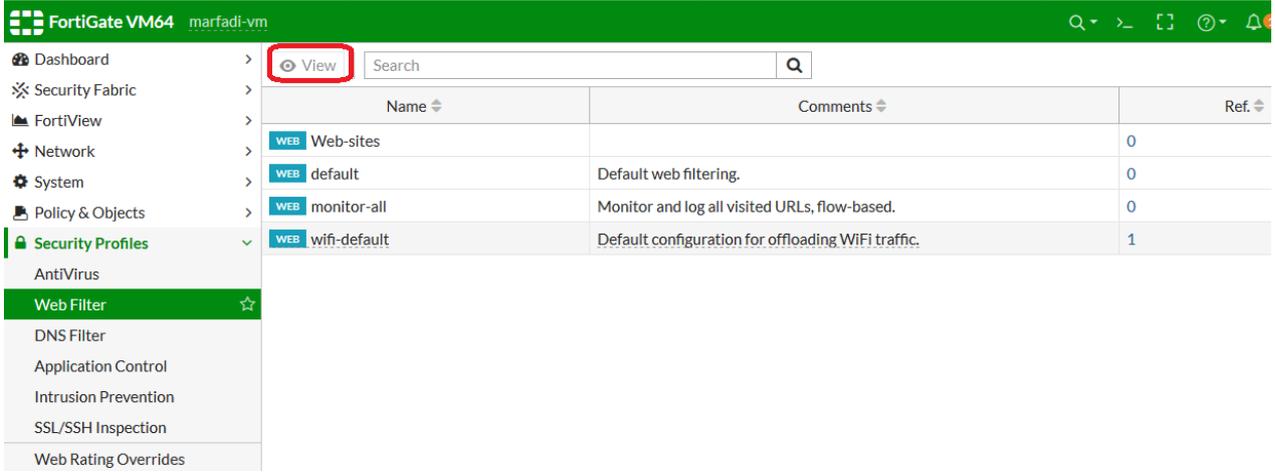
Certificates

Policy & Objects

Security Profiles

VPN

User & Device



Dashboard > View Search

Name	Comments	Ref.
WEB Web-sites		0
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WiFi traffic.	1

Web Filter

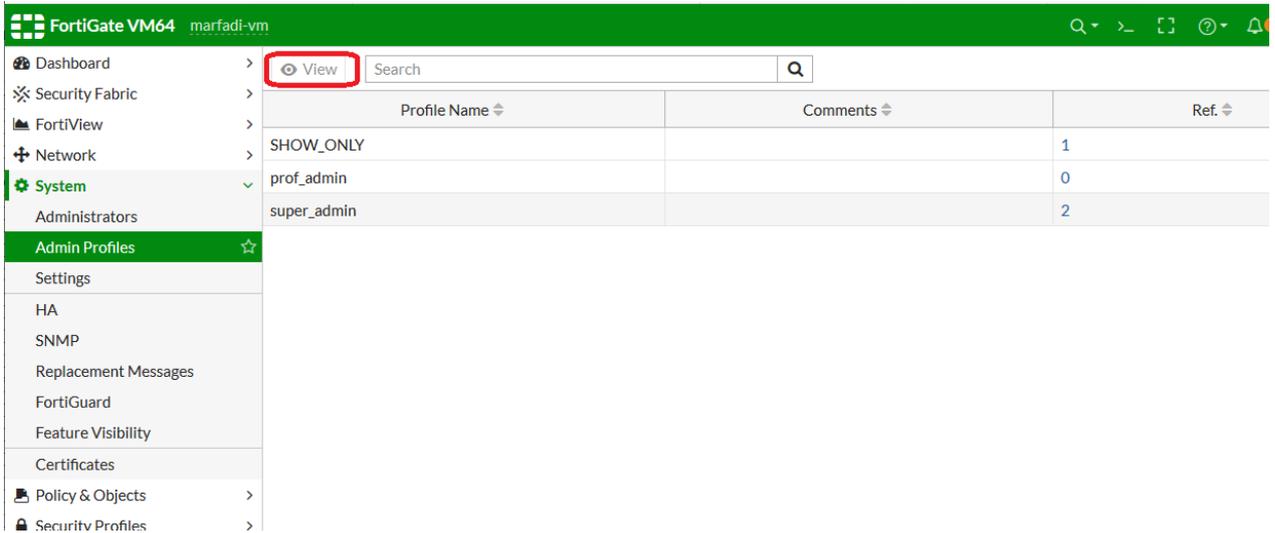
DNS Filter

Application Control

Intrusion Prevention

SSL/SSH Inspection

Web Rating Overrides



Dashboard > View Search

Profile Name	Comments	Ref.
SHOW_ONLY		1
prof_admin		0
super_admin		2

Admin Profiles

Settings

HA

SNMP

Replacement Messages

FortiGuard

Feature Visibility

Certificates

Policy & Objects

Security Profiles

ملاحظ بان الشاشات بهذا اليوزر هي read only ولا يمكن لهذا اليوزر التعديل ...

سوف نقوم بإنشاء بروفائل جديد باسم Yasser-it حيث تم إخفاء عنه بعض الشاشات مثل security fabric و fortiView ،

كما تم تحديد صلاحيةه read/write بعض الشاشات وتخصيص بعضها كما بالظهور ادناه :

- Dashboard >
- Security Fabric >
- FortiView >
- Network >
- System >
- Administrators >
- Admin Profiles ☆
- Firmware >
- Settings >
- HA >
- SNMP >
- Replacement Messages >
- FortiGuard >
- Feature Visibility >
- Certificates >
- Policy & Objects >
- Security Profiles >
- VPN >
- User & Device >
- Log & Report >
- Monitor >

New Admin Profile

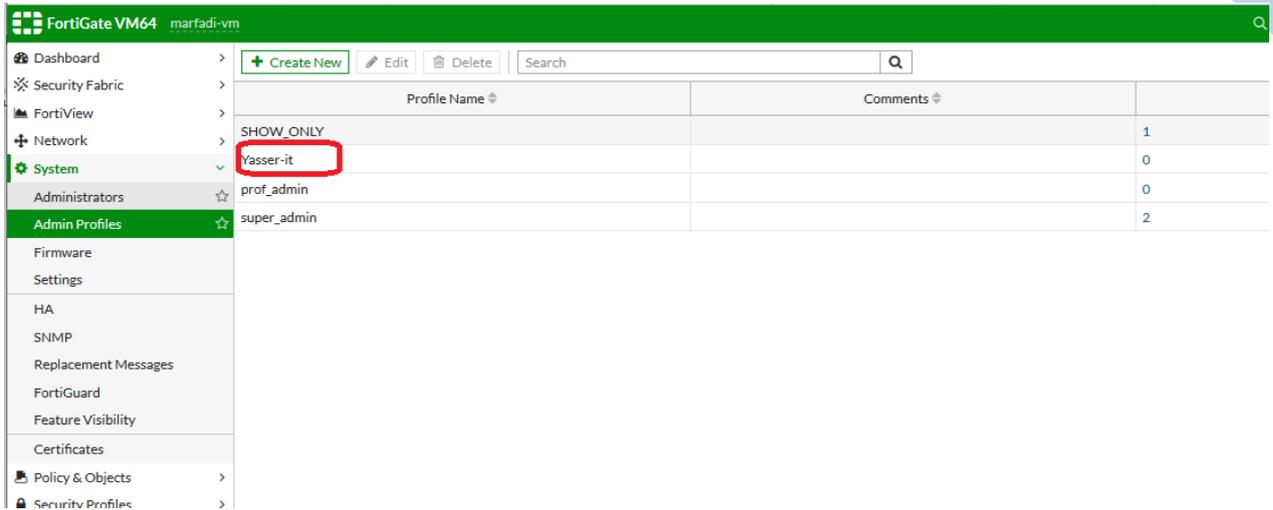
Name

Comments 0/255

Access Permissions

Access Control	Permissions Set All ▾
Security Fabric	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
FortiView	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Firewall	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Log & Report	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input checked="" type="radio"/> Custom
Antivirus	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
IPS	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Web Filter	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write

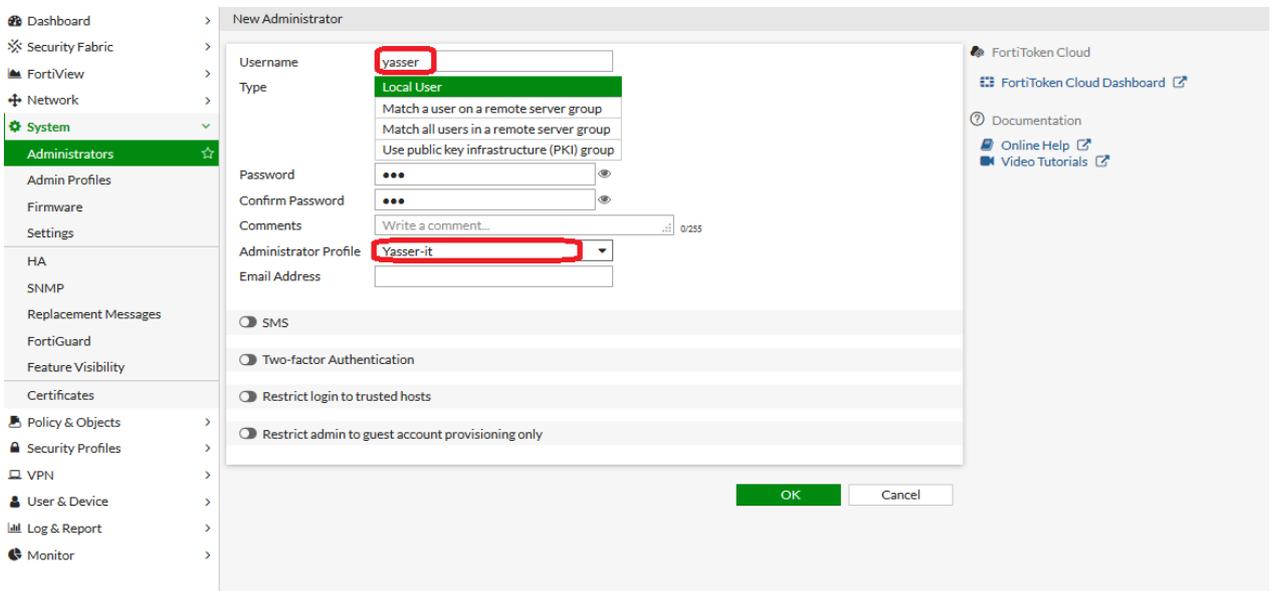
Antivirus	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
IPS	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Web Filter	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Email Filter	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Data Loss Prevention	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Application Control	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
ICAP	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
VoIP	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Web Application Firewall	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
DNS Filter	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Endpoint Control	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
VPN	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WiFi & Switch	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write



FortiGate VM64 marfadi-vm

Profile Name	Comments	
SHOW_ONLY		1
Yasser-it		0
prof_admin		0
super_admin		2

الآن سنقوم بإنشاء يوزر باسم Yasser مثلا ونحدد له البروفايل Yasser-it .



New Administrator

Username:

Type: Local User

Match a user on a remote server group

Match all users in a remote server group

Use public key infrastructure (PKI) group

Password:

Confirm Password:

Comments:

Administrator Profile:

Email Address:

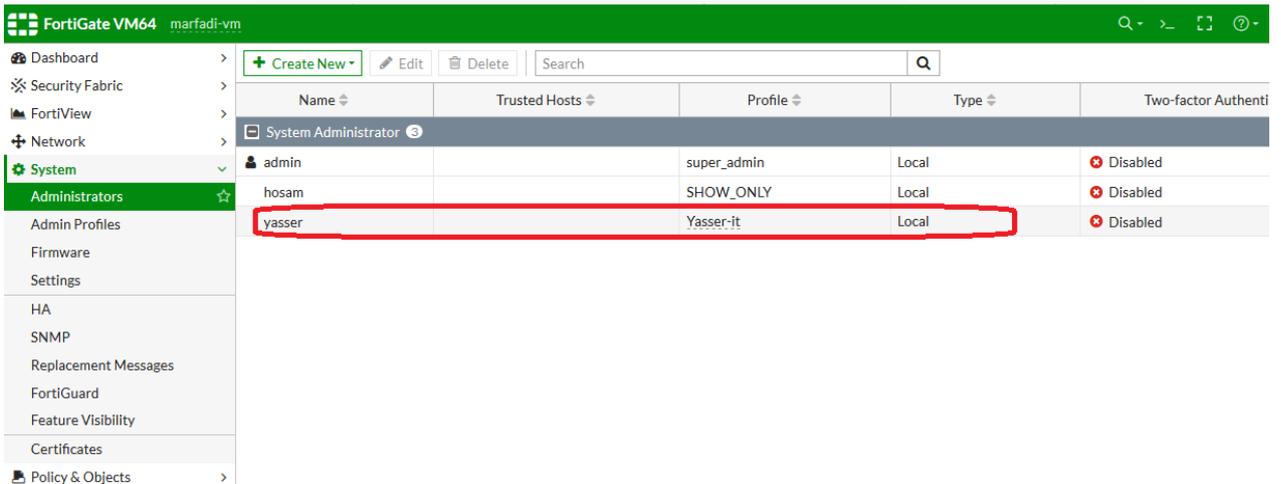
SMS

Two-factor Authentication

Restrict login to trusted hosts

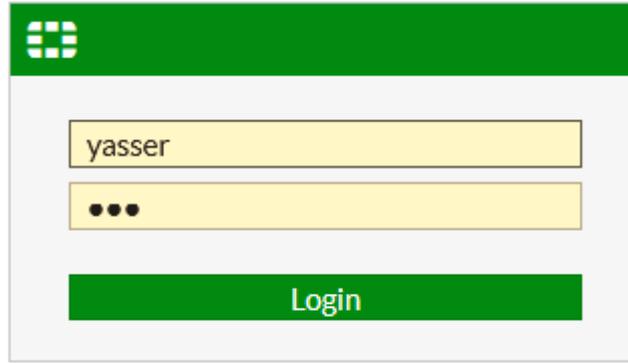
Restrict admin to guest account provisioning only

OK Cancel



FortiGate VM64 marfadi-vm

Name	Trusted Hosts	Profile	Type	Two-factor Authent
System Administrator				
admin		super_admin	Local	Disabled
hosam		SHOW_ONLY	Local	Disabled
yasser		Yasser-it	Local	Disabled

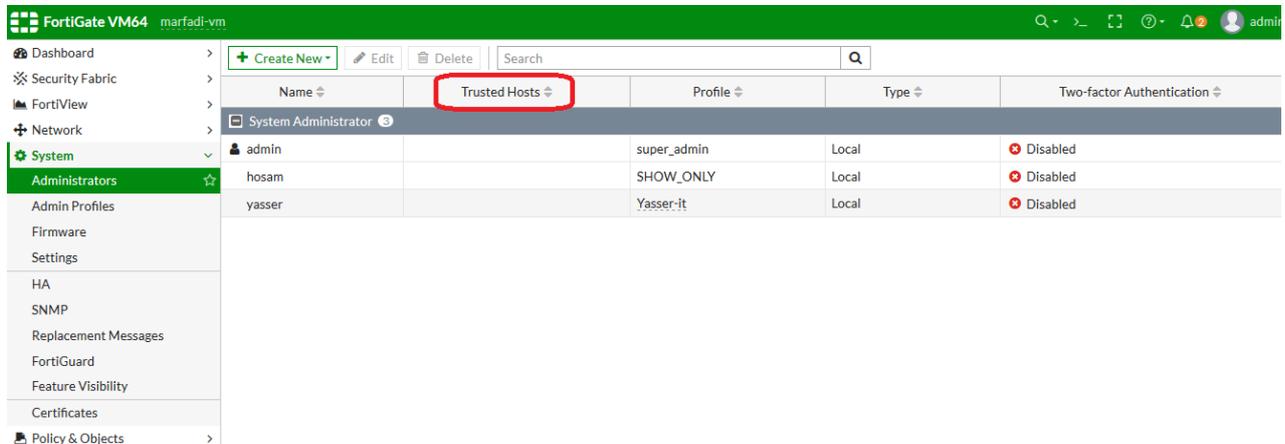


سيتم الدخول لهذا اليوزر بالصلاحيات والشاشات التي تم تحديدها بالبروفيل Yasser-it .

❖ ملاحظة :

ممکن تعطي يوزر معين بأن يكون له صلاحيات لـ vpn connection بالشركة فقط فلذا ليس له داعي ان يفتح كل الصلاحيات ويعدل عليها وبهذا انارفعت مستوى الأمان وقمت بعمل تخصيص للأعمال ..

➤ ما هو Trusted hosts :



Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator				
admin		super_admin	Local	Disabled
hosam		SHOW_ONLY	Local	Disabled
yasser		Yasser-it	Local	Disabled

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Administrators

Edit Administrator

Username: yasser [Change Password]

Type: Local User

Comments: Write a comment... 0/255

Administrator Profile: Yasser-it

Email Address: [Empty]

Restrict login to trusted hosts

Trusted Host 1: 192.168.2.140/32

Restrict admin to guest account provisioning only

OK Cancel

هذا الخيار معناه قم بتقييد اليوزر المسمى Yasser بأنه لا يمكنه الدخول الى الفورتى جيت الا عن طريق اجهزه معينه (جهز موثوق فيه) مثلا احدد جهز معين عندي بالشبكة فقط وليكن 255.255.255.255/192.168.2.140 حيث لو حاول هذا اليوزر بالدخول الى الفورتى جيت من أي جهز اخر فإنه لن يستطيع ذلك .

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator				
admin		super_admin	Local	Disabled
hosam		SHOW_ONLY	Local	Disabled
yasser	192.168.2.140/32	Yasser-it	Local	Disabled

أي ان اليوزر Yasser لن يستطيع الدخول الى الفورتى جيت إلا من الجهز 192.168.2.140 حتى وان كان لديه اليوزر نيم والباسورد ..

قمنا بالدخول الى الفورتى جيت من خلال جهز الكلاينت 192.168.2.140

فلو قمت بتغيير ايبي الجهاز الى 192.168.2.160 بدلا عن 192.168.2.140 فان اليوزر Yasser لا يمكنه الدخول الى الفورتى جيت بالرغم من ان اليوزر نيم والباسورد صحيحين ..

Interface ip address ❖

للتعامل مع ال interfaces التابعة للفورتني جيت كما بالصورة التالية

حيث يظهر لك كل ال interfaces لجهاز الفورتني جيت

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
port1	Physical Interface		192.168.2.20/255.255.255.0	PING HTTPS SSH HTTP TELNET			1
port10	Physical Interface		0.0.0.0/0.0.0.0				0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
port9	Physical Interface		0.0.0.0/0.0.0.0				0
WAN (port2)	Physical Interface		192.168.1.60/255.255.255.0	PING HTTPS HTTP			2
WAN2 (port3)	Physical Interface		192.168.35.60/255.255.255.0	PING HTTPS HTTP			0

حيث بتوضح اسم ال interfaces ونوعه والايي وطريقة الوصول اليه (administrative access) ...

حيث في ال vm يتم تسميه ال interfaces ب port ويمكن التعديل على تلك الأسماء كما تريد ،

اما بجهاز الفورتني الحقيقي يكون اسمه internal او wan1 او wan2 او dmz .

فعندما تريد ضبط اعدادات interface معين وليكن port1 فأنا ننقر عليه نقرتين فتكون كما بالشكل

التالي

أساسيات فورتى جيت

The screenshot shows the 'Edit Interface' configuration for 'port1'. Key settings include:

- Name: port1
- Alias: (empty)
- Type: Physical Interface
- Role: Undefined
- Addressing mode: Manual
- IP/Netmask: 192.168.2.20/255.255.255.0
- Administrative access:
 - IPv4: HTTPS, HTTP, PING, FMG-Access, SSH, SNMP, TELNET, FTM, Security Fabric Connection
 - Receive LLDP: Use VDOM Setting, Enable, Disable
 - Transmit LLDP: Use VDOM Setting, Enable, Disable
- DHCP Server: Disabled
- Device detection: Disabled

اسم الinterface هو port1 ويمكن عمل له alias باي اسم تريد ان تعبر عن هذا المنفذ مثلا lan1 ونحدد طريقة تحديد (تعيين) الايبي للinterface هل manual or dhcp حيث يفضل في الlan يكون manual اما للwan يكون dhcp

وملاحظ بأن طريقة الوصول كما بالصورة أعلاه لهذا interface عن طريق ping http https

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
LAN1 (port1)	Physical Interface		192.168.2.20/255.255.255.0	PING HTTPS SSH HTTP TELNET			1
port10	Physical Interface		0.0.0.0/0.0.0.0				0
port4	Physical Interface		0.0.0.0/0.0.0.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0

اما خيلر secondary ip address فهو في حالة تريد إعطاء الinterface اكثر من ايبي حيث يمكنك الوصول اليه بأي ايبي منهم..

أساسيات فورتى جيت

Edit Interface

Name: LAN1 (port1)
Alias: LAN1
Type: Physical Interface
Role: Undefined

Address

Addressing mode: Manual DHCP
IP/Netmask: 192.168.2.20/255.255.255.0
Secondary IP address:

+ Create New Edit Delete Search

IP/Netmask	Administrative access
No results	

Administrative access

IPv4

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input checked="" type="checkbox"/> TELNET	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting
<input type="checkbox"/> Security Fabric		

FortiGate: marfadi-vm
Status: Up
MAC address: 00:0c:29:1a:58:9c
Documentation: Online Help, Video Tutorials

Edit Secondary IP

IP/Netmask: 10.0.0.20/255.255.255.0

Administrative Access

<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input type="checkbox"/> FMG-Access	<input type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input type="checkbox"/> TELNET	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting
<input checked="" type="checkbox"/> Security Fabric Connection		

OK Cancel

FortiGate VM64 marfadi-vm

Dashboard >
Security Fabric >
FortiView >
Network >
Interfaces ☆
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System >
Policy & Objects >
Security Profiles >
VPN >
User & Device >

Edit Interface

Name LAN1 (port1)
Alias LAN1
Type Physical Interface
Role Undefined

Address

Addressing mode Manual DHCP
IP/Netmask 192.168.2.20/255.255.255.0
Secondary IP address

IP/Netmask	Administrative access
10.0.0.20/255.255.255.0	PING, HTTP, HTTPS

Administrative access

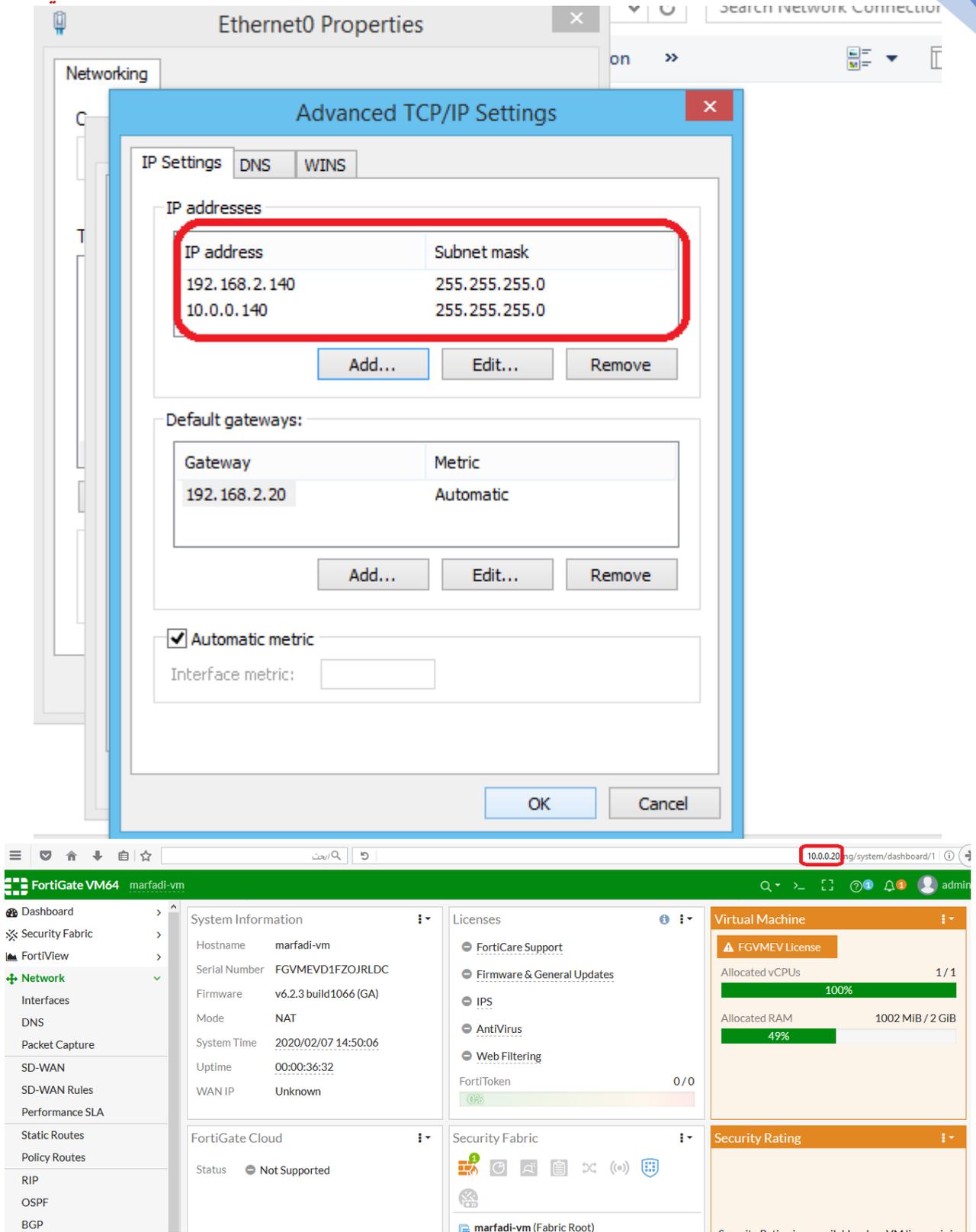
IPv4 HTTPS HTTP PING
 FMG-Access SSH SNMP
 TELNET FTM RADIUS Accounting

حيث اصبح لدينا 2 ابيي للinterface المسى lan1 واهما

192.168.2.20 و 10.0.0.20

حيث نقوم بالدخول على جهاز الكلاينت 192.168.2.140 ونظيف لكرت الشبكة ابيي إضافي من نفس

الرينج مثلا 10.0.0.140



كما بالصورة أعلاه تمكنا بالدخول الى الفورتى عبر الايبي 10.0.0.20 طبيعي جدا ..

أساسيات فورتني جيت

اما في ال interface الذي سنجعله ك wan فأننا سنجعله يأخذ الايبي من dhcp server وهو الروتر (المودم) لأننا ليس بحاجة ان ادخل الى الفورتني جيت من خلاله في الواقع لذا ليس من الضروري ان نقوم بجعله static ip

The screenshot shows the configuration for the WAN (port2) interface. Key settings include:

- Name: WAN (port2)
- Alias: WAN
- Type: Physical Interface
- Role: WAN
- Estimated bandwidth: 0 kbps Upstream and 0 kbps Downstream
- Addressing mode: Manual DHCP
- Retrieve default gateway from server: Enabled
- Distance: 5
- Override internal DNS: Enabled
- Administrative access (IPv4):
 - HTTPS: Enabled
 - HTTP: Enabled
 - PING: Enabled
 - FMG-Access: Disabled
 - SSH: Disabled
 - SNMP: Disabled
 - FTM: Disabled
 - RADIUS Accounting: Disabled
 - Security Fabric Connection: Disabled
- Receive LLDP: Use VDOM Setting, Enable, Disable
- Transmit LLDP: Use VDOM Setting, Enable, Disable

تم تحديد بأن تعيين الايبي للبورت port2 سيكون من خلال dhcp server

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ra
port10	Physical Interface		0.0.0.0/0.0.0.0	TELNET		
port4	Physical Interface		0.0.0.0/0.0.0.0			
port5	Physical Interface		0.0.0.0/0.0.0.0			
port6	Physical Interface		0.0.0.0/0.0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0.0			
port9	Physical Interface		0.0.0.0/0.0.0.0			
WAN (port2)	Physical Interface		192.168.1.102/255.255.255.0	PING HTTPS HTTP		
WAN2 (port3)	Physical Interface		192.168.35.60/255.255.255.0	PING HTTPS HTTP		

كما بالصورة أعلاه تم اخذ الايبي 192.168.1.102 من الروتر (المودم) الخاص بي في البيت .. ملاحظة: في حالة dhcp فإنه لا يحتوي على خاصية secondary ip address .

❖ Static route(default gateway)(static gateway)

طريقة لجعل جهاز الفورتى جيت يطلع الى الانترنت (يحصل على الانترنت).

لماذا نريد ان يحصل جهاز الفورتى جيت على الانترنت :

1- لأن الفورتى جيت هو البوابة للشبكة الداخليه فلو كان الفورتى جيت غير قادر على الوصول الى الانترنت فأکید جميع الاجهزه بالشبكة الداخليه لن يوصلوا الى الانترنت .

3- جهاز الفورتى جيت يجب ان يكون واصل له انترنت لكي يحصل على التحديث من الفورتى جلد فبدون انترنت لا يمكن للفورتى جيت تجديد الايسزولا يستطيع تحديث قواعد بيانات كل من الAV وIPS وWeb filtering و... الخ

الفكره في static route هي عمليه توجيه البيانات من الشبكة الداخليه (lan) الى الانترنت ...

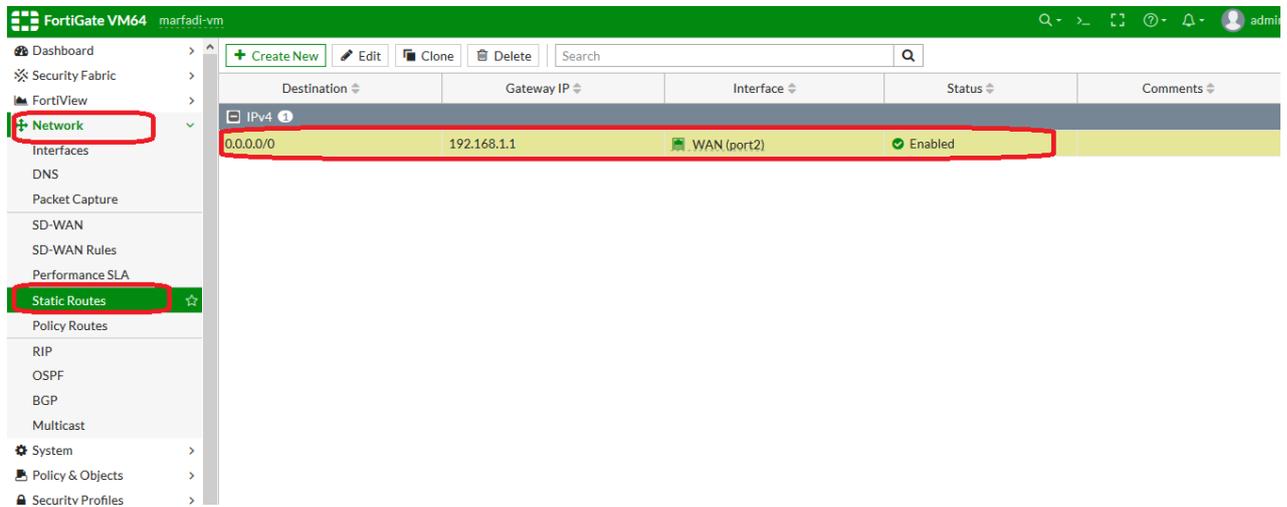
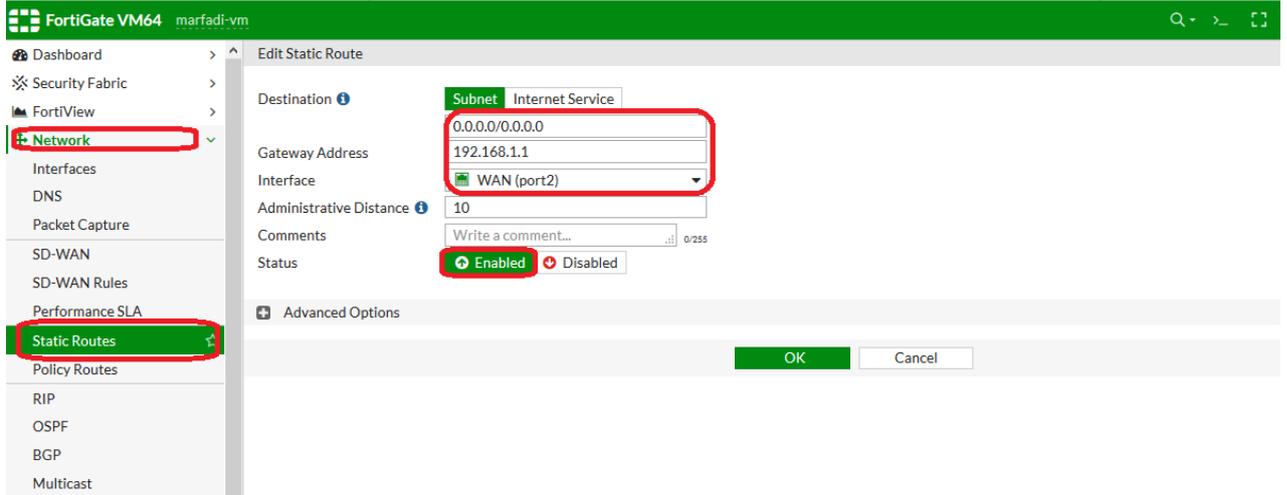
أولا نقوم بتعيين ايى لكرت الwan من نفس رينج الروتر او نجعله يأخذ من DHCP .

The screenshot shows the 'Edit Interface' configuration page for 'WAN (port2)'. The interface is a physical interface with a role of 'WAN'. The addressing mode is set to 'Manual' with an IP address of 192.168.1.60 and a netmask of 255.255.255.0. Administrative access is configured with IPv4 enabled for HTTPS, HTTP, PING, and Security Fabric Connection. LLDP settings are also visible.

ثم نتأكد فقط من اعدادات الـ dns للفورتيجيت بالرغم ان بشكل افتراضي تكون مفعلة fortiguard

DNS

The screenshot shows the 'DNS Settings' configuration page. The 'DNS Servers' are set to 'Use FortiGuard Servers'. The primary DNS server is 208.91.112.53 and the secondary is 208.91.112.52. The 'DNS over TLS' setting is set to 'Disable'. An 'Apply' button is visible at the bottom right.



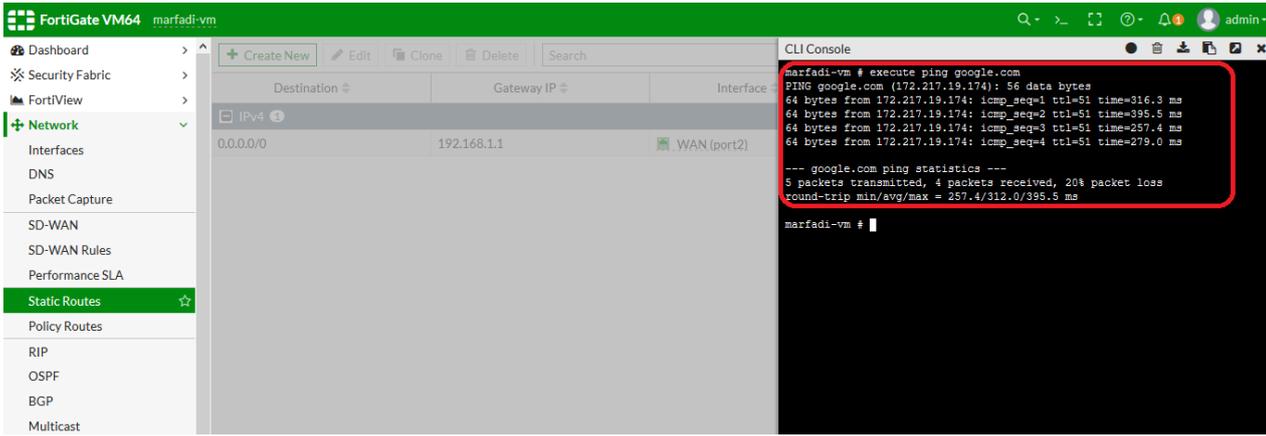
حيث قمنا بإنشاء static route

حيث قمنا بعمل التالي :

لو أي شخص يريد الوصول الى ال 0.0.0.0/0.0.0.0 الذي هو الانترنت (شبكة الانترنت) عن طريق المنفذ wan(port2) خرجني عبر الجيتواي 192.168.1.1 الذي هو ايبي الروتر(المودم) .

بعدها ندخل الى cli ونختبر هل جهاز الفورتى حصل على الانترنت ام لا

Execute ping google.com



كما بالصورة أعلاه توضح بأن الفورتى جيت حاصل على الانترنت حالياً...

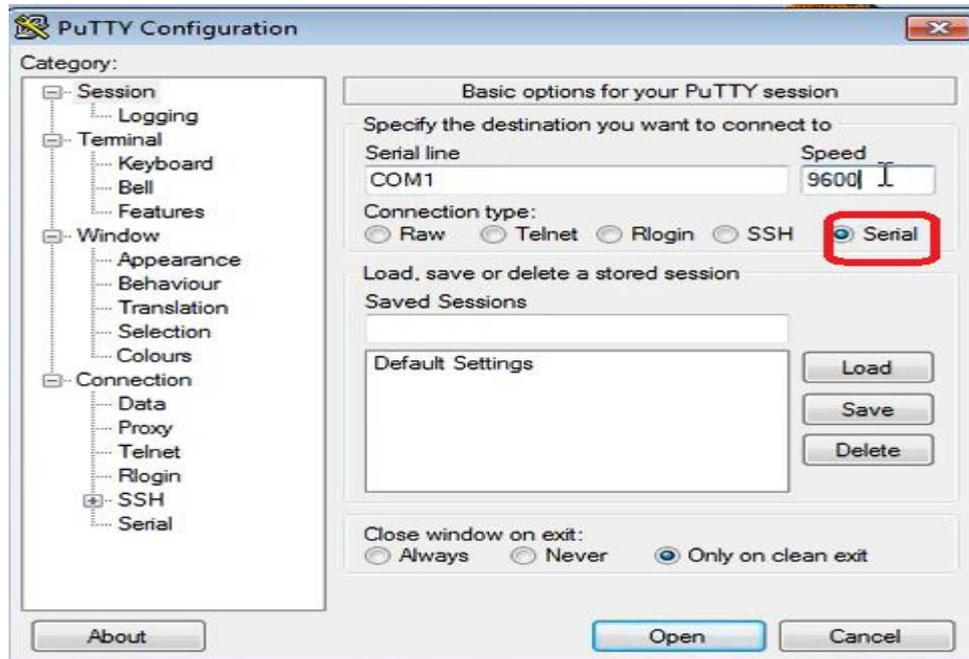
Password recovery: طريقة لاستعادة الباسورد في حالة نسيان الباسورد التابع

للـ admin وذلك كالتالي:

- 1- ندخل عن طريق الكونسول بواسطة تركيب كيبيل الكونسول للفورتى جيت ثم بواسطة برنامج الـ Putty و بالإعدادات كما بالصورة ادناه



Setting	Value
Speed	Baud 9600
Data Bits	8Bit
Parity	None
Stop Bits	1
Flow Control	No Hardware Flow Control
Com Port	The correct com-port



- 2- ثم الدخول في وضع الصيانة (maintainer) نقوم بتعيين باسورد جديد له ليوزر admin حيث في هذا الوضع سوف اكتب اليوزر نيم هو maintainer والباسورد هو السيريال الخاص بجهاز الفورتى جيت ثم اكتب الأوامر التالية :

أساسيات فورتى جيت

```
FortiGate login: maintainer
Password: *****
Welcome !

FortiGate #
FortiGate #
FortiGate # config system admin

FortiGate (admin) # edit admin

FortiGate (admin) #
FortiGate (admin) #
FortiGate (admin) #
FortiGate (admin) # set password 1010

FortiGate (admin) #
FortiGate (admin) #
FortiGate (admin) # end
```

ثم نقوم بإعادة تشغيل الفورتى بواسطة الامر

```
#execute reboot
```

ومن ثم ندخل باليوزر admin والباسورد التي تم تعيينها وهي 1010 .

ملاحظة: هذه الطريقة يجب أن يكون maintainer mode يكون enabled لكي نستطيع ان اطبق هذه الطريقة وللعلم هذا ال mode مفعّل بشكل افتراضي فلو قمنا بجعلها DISABLED فلن تتمكن من تطبيق هذه الطريقة ..

ملاحظة: في شاشة ال maintainer mode يعطيك فقط 14 ثانية فقط لإدخال اليوزرنيوم والباسورد لذا يجب ان تكون سريع في كتابه maintainer والباسورد ..

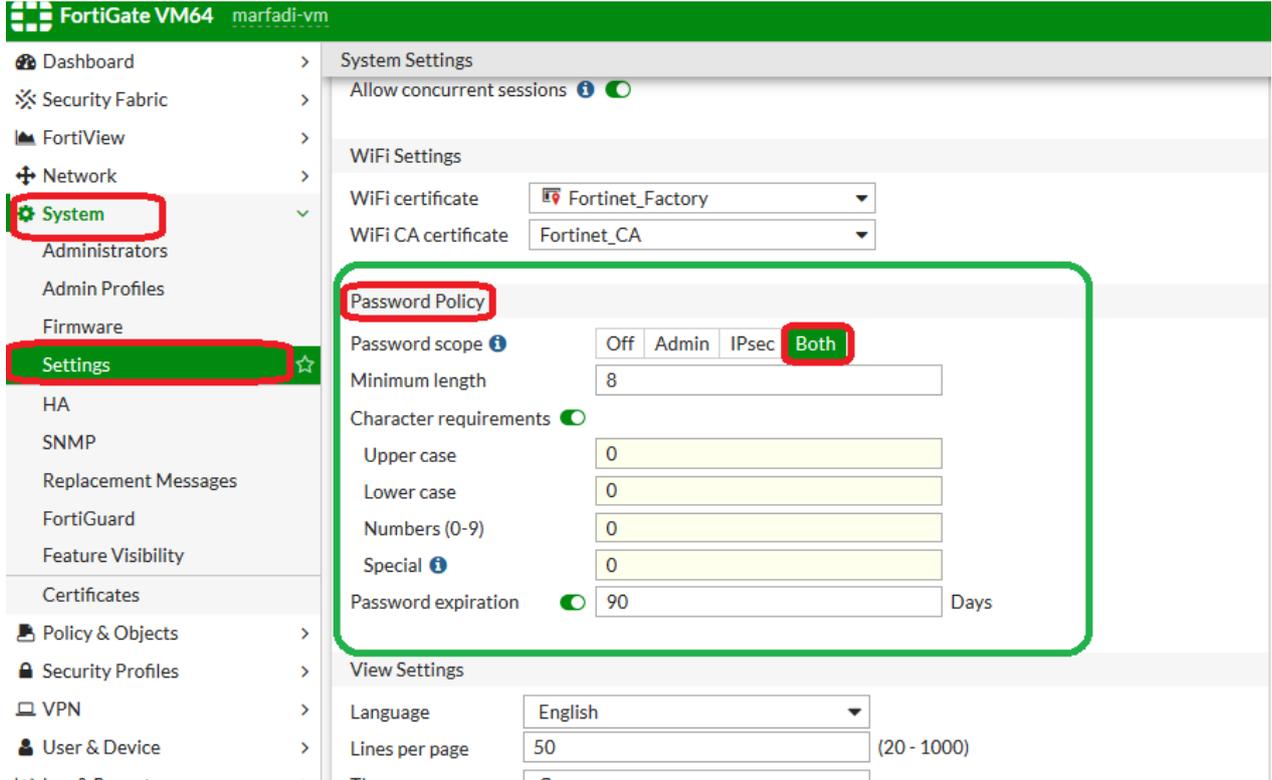
❖ طريقة عمل DISABLE MAINTAINER MODE كما بالأوامر التالية :

```
#config sys global
```

```
#set admin-maintainer disable
```

ولو تريد تفعيلها مره أخرى نكتب enable .

Password policy: سياسه اعدادات الباسورد عند الوصول للفورتي جيت مثلا يوزرنيم admin حيث ممكن الباسورد له 123 وهذا غير آمن ويجب ان تكون اكثر تعقيدا لذا يجب ان تفرض على الفورتي جيت ان يجبر administrator ان يقوموا بتعيين باسوردات معقده



كما بالصورة أعلاه

- 1- تم تفعيل password policy ليكون ليويزات ال admin الذي يقوموا بعمل اداره لجهاز الفورتي جيت وايضا ل pre-shared key الخاص ب IPsec الخاص ب vpn (وهو الباسورد الذي يكون بين الكلاينت والسيرفر في حالة الاتصال بطريقة vpn). حيث ممكن تحديد مستوى ال password policy لأحدهما فقط وليس لكليهما .
- 2- طول الباسورد يكون على الاقل 8 حرف
- 3- ثم حسب ما تريد هل تريد ان تجبر الادمين ان يجعل الباسورد يحتوي على حروف كبيتل و اسمول وأرقام ورموز وأيضا ان تجعل مده انتهاء الباسورد هي 90 يوم بعدها يطلب من الادمين تغييرها اجباري ...

Name	Requirement
Minimum Length	10
Upper case	1
Lower case	3
Numbers	3
Special	1
Expiration days	60

بحسب الصوره أعلاه :

اقل عدد من الحروف (ارقام اورموز) للباسورد هو 10
على الأقل يجب ان يكون هناك حرف واحد كبتل في الباسورد
على الأقل يجب ان يكون لديك 3 حروف سمول في الباسورد
على الأقل يجب ان يكون لديك 3 لرقام في الباسورد
يحتوي على الأقل رمز واحد (special) مثلا ! @ \$ #
يجب خلال 60 يوم ان تقوم بتغيير الباسورد

Change Password

 Your password does not conform to the password policy, please input a new password.

New password must include:

- 1 Upper Case Letters
- 3 Lower Case Letters
- 3 Numbers (0-9)
- 1 Special Characters
- 10 Minimum length

Old Password

.....

.....

OK

 Logout

ملاحظ كما بالصورة أعلاه بأنه عند مطالبي بتعيين الباسورد تم الاشارة الى تعقيدات الباسورد ..

مثلا :

M@rfadi123

❖ كيف تفعيل DHCP server على الفورتى جيت بحيث الاجهزه بالشبكة

تأخذ الاعدادات (DNS،Gateway،IP) من جهاز الفورتى جيت :

❑ DHCP Concept

✓ DHCP working method

1- Discover message

Source IP / 0.0.0.0

Source MAC / NIC address

Dest IP / 255.255.255.255

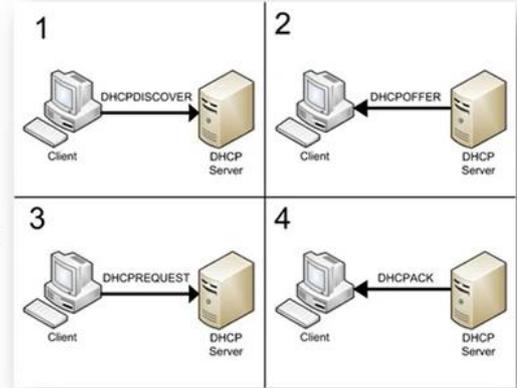
Dest Mac / FF-FF-FF-FF-FF-FF

2- Offer message (DHCP server on demand)

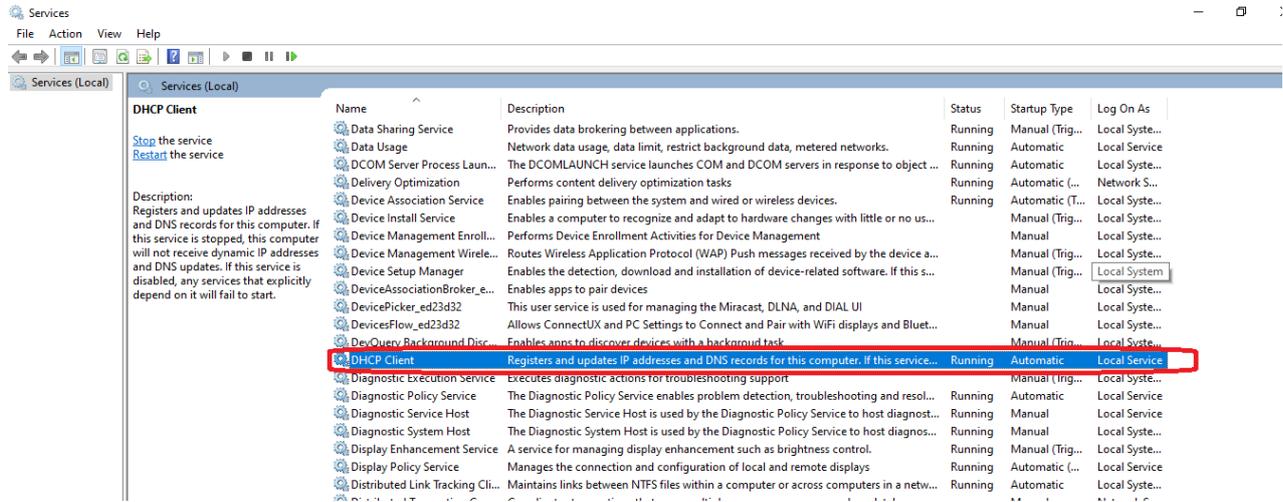
3- Request message (need TCP/IP configuration)

4- ACK message (hand over)

Note : all DHCP traffic at first time are broad Cast

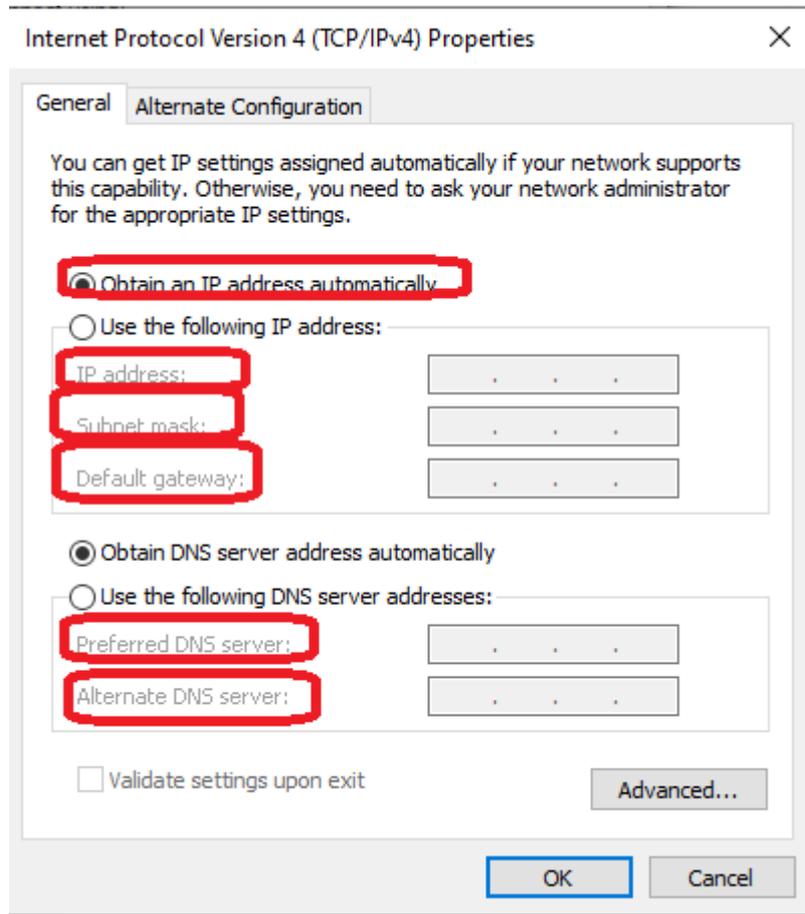


Dhcp client هي الservice التي بتتيح لك بأن تستفيد من خدمات السيرفر (Dhcp server) حيث يجب ان تكون started و enabled في جهاز الكلاينت (by default).



*صوره من جهاز الكلاينت ..

حيث ال dhcp server سوف يقوم بتوزيع الاعدادات التالية لأجهزه الكلاينت ..



حيث بمجرد ان تقوم بتفعيل الخيار Obtain an IP address automatically في كروت الشبكة لاجهزه الكلايننت فأن ال dhcp server سيقوم بتوزيع الاعدادات كما بالصورة أعلاه اما في حالة عدم وجود dhcp server شغال بالشبكة فأن اجهزه الكلايننت ستأخذ ايبي من apipa(automatic private ip address) وهذا رينج من الايبهات يبدأ من 169.254.0.1 -169.254.255.254 حيث سيأخذ الكلايننت هذا الايبي الى ان يصبح ال dhcp server متاح بالشبكة ويوزع ايبي للكلايننت ..

حيث ساقوم بتفعيل ال dhcp server في جهز الفورتى جيت على ال lan1 interface لأن هذا الكرت الذي متوصل بالشبكة الداخليه لكي يوزع الاعدادات لكل اجهزه في الشبكة الداخليه ...

ملاحظة :

أساسيات فورتى جيت

بمجرد ان تقوم بتفعيل الخيل Obtain an IP address automatically في كروت الشبكة لاجهزه الكلاينت فأن جهز الكلاينت هو الذي يطلب الاعدادات من ال dhcp server وذلك عن طريق عمل رساله broadcasts في الشبكة لكل الاجهزه.

dhcp server هو الذي سيرد على هذا الجهز بال configuration بالإضافة الى فتره العقد او اليجار (وهي الفترة التي سيحتفظ فيها الكلاينت بالاعدادات المرسله من dhcp server في الشبكة وبعد ذلك ينتهي) حيث يسمى هذا العقد بـ leased duration .

حيث نفترض بان leased duration = 7 days فأن بعد 7 أيام سيفقد الكلاينت الاعدادات المرسله من dhcp server ويجب ان يقوم بعدها الكلاينت بعملية الطلب مره أخرى ..

الآن سنقوم بعمل الاعدادات على جهز الفورتى جيت :

يجب ان يكون الكرت lan1 يأخذ أي static Manual ...

The screenshot shows the 'Edit Interface' configuration for 'port1'. The 'Name' field is 'port1'. The 'Type' is 'Physical Interface'. The 'Addressing mode' is 'Manual' and the 'IP/Netmask' is '192.168.2.20/255.255.255.0'. The 'Administrative access' section shows various protocols like HTTPS, HTTP, SSH, TELNET, and PING are checked. The 'Receive LLDP' and 'Transmit LLDP' options are set to 'Use VDOM Setting'.

كما بالصورة ادناه قمنا بتفعيل ال dhcp server

أساسيات فورتني جيت

Dashboard >
Security Fabric >
FortiView >
Network >
Interfaces ☆
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System >
Policy & Objects >

Edit Interface

DHCP Server

Address range 192.168.2.21-192.168.2.254

Netmask 255.255.255.0

Default gateway Same as Interface IP Specify

DNS server Same as System DNS Same as Interface IP Specify

Lease time 604800 second(s)

FortiClient On-Net Status

Advanced

Network

Device detection

Security mode

Traffic Shaping

Outbound shaping profile

وأيضاً الـرينج من الـايبهات التي سيتم توزيعها سوف تكون 192.168.20.21-192.168.20.254 حيث كل اجهزه الكلايننت سوف يكون الـايبي التابع لها من نفس هذا الـرينج ..

وأيضاً سيقوم بتوزيع الـmask=255.255.255.0

و Default getwat=Same as interface ip والذي سيكون نفس ابي كرت الـlan1=192.168.2.20
و DNS server= Same as system DNS والذي سيكون نفس ابي كرت dns التابع للـفورتني جيت والذي

قمنا بتحديدده سابقاً في قائمه الـdns كالتالي 8.8.8.8 8.8.4.4

او تختلر Same as interface ip وسوف يكون هو ابي الـlan1 للـفورتني جيت
ويمكنك تخصيص أي ابي تريده وذلك بتحديد الخيلر Specify وتكتب الـايبي المطلوب توزيعه ك DNS
مثلاً ابي الـدومين DC .

بعض الأوامر (Cmd) التي يتم تطبيقها على اجهزه الكلايننت :

Ipconfig

امر يقوم باستعراض كل الاعدادات لكروت الشبكة من ip,mask,gateway,dns

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\HSAMES>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . .             : 192.168.2.21
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.2.20

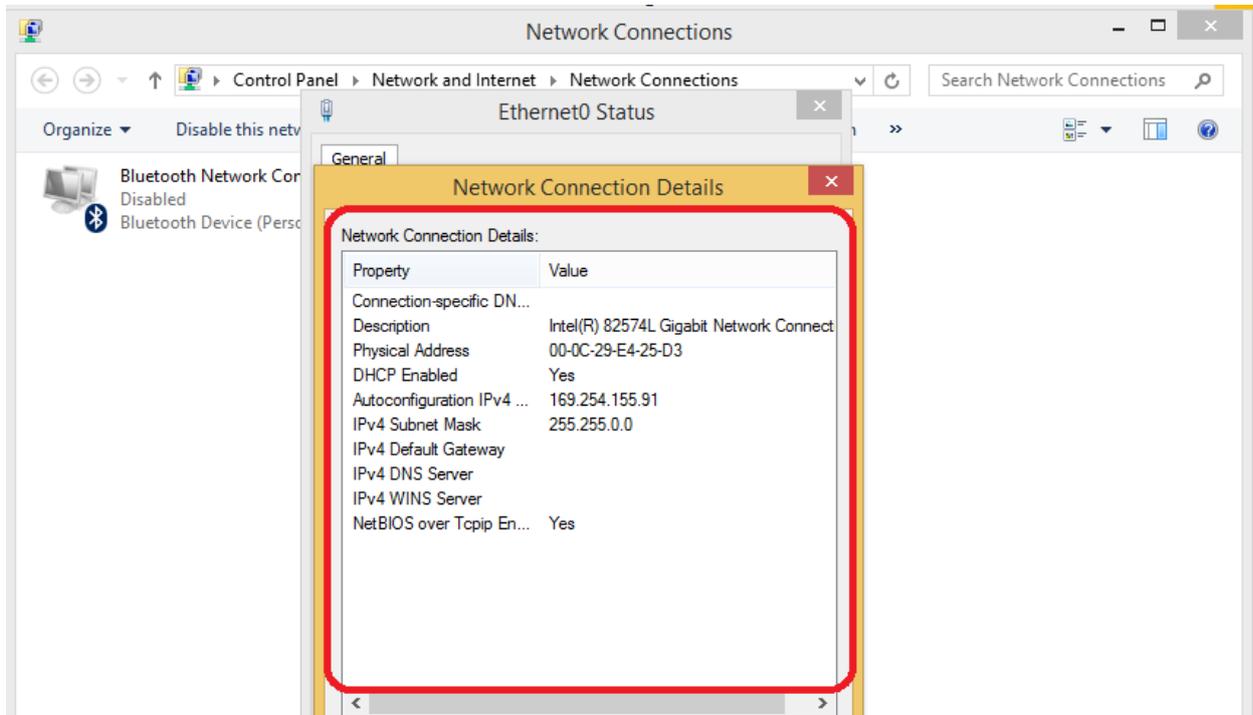
Tunnel adapter isatap.{8030AD14-A158-4F96-B78A-1DDCE09D70FF}:

    Media State . . . . .             : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\HSAMES>_
```

Ipconfig /release

معناها افقد (تخلص) من الايبي اللي عندك (على جهاز الكلاينت)
حيث يصبح كرت الشبكة للكلاينت بلا أي ايبي ولا أي اعدادات.



معناه ابحث لي عن اعدادات جديده من أي dhcp server
او ممكن عمل disable و enable لكروت الشبكة على جهاز الكلاينت بدلا عن الامر ..

```

C:\Windows\system32\cmd.exe
Default Gateway . . . . . :
Tunnel adapter isatap.{8030AD14-A158-4F96-B78A-1DDCE09D70FF}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
C:\Users\HSAMES> ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix . . . . . :
    IPv4 Address. . . . . : 192.168.2.21
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.2.20

Tunnel adapter isatap.{8030AD14-A158-4F96-B78A-1DDCE09D70FF}:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :
C:\Users\HSAMES>
    
```

Ethernet0 Status

Network Connection Details

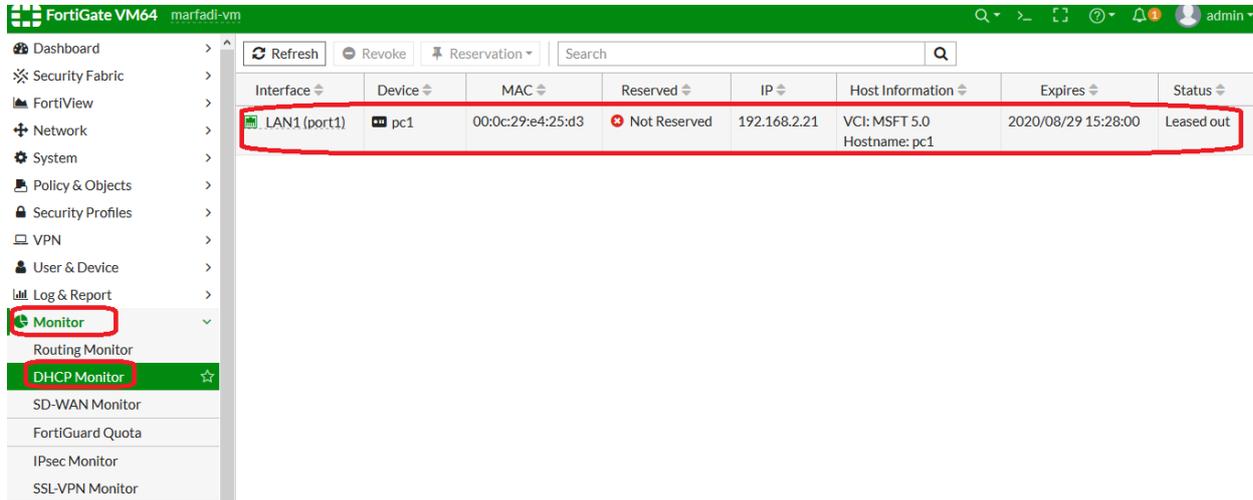
Network Connection Details:

Property	Value
Connection-specific DN...	
Description	Intel(R) 82574L Gigabit Network Connect
Physical Address	00-0C-29-E4-25-D3
DHCP Enabled	Yes
IPv4 Address	192.168.2.21
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Thursday, July 30, 2020 3:28:05 PM
Lease Expires	Saturday, August 29, 2020 3:28:05 PM
IPv4 Default Gateway	192.168.2.20
IPv4 DHCP Server	192.168.2.20
IPv4 DNS Servers	208.91.112.53 208.91.112.52
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes

Close

ملاحظ كما بالصورة أعلاه بأن جهاز الكلاينت اخذ الاعدادات من ال. dhcp server

في حالة لردت ان تعرف ماهي الأجهزة التي اخذت اعدادات من ال dhcp server عن طريق الفورتى جيت نقوم بالدخول كما بالصورة ادناه.



Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	pc1	00:0c:29:e4:25:d3	Not Reserved	192.168.2.21	VCI: MSFT 5.0 Hostname: pc1	2020/08/29 15:28:00	Leased out

حيث اسم الجهاز الكلاينت هو pc1 والمالك ادرس موجود والايي الذي اخذه هذا الجهاز وأيضا leased duration

❖ طريقة تعديل ال leased duration في ال: dhcp server

القيمة الافتراضى ل leased duration هي 7 أيام حيث يمكن تعديل هذه القيمة من خلال CLI في الفورتى جيت كما بالتالى:

حيث الهدف من تعديل الفترة (القيمة) هو تقليل ال traffic ما بين الكلاينت والسيرفر حيث في الغالب اجهزه الكلاينت من نوع PC مش محتاج ان تقوم بتغيير الايبي كل فتره وأخرى لأن تلك الاجهزه ثابتة في الشركة بعكس اجهزه الموبايل و الابتوبات التي ممكن تتغير كل فتره وفترة..

لذا بحسب السيناريو عندك بالشركة فلو كانت اجهزه pc فالأفضل ان تقوم بزيادة فتره leased duration لكي نقلل من ال traffic

الان سنبدأ عملية التعديل من خلال للفورتى جيت:

أساسيات فورتى جيت

دائما فتره ال leased duration ستكون التعديل بالفورتى بالثواني فقط ويجب ان يكون ما بين

300 ثانية – 8640000 ثانية ،اي ما بين 5 دقائق الى 100 يوم

وفي حالة لردت ان تكون الفترة غير محدودة فنكتب القيمة 0

حيث لحساب عدد الثواني مثلا لـ 30 يوم

24 hours x60 min x60 sec x 30 days= 2592000 sec

ثم سنقوم بتنفيذ الامر ipconfig /renew على جهاز الكلاينت وسلاحظ بأنه تم تعديل ال leased

duration

بعد كتابه الامر ipconfig /all في جهاز الكلاينت ظهرت كل المعلومات لهذا الجهاز (ip,mac address

,subnet mask,gateway,dns, leased obtained,leased expires)

حيث سنقوم بتعديل ال lease time الى 3 اشهر =7776000 ثانية ..

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar is expanded to 'Network' > 'Interfaces'. The main panel is titled 'Edit Interface' and shows various configuration options. The 'Lease time' field is highlighted with a red box and is set to 7776000 seconds. Other fields include Netmask (255.255.255.0), Default gateway (Same as Interface IP), and DNS server (Same as System DNS). The 'Advanced' section is also visible, showing options for Device detection, Security mode, and Traffic Shaping.

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	pc1	00:0c:29:e4:25:d3	Not Reserved	192.168.2.21	VCI: MSFT 5.0 Hostname: pc1	2020/10/28 15:44:07	Leased out

وأيضاً كما بالصورة أعلاه من الفورتى جيت بأن ال leased duration هو 3 اشهر..

فلو اردنا عمل تعيين ايى محدد لجهاز ما وليكم PC1

نقوم بالدخول الى dhcp Monitor ثم نحدد الجهاز المراد تخصيص ايى محدد وليكن مثلاً

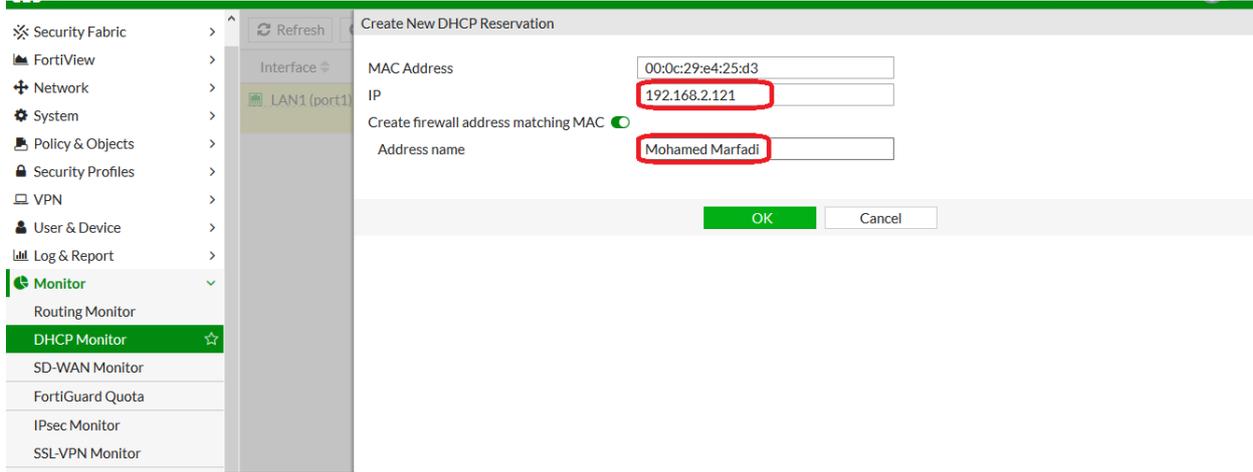
192.168.2.21 ومن ثم نختار التبريب المسمى Reservation

ثم create ثم

ملاحظ بأن الجهاز الكلاينت المسمى pc1 كان اخذ ايى 192.168.2.21 والان سوف نجعله دائماً يأخذ

الايى 192.168.2.121

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	pc1	00:0c:29:e4:25:d3	Not Reserved	192.168.2.21	VCI: MSFT 5.0 Hostname: pc1	2020/10/28 15:44:07	Leased out

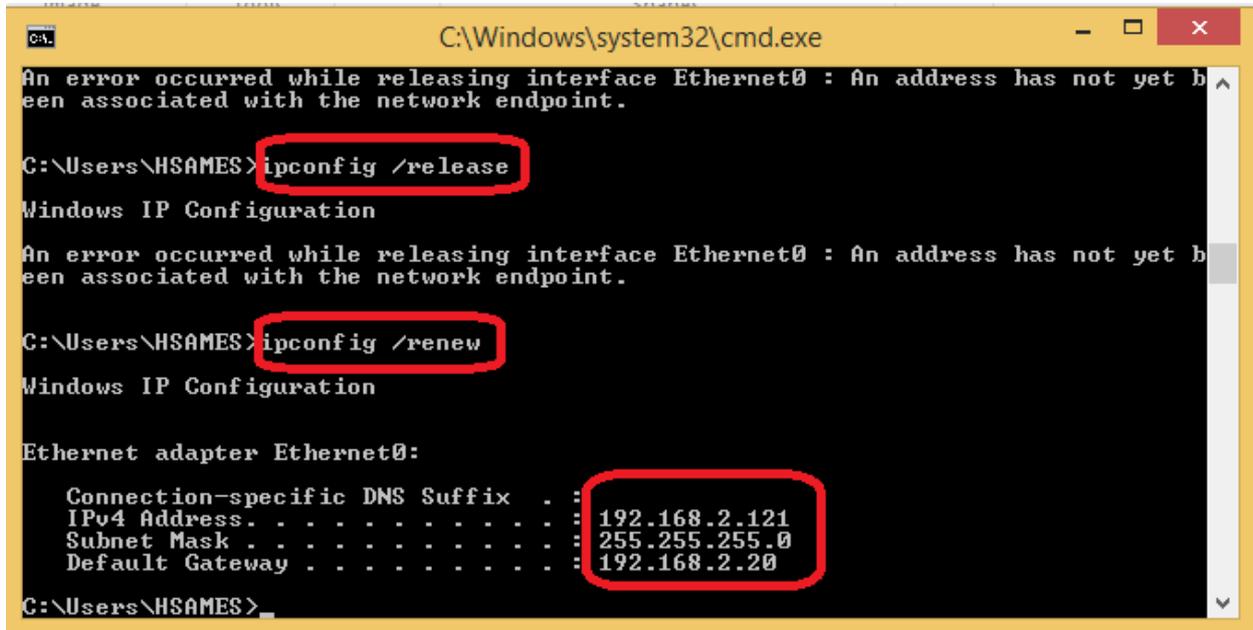


تم تحديد بأن الجهاز PC1 صاحب الماك ادرس أعلاه يجب تخصيص له الايبي 192.168.2.121 .

الان سوف ندخل على الكلايننت ونعمل له الامر

Ipconfig /renew

او اعداه تشغيل للجهاز او disable و enable لكروت الشبكة فسلاحظ بان الجهاز اخذ الايبي 192.168.2.121 كما تم تحديده.



وايضا في الفورتي جيت ملاحظ بأن الجهاز اخذ reserved كما بالصورة ادناه الايبي 192.168.2.121

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	pc1	Mohamed Marfadi	Reserved	192.168.2.121	VCI: MSFT 5.0 Hostname: pc1	2020/10/28 15:52:12	Leased out

DNS(domain name service)

ال dsn عبوره عن شي اختيلري بالشركة حيث انه مهم في حالات كثيره ولكنه ليس أساسي..

ووظيفته هي تحويل من الاسم الى الايبي او العكس ، عند طلب موقع معين مثلا www.bab.com فإن ال dns يقوم بعمل resolve من الاسم الى الايبي لأن الشبكة-الأجهزة- لا تعرف تتعامل مع الأسماء بل مع الايبيات فقط..

فلوا اردت معرفة الايبي لأي جهاز كمبيوتر او لأي موقع فأننا نقوم بعمل بينج وهو سيظهر لك الايبي لهذا الجهاز او الموقع

Ping bab.com

حيث يحتوي ال dns server على database مكونه من records from name to ip(host)

حيث الفورتى جيت يشتغل ك dns forwarder او dns server .

حيث لو كانت ال database موجودة على جهاز الفورتى جيت فهذا يعمل ك dns server

ام الخيار dns forwarder فهذا يعني بان الفورتى جيت لا يوجد لديه dns ل database ولكنه بيسال dns

server اخر . في حالة يوزر طلب موقع مثلا ياهو فان الفورتى جيت اكيد غير مخزن ال database لكل

المواقع بالعالم لذا سيتم بتحويل الطلب الى dns forwarder الذي قمنا بأعداده سابقا 8.8.4.4 , 8.8.8.8

اما ان قام يوزر بطلب الوصول الى طابعه او أي resources بالشبكة فان ال database تكون موجودة و

مخزنه على الفورتى جيت وهنا سوف يكون dns server .

الخلاصة:

لو أي احد سال ال dns التابع للفورتى جيت عن أي شي غير موجودة عنده على ال database فأنه سوف

يقوم بتحويله الى dns forwarder

وهو google dns server

8.8.8.8 , 8.8.4.4

FortiGuard Concept

الفورتى جلد:(FDN) هي عبره عن شبكة كبيره مسؤوله عن توزيع التحديثات الخاصة بـ

- 1 Ips
- 2 App Control
- 3 Antivirus
- 4 Web filtering
- 5 Email filtering
- 6 Vulnerability scanning
- 7 Message services

على اجهزه الفورتى جيت المشتركه عند الفورتى جلد.

حيث بمجرد ما تشتري جهاز الفورتى جيت تقوم بعمل تسجيل على fortiguard لكي يصل اليك التحديثات للاشياء أعلاه حيث انها خدمه سنويه حيث بعضها خدمات اختياريه ممكن تشترك فيها وممكن لا مثل messaging service

ips: يحتوي على حلول لتهديدات او الهجمات attack حيث يقوم IPS باكتشاف هذا النوع من أنواع الهجمات من خلال سلوكها بغض النظر نوعه او اسمه ويعمل له. Block

App control: عبره عن نظام موجود على جهاز الفورتى جيت تقدر من خلاله التحكم بأكثر من 1000 تطبيق على اجهزه الكلاينت

Antivirus: عبره عن نظام موجود على الفورتى جيت ويحتاج الى لايسنز لكي يتمكن الجهاز من عمل التحديث من الفورتى جلد

Web filtering: يقوم بتوفير خدمه web category حيث يحتوي على الآف التصنيفات) تحتوي على ملايين المواقع(مثلا لو تريد اغلاق كل المواقع التابعه للرياضه فأنك بمجرد اختيار ال category sports سيتم اغلاق جميع المواقع الرياضيه بالشبكة لديك..

حيث توجد الكثير من التصنيفات (categories) مثل social media ,sport,porn,email,streaming وغيرها

Email filtering: يحميك من الاسبام وغيرها لكي يحميك من الهجمات التي تأتي من خلال الايميلات

Vulnerability scanning: مبدا بيتعامل مع الكونفجراشن والباتشات

Messaging service: تعطيك رسائل تحذيره للإيميل و sms لكي يصل اليك عند وصول هجوم معين.

أساسيات فورتى جيت

DDNS: هي عبارة عن خدمة تستخدم منها بمجرد الاشتراك مع فورتى جلد بتسمح لك ان تكون لديك dns اكثر امانا بالإضافة الى الحصول تلقائيا على web filtering حتى لو لم تقم بعمل web filter على جهاز الفورتى جيت..

حيث الخدمات الثمانية المذكورة أعلاه لو تقم بتجديدها فأن جهاز الفورتى جيت سوف يعمل كروتر و vpn لكن ك security profile لن يعمل الا بتجديد الاشتراك في الفورتى جلد حيث يوجد علامات توضح حالة الخدمات التي لديك كما بالشرح ادناه :

الرمادي: بأنك مشترك بالخدمة ولكن يوجد مشكله بالاتصال مع الفورتى جلد فيجب ان تحل لها البرتقالي: انت غير مشترك بالخدمة

الأصفر: الخدمة أصبحت منتهيه ويجب تجديدها لتصبح خضراء

الأخضر: الخدمة شغاله بدون أي مشاكل ان يوجد اتصال ب FDN التابع للفورتى جلد.

حيث بمجرد اقتراب موعد انتهاء الاشتراك تقوم شركه فورتى جيت بارسال ايميل بقرب انتهاء الاشتراك..

Fortiguard distribution network (FDN)

من خلال هذه الشاشة يمكنك متابعه العقد(الاشتراك) الخاص بك مع الفورتى نت متى ينتهي ومن الشخص الذي قام بتسجيل العقد والايمل أيضا..

وأيضا يوضح لك كل خدمه (security profile) متى ينتهي الاليسنز الخاص بها

وتقدر تعمل تحديث (Manual) من خلالها للخدمات التي موجوده لديك ومتى اخر تحديث حصل.. الخ

فلو اردت ان تقوم بعمل تحديث من ال FDN تلقائي بمجرد وجود تحديث جديد بشرط ان يكون جهاز الفورتى جيت متصل بالإنترنت نقوم بالخيار التالي:

Accept push updates

FortiGate VM64 marfadi-vm

Dashboard > FortiGuard Distribution Network

Security Fabric >

FortiView >

Network >

System >

Administrators

Admin Profiles

Firmware

Settings

HA

SNMP

Replacement Messages

FortiGuard ☆

Feature Visibility

Certificates

Policy & Objects >

AntiVirus & IPS Updates

Accept push updates

Use override push

Scheduled Updates Every 2 Hours

Improve IPS quality

Use extended IPS signature package

Update AV & IPS Definitions

Update Server Location

US only Lowest latency locations

Filtering

Web Filter Cache Clear cache after 60 Minutes

Anti-Spam Cache Clear cache after 30 Minutes

FortiGuard Filtered Protocols HTTPS UDP

ولو تريد ان تعمل تحديث الان نقوم بالنقر على الزر Update AV&IPS Definitions حيث ينفذ هذا الخيار في حالة جهاز الفورتى جيت كان متوقف عن التحديث لأي سبب فتريد ان تقوم بتحديثه حالا... وبعد كذا سوف يقوم بتزليل أي تحديث جديد بشكل اوتوماتيكي لأن الخيار الاخر قمنا بتفعيله

Accept push updates

او يمكنك تحديد أوقات محدده لعملية التحديث من ال FDN وذلك بتفعيل الخيار

Schedule updates

ونحدد الوقت واليوم لعملية التحديث...

كل يوم الساعة 12 صباحا يتم البحث عن التحديثات من ال FDN

أساسيات فورتني جيت

The screenshot shows the FortiGuard settings interface. The left sidebar contains a navigation menu with 'System' selected. The main content area is titled 'AntiVirus & IPS Updates'. Under 'Accept push updates', the 'Scheduled Updates' section is highlighted with a red box, showing a dropdown set to 'Daily', a text input field with '12', and a dropdown set to 'AM'. Below this, there are options for 'Improve IPS quality' and 'Use extended IPS signature package'. A button labeled 'Update AV & IPS Definitions' is present. The 'Update Server Location' section shows 'US only' and 'Lowest latency locations'. The 'Filtering' section includes 'Web Filter Cache' (60 minutes), 'Anti-Spam Cache' (30 minutes), 'FortiGuard Filtering Protocol' (HTTPS and UDP), 'FortiGuard Filtering Port' (443, 53, 8888), and 'Filtering Services Availability' (Check Again).

ولكن الأفضل جعل الخيار allow push updates لكي يقوم بتزليل التحديث بمجرد وجود تحديث جديد على FDN.

في خيار اخر على مستوى antispan cache و web filter cache

الكاش هو التخزين،

حيث جهاز الفورتني جيت يستلم طلبات كثيره من الاجهزه الموجودة بالشبكة الداخليه لموقع معين او على ايبي معين ترسل له ايميل فالذي يحصل كالاتي ان جهاز الفورتني جيت بيتصل مع ال FDN بيقول له لدي طلب وصل لي بخصوص الموقع الفلاني هل الموقع هذا في القائمة السوداء او يوجد فيه مشكله فأن في كلا الحالتين يجب ان يقوم ال FDN بالرد على جهاز الفورتني جيت حيث هذه المعلومة ستصل الى جهاز الفورتني جيت وبدوره جهاز الفورتني جيت سيقوم بتوصيلها لجهاز الكلاينت سواء BLOCK او ALLOW حيث يقوم جهاز الفورتني جيت بالاحتفاظ بهذه المعلومة عنده لمدة 60 دقيقه كما بالصورة أعلاه..

حيث لو أي جهاز كلاينت طلب نفس الموقع خلال تلك الفترة فأن الفورتني جيت لا يقوم بالذهاب الى ال FDN مره أخرى بل جهاز الفورتني جيت هو الذي يرد على جهاز الكلاينت مباشرة فبذلك قمنا بتوفير الترافيك والوقت بين الفورتني جيت وال FDN وهذا يتم زياده سرعه الشبكة لدي.

أيضا نفس الكلام بيحصل على مستوى ... ANTISPAM

حيث يمكن تعديل تلك القيم من 5 دقائق الى يوم كامل فقط..

ملاحظة: البورت الافتراضي لوصول الفورتى جيت الى الفورتى جرد هو 8888 كما بالصورة ادناه

The screenshot shows the FortiGuard Distribution Network configuration page. The left sidebar contains a navigation menu with 'FortiGuard' selected. The main content area is titled 'FortiGuard Distribution Network' and includes several sections: 'Update AV & IPS Definitions' with a refresh button, 'Update Server Location' with a dropdown set to 'US only' and 'Lowest latency locations', 'Filtering' section with 'Web Filter Cache' and 'Anti-Spam Cache' both enabled, 'FortiGuard Filtering Protocol' set to 'HTTPS', and 'FortiGuard Filtering Port' set to '8888'. Below this is a 'Filtering Services Availability' section with a 'Check Again' button and a table for 'Web Filtering' and 'Anti-Spam'. At the bottom, there is an 'Override FortiGuard Servers' section with 'Create New', 'Edit', and 'Delete' buttons.

FortiExplorer

هو عبره عن تطبيق نستطيع بواسطته عمل ادارة الاعدادات الأساسية فقط لجهاز الفورتى جيت سواء بواسطة ال web او بواسطة ال CLI من خلال منفذ USB management التابع لجهاز الفورتى جيت، حيث هذا المنفذ موجود في بعض اجهزه الفورتى جيت وليست جميعها.

حيث تقوم بتوصيل منفذ USB MGMT بالابتوب ومن ثم بواسطة التطبيق fortExplorer الذي يمكنك تزيله مجاناً.

يمكن عن طريقة عمل تغيير للباسورد الخاص بال administrator واختيار المنطقة الزمنية وإعدادات كروت الشبكة... الخ

حيث بعد تزيله على الكمبيوتر (الابتوب) الموصل بمنفذ ال USB MGMT سوف يظهر لك البرنامج على شكل wizard حيث تقوم بالإعدادات الأساسية فقط..

ملاحظة: لا يمكن تطبيق FortiExplorer على FortiGate VM بل على فايرول حقيقي

Fortigate firewall policy

حيث سنستخدمه في عملية الترافيك و ال vpn و traffic shaper و security وغيرها..

ماهي البوليسي:

مجموعة من القواعد تتحكم في الترافيك اما بالسماح او المنع (allow,deny) أي انك تستطيع التحكم بالترافيك من internal to external او العكس او من vpn to internal و يمكنك التحكم بالخدمات (services) او تريد ترافيك يمر في وقت معين وترافيك في أوقات أخرى يتم منعه... الخ كل ذلك يتم عن طريق البوليسي..

إذا البوليسي هي سلاحك في أي فايرول تستخدمه...

ملاحظة: أي فايرول بوليسي يكون بشكل افتراضي Deny any any

أي امنع أي ترافيك يخرج الى أي مكان لذا لا يمكن لأي ترافيك ان يمر الا لو قمت بعمل بوليسي تسمح بذلك...

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	FSSO-GROUP-IT	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
3	public	Subnet1	all	always	ALL	DENY			Disabled	0B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0B

تكون موجودة بشكل افتراضي بكل فايرول ولا يمكن حذفها ابدا او التعديل عليها...

شرح البوليسي الافتراضية (Implicit Deny) المشر لها باللون الأحمر بالصورة أعلاه..

لوفي أي source ورايح الى أي Destination في أي وقت وبأي خصائص و services قم بمنعها .

لكي تقوم بإنشاء أي بوليسي يجب ان تقوم أولاً بإنشاء مجموعة من العناصر حيث العناصر هي التي بتكون منها البوليسي حيث تسمى هذه العناصر بـ objects حيث تصنف الى صنفين احدهما ضروري ولا غنى عنها والأخرى اختياريه.

❖ ماهي انواع الـ objects الأساسية (الضرورية)

1- Interfaces يجب ان يكون لدي على الأقل 2 كروت واحد lan والأخرى wan

حيث الـ interface له أنواع ممكن يكون physical interface او virtual interface

طريقة عمل: virtual interface

Create New>interface >

تم إعطاء اسم للكروت باسم vlan1 وعنوان له مثلا 1 virtual interface ونوعه Vlan أي انه كرت وهمي وليس حقيقي لذا يجب ان يكون جزء من كرت حقيقي(ابن من الكرت الحقيقي) ولذا تم اختيار LAN1 وبعدها تم إعطاء الكرت الايبي 192.168.3.100/255.255.255.0 واعطائها administrative access لـ https ping حيث بعد ذلك يصبح هذا المنفذ المسمى VLAN1 كأنه منفذ حقيقي ويمكن تطبيق عليه أي بوليسي

حيث ظهر الان interface باسم VLAN1 ونوعه VLAN يتفرع من الـ interface الحقيقي LAN1

لذا في حالة انشاء البوليسي فأن الـ object المسمى interface ممكن يكون physical interface او VLAN او ANY أي حاه..

1- Address الناس التي حيتم تطبيق البوليسي وينقسموا الى الأنواع

التالية:

- 1 Subnet :
- 2 Ip range
- 3 Geography :
- 4 FQDN (fully qualified domain name) :
- 5 Device mac address

فلو اخترت الخيار All فهذا يعني بأنه كل العناوين..

- 2 Services : تتكون من حاجتين اما بروتوكول (dns,http,https,ping,smtp,pop,ssh.....) او بورت (53,80) حيث يعتبر هذا الخيار من اقصى أنواع التحكم بالشبكة حيث استطيع التحكم بالبورت والسيرفيس. حيث لو اخترت بروتوكول معين وليكن https فهذا يعني بأنه هو فقط الذي سيتطبق عليه البوليسي اما لو اردت كل البروتوكولات يتم التطبيق عليها فنختار. All

- 3 Sechdual : متى تريد تطبيق هذه البوليسي!! هل في أوقات معينه او مره واحده فقط فلو اخترت الخيار Always يعني باي وقت.

- 4 Action : تسمح allow لهذه البوليسي

Deny تمتع هذه البوليسي..

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > IPv4 Policy

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
3	public	Subnet1	all	always	ALL	DENY			Disabled	0B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
5	3	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0B

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > IPv4 Policy

New Policy

Name: policy1

Incoming Interface: LAN1 (port1)

Outgoing Interface: SD-WAN

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

NAT:

IP Pool Configuration: Use Outgoing Interface Address Use Dynamic IP Pool

Preserve Source Port:

Protocol Options: PRX default

Security Profiles

AntiVirus:

Web Filter:

DNS Filter:

ثم نقوم باختيار ال objects كما تكلمنا عنها سابقا

Name : اسم البوليسي

Incoming interface : ال interface الذي سيمر منه الترافيك

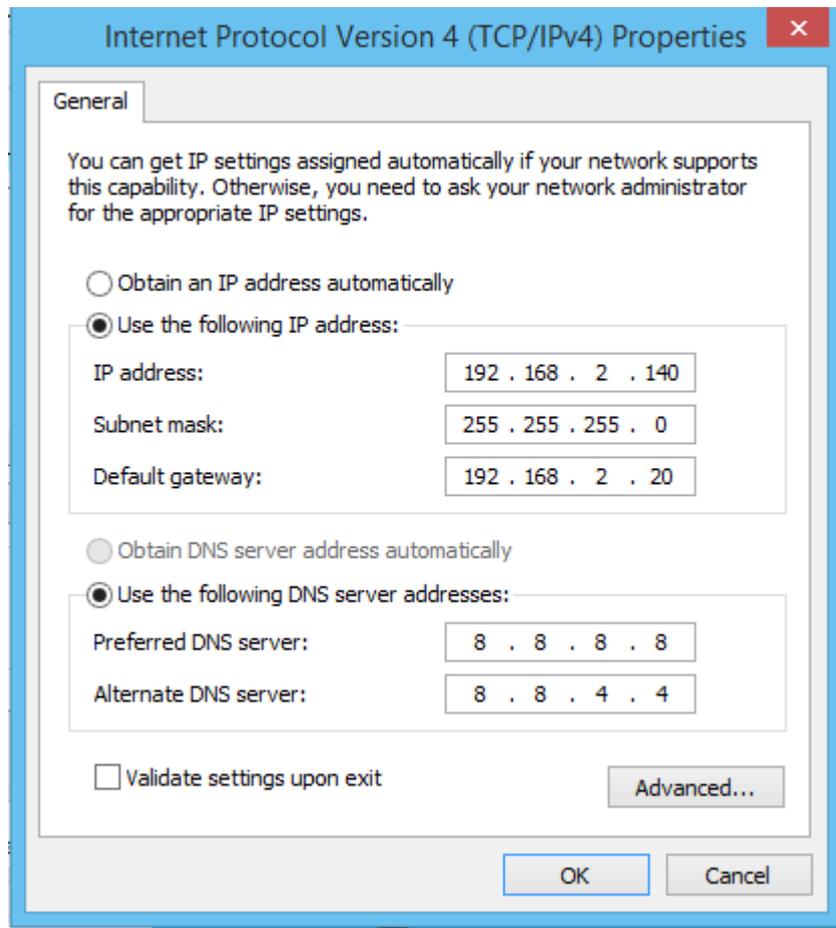
Outgoing interface : ال interface الذي سيمر اليه الترافيك

: Source

تصميم الشبكة لدينا كما بالرسمه التاليه:

حيث اجهزه الشبكة المحلية سوف يكون ال Gateway لهم هو 192.168.2.20 وهو نفس ابي كرت الشبكة LAN1 في الفورتني جيت.

حيث لا يمكن لأي جهاز من اجهزه الشبكة المحلية ان يطلع الى خارج الشبكة الا عن طريق هذا الابي.



كما بالصورة أعلاه لأحد اجهزه الكلايننت في الشبكة الداخليه الذي يوضح اعدادات كرت الشبكة من

ابي وبوابه افتراضيه و.. DNS

❖ انشاء اول بوليسي في الفورتني جيت للسماح للجهاز الكلاينت الحصول على الانترنت

اسم البوليسي(الرول)allow_all:

توجيه الترافيك من LAN1 الى WAN1 و اسمح لأي عنوان ان يخرج الى أي عنوان وبأي وقت وبأي خدمه سواء http او https الخ.

يجب ان تقوم بتفعيل الخيار NAT لأنه طالما أي شبكة تريد ان تتواصل مع شبكة أخرى بـ subnet مختلفه فلازم يكون هناك عمليه الـ NAT لذا يجب تفعيل هذا الخيار لكي يعمل NAT بين الشبكة الداخلية(LAN) وبين الانترنت..(WAN)

ثم موافق...

ملاحظة: أي جهاز في الشبكة المحلية سوف يحصل على الانترنت بمجرد انشاء هذه الرول.

The screenshot shows the 'Edit Policy' configuration page in FortiGate. The 'Name' field is set to 'allow_all'. The 'Incoming Interface' is 'LAN1 (port1)' and the 'Outgoing Interface' is 'WAN (port2)'. The 'Source' and 'Destination' are both set to 'all'. The 'Schedule' is 'work_time' and the 'Service' is 'ALL'. The 'Action' is 'ACCEPT'. The 'Inspection Mode' is 'Flow-based'. The 'NAT' toggle is turned on. The 'IP Pool Configuration' is set to 'Use Outgoing Interface Address'. The 'Protocol Options' are set to 'PRX default'.

وكما بالصورة أعلاه نقوم بتفعيل هذا البوليسي فلو قمت بعمل disable لهذا الخيار فأن هذه البوليسي ستكون موجودة ولكن غير مفعله فلذا لن يتم تطبيقها. فلو انت لا تريد حذف البوليسي بشكل نهائي بل لا تريد تفعيلها فاننا نقوم بعمل الخيار. Enable this policy=off

أساسيات فورتى جيت

The screenshot shows the configuration page for an IPv4 Policy in FortiGate. The left sidebar shows the navigation menu with 'Policy & Objects' selected. The main content area shows the configuration for the policy, including IP Pool Configuration, Security Profiles, and Logging Options. The 'Enable this policy' toggle is highlighted with a red box.

The screenshot shows the Policy Lookup table in FortiGate. The table has columns for ID, Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. The 'allow_all' policy is highlighted with a red box.

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	FSSO-GROUP-IT	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
3	public	Subnet1	all	always	ALL	DENY			Disabled	0B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
1	allow_all	all	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
5	3	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0B
6	Implicit Deny	all	all	always	ALL	DENY			Disabled	0B

ملاحظ بالصورة أعلاه بان البوليسي allow_all معمول لها disabled .

Firewall objects

هي مجموعة العناصر التي أقوم بإنشائها لكي يتم اختيارها في البوليسي وهذا ما تم ذكره سابقا...

: Address

ملاحظ بالصورة ادناه بان هناك مجموعة من العناوين التي موجودة بشكل افتراضي..

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	1
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
wildcard.dropbox.com	FQDN	*.dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1

ولأنشاء عنوان جديد نقوم بالخطوات التالية:

: Subnet

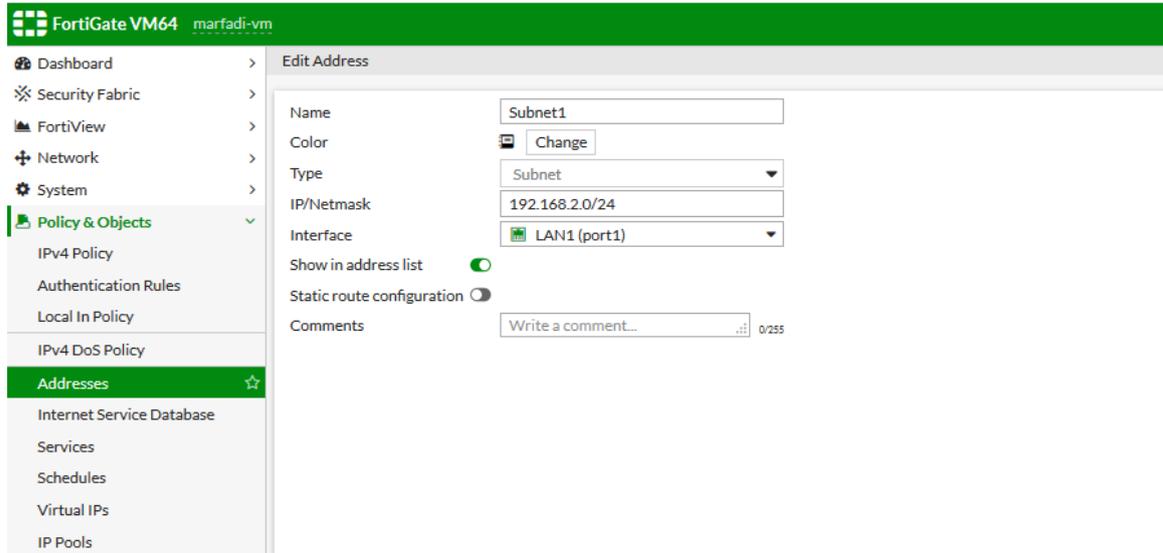
هذا النوع يعبّر فيها عن الشبكة (Subnet) Network

او تعبر فيها عن جهاز معين (ايبي محدد)

او تعبر فيها عن كل العناوين (all ip's)

الطريقة الأولى:

التعبير عن شبكة كامله (شبكة معينه)



192.168.2.0/24 او 192.168.2.0/255.255.255 كل الطرق صحيحة وبعدها تم ربط هذه الـ subnet

المسماة subnet1 بـ كرت الشبكة LAN1.

ملاحظ كما بالصورة ادناه بان العنوان تم اظهاره...

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (sslroot)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0

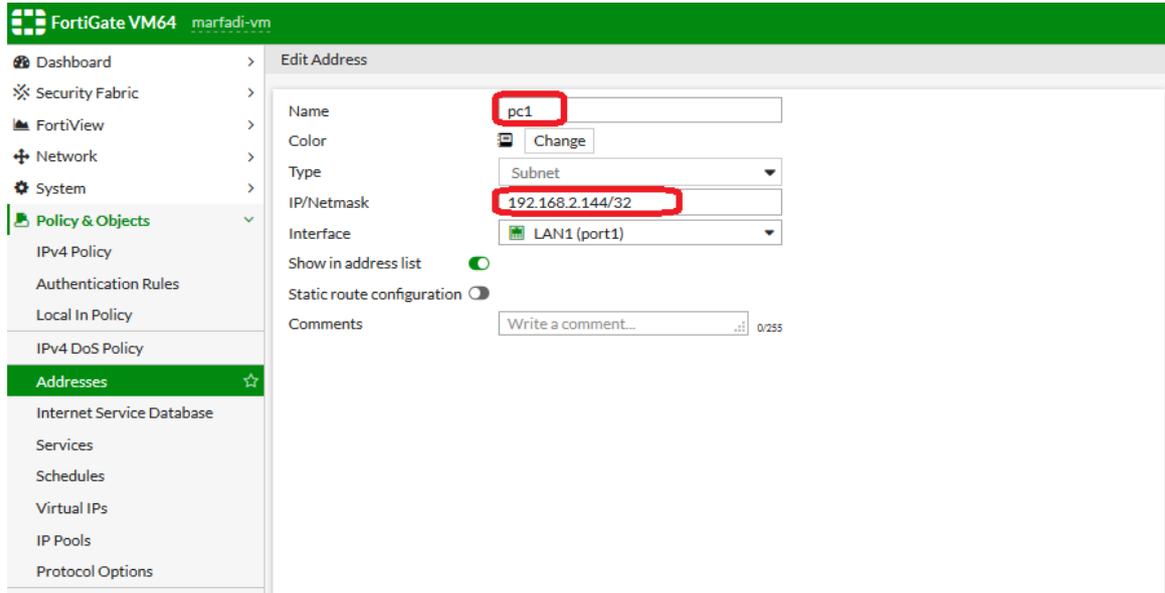
الطريقة الثانية:

التعبير فيها عن جهاز معين- ابي محدد-

اما اني اكتبه بالطريقة التالية

192.168.2.144/32 او 192.168.2.144/255.255.255.255

لكي اعبر عن جهاز معين) (Single host



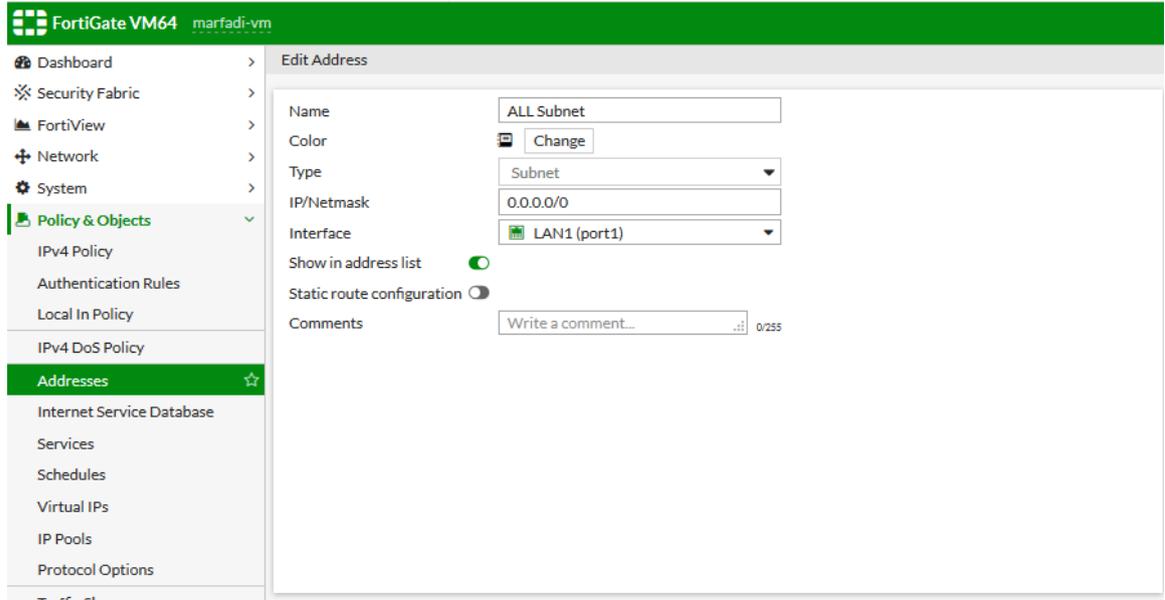
ملاحظ بان العنوان المضلل يعبر عن جهاز معين اسمه pc1 وله ايبي. 192.168.2.144

Address	Type	IP Range	Interface	Visible	Count
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	1
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1
ALL Subnet	Subnet	0.0.0.0/0	LAN1 (port1)	Visible	0

الطريقة الثالثة:

تعبير فيها عن كل العناوين (كل الشبكات (all ip's))

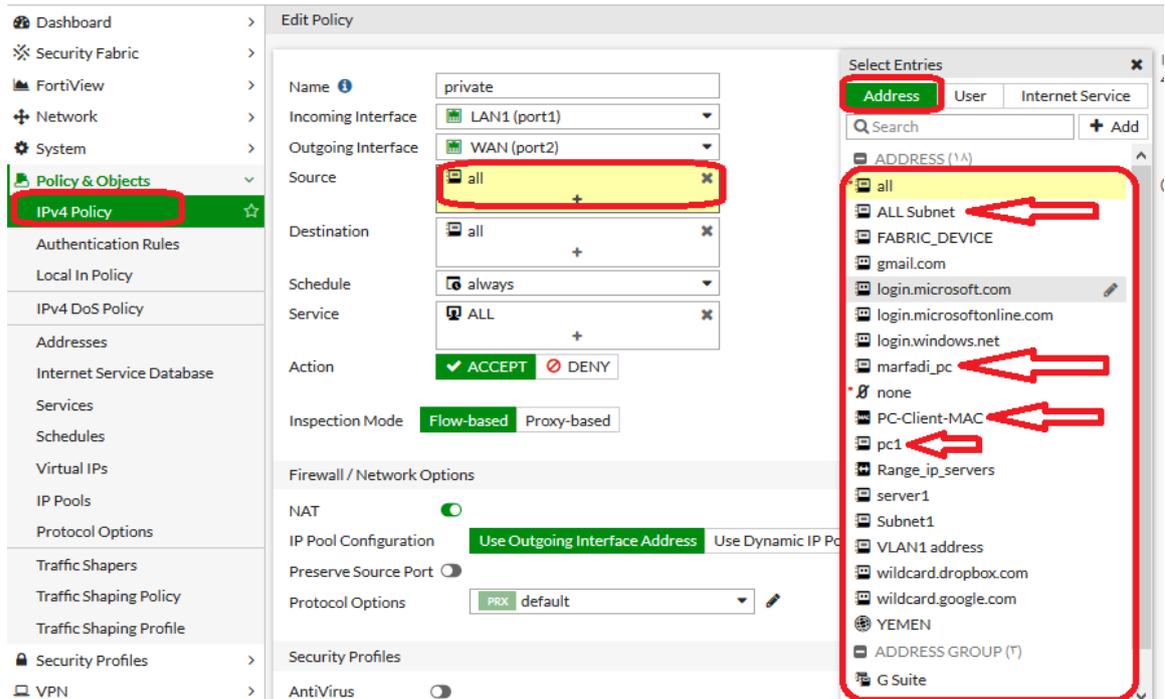
حيث يتم كتابتها كالتالي 0.0.0.0/0.0.0.0 أي كل الشبكات.



ملاحظ بان كل العناوين وبكل الأنواع موجودة التي أنشأناها كما بالصورة أعلاه.

فعند انشاء البوليسي(الرول) (وعند اختيار ال source address و destination address فإنه يظهر لنا العناوين التي قمنا بانشائها سابقا

كما بالصورة ادناه



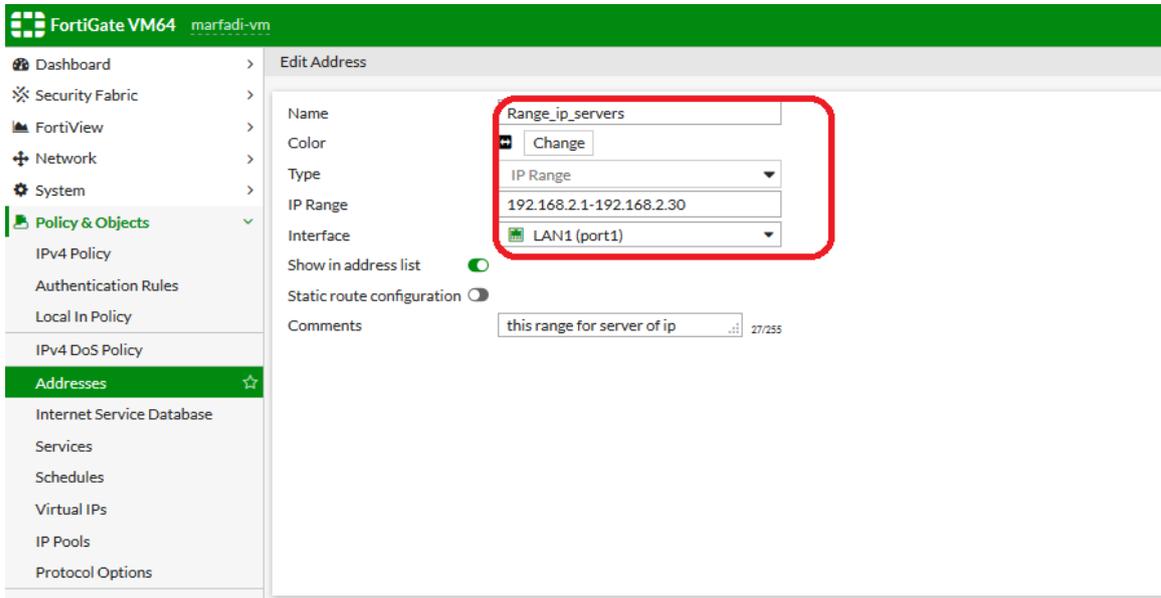
فلو اخترت العنوان pc1 والذي له الايبى المحدد 192.168.2.144

فان فقط الجهاز صاحب الايبى 192.168.2.144/32 هو الذي سيستطيع ان يحصل على الانترنت فقط من اجهزه الشبكة الداخليه..

: Ip range

يعبر عن مدى معين من الايبهات) من- الى (وأريد ان اخصهه لكي أقوم بتطبيق بوليسي معينه عليه.

على سبيل المثال لدينا رينج ايبهات مخصصه للسيوفرات من 192.168.2.1-192.168.2.30



The screenshot shows the FortiGate VM64 configuration interface. The 'Addresses' table is displayed, showing the configuration for 'Range_ip_servers' highlighted in red.

Name	Type	Details	Interface	Visibility	Ref.
Address					
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1

حيث يمكنني ان اطبق عليهم بوليسي معينه..

حيث يتم استخدام ال ip range مع VPN فإذا كان لديك vpn clients

أساسيات فورتى جيت

ويريدوا ان يصلوا الى الشبكة الداخليه عبر الفورتى جيت من خرج الشركة) من المنزل مثلا(فستقوم بتوزيع مجموعة ايبهات محدده (range ip) كما قمنا بعمل بالسابق..

: FQDN

بيتم استخدامه من اجل الويب سيرفر (خارجي) او ويب سيرفر داخل الشبكة او يمكن استخدامه في load balancing حيث سوف نقوم بإنشاء FQDN لموقع معين لكي نستطيع الاتصال به عبر الاسم بدلا عن الايبي

فيمكن كتابته بعده صيغ:

www.marfadi.com

marfadi.com

*.marfadi.com

Geography : انشاء عنوان بحسب الموقع) المنطقة الجغرافيه)

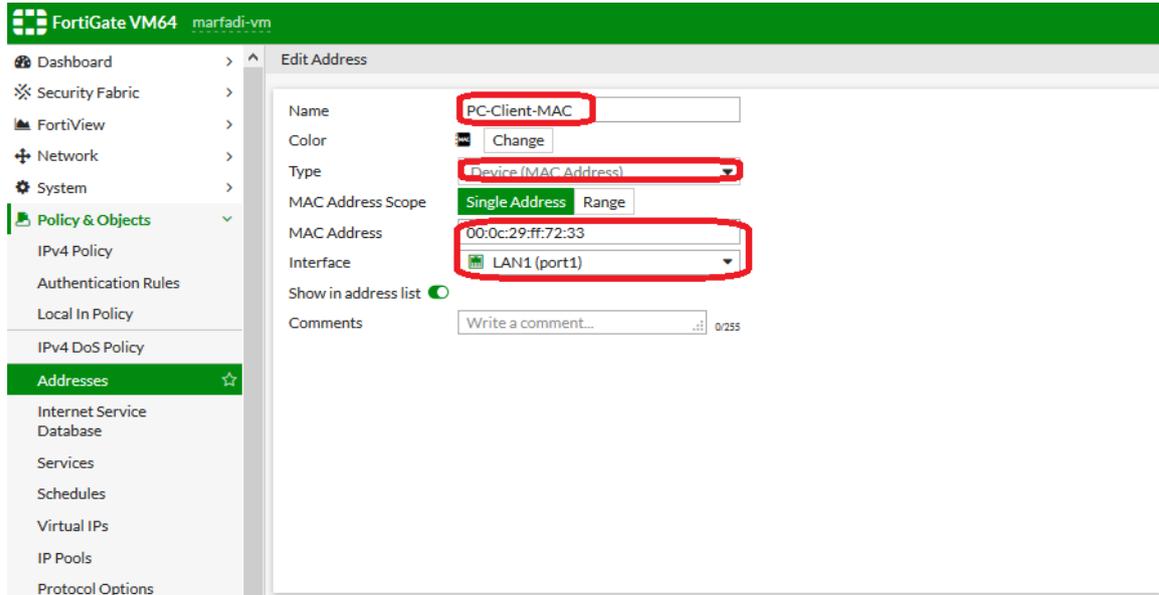
مثلا لديك موظفين موجودين في مصر ويديروا الدخول الى الشبكة الداخليه التي عندي عبر الفورتى جيت بواسطة الvpn

حيث قمت بعمل بولييسي وتقول فيها انا لريد فقط ال VPN Clients القادم من مصر فقط فلو أي شخص حاول الدخول من دوله أخرى فلن يقدر لأنى حددت العنوان بالمنطقة) مصر

او مثلا سمعت عن هجمات الكترونية من دوله معينه فتقوم بإنشاء عنوان بحسب المنطقة تلك ومن ثم تعمل بولييسي تمنع فيها المنطقة المحدده.

MAC DEVICE : -1

عمل عنوان بحسب الماك ادرس للجهاز



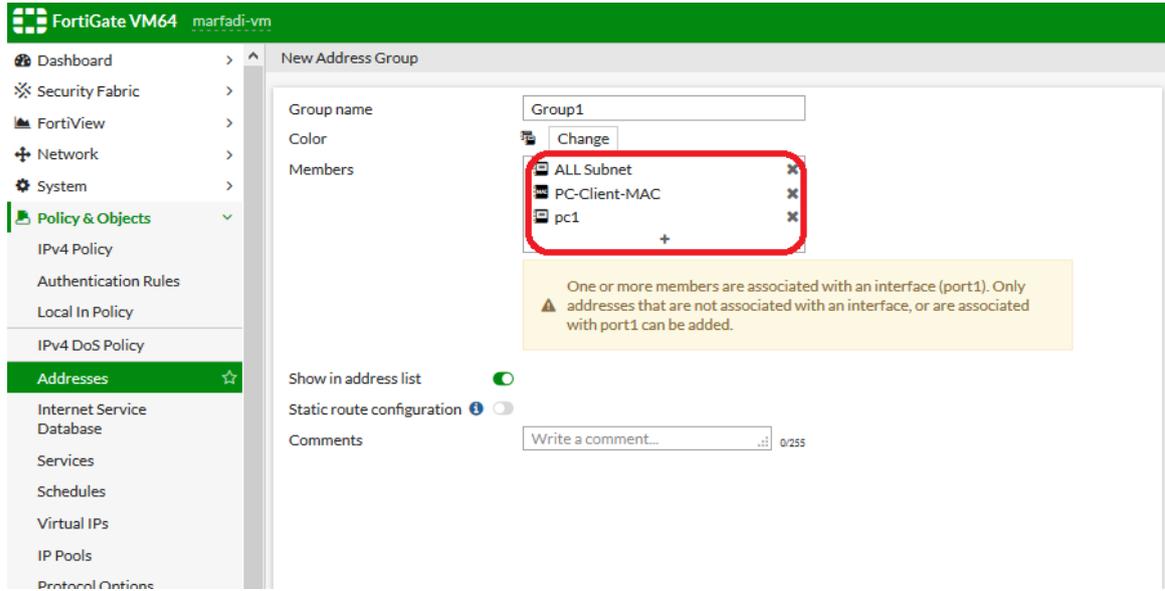
ماهي فكره الـ Address group

الجروب هي مجموعة من العناوين..

حيث ساقوم بإنشاء جروب باسم Group1 واختار منها أي عنوان لريده من العناوين التي قمت بإنشاءها سابقا لكي اطبق عليهم شيء معين..

طريقة انشاء Address group

Name	Type	Details	Interface	Visibility	Ref
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	2
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (sslroot)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1



❖ شرح بعض اعمده الـ address list :

Visibility : هو عمود يوضح بأن العنوان المحدد متاح (visible) او مخفي (Hidden) وهذا معناه بأن هذا

العنوان سوف يظهر او لا في البوليسي ..

فلو معمول له صح فأن هذا العنوان سيكون متاح وسوف يظهر في البوليسي .

اما لو كان معمول له X فهذا يعني بأن العنوان لن يظهر في البوليسي .

لاحظ بان العنوان pc1 معمول له visible لذا سوف يكون متاح في البوليسي كما بالصورة التالية:

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	2
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	2
pc2	Subnet	192.168.2.122/32		Visible	0
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1

أساسيات فورتني جيت

The screenshot shows the FortiGate configuration interface for an IPv4 Policy. The 'Source' field is set to 'pc1' and the 'Destination' field is set to 'all'. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Flow-based'. The 'Firewall / Network Options' section shows 'NAT' is enabled and 'IP Pool Configuration' is set to 'Use Outgoing Interface Address'. The 'Security Profiles' section shows 'AntiVirus' and 'Web Filter' are disabled. A 'Select Entries' dialog box is open on the right, showing a list of entries with 'pc1' selected.

فلو قمنا بتغيير الخاصية الى Hidden للعنوان pc1 كما بالصورة التالية:

The screenshot shows the 'Edit Address' configuration for 'pc1'. The 'Name' is 'pc1', 'Type' is 'Subnet', 'IP/Netmask' is '192.168.2.144/32', and 'Interface' is 'LAN1 (port1)'. The 'Show in address list' checkbox is unchecked, and a red arrow points to it. The 'Static route configuration' checkbox is also unchecked.

فلاحظ بان الخاصية في address list للعنوان pc1 أصبحت Hidden.

System	Object Name	Type	Value	Visibility	Count
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	2
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Hidden	2
pc2	Subnet	192.168.2.122/32		Visible	0
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1

لذا عند محاوله اختيار العنوان pc1 في البوليسي فانه لن يظهر أصلا

The screenshot shows the 'Edit Policy' window in Fortinet's management console. The policy name is 'private'. The incoming interface is 'LAN1 (port1)' and the outgoing interface is 'WAN (port2)'. The source is set to 'all' and the destination is also 'all'. The schedule is 'always' and the service is 'ALL'. The action is 'ACCEPT'. The inspection mode is 'Flow-based'. Under 'Firewall / Network Options', NAT is disabled, and 'Use Outgoing Interface Address' is selected. The 'Security Profiles' section shows 'AntiVirus' is disabled. On the right, the 'Select Entries' list shows various objects, but 'pc1' is not visible, while other subnets like 'all', 'server1', and 'servers' are visible.

لاحظ كما بالصورة أعلاه بأن العنوان PC1 غير متاح حاليا...

Visibility مرتبط بـ interface.

مثلا العنوان pc1 في عمود ال interface غير مكتوب فيه أي شيء فهذا يعني بأن العنوان pc1 مرتبط مع

any interface اي سوف يظهر لأي interface سواء lan او wan.

أساسيات فورتني جيت

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	2
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl/root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32		Visible	2
pc2	Subnet	192.168.2.122/32		Visible	0
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0

لاحظ بالصورة أعلاه بأن العنوان PC-Client-MAC معمول له visible ومرتبطة مع ال LAN1(port1) interface فإذنا interface يعني بأن هذا العنوان لن يظهر إلا لو كان ال interface نوع LAN1 ماعدا ذلك فإنه لن يظهر كما بالصورة أدناه:

حيث ظهر العنوان PC-Client-MAC في خانة ال source لـ LAN1 incoming interface = outgoing interface = WAN(port2) لأننا قمنا بربط العنوان PC-Client-MAC مع ال LAN1 interface فقط..

أساسيات فورتني جيت

The screenshot shows the 'Edit Policy' configuration in Fortinet FortiGate. The 'Outgoing Interface' is set to 'WAN (port2)' and the 'Destination' is set to 'all'. A 'Select Entries' dialog box is open, showing a list of entries with 'all' selected. The 'Source' is set to 'PC-Client-MAC'. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is set to 'Flow-based'.

Outgoing interface = wan لأن Destination لم يظهر في PC-Client-MAC أعلاه بالصوره أعلاه
لذا لن يظهر ال PC-Client-MAC الا ان كان outgoing interface = lan1 لأن في الأساس رابط العنوان
PC-Client-MAC مع ال interface = lan1

الخلاصة:

العنوان لو تم ربطه بال interface نوعه any فهذا يعني بان هذا العنوان سيظهر في كل ال interfaces
اما لو تم ربط العنوان بال interface مثلا LAN1 فهذا يعني بأن هذا العنوان لن يظهر الا مع ال interface
Lan1 فلو تم اختيار ال interface = lan2 فأن هذا العنوان لن يظهر..

Incoming interface = source

Outgoing interface = Destination

Ref : عمود فيه ارقام يدل على ربط (استخدام) هذا العنوان مع أشياء في الفورتني جيت سواء مع بولييسي
او جروب او غيرها ...

أساسيات فورتني جيت

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:c2:9f:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	0
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	2
pc2	Subnet	192.168.20.122/32	WAN (port2)	Visible	0
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1
ALL Subnet	Subnet	0.0.0.0/0	LAN1 (port1)	Visible	0

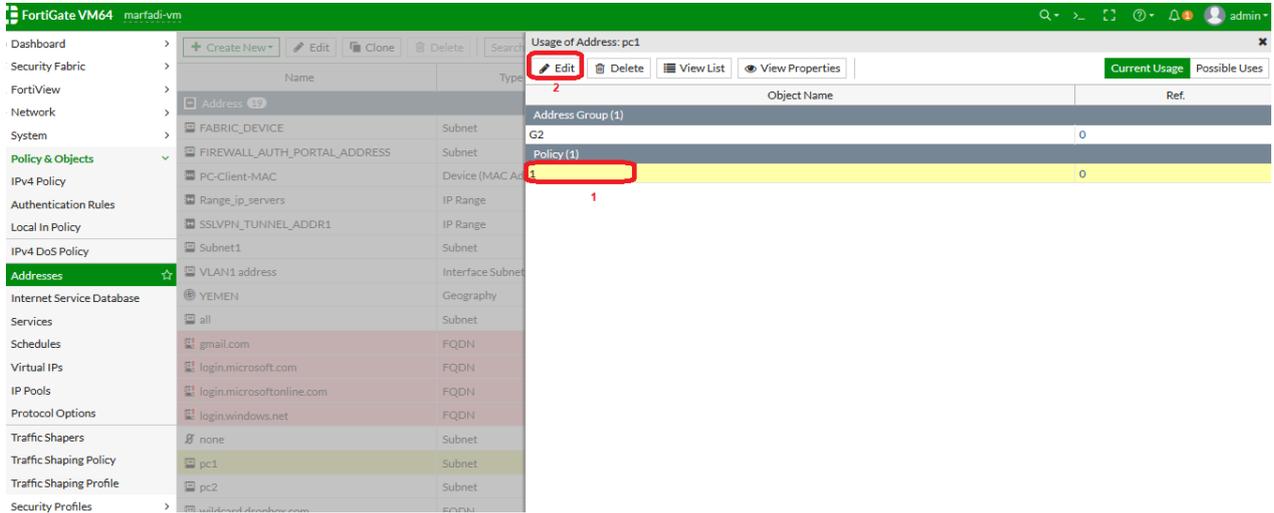
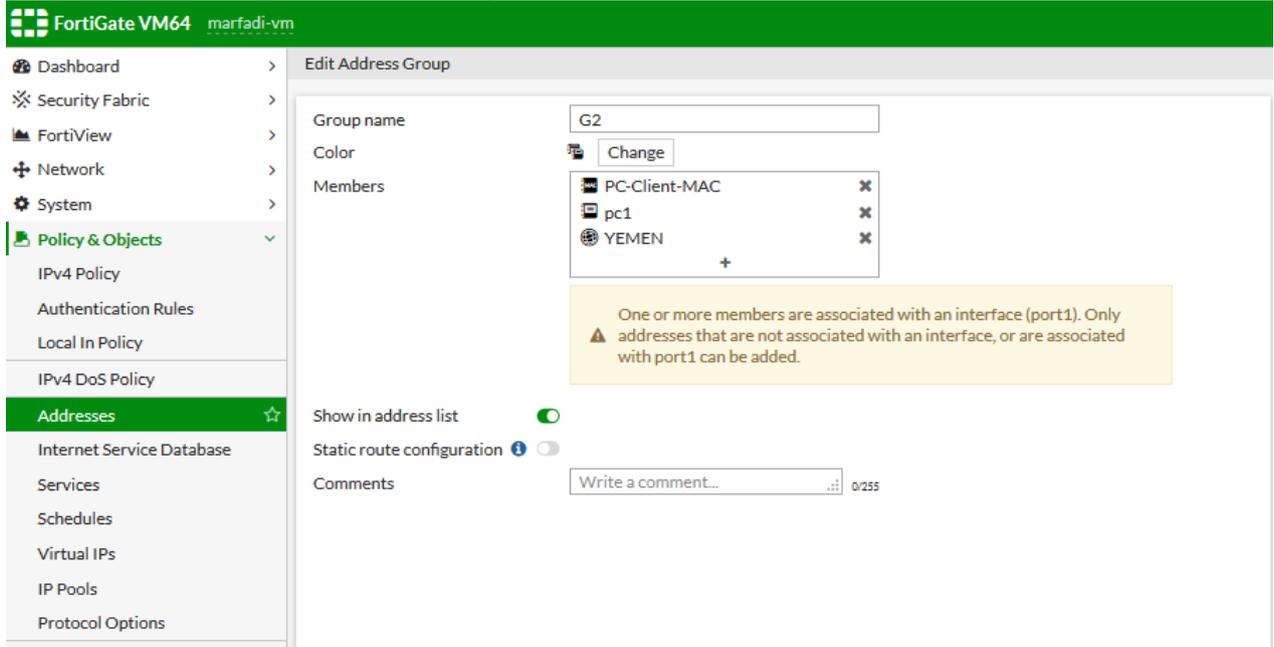
Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:c2:9f:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	0
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	2
pc2	Subnet	192.168.20.122/32	WAN (port2)	Visible	0
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1
ALL Subnet	Subnet	0.0.0.0/0	LAN1 (port1)	Visible	0

لاحظ بأن العنوان pc1 الـ ref=2 وهذا يدل بأن العنوان مرتبط مع 2 أشياء فبمجرد النقر على العدد 2 يفتح لك مكان الربط

Object Name	Ref.
Address Group (1)	0
Policy (1)	0

كما بالصورة أعلاه فإن العنوان مرتبط مع address group=G2 ..

فلو حددت على الجروب G2 ثم نقرت على edit سوف يفتح لك الجروب المسماة G2 كما بالصورة ادناه
فيمكنك التعديل على الجروب او حذف العنوان pc2 من هذا الجروب ... الخ .



عند النقر على ال (1) policy سوف يظهر شاشة ال policy كما بالصورة التالية:

Services

أساسيات فورتني جيت

عبره عن بروتوكولات وبورتات حيث أي نظام تشغيل يحتوي على بورتات يستخدمها لكي يقوم بعملية الإرسال والاستقبال للبيانات مع جهاز آخر.

حيث كل بروتوكول يستخدم بورت معين حيث من 1-1024 هذا لرقام بورتات محجوزة للأعمال القياسية ومن 1025- 65535

يمكن استخدامه لأي تطبيق..

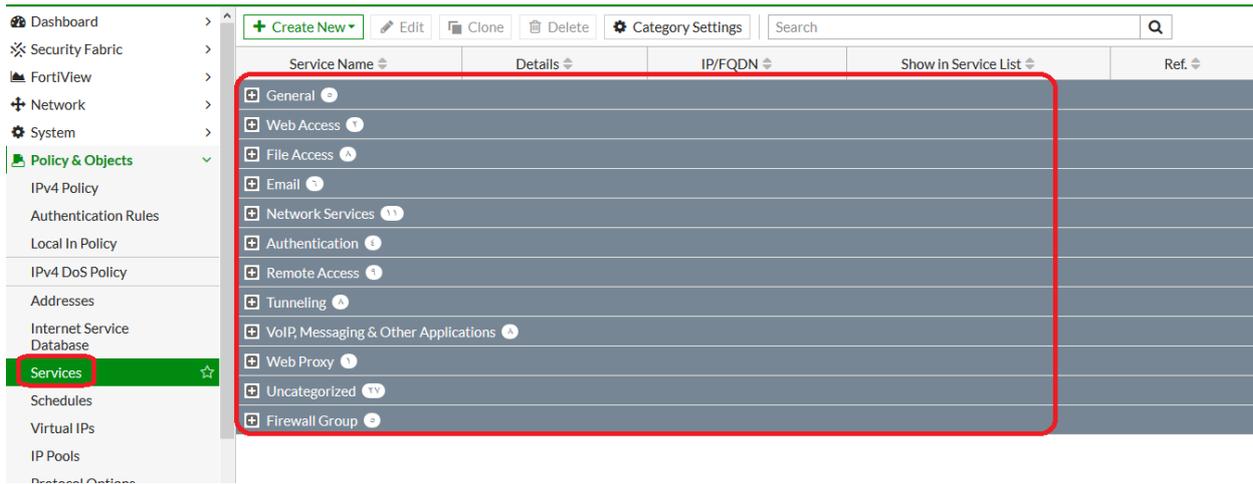
لوقدرت تتحكم في البروتوكولات والبورتات فأنتك تستطيع التحكم بالتطبيقات التي يستخدمها المستخدم..

الفورتني جيت يستخدم السيرفيس لتحديد رقم البورت لعمل

Accept or deny للترافيك

All معناها كل البورتات ..

حيث تظهر لك كل السيرفيس الموجودة بالفورتني جيت بشكل افتراضي حيث تم تقسيم البروتوكولات بشكل تصنيفات كما بالصورة ادناه.



حيث توضح التصنيف مثللا ويب اكسس او ايميلات اوريموت اكسس.. الخ وماهي البروتوكولات المدرجه تحته وكم لرقامها

أساسيات فورتى جيت

Service Name	Protocol	IP/Port	IP/Port	Visibility	Count
DCE-RPC	TCP/135 UDP/135	0.0.0.0	0.0.0.0	Visible	2
PC-Anywhere	TCP/5631 UDP/5632	0.0.0.0	0.0.0.0	Visible	0
ONC-RPC	TCP/111 UDP/111	0.0.0.0	0.0.0.0	Visible	0
SSH	TCP/22	0.0.0.0	0.0.0.0	Visible	0
TELNET	TCP/23	0.0.0.0	0.0.0.0	Visible	0
X-WINDOWS	TCP/6000-6063	0.0.0.0	0.0.0.0	Visible	0
RDP	TCP/3389	0.0.0.0	0.0.0.0	Visible	0
VNC	TCP/5900	0.0.0.0	0.0.0.0	Visible	0
WINS	TCP/1512 UDP/1512	0.0.0.0	0.0.0.0	Visible	0

الصورة أعلاه توضح التصنيف الخاص بالوصول عن بعد وماهي البروتوكولات وأرقام البورتات المستخدمة في هذا التصنيف.

ماهي أنواع الـ services ؟

1- Services

2- Service group : مجموعة من الـ services سوف تقوم بتطبيق بوليسي معينه عليهم حيث تعتبر كنوع من التنظيم .

3- Category : مجموعة من الـ services تتشابه في نفس الخصائص مثل category خاصه بـ web access الخاصة بتصفح الانترنت حيث تحتوي على http و https او الخاصة باستقبال وارسال الايميل

المسماة email وتحتوي على البروتوكولات الاتيه imap,pop,smtp وغيرها

Service Name	Protocol	IP/Port	IP/Port	Visibility	Count
HTTP	TCP/80	0.0.0.0	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	0.0.0.0	Visible	2

Service Name	Details	IP/FQDN	Show in Service List	Ref
HTTP	TCP/80	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	Visible	2
IMAP	TCP/143	0.0.0.0	Visible	1
IMAPS	TCP/993	0.0.0.0	Visible	1
POP3	TCP/110	0.0.0.0	Visible	1
POP3S	TCP/995	0.0.0.0	Visible	1
SMTP	TCP/25	0.0.0.0	Visible	1
SMTPS	TCP/465	0.0.0.0	Visible	1

مثلا لريد انشاء services لجهاز الـ DVR حيث لريد تخصيص بورتات معينه للتعامل مع هذا الجهاز :

Service Name	Details	IP/FQDN	Show in Service List	Ref
HTTP	TCP/80	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	Visible	2
IMAP	TCP/143	0.0.0.0	Visible	1
IMAPS	TCP/993	0.0.0.0	Visible	1
POP3	TCP/110	0.0.0.0	Visible	1
POP3S	TCP/995	0.0.0.0	Visible	1
SMTP	TCP/25	0.0.0.0	Visible	1
SMTPS	TCP/465	0.0.0.0	Visible	1

Show in Service List لكي تظهر معك بالبوليسي .

TCP : Protocol يكون اكثر موثوقية ولكن بطئ مقلنه بالبروتوكول UDP الذي يعتبر اقل موثوقية واكثر سرعه ..

البروتوكولات التي من نوع TCP هي HTTP وHTTPS... الخ

UDP يستخدم لنقل البيانات التي تحتاج الى سرعه ولا تهتم بالوثوقيه (يعني في حالة نقصان او ضياع البيانات في الارسال فإنه لا يقوم بإعادة الارسال مره اخرى بعكس الـ TCP) مثل الصوت والفيديو وغيرها ومن اشهر البروتوكولات التي بيتعامل مع UDP هي (DNS-VOIP-NTP-media stream protocols)

حيث تختلر نوع البروتوكول هل TCP او UDP حسب السيرفيس المستخدمة

SCTP: هذا النوع من البروتوكولات يعتبر يجمع بين الtcp و udp حيث انه سريع وبنفس الوقت موثوق

The screenshot shows the 'New Service' configuration page in the FortiGate VM64 interface. The 'Name' field is set to 'NVR'. The 'Comments' field contains 'This service for NVR Device'. The 'Color' field is set to 'Change'. The 'Show in Service List' checkbox is checked. The 'Category' dropdown is set to 'Uncategorized'. Under 'Protocol Options', the 'Protocol Type' is set to 'TCP/UDP/SCTP'. The 'Address' field is set to 'IP Range' with 'FQDN' and '0.0.0.0'. The 'Destination Port' section has two entries: 'UDP 10000' and 'TCP 10000', both with 'High' priority. The 'Specify Source Ports' checkbox is unchecked. The 'OK' button is highlighted.

كما بالصورة أعلاه تم انشاء service باسم NVR وسوف تندرج تحت التصنيف Uncategorized ونوع البروتوكول سوف يكون UDP والبورت الافتراضي لأغلب اجهزه الNVR تكون 10000 حيث اخترنا نوع البروتوكول UDP لأننا سوف ننقل بيانات من نوع streaming أي فيديو وصوت .. الخ

وايضا اجهزه الNVR تستخدم الip وهذا يحتاج الى البروتوكول TCP والبورت أيضا 10000 ..

حيث قمنا بتحديد بأن الnvr سوف يكون هدف (Destination Port) وليس مصدر أي اننا لو اردنا الوصول الى جهاز الnvr سوف يكون على البورت 10000

اما لو اردنا ان نقوم بتحديد اكثر ونريد ان نقوم بإخراج جهاز الnvr من بورت معين فأننا سوف بتفعيل الخيار Specify Source Ports ..

أساسيات فورتى جيت

Service Name	Protocol	Ports	IP Address	Visibility	Count
TIMESTAMP	ICMP/ANY			Hidden	0
INFO_REQUEST	ICMP/ANY			Hidden	0
INFO_ADDRESS	ICMP/ANY			Hidden	0
QUAKE	UDP/26000 UDP/27000 UDP/27910 UDP/27960			Hidden	0
RAUDIO	UDP/7070			Hidden	0
REXEC	TCP/512			Hidden	0
RLOGIN	TCP/513			Hidden	0
RSH	TCP/514			Hidden	0
TALK	UDP/517-518			Hidden	0
MGCP	UDP/2427 UDP/2727			Hidden	0
UUCP	TCP/540			Hidden	0
VDOLIVE	TCP/7000-7010			Hidden	0
WAIS	TCP/210			Hidden	0
WINFRAME	TCP/1494 TCP/2598			Hidden	0
PING6	ICMP6/ANY			Hidden	0
RADIUS-OLD	UDP/1645 UDP/1646			Hidden	0
CVSPSERVER	TCP/2401 UDP/2401			Hidden	0
MMS	TCP/1755 UDP/1024-5000			Hidden	0
NONE	TCP/0			Hidden	0
Marfadi	TCP/8885			Visible	0
NVR	TCP/1000 UDP/10000			Visible	0

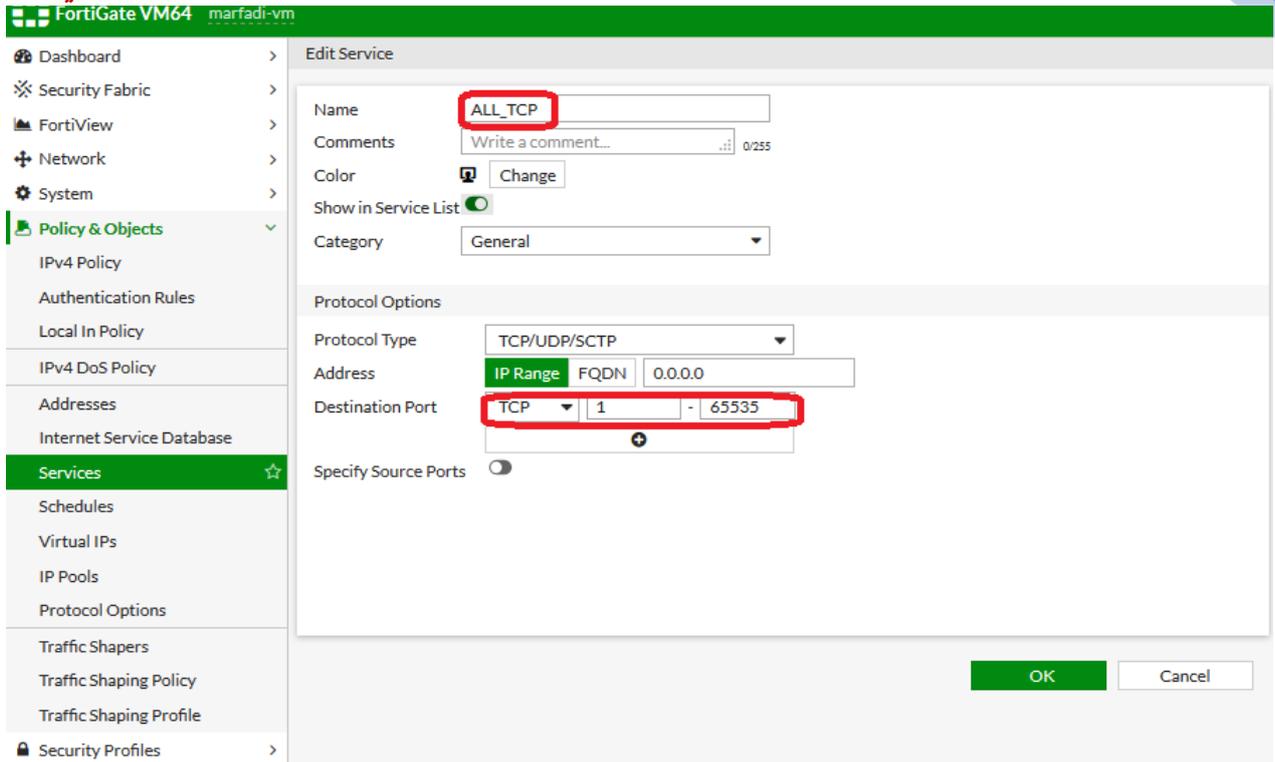
تمت الاضافة بنجاح لل service المسماة NVR ..

حيث يمكن استخدامها في البولي سي كما بالصورة ادناه

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar is expanded to 'Policy & Objects' and 'IPv4 Policy'. The main area displays the 'Edit Policy' configuration for a policy named 'allow_all'. The configuration includes:

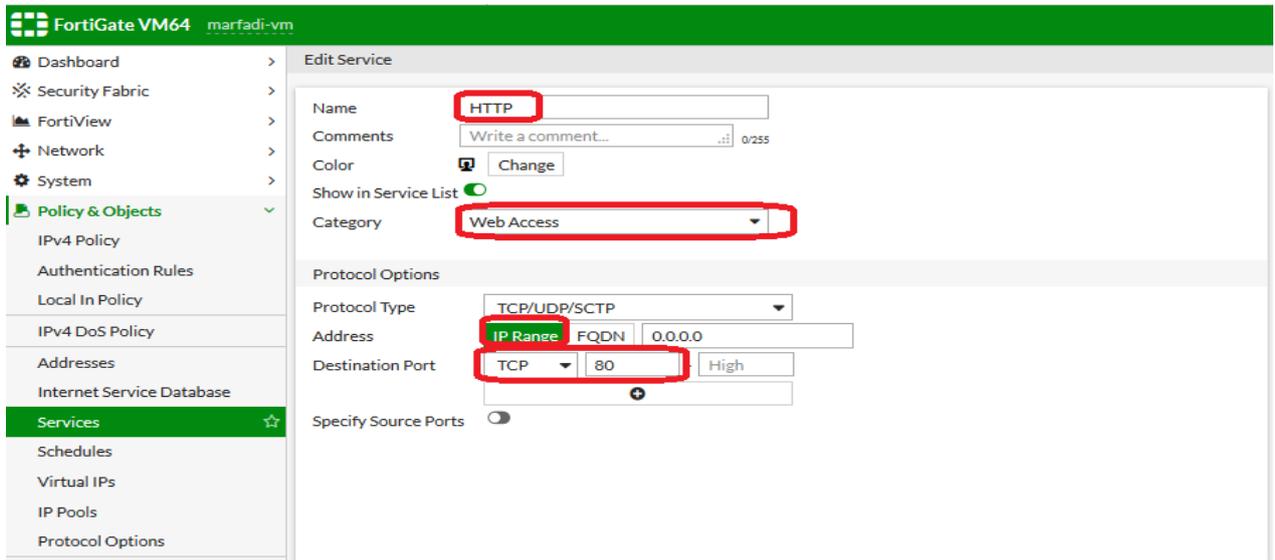
- Name:** allow_all
- Incoming Interface:** LAN1 (port1)
- Outgoing Interface:** WAN (port2)
- Source:** pc1
- Destination:** all
- Schedule:** always
- Service:** NVR (highlighted with a red box)
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:**
 - NAT:** Enabled
 - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool (unselected)
 - Preserve Source Port:** Disabled
 - Protocol Options:** PRX default
- Security Profiles:** AntiVirus (disabled)

فمن ال services الافتراضية التي منشاه أصلا هي all_tcp كما موضح بالصوره



نوع الـ Destination port=Tcp البورت من 1-65535 .

وأيضاً الـ service الخاصة بـ http كما بالصورة ادناه



وأيضاً لـ pop كما بالصورة ادناه ...

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Services

Edit Service

Name: POP3

Comments: Write a comment... 0/255

Color: Change

Show in Service List:

Category: Email

Protocol Options

Protocol Type: TCP/UDP/SCTP

Address: IP Range FQDN 0.0.0.0

Destination Port: TCP 110 High

Specify Source Ports:

OK Cancel

ما هو الـ service group :

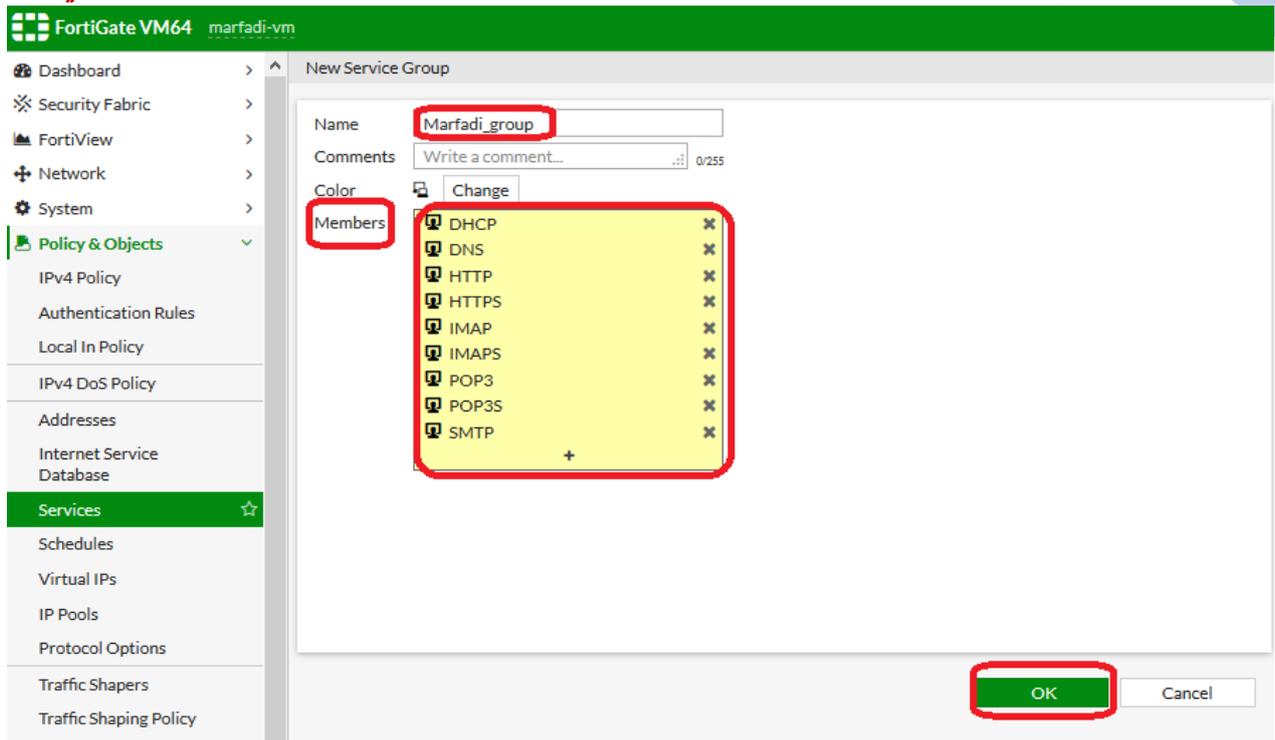
هي عملية انشاء group تتكون من مجموعة من الـ service التي أنشأناها مسبقا .

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Services

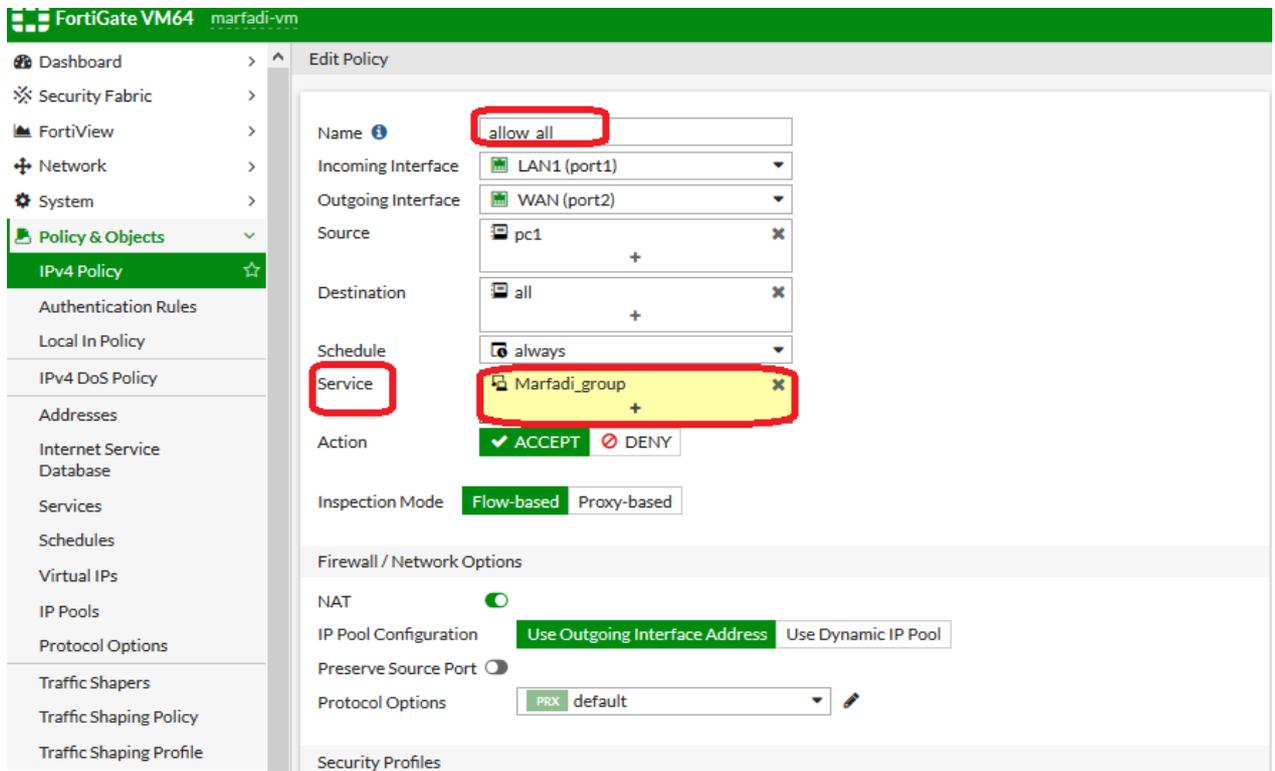
+ Create New - Service Service Group

Service Name	Details	IP/FQDN	Show in Service List	Ref.
ALL	ANY		Visible	0
ALL_TCP	TCP/1-65535	0.0.0.0	Visible	0
ALL_UDP	UDP/1-65535	0.0.0.0	Visible	0
ALL_ICMP	ANY		Visible	0
ALL_ICMP6	ANY		Visible	0
Web Access				
HTTP	TCP/80	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	Visible	2
File Access				
Email				
IMAP	TCP/143	0.0.0.0	Visible	1
IMAPS	TCP/993	0.0.0.0	Visible	1
POP3	TCP/110	0.0.0.0	Visible	1



وبهذا قمنا بإنشاء مجموعة اسمها Marfadi_group تحتوي على مجموعة من ال service كما بالصورة أعلاه ..

فبهذا لو اردنا تطبيق البوليسي ونختار ال Marfadi_group التي انشاناها مؤخرا ..



هي عبارة عن احدى العناصر التي سيتم اختيارها عند انشاء البوليسي .

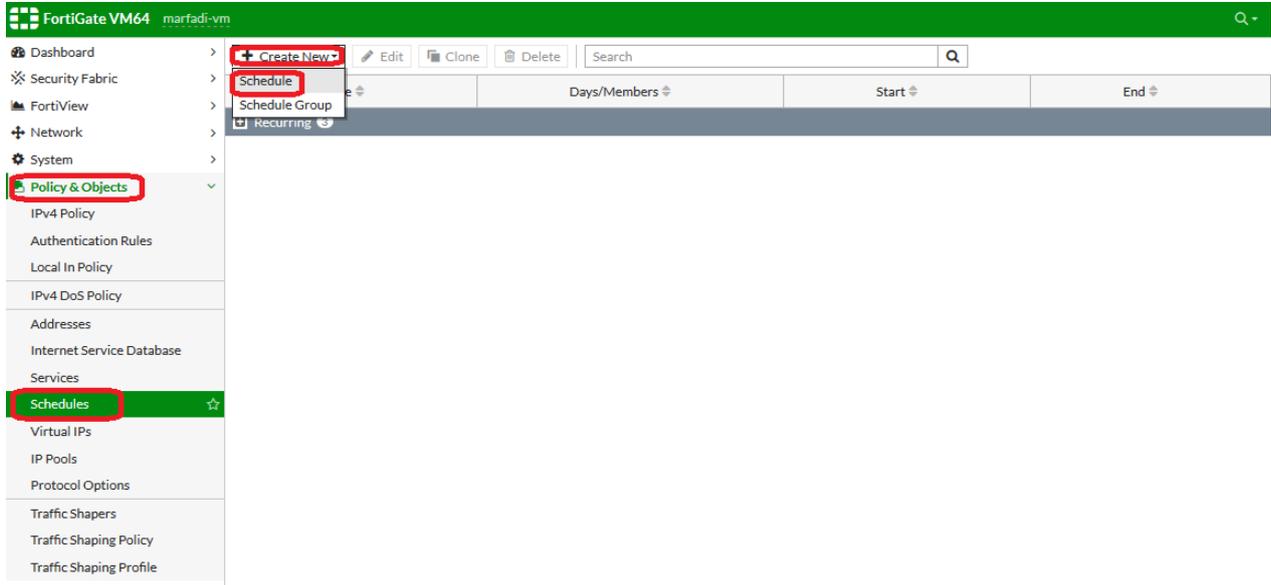
لماذا أقوم بعمل جدول زمني (schedule) عند تطبيق البوليسي ؟

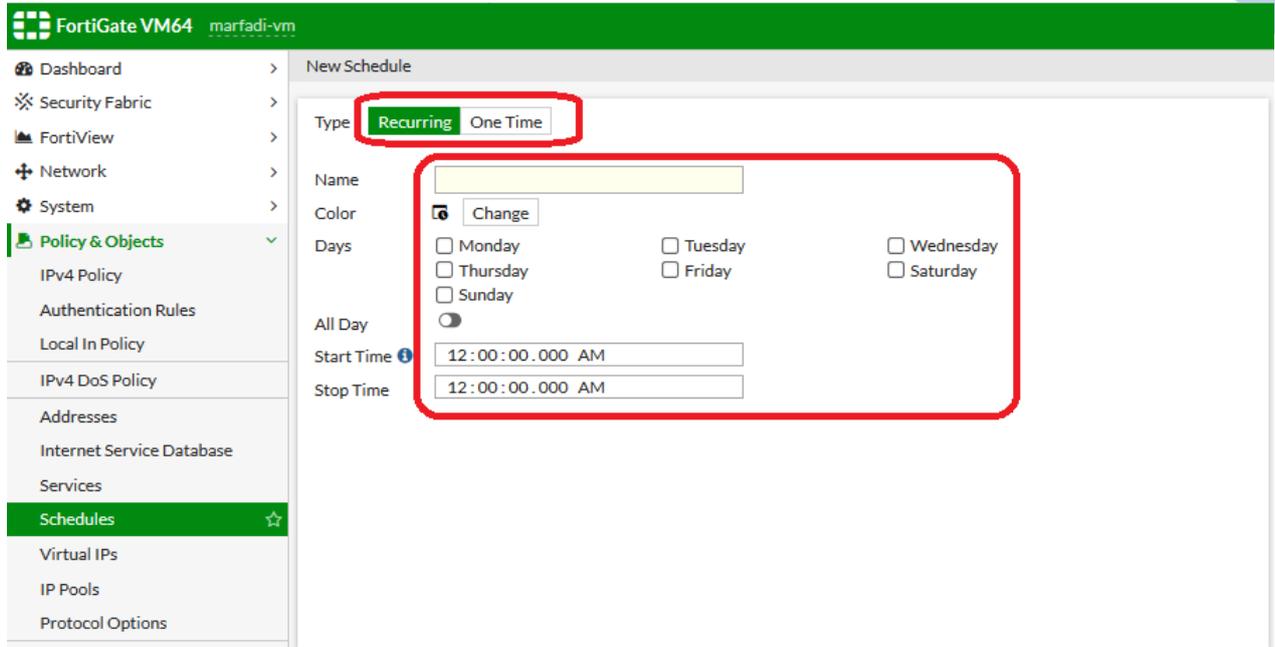
لأن بعض الأحيان اريد ان أقوم بتطبيق البوليسي في وقت معين او حدث معين .حيث لا يمكنك ان تنشئ بوليسي بدون تحديد الـ schedule حيث القيمة الافتراضية له هي always يعني ان هذا البوليسي سوف تطبق بشكل دائم.

الـ schedule مقسم الى نوعين :

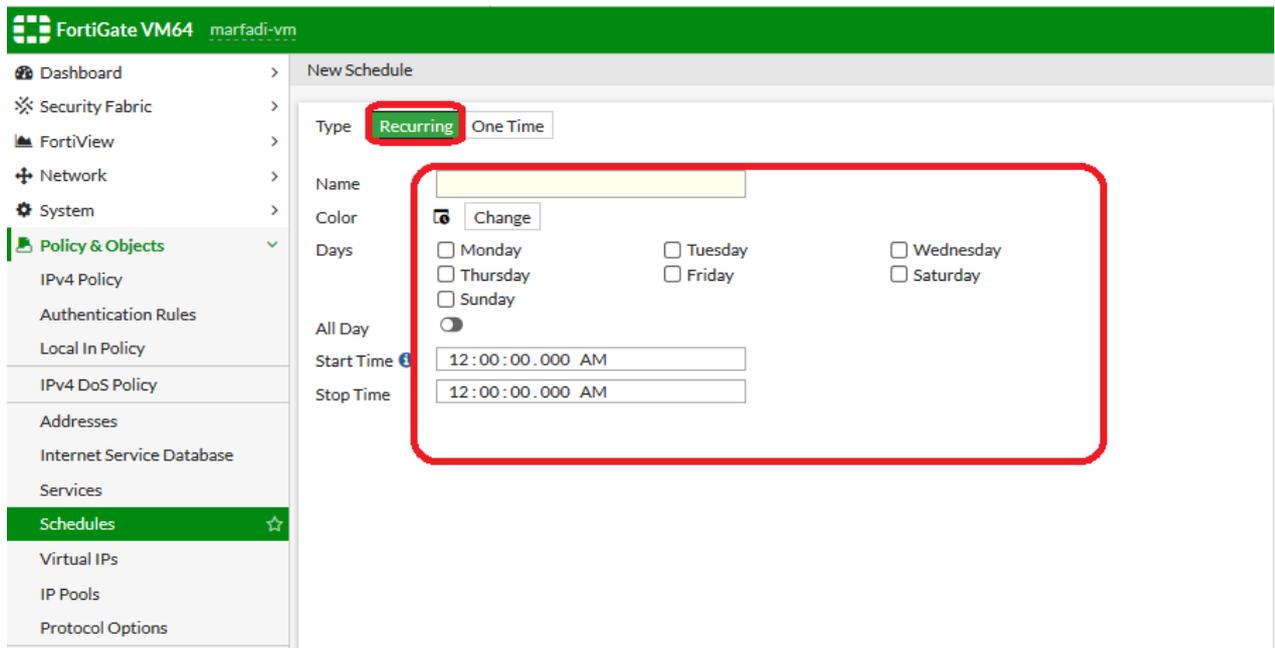
- 1 Recurring :بوليسي سوف تطبق بشكل متكرر مثلا اريد تطبيقها كل أسبوع او كل يوم او كل يوم معين او مرتين بالأسبوع ..الخ أي ان العملية متكرره .
- 2 One-time : بوليسي سوف تطبق مره واحده وفي وقت محدد فقط .

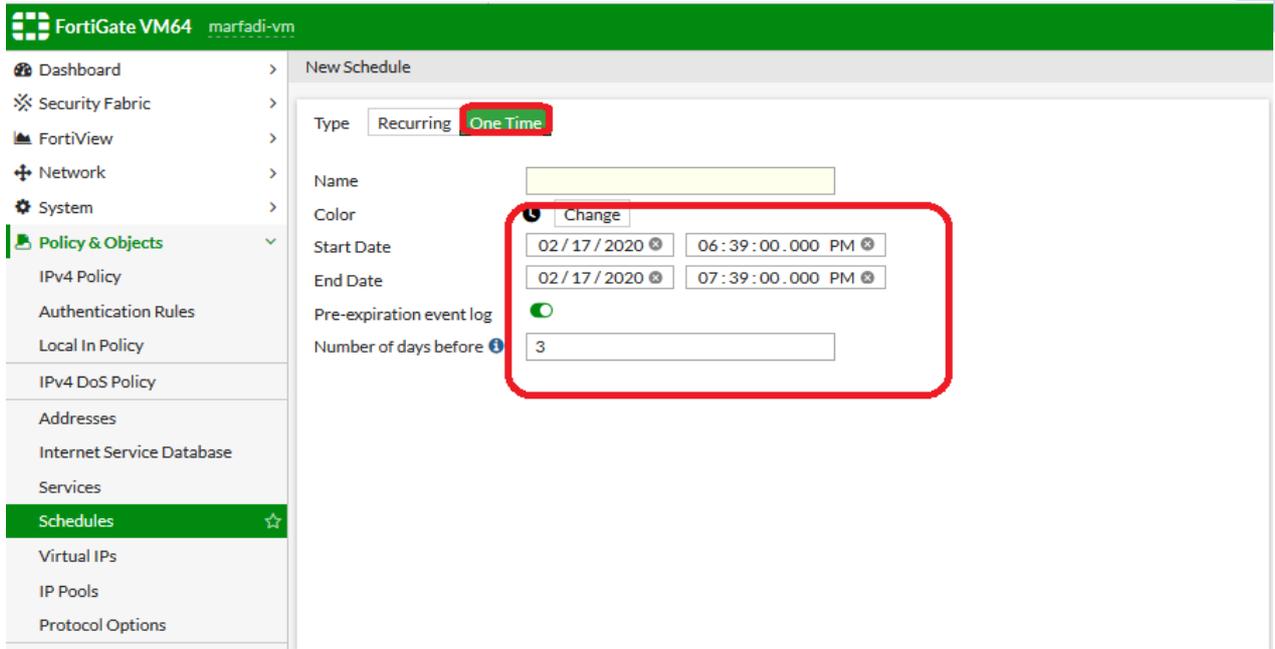
➤ **طريقة انشاء schedule جديد :**



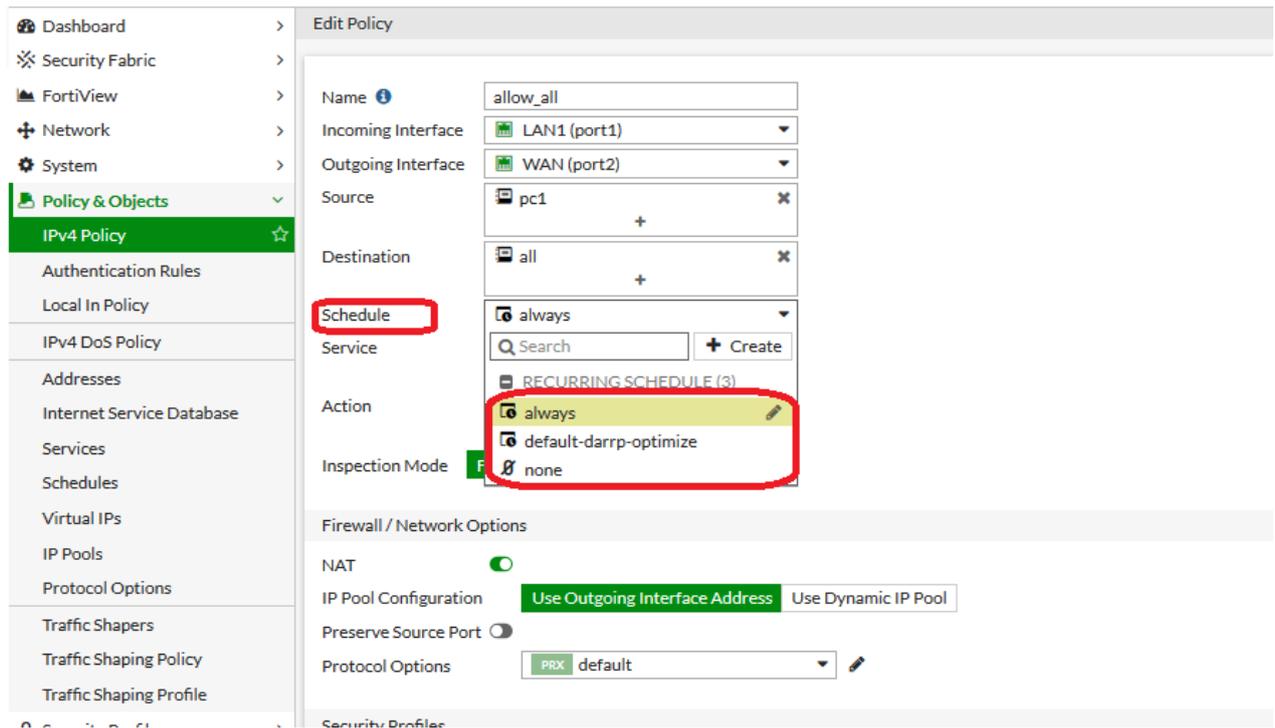


ثم نحدد النوع كما شرحناه سابقا ..





حيث نلاحظ بأنه يوجد لدينا 3 قيم افتراضيه من ال schedule كما بالصورة ادناه



حيث الاختيار always معناها طبق البوليسي بشكل دائم .

اما الخيار none وهذا معناها بان لا تقوم بتطبيق البوليسي وكأنك عملت في ال deny=action أي لا احد سوف يتم تطبيق هذه البوليسي عليه ..

Name	Days/Members	Start	End	Ref
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	1
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0

كما بالصورة أعلاه يوضح بأن الخيار `always` سيتم تطبيقه في كل الأيام وفي كل الأوقات من `00:00:00` الى `00:00:00`

اما الخيار `none` فهذا يعني بأنه لن يتطبق بأي يوم ولا في أي وقت .

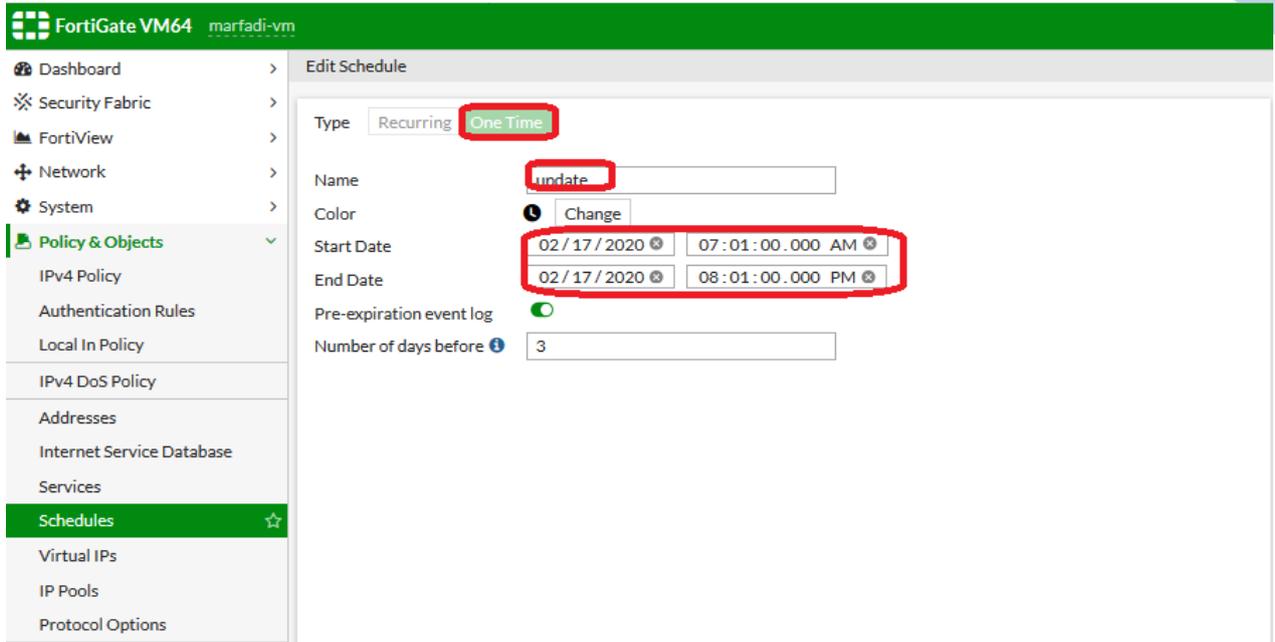
مثلا سوف أقوم بإنشاء `schedule` باسم `work_time` أي أوقات العمل بالشركة :

The image shows two screenshots from the FortiGate VM64 management interface. The top screenshot displays the 'New Schedule' configuration window. The 'Type' is set to 'Recurring', and the 'Name' is 'work time'. The 'Days' section is checked for Monday, Tuesday, Wednesday, Thursday, and Saturday. The 'Start Time' is 08:00:00.000 AM and the 'Stop Time' is 03:00:00.000 PM. The bottom screenshot shows the 'Schedules' table with the following data:

Name	Days/Members	Start	End	Ref
Recurring				
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	1
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0
work_time	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	0

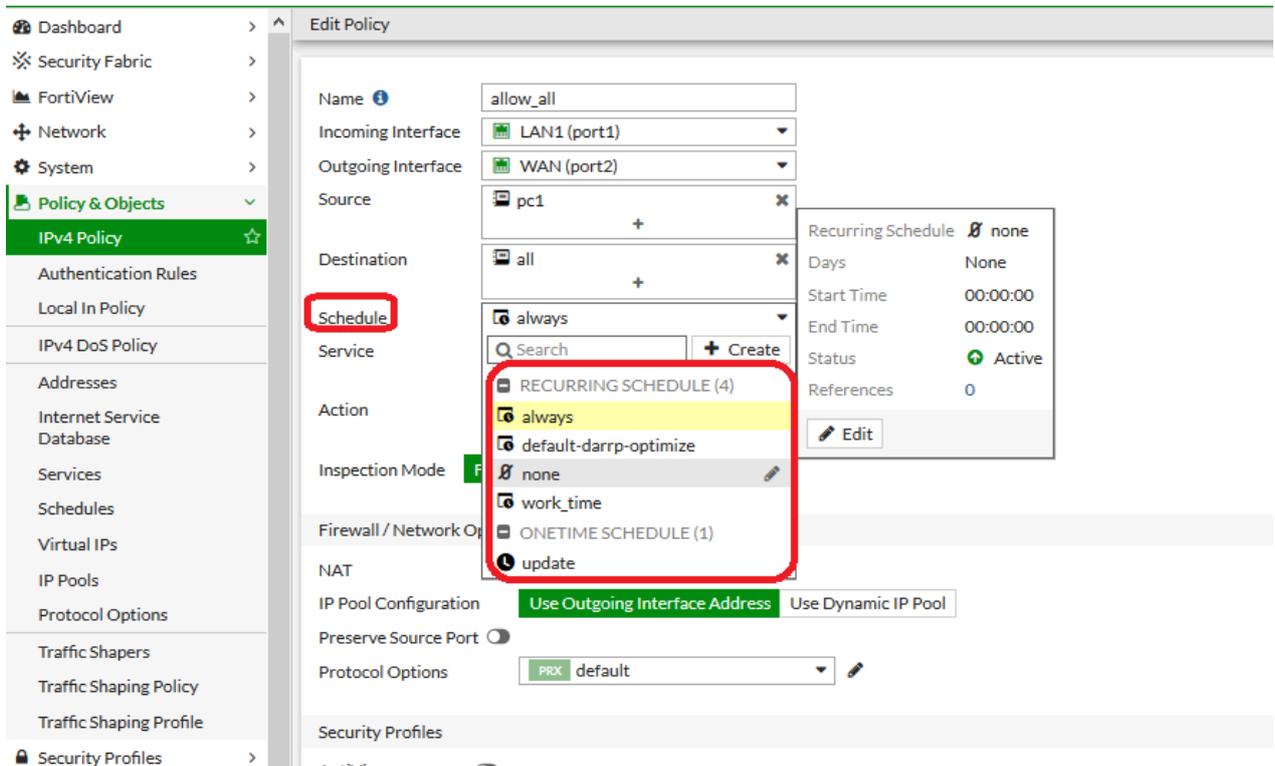
الآن سوف نقوم بإنشاء schedule باسم update حيث لن تعمل الا مره واحده وبتاريخ معين ووقت

معين



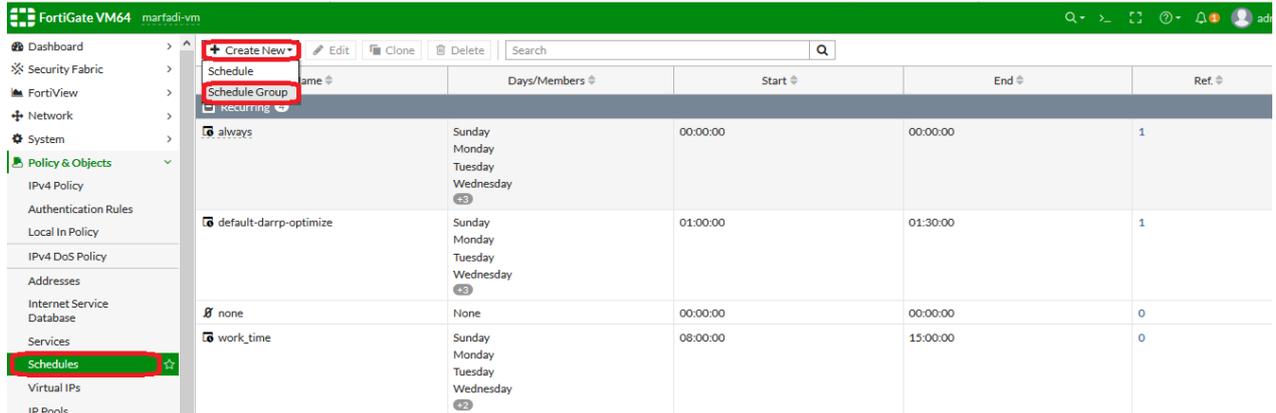
النوع One-time يستخدم في حالة كان لديك في الشركة اجتماع في تاريخ معين مره واحده ويحتاجوا يفتحوا مثلا موقع معين وليكن اليوتيوب فأننا سوف أنشئ هذه ال schedule واختارها في البوليسي حيث هذه البوليسي سوف يتم تطبيقها مره واحده وبيوم واحد فقط ولن تتكرر ..

الان بعد انشاء ال schedule سوف نختارها عند انشاء البوليسي ما نريده هل
: always,none,work_time,update



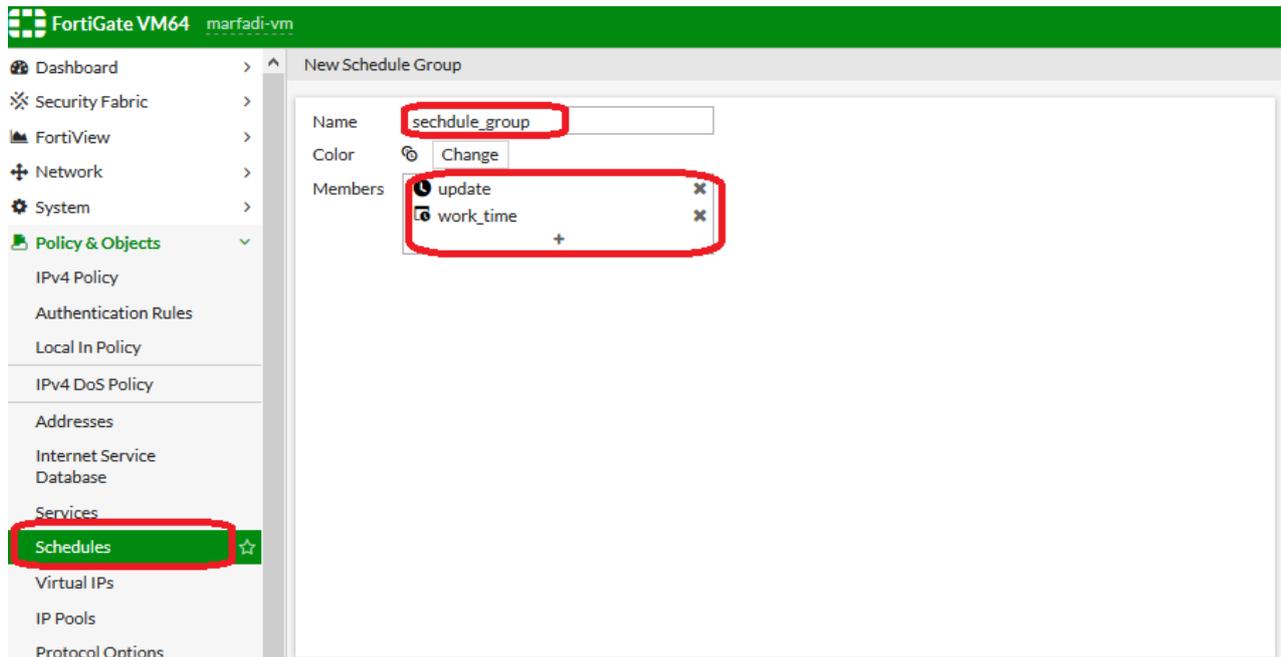
طريقة انشاء *schedule group* :

يتم استخدامها لإنشاء مجموعة مكونة من أكثر من *schedule* بغض النظر عن نوعها هل *one-time* او *recurring* ..



The screenshot shows the FortiGate VM64 interface with the Schedules page open. The 'Create New' button is highlighted in red, and the 'Schedule Group' dropdown menu is also highlighted in red. The table below lists existing schedules:

Name	Days/Members	Start	End	Ref
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	1
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0
work_time	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	0



The screenshot shows the 'New Schedule Group' form in the FortiGate VM64 interface. The 'Name' field is set to 'sechedule_group' and is highlighted in red. The 'Members' field contains 'update' and 'work_time', both highlighted in red. The 'Schedules' menu item in the left sidebar is also highlighted in red.

Name	Days/Members	Start	End	Ref.
Recurring				
always	Sunday Monday Tuesday Wednesday	00:00:00	00:00:00	1
default-darrp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	1
none	None	00:00:00	00:00:00	0
work_time	Sunday Monday Tuesday Wednesday	08:00:00	15:00:00	1
One Time				
update		2020/02/17 07:01:00	2020/02/17 20:01:00	1
Group				
schedule group	update work_time			0

➤ نفترض بأن لدينا شركة مواعيد العمل فيها من 8 ص الى 3 عصرا كل يوم ماعدا الجمعة ..

يعني نريد الانترنت على اجهزه الكلاينت يكون فيها متاح خلال دوام العمل فقط ..

اما في السيرفرات يكون الانترنت طوال الوقت .

الحل :

1 – انشاء عنوان باسم subnet1 تحتوي على رينج الشبكة الداخليه كامله
(255.255.255.0/192.168.2.0)

2 – السيرفرات سوف نقوم بعمل ايبيمات استاتيكي حيث سيتم انشاء عنوان باسم server1 بايبي
. 192.168.2.122

3 – انشاء schedule باسم work_time سيكون اوقات العمل .

4 – انشاء 2 بوليسي التي سوف تنفذ ما نريده أعلاه ...

الحل :

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	0
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	1
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	1
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0

كما بالصورة أعلاه تم انشاء العناوين للكلابنت من الـ subnet1 وهي من الـ رينج (32/192.168.2.0) أيضا للسيرفر تم تحديد العنوان server1 وتم تحديد الايبي 192.168.2.122 .

Edit Schedule

Type: **Recurring** One Time

Name: work_time

Color:

Days: Monday Tuesday Wednesday Thursday Friday Saturday

All Day:

Start Time: 08:00:00.000 AM

Stop Time: 03:00:00.000 PM

تم انشاء schedule باسم work_time مسموح فيها من 8 صباحا الى 3 عصرا لكل أيام الاسبوع ماعد الجمعة ..

الآن سوف نقوم بإنشاء البولييسي باسم allow_internet

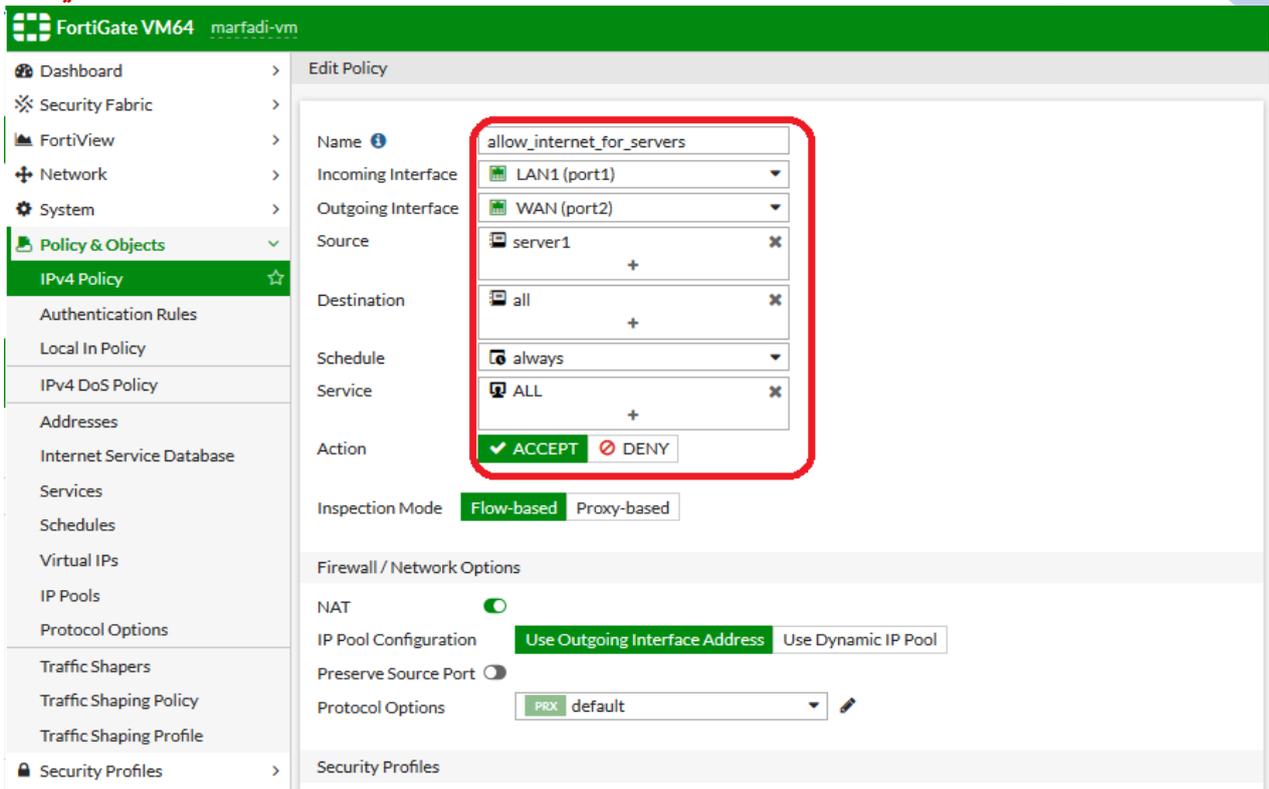
The screenshot shows the 'New Policy' configuration page in FortiGate VM64. The policy is named 'allow_internet'. The configuration details are as follows:

- Name:** allow_internet
- Incoming Interface:** LAN1 (port1)
- Outgoing Interface:** WAN (port2)
- Source:** Subnet1
- Destination:** all
- Schedule:** work_time
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:**
 - NAT:** Enabled
 - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool (unselected)
 - Preserve Source Port:** Disabled
 - Protocol Options:** PRX default

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	912.25 kB

كما

بالصورة أعلاه توضح البوليسي allow_internet بأنه سوف يسمح الانترنت لـ subnet1 (التي ستكون هي اجهزه الكلاينت) في أوقات العمل من السبت الى الخميس (8 صباحا-3 عصرا) فقط .
سوف نظيف بوليسي أخرى باسم allow_internet_for_server والتي ستسمح فيها للسيرفرات بأن تصل الى الانترنت في كل أوقات الأسبوع كما بالصورة ادناه



حيث العنوان server1 تم إعطائه الايبي 192.168.2.122 ولذا فقط السيرفر صاحب هذا العنوان سوف يكون لديه انترنت طوال اليوم حيث نلاحظ بان ال schedule =always .

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	2.06 MB
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	58.45 KB
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	997.72 kB

Policy order ❖

عبارة عن ترتيب البولييسي ..

حيث أحيانا يحصل تداخل في البولييسي (overlap) حيث بمجرد انشاء البولييسي فإن الفورتى جيت يعطيها رقم يسمى policy id ..

حيث البولييسي يتم تطبيقها أولا بحسب الـ policy id (من فوق الى تحت).

حيث اول بولييسي يكون رقمها 1 ثم 2 ثم 3.... الخ ولتفادي تداخل البولييسي يتم ترتيب البولييسي يدويا وذلك بسحب البولييسي الخاصة للأعلى .. الخ.

دائما تقوم بترتيب البولييسي بحيث تكون البولييسي الخاصة بالأعلى والبولييسي العامة تحت وهكذا ..

مثال :

سوف نقوم بإنشاء 2 بولييسي واحده خاصه (الأكثر تعقيدا) وواحدة عامه

العامة: نمنع عمليه الـ ping لكل الـ subnet (الشبكة الداخليه)

الخاصة: اسمح لجهاز server1 ان يعمل الـ ping .

The screenshot shows the FortiGate VM64 configuration interface for a new policy. The policy is named 'Public'. The incoming interface is 'LAN1 (port1)' and the outgoing interface is 'WAN (port2)'. The source is 'Subnet1' and the destination is 'all'. The schedule is 'always' and the service is 'PING'. The action is set to 'DENY'. The 'Log Violation Traffic' checkbox is checked. The 'Enable this policy' checkbox is also checked.

أساسيات فورتى جيت

كما بالصورة أعلاه تم انشاء بوليسي عامه باسم public بتمنع الping على كل الsubnet1 .

ثم سنقوم بإنشاء بوليسي خاصه باسم private حيث نسمح للجهاز server1 بأن يعمل ping ..

The screenshot shows the 'Edit Policy' configuration for a policy named 'private'. The configuration is as follows:

- Name: private
- Incoming Interface: LAN1 (port1)
- Outgoing Interface: WAN (port2)
- Source: server1
- Destination: all
- Schedule: always
- Service: PING
- Action: ACCEPT (checked), DENY (unchecked)
- Inspection Mode: Flow-based

Below the policy configuration, the 'Firewall / Network Options' section is visible, showing NAT settings and IP Pool Configuration.

ثم نلاحظ كيف اصبح ترتيب البوليسي ..

The screenshot shows the 'Policy & Objects' section of the FortiGate VM64 configuration. The table below lists the policies:

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	public	Subnet1	all	always	PING	DENY		Disabled	UTM	0 B
4	private	server1	all	always	PING	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY		Disabled		1.30 kB

الان أي جهاز من الشبكة الداخليه(subnet1)192.168.2.0/32 سوف يحاول يعمل ping لأي موقع مثلا ping 8.8.8.8 -t فانه لن يستطيع حتى وان كان الجهاز هو server1 وذلك لأن ترتيب البوليسي يطبق من اعلى الى اسفل..لكننا لو قمنا بإعادة ترتيب البوليسي وذلك بالسحب والافلات كما بالصورة ادناه

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	public	Subnet1	all	always	PING	DENY			Disabled	0 B
4	private	server1	all	always	PING	ACCEPT		no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT		no-inspection	UTM	0 B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT		no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	1.30 kB

وتصبح البوليسي بهذا الترتيب :

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT		no-inspection	UTM	0 B
3	public	Subnet1	all	always	PING	DENY			Disabled	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT		no-inspection	UTM	0 B
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT		no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	1.30 kB

بحيث تصبح البوليسي الأكثر (تعقيدا) (الخاصة) هي التي في الأعلى والبوليسي العامه في الأسفل ..

حيث الآن الجهاز server1 لو حاول يعمل t- ping 8.8.8.8 سوف تنجح العملية ..

اما باقي الاجهزه في ال subnet1 سوف لن يقدرروا ..

مثال اخر:

لوقمنا بإنشاء 2 بوليسي كما بالصورة ادناه

حيث الأولى بتسمح للجهاز server1 انه يعمل ping فقط لأي مكان مثلا

فلوا قام بفتح أي موقع لن يفتح معاه ابدأ لأن البوليسي المسماة public تمنع أي سيرفيس (all).

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT	Enabled	no-inspection	UTM	96.98 kB
3	public	Subnet1	all	always	PING	DENY	Enabled	no-inspection	Disabled	96.10 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5		all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	28.14 MB
0	Implicit Deny	all	all	always	ALL	DENY	Enabled	no-inspection	Disabled	17.20 kB

الـ 2 بوليسي معمول لهم
disabled اي انها لن تكون مفعلة ..

الـ 3 هذه التي اسمها
هي التي تسمح لكل ان
يفتح الانترنت...

نلاحظ اول رول (بوليسي) اسمها private وبتقول بأن الجهاز الي اسمه server1 يمكنه ان يعمل ping وهذا صحيح..فلو قمت بعمل بينج الى أي موقع من الجهاز server1 فانه سيتمكن من ذلك .. لكن لما ان حاولت ان تفتح أي موقع سواء www.google.com او غيره فأنتك سيتمكن من فتحه بالرغم من اني حددت فقط بأن ping هو الي مسموح !!
الجواب هو :

اول رول سمحت فقط له بعمل ping فقط ومن ثم سوف ينزل الى الرول الثانية التي اسمها public والتي تقول بأن الـ subnet1 كلها لا يمكنها الوصول الى الـ ping ولم تقل له بأنك تمنع أي شيء (all) بل حددت بأنك تمنع فقط الـ ping .

طيب لماذا لازال الجهاز server1 قادر على فتح جميع المواقع !!

الاجابة هي بسبب الرول المسماة 3 والتي مضلله باللون الأحمر كما بالصورة أعلاه والتي بتسمح بكل السيرفس (all) وهذه فكره ترتيب البوليسي ..

طيب السيناروا الأخير:

ماذا لو قمت بعمل تعطيل (disabled) للبوليسي التي باسم 3 !! كما بالصورة ادناه

أساسيات فورتى جيت

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT	Enabled	no-inspection	UTM	148.64 kB
3	public	Subnet1	all	always	PING	DENY	Disabled	no-inspection	UTM	96.10 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	23.88 MB
0	Implicit Deny	all	all	always	ALL	DENY	Disabled	no-inspection	UTM	76.94 kB

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT	Enabled	no-inspection	UTM	148.64 kB
3	public	Subnet1	all	always	PING	DENY	Disabled	no-inspection	UTM	96.10 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	23.88 MB
0	Implicit Deny	all	all	always	ALL	DENY	Disabled	no-inspection	UTM	76.94 kB

فأن الجهاز server1 يستطيع فقط ان يقوم بعمل ping لأي موقع ولكنه لن يتمكن من فتح أي موقع لأن لا توجد رول بتسمح له بذلك بالإضافة ان اخبوليسي(الافتراضي)(Implicit policy) بتمنع أي ترافيك بحسب الصورة ادناه ..

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT	Enabled	no-inspection	UTM	148.64 kB
3	public	Subnet1	all	always	PING	DENY	Disabled	no-inspection	UTM	96.10 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	23.88 MB
0	Implicit Deny	all	all	always	ALL	DENY	Disabled	no-inspection	UTM	76.94 kB

اخر مثال :

لوقمت بإنشاء بوليسي كما بالصورة ادناه

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	server1	all	always	PING	ACCEPT	Enabled	no-inspection	UTM	204.92 kB
3	public	Subnet1	all	always	ALL	DENY			Disabled	96.10 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	242.94 kB
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	154.44 kB

هل

يستمكن الجهاز server1 من ان يعمل ping ؟ لماذا؟؟

هل سيتمكن الجهاز server1 من ان يفتح أي موقع ؟؟ لماذا؟؟

الاجابة على السؤال الأول هي نعم لأن البولييسي الأولى بتسمح ping.

الاجابة عن السؤال الثاني هي لا ..

لن يتمكن الجهاز server1 ان يفتح أي موقع وهذا بسبب الرول رقم 2 المسماة public وذلك لأنى عملت

all services =deny فمجرد ان deny حصل فأن الفورتي جيت لا ينظر الى البولييسي اللي تحته ..

بالرغم ان البولييسي الأخيرة التي بالاسم 3 مفعله وتتيح لكل الاجهزه ان تصل الى الانترنت ولأي موقع ..

❖ Managing devices

يقصد بها ادارة الأجهزة..

الfortiOS (نظام التشغيل التابع للفورتي جيت) يستطيع ادارته والتحكم بكل الاجهزه الموجودة بالشبكة

حيث يقوم باكتشاف الاجهزه (pc,laptop,tablet,mobile) سواء كنت وايرلس او واير.

حيث الفورتي جيت بيتعرف ويراقب كل الاجهزه الموصلة بالشبكة سواء كانت تلك الاجهزه

وايرلس (مرتبطة بـ access point) او واير (موصلة بالسويتش).

❖ كيف يقوم فورتى جيت بإدارة الأجهزة ؟

يعمل بأحدى الطرق :

1 – Agent based : يكون هنالك وكيل (برنامج الفورتى كلاينت) يتم تنزيله على تلك الاجهزه .

2 – Agentless : بدون وكيل على تلك الاجهزه .

الآن سنتعامل مع طريقة Agentless :

يتم توصيل تلك الاجهزه بالشبكة بالفورتى نت سواء بالسويتش او بالاكسس بوينت حيث مثلا اعطى الباسورد لأي احد مثلا يريد الوصول الى شبكة الوايرلس وهذا انا قمت بتجميع المعلومات للأجهزة بالشبكة سواء واير او وايرلس حيث بعد ذلك يتم التحكم بتلك الاجهزه عبر الماك ادرس (mac address) حيث ستمكن من السماح او منع تلك الاجهزه بحسب الماك ادرس .

بعد ذلك سوف استخدم البوليسى للتحكم بهذه الاجهزه مثلا اريد امنع كل الاجهزه من نوع الجلاكسي او من نوع ابل ... الخ من الوصول الى الانترنت والسماح للأنواع الأخرى مثل بلاك بيرى او الوندوز .. الخ أي ان جهاز الفورتى جيت اصبح يتحكم بالأجهزة بحسب نظام التشغيل لتلك الاجهزه .

او مثلا عمل بوليسى معينه باني امنع الاجهزه التي بالشبكة التي نظام التشغيل من نوع لينكس ..

وبذلك أصبحت قادر بالتحكم على الاجهزه بحسب نظام التشغيل لتلك الاجهزه او بحسب ال category او بحسب الماك ادرس او اسم الجهاز او بالايي للجهاز.

أي ان الفورتى جيت يعمل على جلب المعلومات التالية بعد توصيلها بالشبكة لكي استطيع التحكم بها بعد ذلك عبر البوليسى :

الماك ادرس

الايي للجهاز

نظام التشغيل للأجهزة

اسم الجهاز

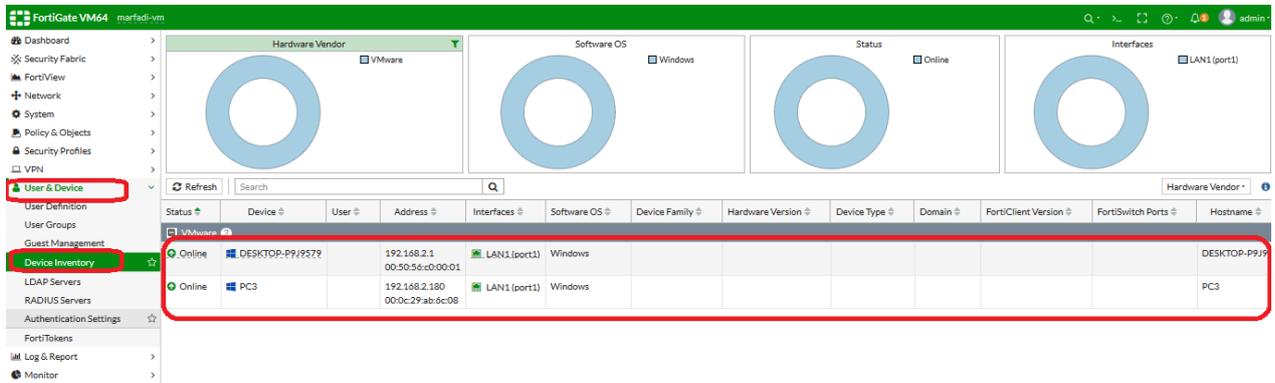
اظهار متي اخر ظهور للجهاز وعلى أي من interface موصل هذا الجهاز (lan1،lan2.... الخ)

ملاحظة :

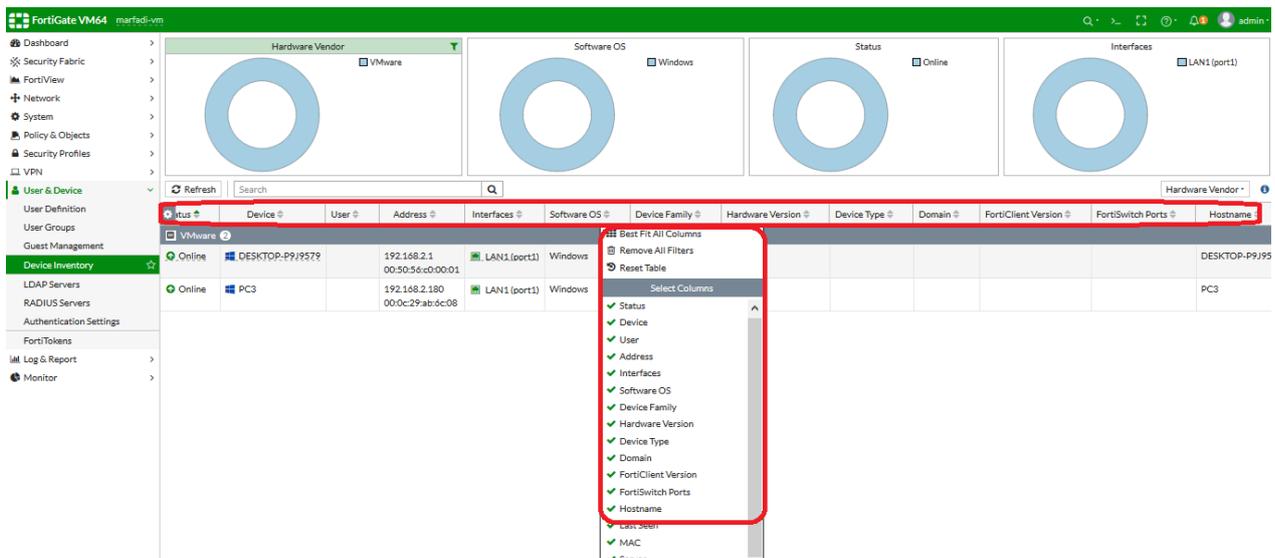
الفورتى جيت بيتحكم بالمستخدمين وبالأجهزة ..

نقوم بفتح الفورتى جيت ونتأكد بأن الفورتى جيت بيدشوف الاجهزه عبر أي من interface حيث كل الاجهزه بتسجل نفسها بشكل اوتوماتيكي في المكان التالي :

User&Device>Device Inventory >



حيث يمكنك اظهار المعلومات (الأعمدة) وذلك بالنقر بالزر الأيمن على الشريط المظلل بالأحمر ومن ثم نختار الخيارات المراد اظهارها ثم apply كما بالصورة ادناه



حيث سوف يظهر لك حالة الاجهزه المتعرف عليها (offline , online) أي الجهاز شغال حاليا ام طافي !!

Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version	Device Type	Domain	FortiClient\
Online	DESKTOP-P9J9579		192.168.2.1 00:50:56:c0:00:01	LAN1 (port1)	Windows					
Offline	PC3		PC3_IP PC3	LAN1 (port1)	Windows					

وأيضاً يظهر لك اسم الجهاز (Device host name) ،

اسم اليوزر (يقوم بإظهار اسم اليوزر لو كان اليوزر ضمن الدومين)

العنوان (الايبي)

والتوصيل المتوصل عليه الجهاز

ونوع نظام التشغيل للجهاز هل 7 او 8.1 او 10

وايضاً هل يحتوي على فورتى كلاينت وما هو إصداره

ومتى اخر ظهور للجهاز

المالك ادرس للأجهزة

حيث الفورتى لكي يقوم بعمل كشف وجلب للمعلومات أعلاه يجب ان تقوم بتفعيل خيار معين على ال interface سواء كانت هذه الاجهزة اخذت ايبي من dhcp server on FG او dhcp server مستقل او الاجهزة لم تأخذ ايبيات أصلاً او اخذت static ip ..

مثال لو اريد ان اجلب المعلومات أعلاه للأجهزة المتوصله عبر ال interface مثلا lan1 أي الاجهزة المتوصله بالشبكة الداخليه يجب ان أقوم بتفعيل الخيار التالي على ال lan 1 interface ..

أساسيات فورتني جيت

The screenshot shows the 'Edit Interface' configuration page in FortiGate. The left sidebar has 'Network' and 'Interfaces' highlighted. The main content area shows the 'DHCP Server' section with fields for Address range (192.168.2.1-192.168.2.19 and 192.168.2.21-192.168.2.254), Netmask (255.255.255.0), Default gateway (Same as Interface IP), DNS server (Same as System DNS), Lease time (2592000), and FortiClient On-Net Status. Below this, the 'Network' section has 'Device detection' checked and highlighted with a red box and a red arrow. Other sections include Security mode, Traffic Shaping, and Miscellaneous.

حيث الخيار Device detection لا يكون مفعّل بشكل افتراضي ويجب تفعيله

لواردت تكتشف وتتعرف (detect) على جميع المعلومات المذكورة سابقاً لتلك الاجهزة والموصلة على المنفذ lan1 مثلاً..

فمجرد الحصول على جميع المعلومات لتلك الاجهزة كما بالصورة ادناه

The screenshot shows the 'Device Inventory' page in FortiGate. The left sidebar has 'User & Device' and 'Device Inventory' highlighted. The main content area shows a table of detected devices. The table has the following columns: Status, Device, User, Address, Interfaces, Software OS, Device Family, Hardware Version, Device Type, Domain, FortiClient Version, FortiSwitch Ports, and Hostname. Two devices are listed:

Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version	Device Type	Domain	FortiClient Version	FortiSwitch Ports	Hostname
Online	DESKTOP-P9J9577		192.168.2.1	LAN1 (port1)	Windows							DESKTOP-P9J9577
Online	PC3		192.168.2.180	LAN1 (port1)	Windows							PC3

فنقوم بتسميه تلك الاجهزة بحسب الماك وذلك بالنقر بالزر الأيمن على اسم الجهاز (pc3)

أساسيات فورتى جيت

The screenshot shows the 'User & Device' configuration page in FortiGate VM64. The 'Device Inventory' section is highlighted. A table lists devices, with 'PC3' selected. A context menu is open over 'PC3', showing options like 'Filter by Device', 'Create Firewall Address', 'Show Matching Logs', and 'Show in FortiView'. The 'Create Firewall Address' option is highlighted, and a sub-menu shows the MAC Address (00:0c:29:ab:6c:08) and IP Address (192.168.2.180) for the selected device.

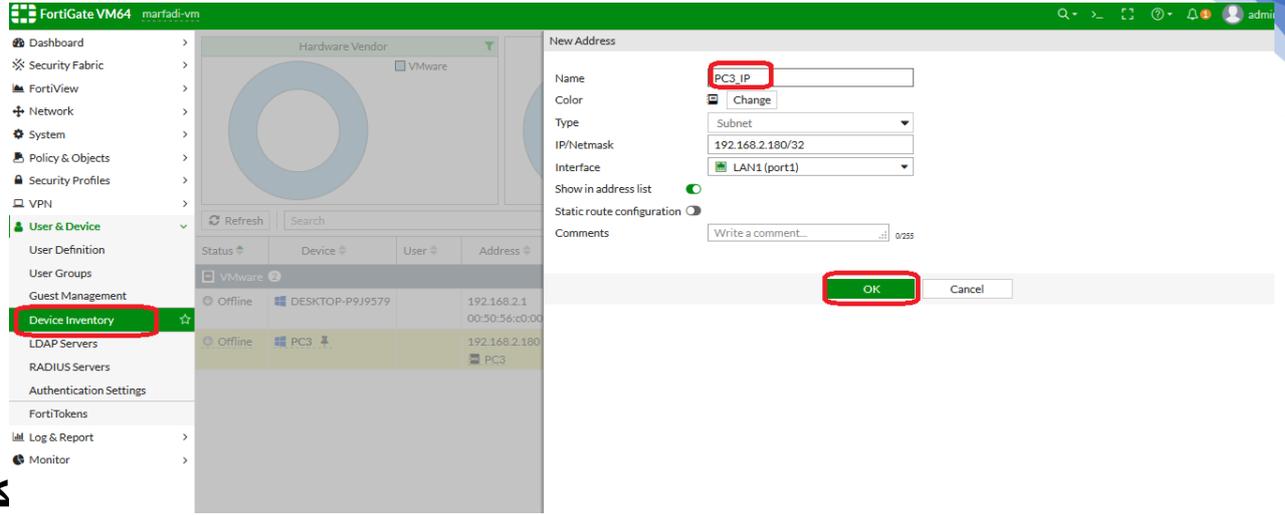
Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version	Device Type	Domain	FortiClient Versio
Online	DESKTOP-P9J9579		192.168.2.1 00:50:56:c0:00:01	LAN1 (port1)	Windows					
Online	PC3		192.168.2.180 00:0c:29:ab:6c:08	LAN1 (port1)	Windows					

The screenshot shows the 'New Address' configuration page in FortiGate VM64. The 'Name' field is set to 'PC3'. The 'Type' is set to 'Device (MAC Address)'. The 'MAC Address Scope' is set to 'Single Address'. The 'MAC Address' field is set to '00:0c:29:ab:6c:08'. The 'Interface' is set to 'LAN1 (port1)'. The 'Show in address list' checkbox is checked. The 'OK' button is highlighted.

اونقوم بأضافه هذا الجهاز بالايي

The screenshot shows the 'User & Device' configuration page in FortiGate VM64. The 'Device Inventory' section is highlighted. A table lists devices, with 'PC3' selected. A context menu is open over 'PC3', showing options like 'Filter by Device', 'Create Firewall Address', 'Show Matching Logs', and 'Show in FortiView'. The 'Create Firewall Address' option is highlighted, and a sub-menu shows the IP Address (192.168.2.180) for the selected device.

Status	Device	User	Address	Interfaces	Software OS	Device Family	Hardware Version	Device Type	Domain	FortiClient Ver
Offline	DESKTOP-P9J9579		192.168.2.1 00:50:56:c0:00:01	LAN1 (port1)	Windows					
Offline	PC3		192.168.2.180 00:0c:29:ab:6c:08	LAN1 (port1)	Windows					

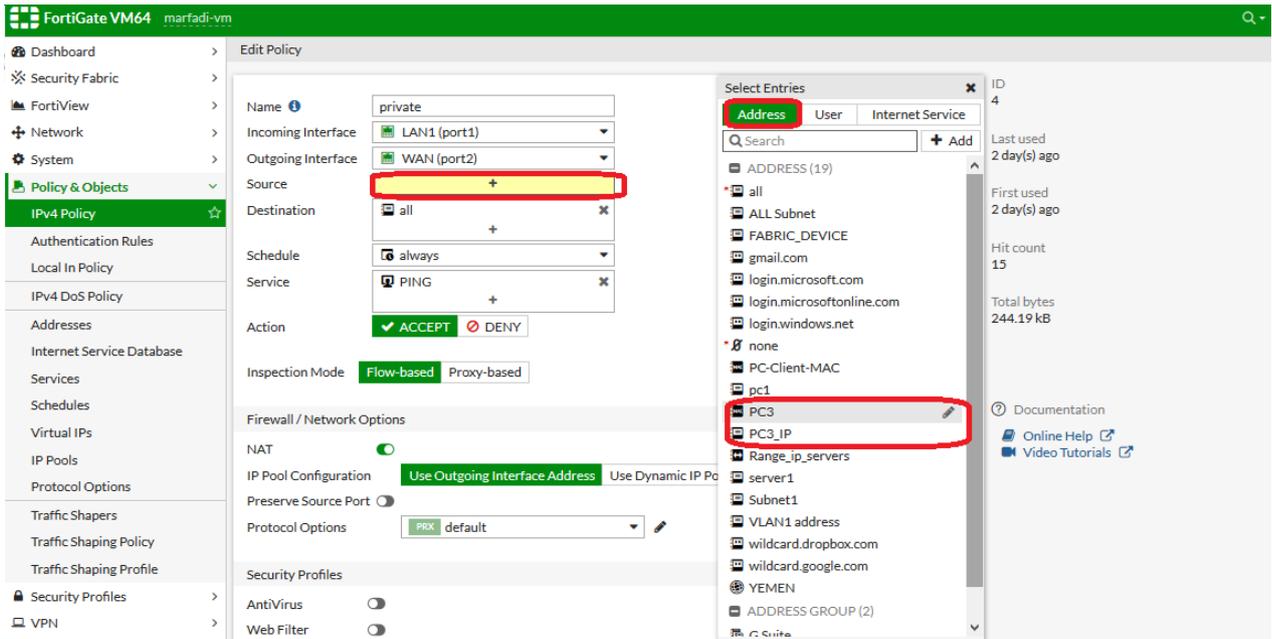


كما

بالصورة ادناه قمت بإنشاء عنوان باسم PC3_IP بحسب الايبي ..

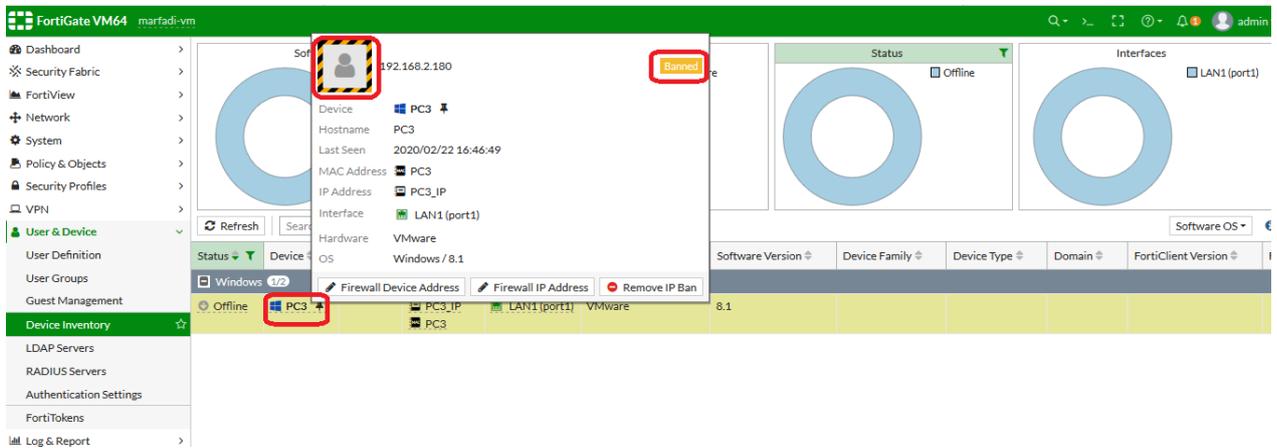
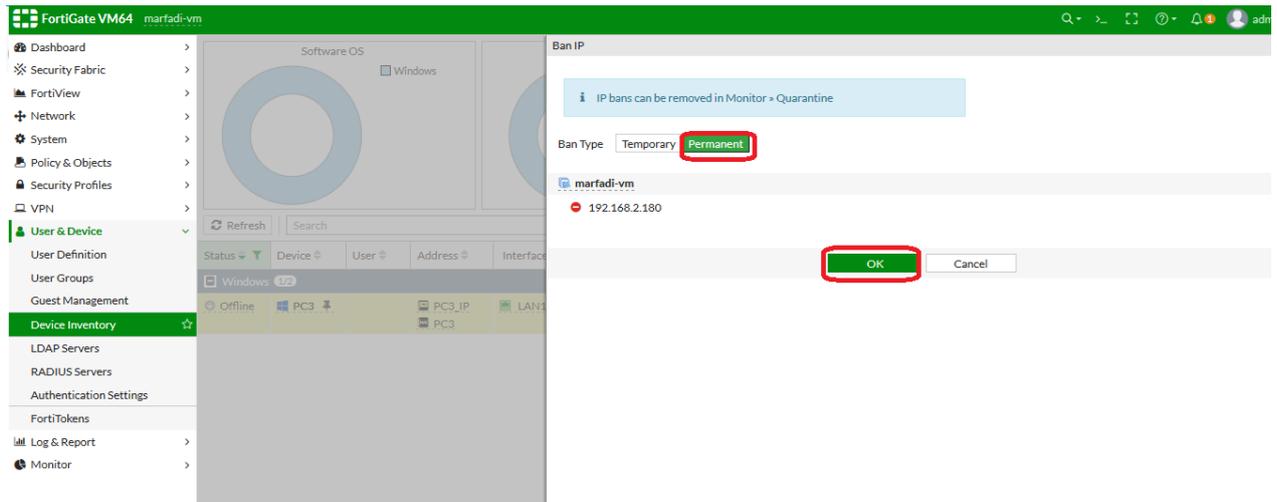
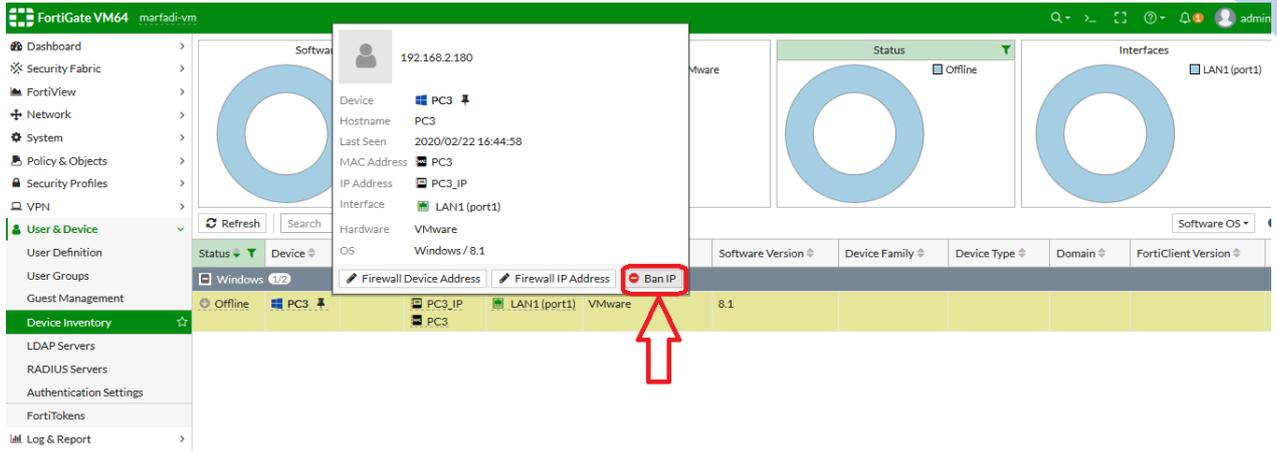
فلذلك لو قمت بإنشاء بولييسي فيمكنني ان اتحكم بهذا الجهاز سواء بالماك او بالايبي كما بالصورة ادناه

..



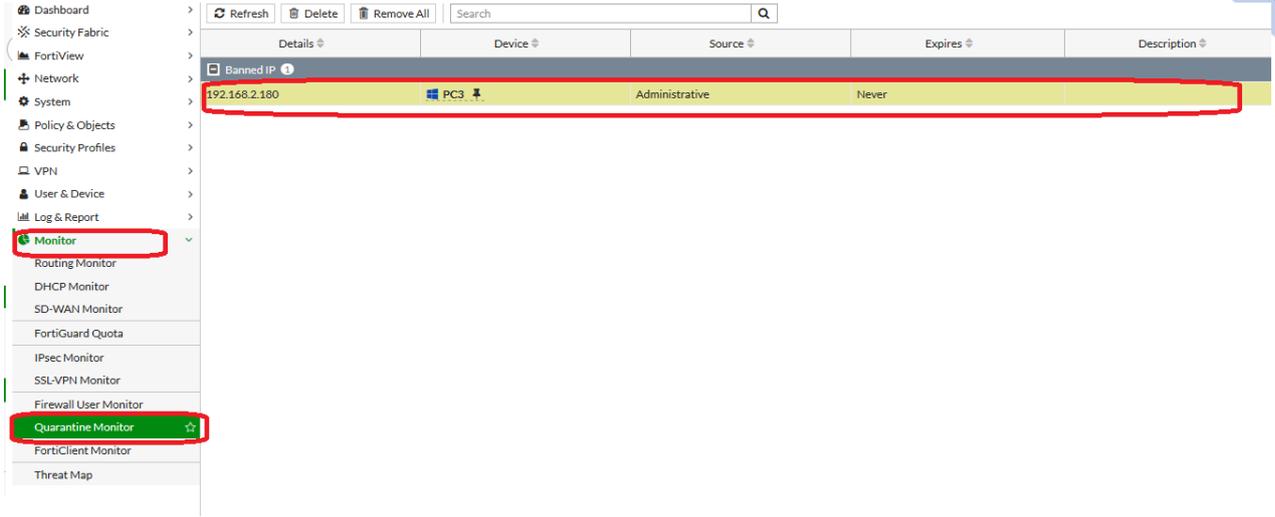
وبهذا استطعت ان اتحكم بالجهاز عبر الماك ادرس لهذا الجهاز او عبر الايبي .

وتكرر نفس العملية لكل الاجهزه التي تظهر لك والتي تم اكتشافها ..



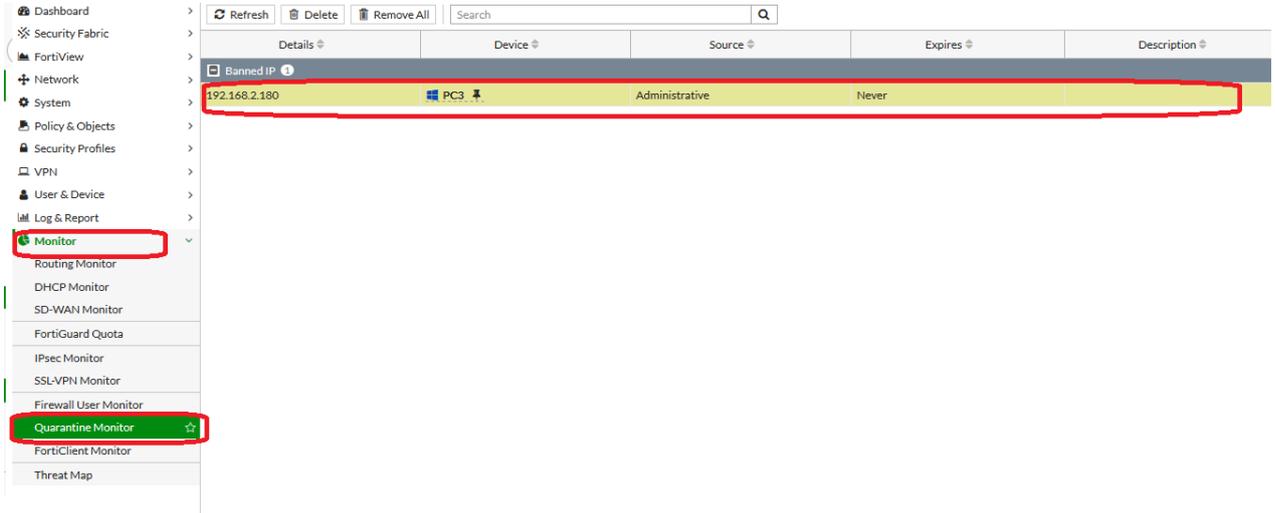
قمت بعمل permanent (أي تم عمل حظر للجهاز 192.168.2.180 بشكل دائم) لذا سوف يتم عمل له بلوك من كل شيء بشكل دائم في الخيار التالي :

أساسيات فورتى جيت



Details	Device	Source	Expires	Description
Banned IP				
192.168.2.180	PC3	Administrative	Never	

حيث تم وضعه بمنطقة الحجر (Quarantine) حيث جهاز الفورتى جيت يعمل حظر (ban) للأجهزة التي يكتشف بوجودها اختراق او فيروسات ويمكنك فك الحظر بالذهاب الى



Details	Device	Source	Expires	Description
Banned IP				
192.168.2.180	PC3	Administrative	Never	

ونحذف الجهاز المحظور لكي يتم رفع الحظر (remove ban)

: Access control list (ACL)

عبارة عن التحكم بقائمه (مجموعة من الاجهزه) من انها توصل الى مصادر الشبكة (service). حيث يتم تسجيل الاجهزه في قائمه Devices inventory حتى وان لم يحصل ذلك الجهاز على ايبى بعد (أي ان الجهاز مثلا يأخذ ايبى 0.0.0.0 او ايبى من ال ipa 169.254.x.x) فجهاز الفورتى جيت ليسجل المالك ادرس لهذا الجهاز في قائمه Devices inventory حتى وان لم يحصل على ايبى بعد .

أساسيات فورتى جيت

ولتفعيل خاصية ACL يجب ان تقوم بتفعيل DHCP server على جهاز الفورتى جيت نفسه وليس كسرفر مستقل وهذه يقوم بالفورتى جيت بتوزيع الايبيات لكل الاجهزة الموجودة في الشبكة الداخليه .. والمفترض بأن ليس أي جهاز يتوصل بالشبكة لدي يحصل على ايبي بل فقط الاجهزة التي اثق فيها بالماك ادرس ،، وهذا اصبحنا نتحكم بالقائمة (lists) بالأجهزة التي لدي بالفورتى جيت من خلال الماك ادرس عبر ACL .

ما هو Mac reservation :

نربط بين الايبي وبين الماك للأجهزة

أي كل مره يأتي الجهاز صاحب الماك الفلاني فأن dhcp server يعطيه الايبي الفلاني في كل مره ..

فلو قمنا بتفعيل ال dhcp server على البورت LAN1 كما بالصورة ادناه

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar lists various network and system settings. The main content area is titled 'Edit Interface' and shows administrative access options for IPv4, including HTTPS, HTTP, PING, FMG-Access, SSH, TELNET, FTM, Security Fabric Connection, and RADIUS Accounting. Below this, there are options for Receive LLDP and Transmit LLDP, both set to 'Use VDOM Setting'. The 'DHCP Server' section is highlighted with a red box and contains the following configuration:

- DHCP Server:** Enabled (toggle)
- Address range:** 192.168.2.1-192.168.2.19 and 192.168.2.21-192.168.2.254
- Netmask:** 255.255.255.0
- Default gateway:** Same as Interface IP
- DNS server:** Same as System DNS
- Lease time:** 2592000 second(s)
- FortiClient On-Net Status:** Enabled (toggle)

The 'Advanced' section below shows 'Device detection' enabled and 'Security mode' disabled.

فندهب الى اجهزه الكلايننت والتي هي على الشبكة الداخليه ونعمل لكروت الشبكة disabled و enabled لتتمكن من الحصول على ايبي من ال dhcp server .

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	PC3	PC3	Not Reserved	192.168.2.30	VCI: MSFT 5.0 Hostname: pc3	2020/02/22 22:39:52	Leased out

نلاحظ بأن الجهاز pc3 حصل على ايبى 192.168.2.30 من dhcp server

Edit Interface

TELNET FTM RADIUS Accounting
 Security Fabric
 Receive LLDP Use VDOM Setting Enable Disable
 Transmit LLDP Use VDOM Setting Enable Disable

DHCP Server

Address range: 192.168.2.30-192.168.2.254
 Netmask: 255.255.255.0
 Default gateway: Same as Interface IP Specify
 DNS server: Same as System DNS Same as Interface IP Specify
 Lease time: 300 second(s)

FortiClient On-Net Status
 Advanced

Network
 Device detection
 Security mode
 Traffic Shaping
 Outbound shaping profile

ندخل على كرت LAN1 ثم نختار الخيار Advanced

Next bootstrap server: 0.0.0.0

Additional DHCP Options

IP Address Assignment Rules

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:ff:72:33	Reserve IP	192.168.2.188
Implicit	Unknown MAC Addresses	Assign IP	

من الخيار Add from DHCP client List سوف يظهر لك كل الاجهزه التي اخذت ايبى من الdhcp server ومن ثم يمكنك اختيار الماك والايبي لعمل reserved (حجز) بحيث هذا الجهاز صاحب الماك الفلاني دائما اعطيه الايبي الفلاني...

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar shows the 'Network' menu with 'Interfaces' selected. The main area displays the 'Edit Interface' configuration. Under 'IP Address Assignment Rules', there is a table with the following data:

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:ff:72:33	Reserve IP	192.168.2.188
MAC Address	MAC address: 00:0c:29:ab:6c:08	Reserve IP	192.168.2.30
Implicit	Unknown MAC Addresses	Assign IP	3

At the bottom of the interface, there is a 'Reserve IP(s)' button highlighted with a red box.

نلاحظ بأنه تم حجز (reserved) الايبي 192.168.2.30 للماك ادرس المشار له بالاحمر..

فإذا اردت انشاء reserve ip مانوال

Dashboard >
Security Fabric >
FortiView >
Network >
Interfaces ☆
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System >
Policy & Objects >
Security Profiles >
VPN >
User & Device >
Log & Report >

Edit Interface
Next bootstrap server 0.0.0.0
Additional DHCP Options
+ Create New Edit Delete Search Q
Code Type Value
No results

IP Address Assignment Rules
+ Create New Filter/Configure Column arch Add from DHCP Client List
Type Match Criteria Action IP
MAC Address MAC address: 00:0c:29:ff:72:33 Reserve IP 192.168.2.188
MAC Address MAC address: 00:0c:29:ab:6c:08 Reserve IP 192.168.2.30
Implicit Unknown MAC Addresses Assign IP 3

Network
Device detection
Security mode
Traffic Shaping

أساسيات فورتني جيت

نقوم بكتابة الماك المطلوب
عمل له حجز ايبي معين
تحده انت بنفسك من الخيار

1

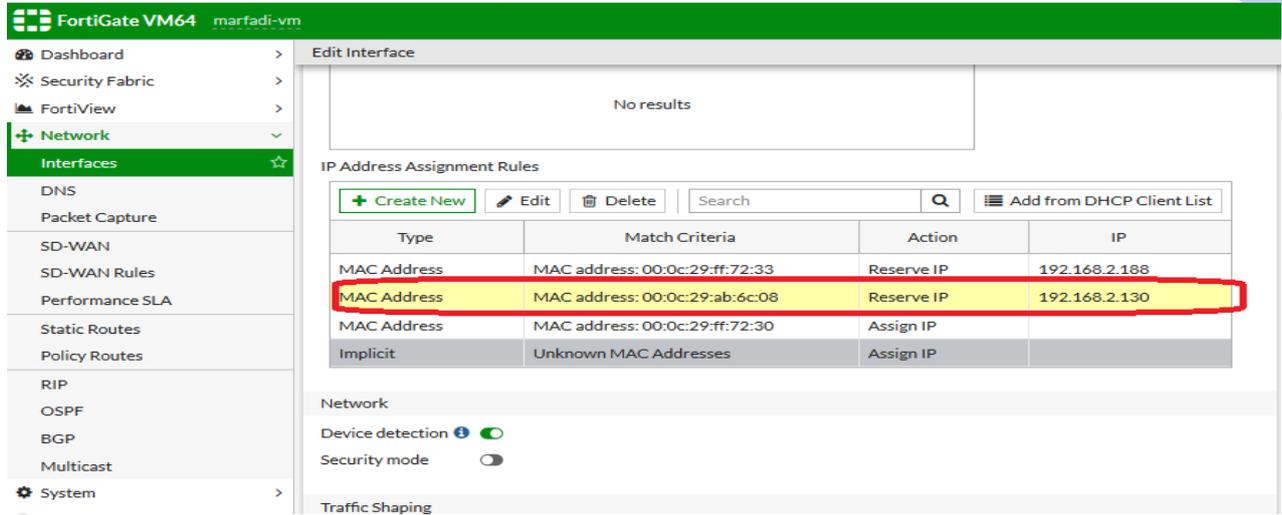
2 او نختار الخيار Assign IP اي سيتم اخذ ايبي من dhcp server-

3 او نختار الخيار Block وذلك لحظر (منع) الماك و ذلك من الحصول على dhcp server

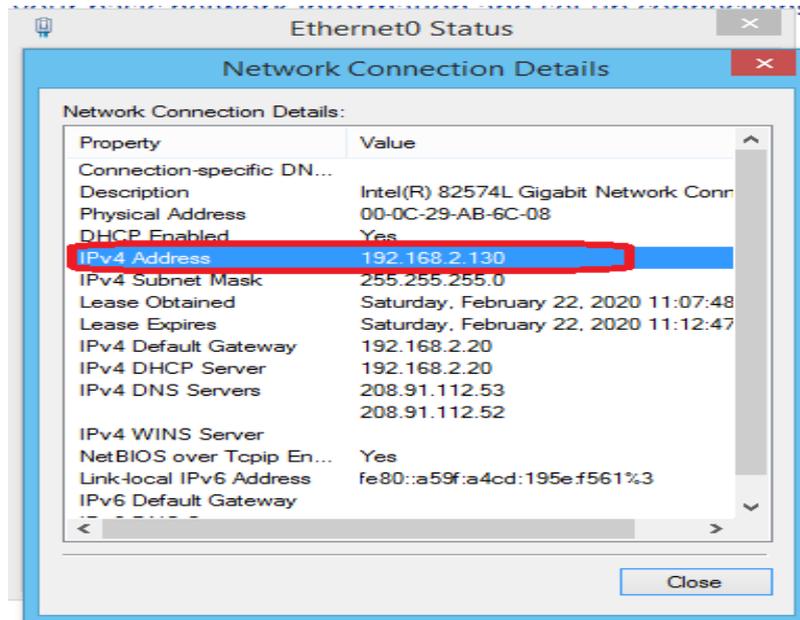
Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:ff:72:33	Reserve IP	192.168.2.188
MAC Address	MAC address: 00:0c:29:ab:6c:08	Block	
MAC Address	MAC address: 00:0c:29:ff:72:30	Assign IP	
Implicit	Unknown MAC Addresses	Assign IP	4

كما بالصورة أعلاه تم حظر الماك ادرس بأن يحصل على ايبي عن طريق dhcp server فعند عمل disabled و enabled لجهاز الكلاينت الذي له هذا الماك ادرس فإنه لن يجد ايبي مهما حصل ...

اما الصورة أعلاه تم كتابه الماك ادرس للجهاز الذي تريد حجزه الايبي 192.168.2.130



فندخل على جهاز الكلاينت ونعمل disabled ومن ثم enabled لكارت الشبكة ونلاحظ بأنه حصل على الايبي 192.168.2.130 كما بالصورة ادناه



ملاحظة هامه :

أساسيات فورتني جيت

Wireless controllers: Same as Interface IP Specify 0.0.0.0
 Time zone: Same as System Specify
 Next bootstrap server: 0.0.0.0

Additional DHCP Options

Code	Type	Value
No results		

IP Address Assignment Rules

Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:ff:72:33	Reserve IP	192.168.2.188
MAC Address	MAC address: 00:0c:29:ab:6c:08	Reserve IP	192.168.2.130
MAC Address	MAC address: 00:0c:29:ff:72:30	Assign IP	
Implicit	Unknown MAC Addresses	Assign IP	

Network

Device detection
 Security mode

المالك ادرس الغير معروف قم بتخصيص له ايبي من dhcp server وهذا بشكل افتراضي كما بالصورة أعلاه.

حيث ان الDHCP server يقوم بتخصيص ايبي لكل جهاز بالشبكة ..

حيث لو قمنا بتغيير الخاصية الى unknown mac address =Block فأن أي جهاز لن يحصل على ايبي من dhcp server الا لو كان معروف ..

Next bootstrap server: 0.0.0.0

Additional DHCP Options

Code	Type	Value
No results		

IP Address Assignment Rules

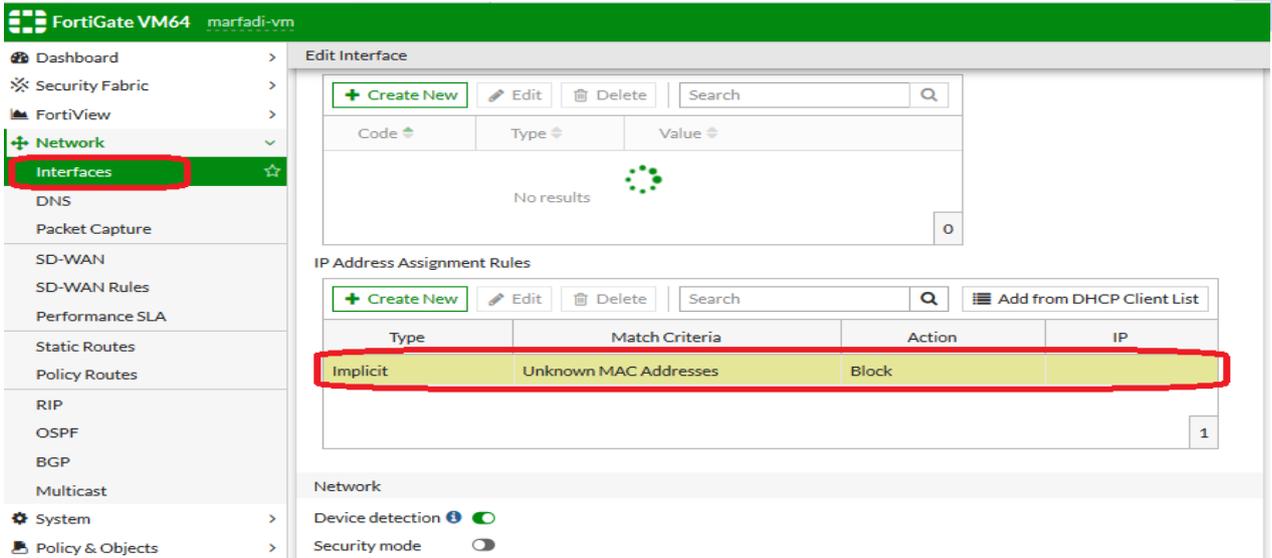
Type	Match Criteria	Action	IP
MAC Address	MAC address: 00:0c:29:ff:72:33	Reserve IP	192.168.2.188
MAC Address	MAC address: 00:0c:29:ab:6c:08	Reserve IP	192.168.2.130
MAC Address	MAC address: 00:0c:29:ff:72:30	Assign IP	
Implicit	Unknown MAC Addresses	Assign IP	

Network

Device detection
 Security mode

Context menu options: Action, Block, Assign IP

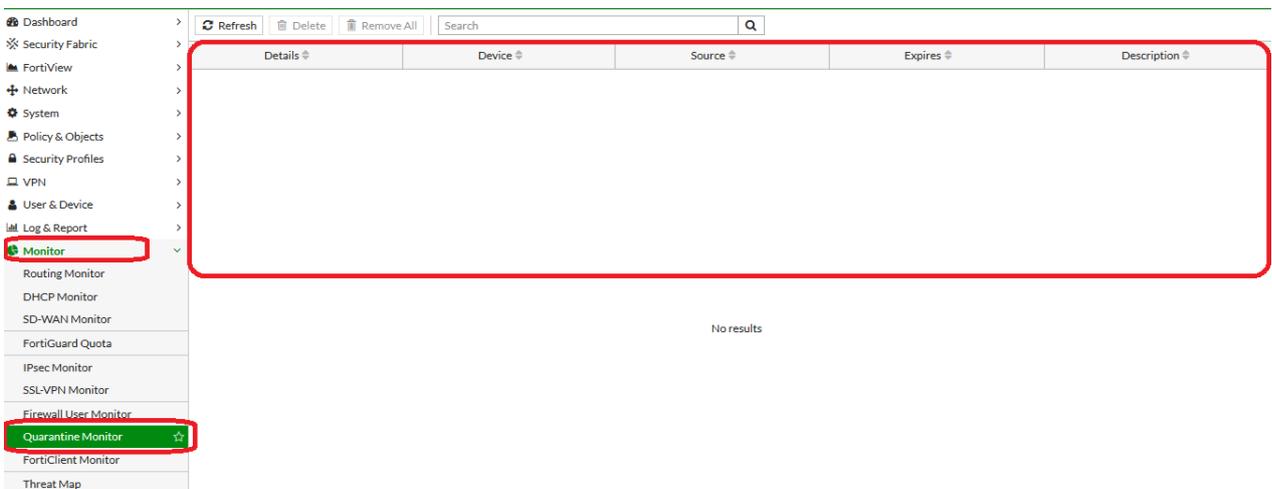
Buttons: OK, Cancel



حيث بالخيار أعلاه لن يتمكن أي جهاز من الحصول على ايبي من DHCP SERVER .

كيفية حظر ايبي معين من الحصول على الانترنت :

نلاحظ بأن منطقته الحجر الى الآن فارغ

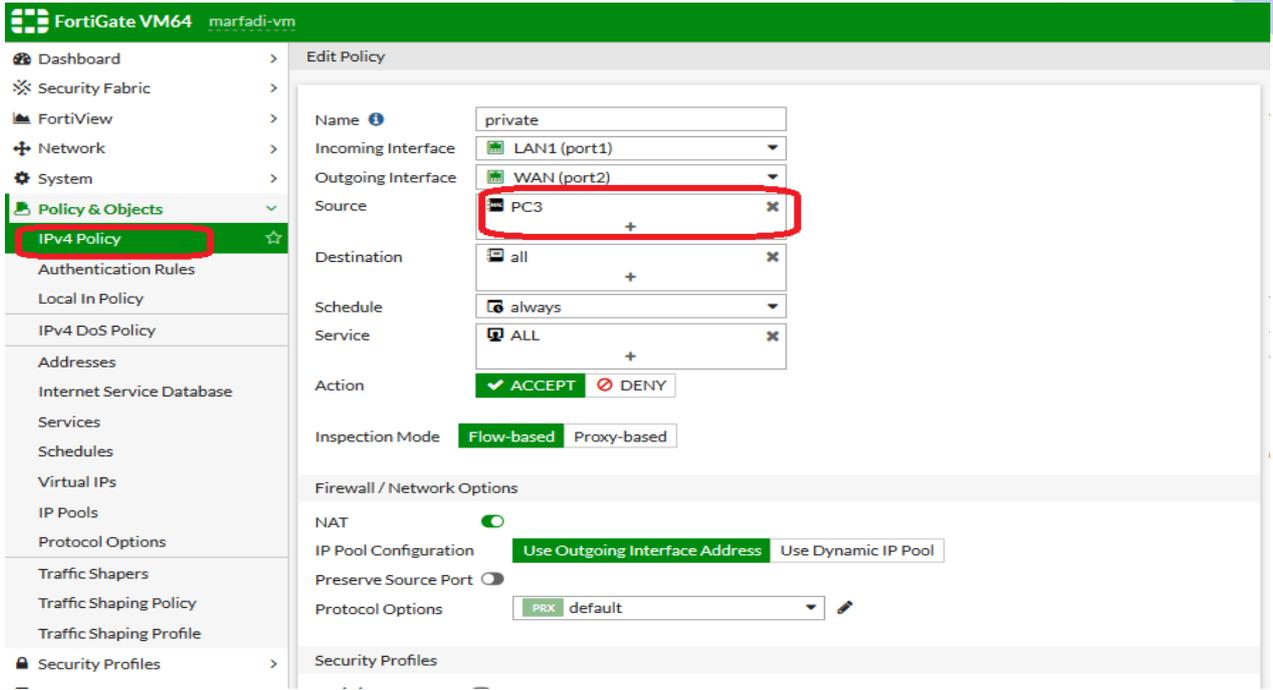


الآن سوف نقوم بعمل حجر للايبي 192.168.2.30 ..

Interface	Device	MAC	Reserved	IP	Host Information	Expires	Status
LAN1 (port1)	PC3		Reserved	192.168.2.30	VCI: MSFT 5.0 Hostname: pc3	2020/02/23 17:17:29	Leased out

Banned IP	Device	Source	Expires	Description
192.168.2.30	PC3	Administrative	Never	

نلاحظ بأن الجهاز PC3 معمول له حظر ولن يحصل على الانترنت مهما حصل الا لوقت بحذف الايبي من ال Quarantine Monitor وذلك بتحديد الجهاز والضغط على الخيار Delete.



تم السماح للجهاز pc3 بالحصول على الانترنت الا ان الجهاز لم يتمكن من الحصول على الانترنت لأنه معمول له Ban ip ..

FortiClient

الآن سوف نشرح تقنية ادارة الاجهزه بواسطة تقنيه (Agent Based) أي سيتم تنزيل برنامج (forticlient) على الاجهزه التي تدير ادارتها سواء كانت اجهزه كمبيوتر او لابتوب او ايباد او موبايل بأنواعها سواء كانت الاجهزه بنفس شبكة ال LAN او موجودة على شبكة ال WAN (على الانترنت) حيث سيقوم فورتى جيت فايروول بتوفير الحماية للأجهزة التي بعيدة عن الشبكة الداخليه وذلك عبر برنامج الفورتى كلاينت .

➤ حيث الفورتى كلاينت يقدم الخدمات التالية :

- 1 – antivirus على اجهزه الموظفين .
- 2 – Web filtering على اجهزه الموظفين
- 3 – Application control حيث سيقوم بالتحكم بالتطبيقات التي موجودة عند المستخدمين
- 4 – VPN
- 5 - mobile configuration

يمكن تنزيل الفورتى كلاينت مجاني على أي الاجهزه .

حيث يوجد اصدارين من الفورتى كلاينت :

١- Basic:نسخه مجانيه

٢- Registered : نسخه غير مجانيه حيث يجب ان تسجل وتجدد كل سنه

FEATURES

	Windows	Mac OS X	Android	iOS
Basic				
IPsec VPN	•	•	•	-
SSL VPN	•	•	•	Web Mode Only
Two-Factor Authentication	•	•	•	•
Antivirus	•	•	-	-
Web Filtering	•	•	•	•
WAN Optimization	•	-	-	-
Client Certificate Support	•	•	•	•
Registered with FortiGate¹				
Centralized Management	•	•	•	•
Policy Compliance Enforcement	•	•	•	•
Configuration Provisioning	•	•	•	• ²
Centralized Logging to FortiAnalyzer/FortiManager	•	•	-	-
Windows AD SSO Agent	•	•	-	-
Application Firewall	•	•	-	-
Vulnerability Scanning	•	•	-	-
Roaming Clients	•	•	-	-
Customizable GUI	•	•	-	-
Custom Install ³	•	•	-	-
VPN Auto-Connect ⁴	•	•	-	-

حيث لو كان لديك فورتى جيت فأن النوع Basic سوف يتيح لك كل المزايا المحدده أعلاه بحسب الجدول أعلاه .

ولكن لو لم يكن لديك فورتى جيت فايروول فيمكن الاستفاده من الفورتى كلاينت ك web filtering و Antivirus فقط .

اما النوع Registered with fortigate فأن اهم ميزه يوفرها لي الفورتى كلاينت هي Centralized management أي اداره مركزيه أي سيتم التحكم بشكل مركزي بكل الفورتى كلاينت عن طريق الفورتى جيت فايروول .

يجب عليك قبل ماتقوم بشراء الفورتى كلاينت فأنك تبحث عن جهاز الفورتى جيت الى حد كم بيدعم forticlients .

مثل FG 30-90 بيدعم فقط الى 200 forticlients .

أساسيات فورتى جيت

فاذا كان لديك عدد اجهزة تريد تنزيل عليها فورتى كلاينت اكثر من 200 جهاز فيجب عليك ان تقوم بشراء جهاز فايروول فورتى جيت بحيث يدعم عدد اكبر من الفورتى كلاينت ..
حيث النسخ (الفورتى كلاينت) يجب ان تقوم بتجديدها سنويا ..

SKU	Description
FC-10-C0102-151-02-12	1 Year FortiClient License Subscription for up to 200 clients on FG/FWF 30-90 Series running FortiOS 5.2 and above. Includes the ability to download the license file, pre-configure the client, create a custom installer and rebrand.
FC-10-C0106-151-02-12	1 Year FortiClient License Subscription for up to 600 clients on FG 100-300 Series running FortiOS 5.2 and above. Includes the ability to download the license file, pre-configure the client, create a custom installer and rebrand.
FC-10-C0103-151-02-12	1 Year FortiClient License Subscription for up to 2,000 clients on FG 500-800 Series and FG VM01-VM02 Series running FortiOS 5.2 and above. Includes the ability to download the license file, pre-configure the client, create a custom installer and rebrand.
FC-10-C0104-151-02-12	1 Year FortiClient License Subscription for up to 3,000 clients on FG 1000 Series and FG-VM04 Series running FortiOS 5.2 and above. Includes the ability to download the license file, pre-configure the client, create a custom installer and rebrand.
FC-10-C0105-151-02-12	1 Year FortiClient License Subscription for up to 20,000 clients on FG 3000-5000 Series and FG-VM08 Series running FortiOS 5.2 and above. Includes the ability to download the license file, pre-configure the client, create a custom installer and rebrand.

حيث الصورة توضح موديل الجهاز الفورتى جيت وعدد الاجهزه التي يدعمها الفورتى كلاينت .
ملاحظة: اشتراك الفورتى جيت جارء يختلف عن اشتراك الفورتى كلاينت ..

❖ طريقة تنزيل الفورتى كلاينت على الاجهزه :

1- تنزيل الفورتى كلاينت على اجهزه المستخدمين في حالة عدم وجود دومين :

يتم تنزيل الفورتى كلاينت بعد تنزيهه من الموقع forticlient.com (مجانا) او من Dashboard ثم Forticlient تقوم بتنزيل ملف بالكيلوبايت ومن ثم تقوم بتنزيهه على كل اجهزه الموظفين حيث اثناء التثبيت يجب ان تكون الاجهزه متاح عليها الانترنت لكي يعمل اتصال مع ال FDN لكي ينزل منه التحديث .
او من السوق بلاي (google play) لأجهزه الاندرويد .

أحيانا تكون هنالك اجهزه مفيرسه ولا يمكن تنزيل عليها برنامج الفورتى كلاينت من الوضع الطبيعي بل يحتاج الدخول الى الوضع الآمن مع الشبكة (safe mode with networking) ومن ثم نقوم بتنزيل برنامج الفورتى كلاينت حيث ستظهر لك رساله خطأ تجاهلها واعمل اعاده تشغيل للويندوز ومن ثم ادخل على الوضع الطبيعي ستلاحظ بأن التطبيق يعمل تنزيل بشكل طبيعي ..

2- نشر الفورتى كلاينت عبر الجروب بوليسي من سيرفر الدومين (Deploy) على الاجهزه في الشبكة، حيث يجب ان يكون الفورتى كلاينت امتداده MSI وليس exe (يتم تحويله عبر برنامج third party).

أساسيات فورتني جيت

طريقة عمل integration بين الفورتني كلاينت و الفورتني جيت لكي نتمكن من عمل تحكم مركزي بكل الفورتني كلاينت عبر الفورتني جيت (تحديث من الفورتني جيت للأجهزة وجميع البيانات لتلك الاجهزة متواجدة في الفورتني جيت... الخ)

➤ شروط عمل integrate بين الفورتني جيت و الفورتني كلاينت :

١- تفعيل خاصيه FortiClient access على ال interface مثلا LAN1 وبذلك انت تسمح للأجهزة التي مثبت عليها الفورتني كلاينت من الوصول الى الفورتني جيت .

The screenshot shows the 'Edit Interface' configuration page for 'LAN1'. The 'Administrative access' section is expanded, showing a table of access types and their status. The 'FMG-Access' checkbox is checked and highlighted with a red box. Other checked options include HTTPS, TELNET, HTTP, SSH, and PING. The 'Use VDOM Setting' checkbox is also checked.

IP/Netmask	Administrative access
10.0.0.20/255.255.255.0	PING, HTTPS, HTTP

IPv4	Administrative access	
<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
<input checked="" type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
<input checked="" type="checkbox"/> TELNET	<input type="checkbox"/> FTN	<input type="checkbox"/> RADIUS Accounting

: Authentication

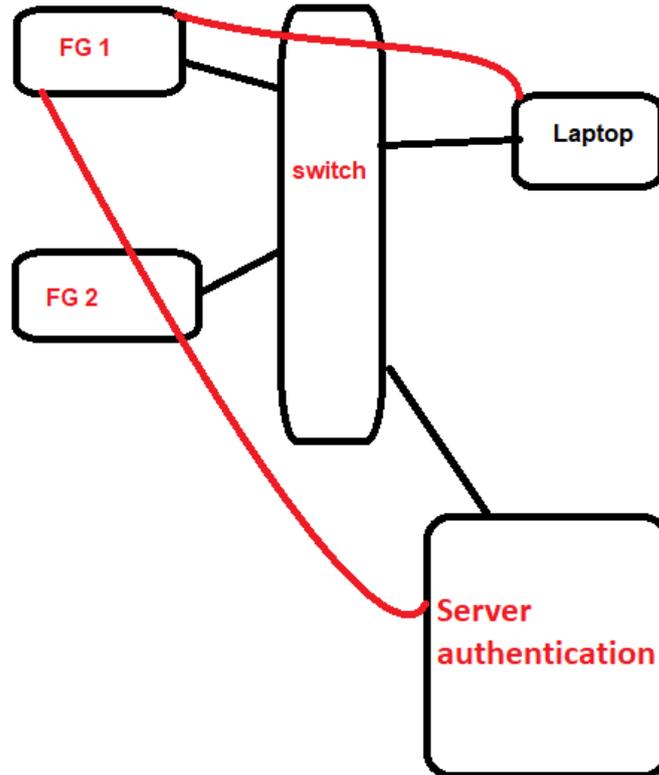
يتم استخدام ال authentication في امن الشبكات .

ماذا يقصد بعملية ال authentication ؟

يقصد بها المصادقة ويتم استخدام اليوزرنيم وكلمه السر للتأكد(التحقق) من هويه المستخدم .. أي عملية التأكد بأن الشخص الذي يستخدم اليوزرنيم والباسورد هو الشخص الحقيقي وذلك عبر ال authentication .

❖ ماهي طرق الـ authentication (التحقق من الهوية) في الفورتى جيت :
➤ Local authentication: اليوزرنيم والباسورد المعتمد عليهم في عملية المصادقة تكون مخزنه على جهاز الفورتى جيت نفسه

-1 Server authentication :



في الشركات الكبيرة بتحتوي على اكثر من جهاز فورتى جيت فايروول بالشبكة فلو قام المستخدم بإدخال اليوزرنيم والباسورد فأن الفورتى جيت يقوم بارسال الطلب الى server authentication سواء كان هذا السيرفر (,TACACS+,RADIUS,LDAP,pop3) للتحقق من اليوزرنيم والباسورد الذي ادخله المستخدم .

-1 Certificate authentication : يقوم جهاز الفورتى جيت بإصدار شهادته (RSAX 509) لجهاز الكمبيوتر التابع للكلابنت ياخذها الجهاز ويتحقق منها كلما يطلب مصدر من مصادر الشبكة

أساسيات فورتى جيت

حيث الذي يقوم بإصدار الشهادة يسمى CA حيث CA ممكن يكون جهاز كمبيوتر او جهاز الفورتى جيت وممكن تكون شركة خارجيه ..

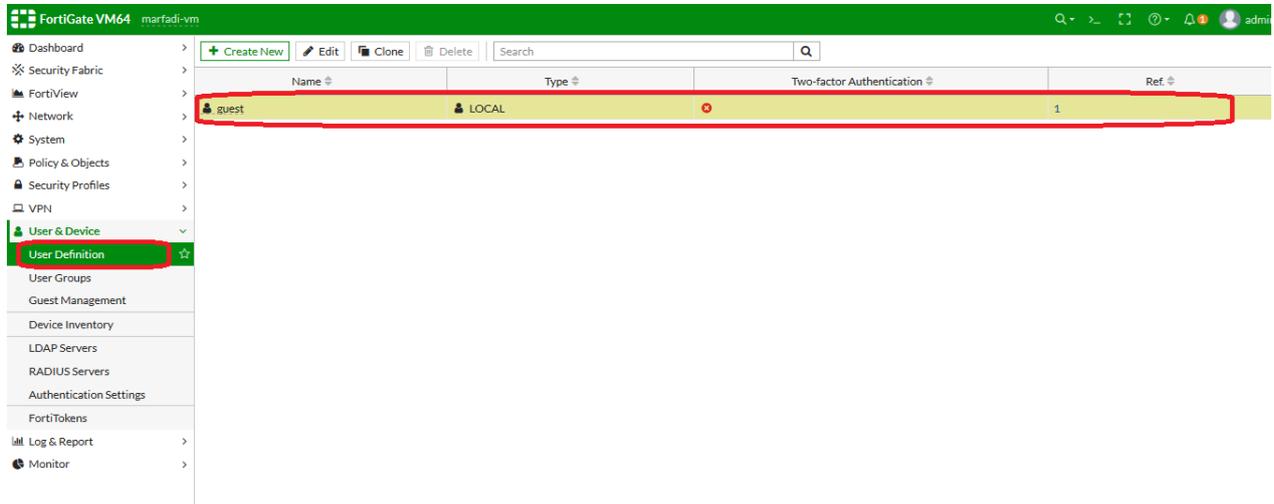
2- Two factor authentication :

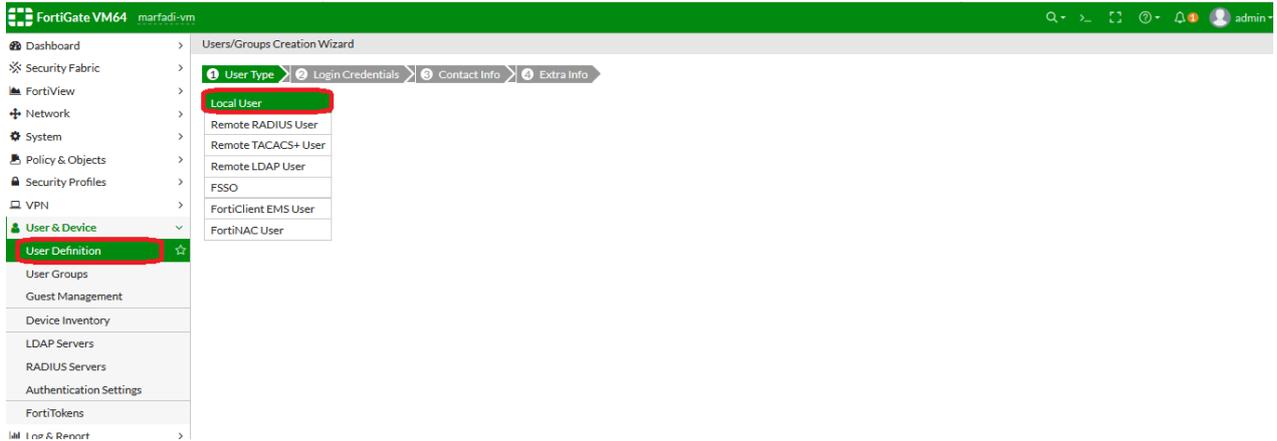
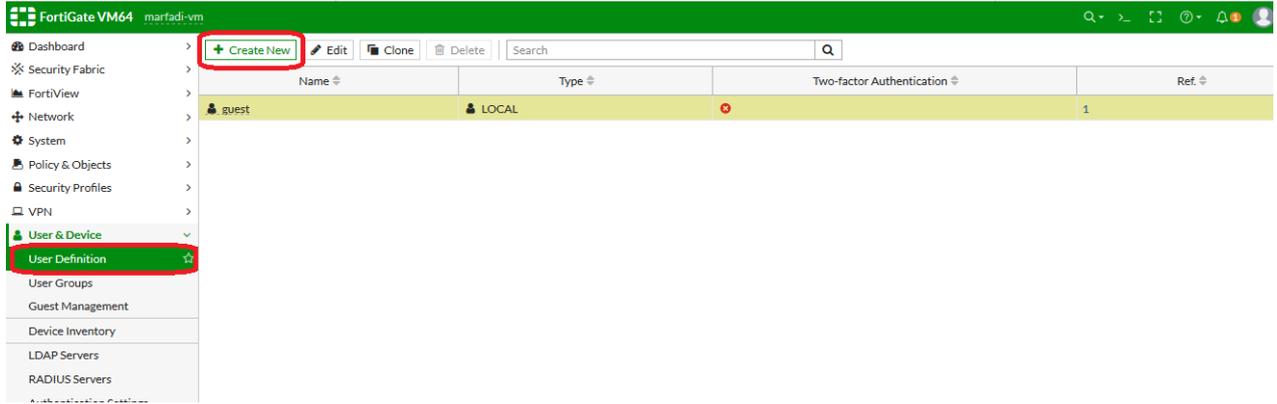
يحتوي على عامل إضافي بجانب الي وزنيم والباسورد حيث تعتبر مستوى اعلى من التحقق .. هذا العامل اسمه ال token لرفع مستوى الحماية . ال token معناها رمز ..

حيث الفورتى جيت بيستخدم طريقة ال token بانه بيقوم بتوليد (one time password) OTP وهي عبارة عن باسورد إضافية يجب ان أقوم بإدخالها بعد ادخال اليوزرنيم والباسورد الأولى . حيث الباسورد الثانية سيقوم جهاز الفورتى جيت بتوليدها كل 60 ثانية ويرسلها على جهاز اخر مثلا SMS او ايميل حيث بعد ادخال اليوزرنيم والباسورد وبالباسورد الثانية المرسله عبر SMS او غيرها سيتم عمل تحقق وتأكد من عمليه ال authentication وبعدها سيسمح لك بالوصول الى مصادر الشبكة لو كانت العملية تمت بنجاح .. حيث أصبحت العملية معقده على الهاكر على الاختراق ..

Local authentication

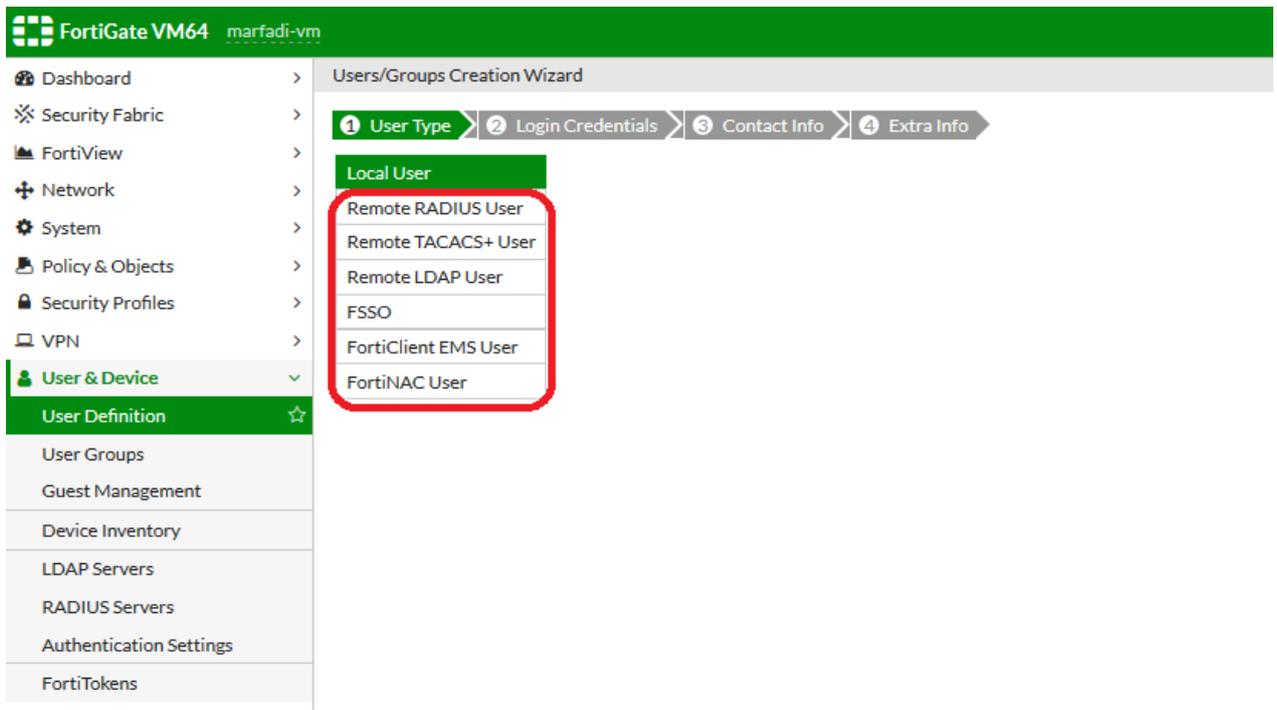
طريقة عمل local authentication على الفايروول . أولاً سنقوم بإنشاء حسابات محليه (يوزرنيم وباسورد) على الفورتى جيت حيث بشكل افتراضي يكون لدينا يوزر باسم Guest ونوعه local كما بالصورة ادناه





حيث سنختار نوع اليوزر الذي نريد انشاءه هو local user (أي ان اليوزر نيم والباسورد موجودين على الفورتى جيت نفسه)

او تريد انشاءه باي أنواع أخرى :



حيث كل يوزر من الأنواع أعلاه سوف تكون له اعدادات معينة ..

نحن الان سنختار النوع الأول Local User .

حيث بعد ذلك سنكتب اليوزرنيم والباسورد التي سنعتمد عليهم في عملية المصادقة بعد ذلك ..

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Username Anwar

Password

ثم لو تريد تحديد ايميل لهذا اليوزر حيث لو لديك اشتراك من فورتى جارد لـ Messaging services فيمكنك استخدام خاصيه الـ sms ويمكنك تخطي خطوه الايميل والـ sms .

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Email Address mohamed.marfadi@gmail.com

SMS

Two-factor Authentication

أساسيات فورتى جيت

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

User Type: Login Credentials Contact Info Extra Info

User Account Status: Enabled Disabled

User Group:

Select Entries: Search + Create

Guest-group

كما بالصورة أعلاه نعمل Enable لهذا اليوزر ولتحتب نضع هذا اليوزر لأي مجموعة منشأه مسبقا (User group).

ثم ننقر على الزر Submit لأتمام عمليه الانشاء ..

FortiGate VM64 marfadi-vm

Dashboard Security Fabric FortiView Network System Policy & Objects Security Profiles VPN User & Device User Definition

User Definition

Name	Type	Two-factor Authentication	Ref
Anwar	LOCAL	0	0
guest	LOCAL	0	1

تم الانشاء اليوزر Anwar وبنفس الطريقة تم انشاء يوزر باسم hosam كما بالصورة ادناه

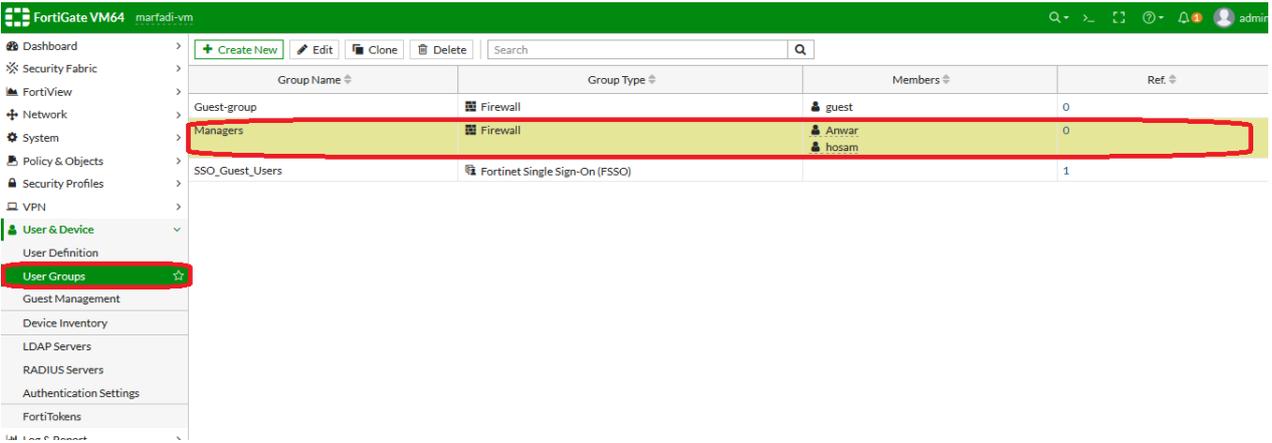
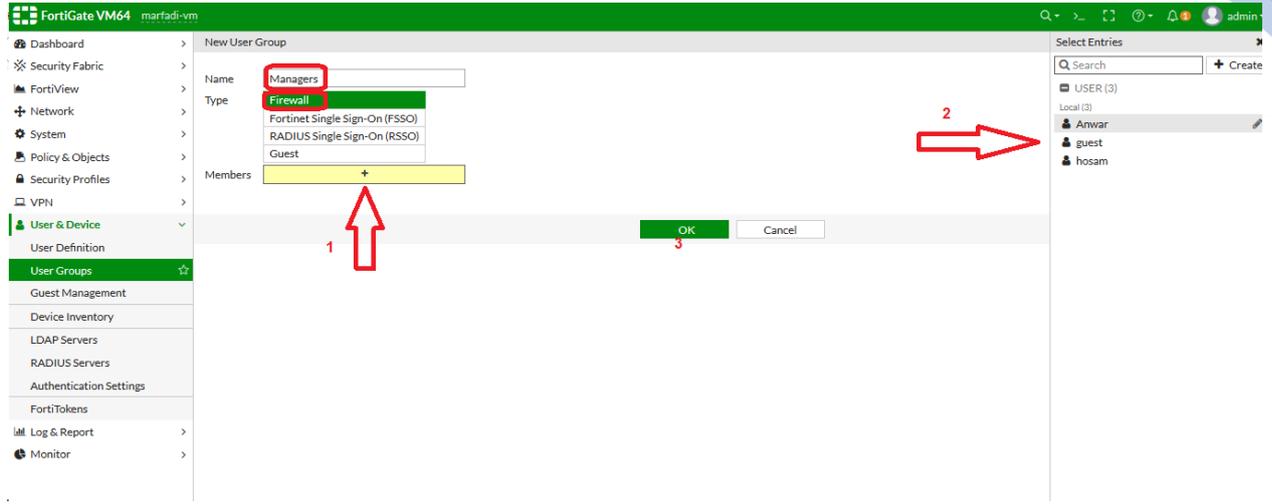
FortiGate VM64 marfadi-vm

Dashboard Security Fabric FortiView Network System Policy & Objects Security Profiles VPN User & Device User Definition

User Definition

Name	Type	Two-factor Authentication	Ref
Anwar	LOCAL	0	0
guest	LOCAL	0	1
hosam	LOCAL	0	0

طريقة انشاء user group باسم Managers ونوعها Firewall واطافة اليوزرات السابقة الى هذه الجروب .



حيث ممكن للموظفين بالشركة استخدام اليوزرات أعلاه بدلا عن الايبي ..

حيث عند تطبيق البوليسي حنختار اليوزروسوف استخدمها في عمليه ال authentication .

أي اني اريد المستخدمين يطلعوا على الانترنت عن طريق اليوزرنيم والباسورد وليس عن طريق الايبي ..
حيث لن يحصل الجهاز على الانترنت ما لم يقوم بفتح متصفح الانترنت ويظهر لك واجهه (portal) ويكتب اليوزرنيم والباسورد .

الآن سوف نقوم بإنشاء بوليسي يسمح للموظفين بالحصول على الانترنت بشرط يكون لديهم local users فقط وليس عن طريق الايبي ..

The screenshot shows the 'Edit Policy' configuration for a policy named 'allow internet'. The configuration includes:

- Name:** allow internet
- Incoming Interface:** LAN1 (port1)
- Outgoing Interface:** WAN (port2)
- Source:** all, Anwar, hosam (highlighted with a red box)
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:**
 - NAT: ON
 - IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool
 - Preserve Source Port: OFF
 - Protocol Options: PRX: default

ملاحظة: تم أضافه العنوان all وبهذا يصبح (Anwar+hosam/all) طبق البوليسي ليوزرات معينه من ال all وهو ضروري لكي يتم قبول البوليسي لأنه يجب على الأقل وجود عنوان (address) والأ سوف يظهر لك رساله الخطأ التالية :

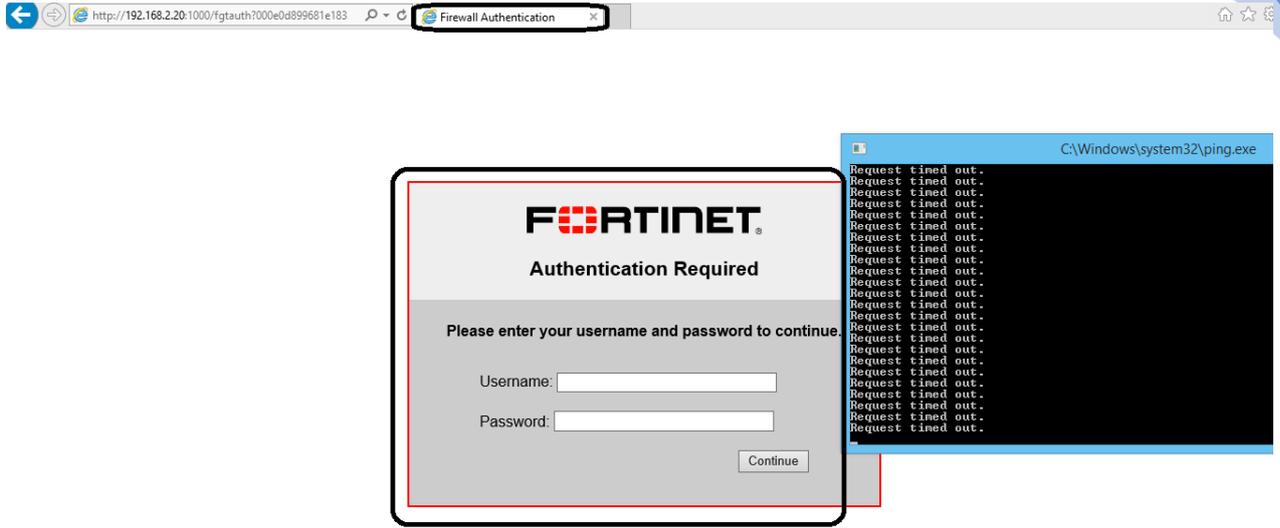
The screenshot shows the 'Edit Policy' configuration for a policy named 'allow internet'. The configuration includes:

- Name:** allow internet
- Incoming Interface:** LAN1 (port1)
- Outgoing Interface:** WAN (port2)
- Source:** Anwar, hosam (highlighted with a yellow box)
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:**
 - NAT: ON
 - IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool
 - Preserve Source Port: OFF
 - Protocol Options: PRX: default

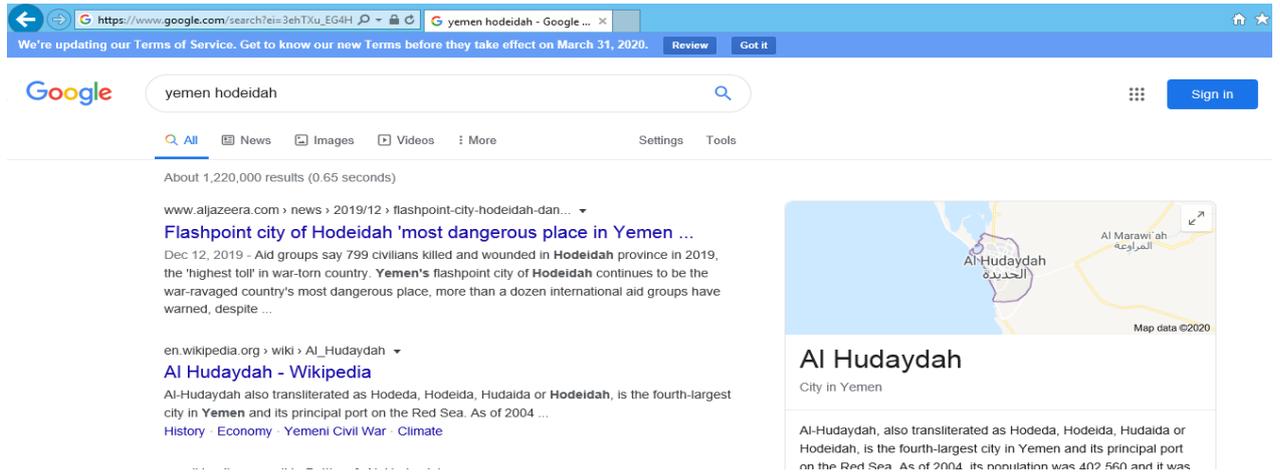
A red error message is displayed: "One address, address group, external resource or Internet service is required".

وأیضا ممكن اختيار الجروب المسماة Managers والتي تحتوي على اليوزرات (Anwar+hosam) بدلا من اختيار اليوزرات واحد واحد

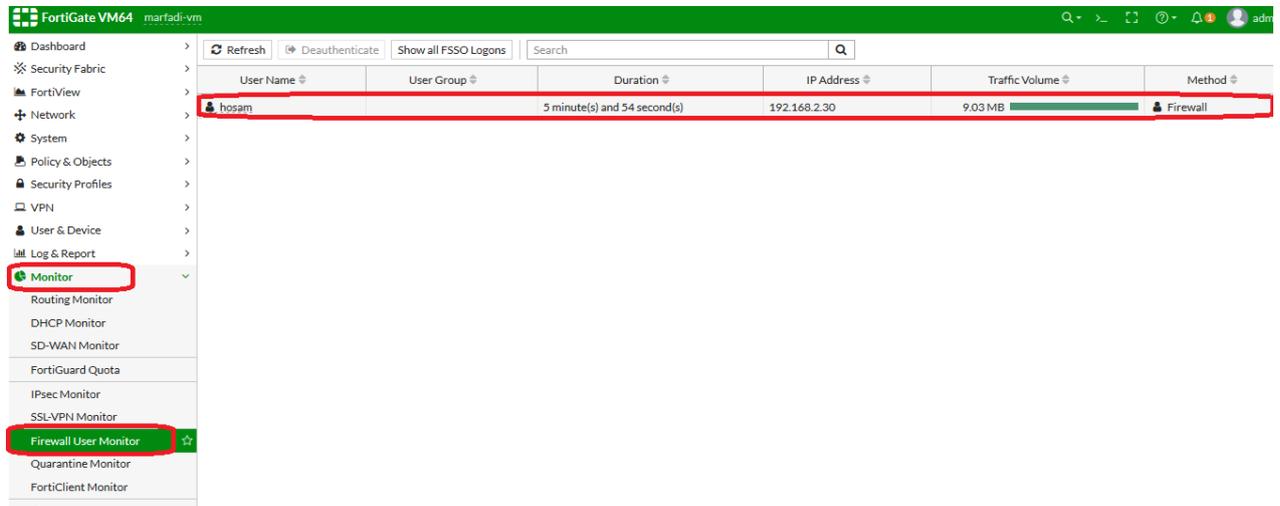
الآن نقوم بالدخول الى احدى اجهزه الشبكة الداخليه فنلاحظ بأن الانترنت ليس موجود حاليا على الجهاز



وبمجرد فتح متصفح الانترنت نلاحظ ظهور واجهه فسنقوم بإدخال يوزرنيم وباسورد hosam والباسورد 123 والذي قمنا بإدخاله سابقا وبعد ذلك يصبح الجهاز قادر على الوصول الى الانترنت حتى بعد اعاده تشغيل الجهاز..



ولمعرفة اليوزرات التي تمكنت من الوصول الى الانترنت من نوع local users



أساسيات فورتى جيت

نلاحظ تم دخول اليوزر hosam والايبي الخاص به هو 192.168.2.30 وتم استخدام 9 ميغا من الترافيك ونوعه firewall .

طريقة الغاء المصادقة (authentication) لايوزر معين من يوزرات ال local user وبذلك لن نستطيع الجهاز الوصول الى الانترنت مالم يقوم بعمل المصادقة وإدخال اليوزرنيم والباسورد مره أخرى على متصفح الانترنت ..

FortiGate VM64 marfadi-vm

Refresh Deauthenticate Show all FSSO Logons Search

User Name	User Group	Duration	IP Address	Traffic Volume	Method
Anwar		16 minute(s) and 24 second(s)	192.168.2.30	23.97 MB	Firewall

Monitor

- Routing Monitor
- DHCP Monitor
- SD-WAN Monitor
- FortiGuard Quota
- IPsec Monitor
- SSL-VPN Monitor
- Firewall User Monitor
- Quarantine Monitor
- FortiClient Monitor
- Threat Map

FortiGate VM64 marfadi-vm

Refresh Deauthenticate Show all FSSO Logons Search

User Name	User Group	Duration	IP Address
Anwar		16 minute(s) and 24 second(s)	192.168.2.30

Confirm

Are you sure you want to deauthenticate the selected user(s)?

OK Cancel

User Name	User Group	Duration	IP Address	Traffic Volume	Method
No results					

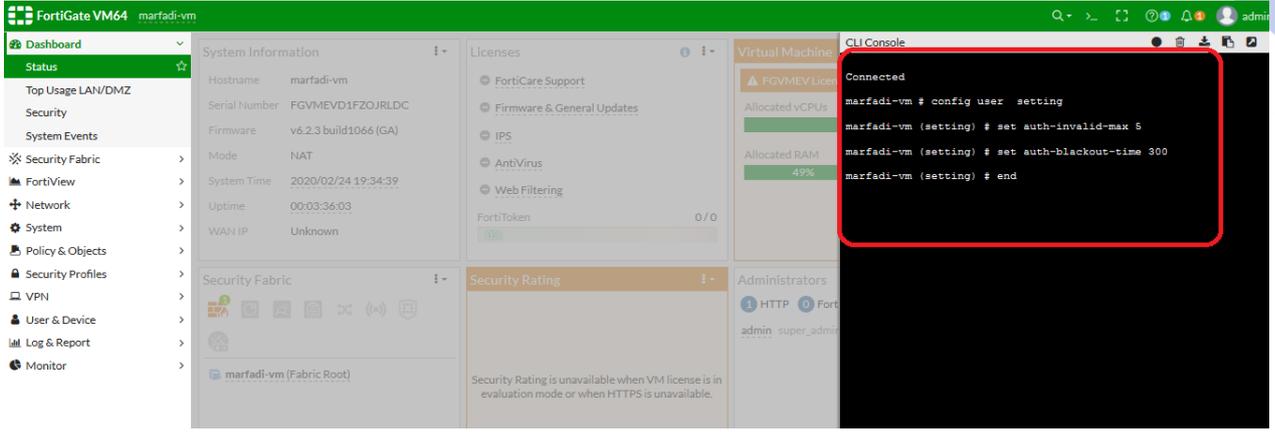
اصبح الان لا يوجد أي يوزر من نوع firewall (local user) ..

بمجرد ادخال اليوزر نيم والباسورد على الجهاز من قبل المستخدم يتم إضافته على القائمة firewall User Monitor كما بالصورة التالية :

User Name	User Group	Duration	IP Address	Traffic Volume	Method
Anwar		11 minute(s) and 4 second(s)	192.168.2.30	51.74 MB	Firewall
hosam		11 second(s)	192.168.2.159	501.21 kB	Firewall

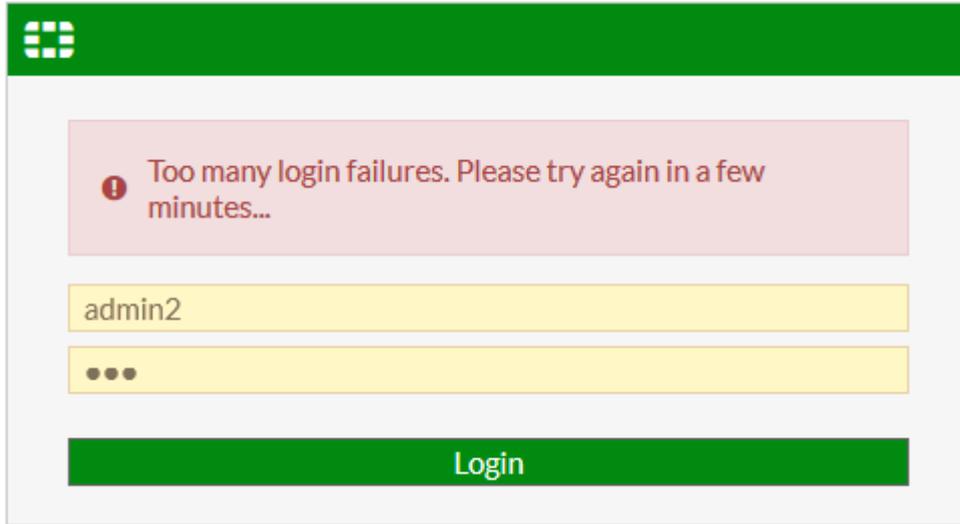
Max invalid authentication

يجب تطبيق سياسته للحد من عدد المحاولات الخاطئة (يوزر نيم او باسورد خطأ) المسموح فيها بعد ذلك نقوم بتطبيق عقوبه بأنه سوف يكون غير مسموح لهذا اليوزر لوقت معين من ادخال اليوزر نيم والباسورد .



مثلا بعد 5 محاولات ادخال خاطئه فأننا نقوم بإغلاق الحساب لمدة 300 ثانية(5 دقائق) .

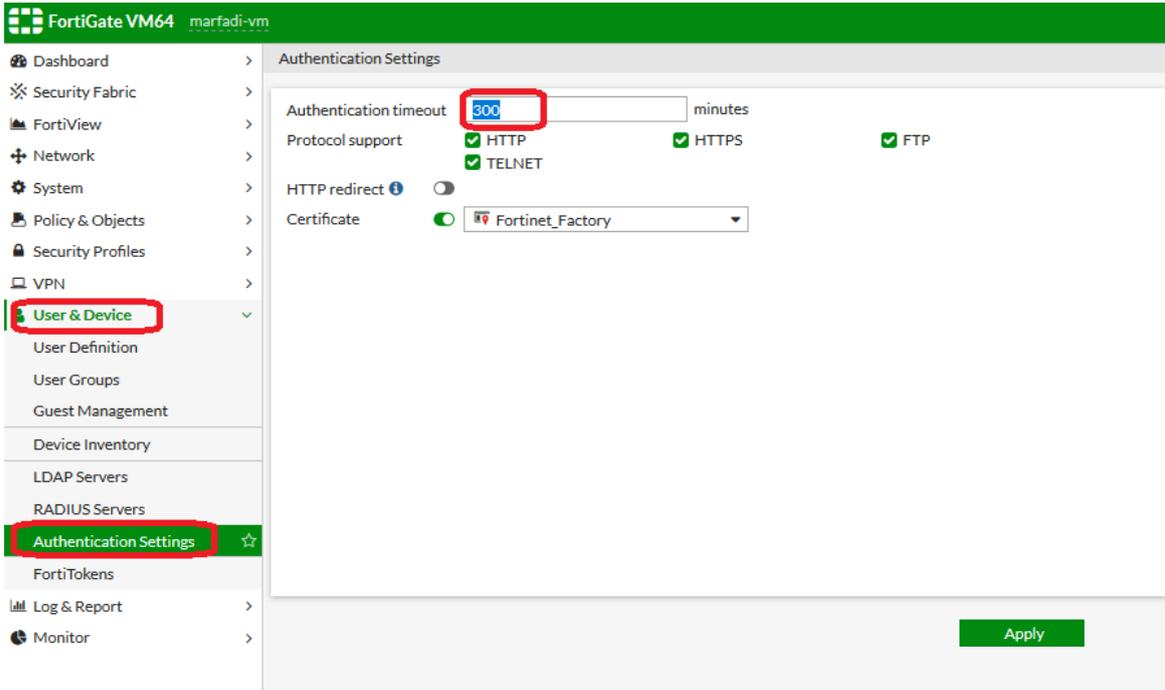
اي ان اليوزر لن يتمكن من المصادقة لأن البورتال (نافذه اليوزر نيم والباسورد لن تظهر خلال 5 دقائق)



Authentication timeout

السياسة الأخرى التي يتم تطبيقها على local users اسمها Authentication timeout بأن لو لم يستخدم الانترنت خلال فتره معينه فأنه يجب ان يعمل re-authentication مره أخرى .

حيث الافتراضي بعد 300 دقيقه بدون ان يقوم اليوزر باستخدام الانترنت فيجب عليه ادخال اليوزر نيم والباسورد مره أخرى ..



طريقة تعديل ال replacement message حيث أي رساله تظهر بالفورتى جيت يمكنك تعديلها ،
الآن سنقوم بتعديل الرساله التابعه ل authentication وتحديد الشاشة Login Page وأيضا شاشه
Login failed Page في حالة انك أدخلت يوزرنيم اوباسورد خطأ .

Name	Description	Modified
Authentication		
Email Collection	Replacement HTML for email collection page	
Email Collection Invalid Email	Replacement HTML for email collection page after user enters invalid email	
FortiToken Page	Replacement HTML for FortiToken authentication page	
Login Failed Page	Replacement HTML for authentication failed page	
Login Page	Replacement HTML for authentication login page	
Device Detection Portal		
Device Detection Portal Failure Page	Replacement HTML for device detection portal failure page	
FortiGuard Web Filtering		
FortiGuard Block Page	Replacement HTML for FortiGuard Web Filter block page	
HTTP		
URL Block Page	Replacement HTML for HTTP URL blocked page	✓
Security Profiles		
Application Control Block Page	Replacement HTML for application control block page	✓
DLP Block Message	Replacement text for DLP block message	
DLP Block Page	Replacement HTML for DLP block page	
Virus Block Message	Replacement text for antivirus block message	

نحدد الشاشة المراد تغييرها ثم edit

Name	Description	Modified
Authentication		
Email Collection	Replacement HTML for email collection page	
Email Collection Invalid Email	Replacement HTML for email collection page after user enters invalid email	
FortiToken Page	Replacement HTML for FortiToken authentication page	
Login Failed Page	Replacement HTML for authentication failed page	
Login Page	Replacement HTML for authentication login page	
Device Detection Portal		
Device Detection Portal Failure Page	Replacement HTML for device detection portal failure page	
FortiGuard Web Filtering		
FortiGuard Block Page	Replacement HTML for FortiGuard Web Filter block page	
HTTP		
URL Block Page	Replacement HTML for HTTP URL blocked page	✓
Security Profiles		
Application Control Block Page	Replacement HTML for application control block page	✓

Message Format: text/html Message Size: 2.6 kB/32.8 kB

```

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset="
<style type="text/css">
.html, body{
height:100%;
padding:0;
margin:0;
}.col
display:table;
width:100%;
height:100%;
}.ic1
display:table-cell;
vertical-align:middle;
height:100%;
}form{
display:block;
background:#ccc;
border:2px solid red;
padding:0 0 25px 0;
width:500px;
font-family:helvetica,sans-serif;
font-size:14px;
margin:10px auto;
text-align:center;
width:350px;
padding:10px;
}.fel{
text-align:left;
}.fer{
text-align:right;
}h1{
font-weight:bold;

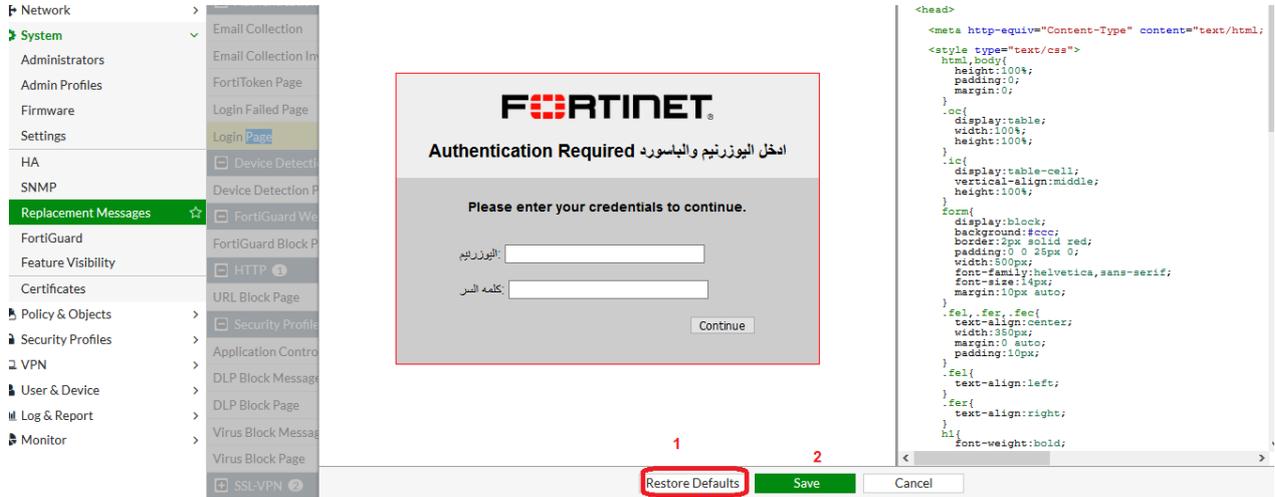
```

ثم نقوم بتعديل ما نريده بكل سهولة ..

ونلاحظ الشاشة بعد التعديل

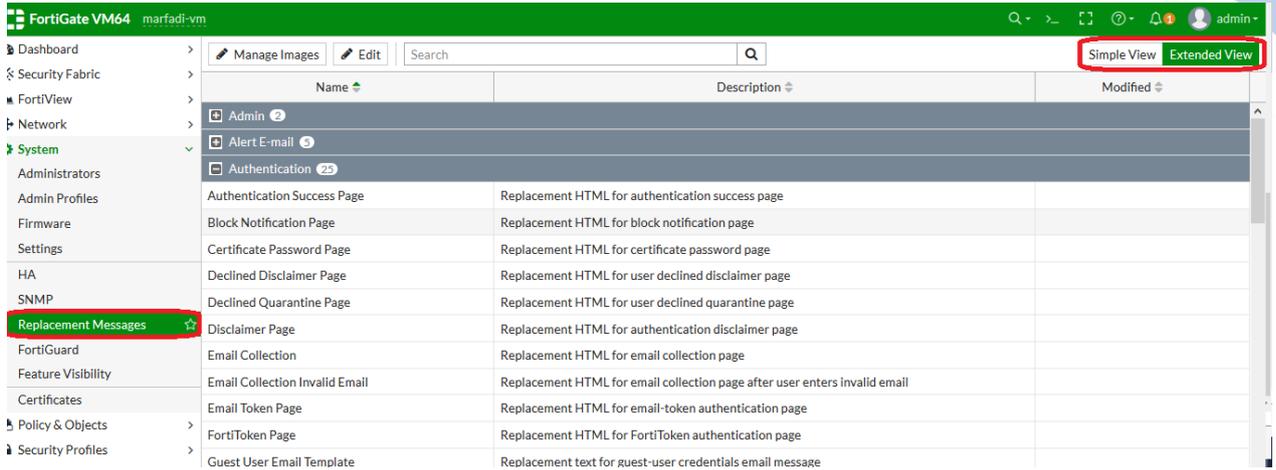


ولو تريد ارجاع الشاشة كما كانت فنقوم بعمل restore defaults ثم save



ملاحظة :

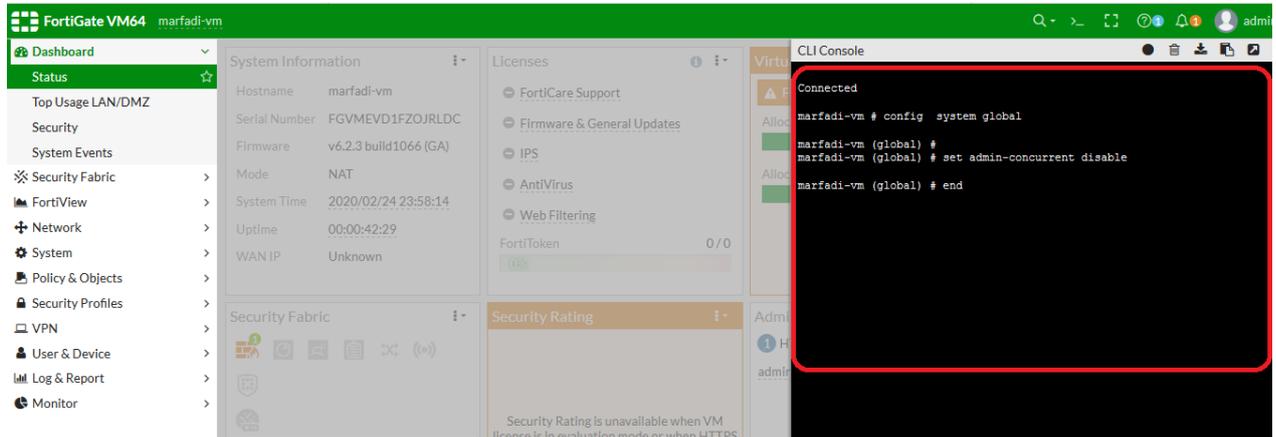
يوجد خيارين لأظهار الرسائل بالفورتني جيت هما extend view والأخر Simple View حيث الخيار Extend view بيظهر كل الرسائل على مستوى الفورتني جيت اما simple View فيظهر لك الرسائل الأساسية فقط..



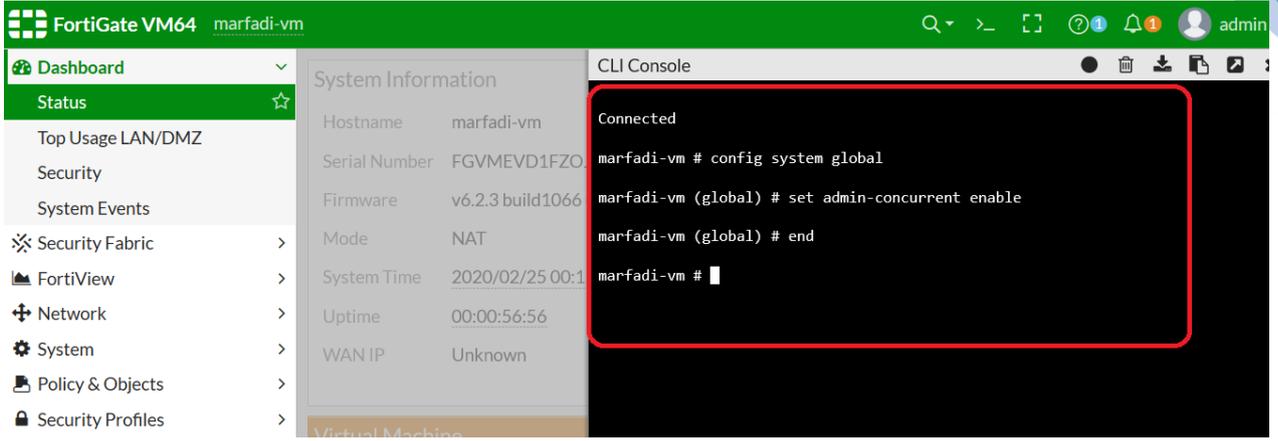
Restricting number of concurrent user logons

كم عدد ال sessions الذي مسموح ال administrator يقدروا يعملوا login على الفورتى جيت او session واحده فقط عبر الويب ، حيث الوضع الطبيعي بأنه مسموح لعدد session غير محدود ..

لتقييد الدخول الى الفورتى جيت لأكثر من administrator (تحدد session واحده فقط) كنوع من ال security وذلك عبر الاوامر التالية :



ولو اردت اعاتها كما كانت كما بالصورة ادناه..



Managing guests

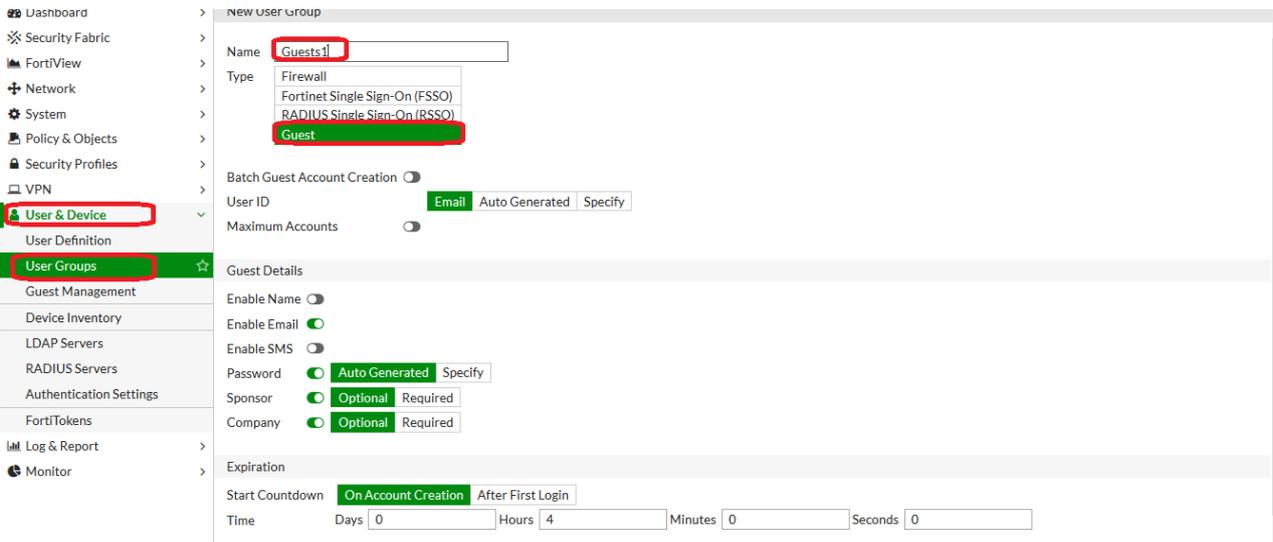
هي عبارة عن ادارة الزوار القادمين للشركه حيث يكونوا لفترة مؤقتة فقط حيث يمكن لجهاز الفورتني جيت ان يعطيك حسابات مؤقتة تنتهي بعد فترة معينه .

حيث سيتم انشاء حسابات لهؤلاء الزوار بشكل عشوائي عبر الفورتني جيت نفسه او بنفس الایميلات الشخصيه لكل زائر ونقوم بتخصيص حسابات بشكل يدوي .

وسيتم تسليم الزائر لحساباتهم اما عن طريق طباعه الحسابات او ارساله بالایمیل او عبر SMS .

لكي أقوم بعمل هذا الشيء يجب تخصيص جروب للزوار (Guests group) تحتوي على عدد من الحسابات .

نقوم الان بإنشاء جروب باسم Guest1 ونوعه guest



حيث لو كان عددهم كبير جدا فانك سوف تقوم بتفعيل الخيار Batch Guest Account Creation

الآن سوف نقوم بإنشاء الحسابات بشكل منفرد وليس مره واحده لذا لن نقوم بتفعيل هذا الخيار

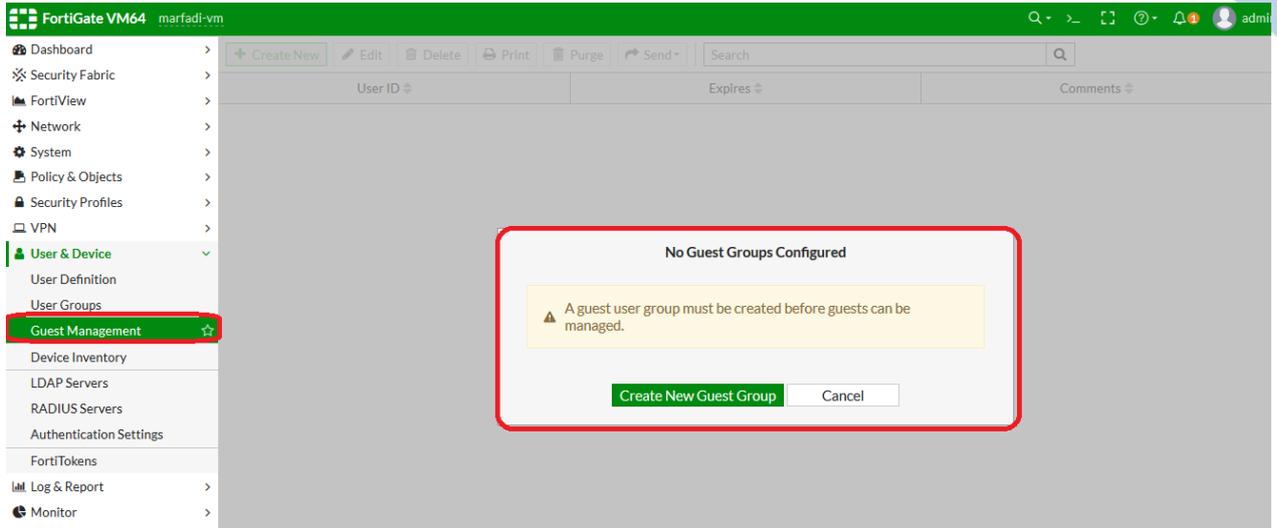
لذا سوف نقوم باختيار نوع الـ User ID بحسب الخيارات التالية:

Email: حيث يكون اسم حساب الزائر هو نفسه ايميل الزائر.

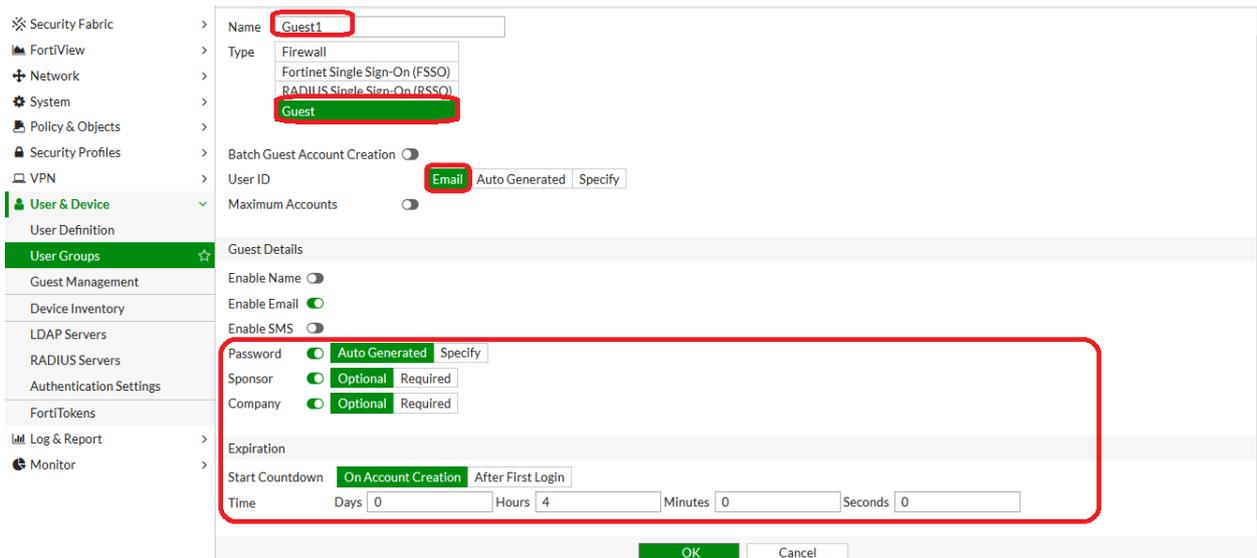
Auto generated: أي ان الفورتني هو الذي سوف يقوم بإنشاء أسماء الحسابات (اليوزرات) بشكل اوتوماتيكي .

Specify: تقوم بكتابه اسم الحساب (اليوزر) (ID) بنفسك ..

حيث لن تستطيع ان قوم بإنشاء يوزر من نوع guest الا لو كنت قد أنشأت جروب من نوع guest أولاً لذا لو حاولت الدخول الى Guest management قبل انشاء الجروب سوف تظهر لك رساله تحذيره كما بالصورة التالية :



لذا أولاً قم بإنشاء الـ Guest group بالنوع التي تريده مثلًا email او auto generated او specify مثلًا
سوف نختار النوع Email

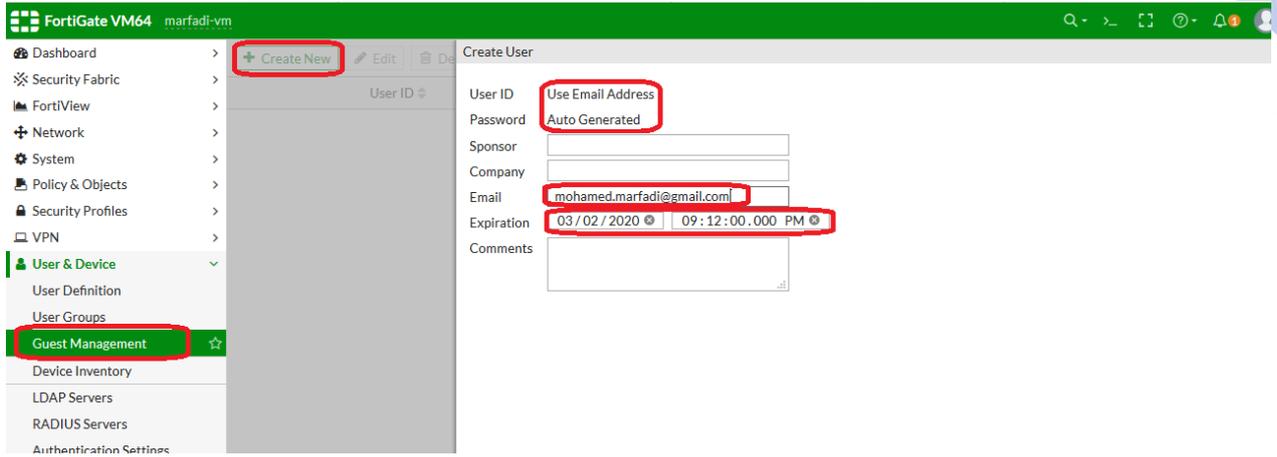


نلاحظ كما بالصورة أعلاه بأننا اخترنا بان الباسورد سوف يتم توليده بشكل اوتوماتيكي عبر الفورتى جيت (Auto Generated) وبأنه سوف تكون نهاية الحساب بعد 4 ساعات من وقت انشاء الحساب ..

لذا عند انشاء الحساب سوف يكون الـ id هو نفسه الايميل الخاص بالزائر

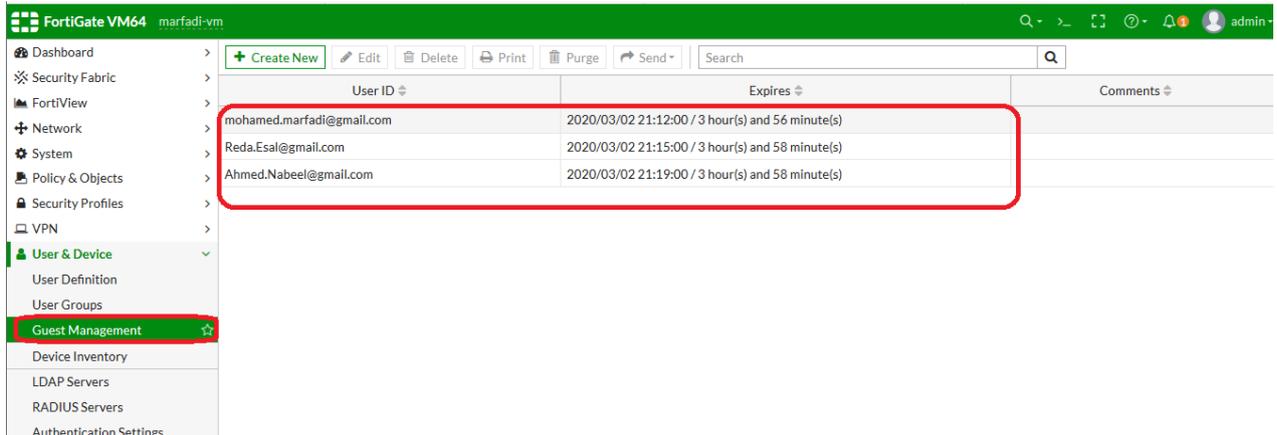
ملاحظة:

لوقمت بجعل Password=disabled فان عند انشاء اليوزر لن يطالبك بالباسورد ابدأ ..

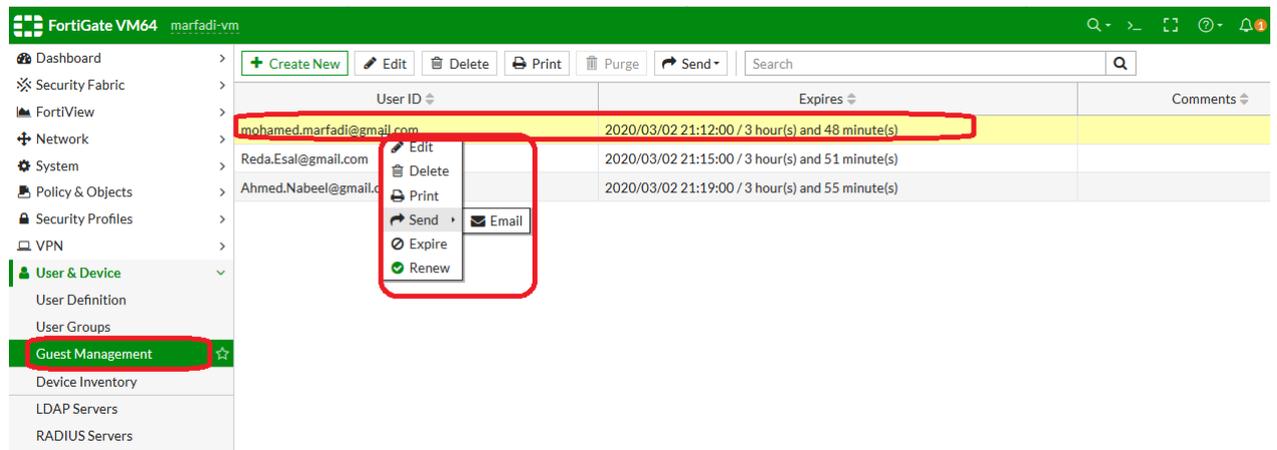


كما بالصورة أعلاه يتبين بأن الـ User Id هو عبارة عن ايميل الزائر ويجب ان تقوم بكتابته مثلا Mohamed.marfadi@gmail.com في الخانة Email والآن تتم عملية الانشاء لهذا الحساب ويتبين بأن مدة انتهاء الحساب بعد 4 ساعات .

حيث سيتم ارسال الحساب على ايميل الزائر المحدد أعلاه بشرط انك تكون قد فعلت بأن الفورتي جيت يمكنه الارسال عبر الايميل..



حيث قمت بإنشاء الحسابات بحسب الايميل كما بالصورة اعلاه ..

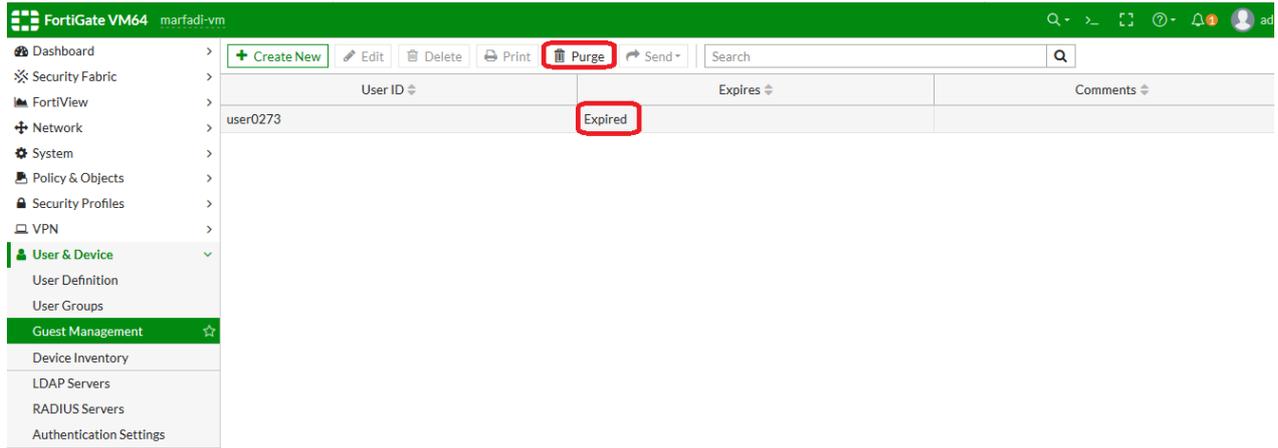


أساسيات فورتى جيت

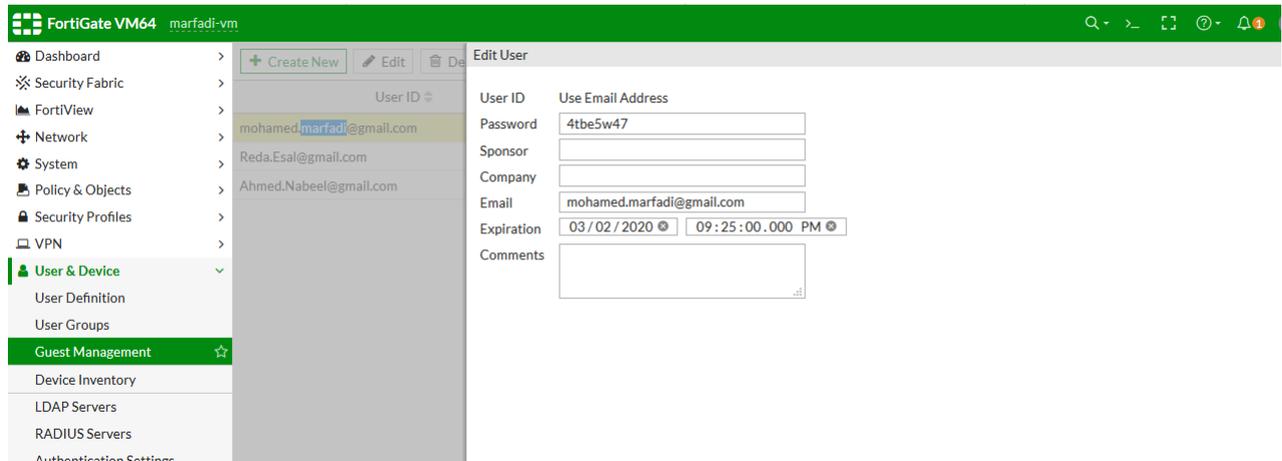
يمكنك التحكم بالحساب من حيث ارسال الباسورد الى ايميل الموظف او مده انتهاء الحساب فورا او حذف الحساب او التعديل عليه او تجديد مده الحساب ...

وهناك خيار اسمه purge حيث عند النقر عليه يقوم بحذف كل الحسابات التي انتهت مدتها ويتبقى لك الحسابات التي لازالت valid .

حيث نلاحظ بأن الخيار Purge لا يفعل الا لو كان هناك حسابات منتهيه كما بالصورة ادناه



ولمعرفة الباسورد الذي قام الفورتى جيت بتوليده بشكل اوتوماتيكي نقوم بالنقر على الحساب نقرتين بزر الفاره الايسر وسوف يظهر لك كما بالصورة ادناه



الان سوف أقوم بتغيير نوع الجروب الى Guest1 Auto Generated

أساسيات فورتى جيت

Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > VPN > User & Device > User Definition > User Groups > Guest Management > Device Inventory > LDAP Servers > RADIUS Servers > Authentication Settings > FortiTokens > Log & Report > Monitor

Name: Guest1
Type: Guest
Batch Guest Account Creation:
User ID: Email **Auto Generated** Specify
Maximum Accounts:

Guest Details
Enable Name:
Enable Email:
Enable SMS:
Password: Auto Generated Specify
Sponsor: Optional Required
Company: Optional Required

Expiration
Start Countdown: On Account Creation After First Login
Time: Days 0 Hours 4 Minutes 0 Seconds 0

OK Cancel

لذا عن انشاء اليوزر في هذا النوع فانك لن تقوم بكتابه اليوزر نيم ولا الباسورد

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > VPN > User & Device > User Definition > User Groups > Guest Management > Device Inventory > LDAP Servers > RADIUS Servers > Authentication Settings > FortiTokens > Log & Report

Create User
User ID: **Auto Generated**
Password: **Auto Generated**
Sponsor:
Company:
Email:
Expiration: 03/02/2020 09:32:00.000 PM
Comments:

حتى ال email يمكنك تركه فارغا ...

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > VPN > User & Device > User Definition > User Groups > Guest Management > Device Inventory > LDAP Servers > RADIUS Servers > Authentication Settings

User ID	Expires	Comments
mohamed.marfadi@gmail.com	2020/03/02 21:25:01 / 3 hour(s) and 52 minute(s)	
Reda.Esal@gmail.com	2020/03/02 21:15:00 / 3 hour(s) and 42 minute(s)	
Ahmed.Nabeel@gmail.com	2020/03/02 21:19:00 / 3 hour(s) and 46 minute(s)	
user0022	2020/03/02 21:32:00 / 3 hour(s) and 58 minute(s)	

تم انشاء الحساب اوتوماتيكيا باسم user0022

النوع الأخير من Guest group هو specify أي انك سوف تقوم بإنشاء اسم اليوزر بشكل يدوي .

أساسيات فورتي جيت

The screenshot shows the configuration page for a Guest user group. The left sidebar lists various system settings, with 'User & Device' expanded to show 'User Groups'. The main area is titled 'Guest1' and contains the following settings:

- Name: Guest1
- Type: Guest
- Batch Guest Account Creation:
- User ID: Email | Auto Generated | Specify
- Maximum Accounts:
- Guest Details:
 - Enable Name:
 - Enable Email:
 - Enable SMS:
 - Password: Auto Generated | Specify
 - Sponsor: Optional | Required
 - Company: Optional | Required
- Expiration:
 - Start Countdown: On Account Creation | After First Login
 - Time: Days 0 | Hours 4 | Minutes 0 | Seconds 0

Buttons for 'OK' and 'Cancel' are at the bottom.

كما نلاحظ بأن خيار انشاء الباسورد هو Auto Generated أي بأن الفورتي جيت هو الذي يقوم بإنشاء
هـ لكل حساب ..

The screenshot shows the 'Create User' configuration page. The left sidebar is the same as the previous image. The main area is titled 'Create User' and contains the following settings:

- User ID: hosam
- Password: Auto Generated
- Sponsor:
- Company:
- Email:
- Expiration: 03/02/2020 | 09:36:00.000 PM
- Comments:

كما الصوره أعلاه قمنا بكتابه اسم الحساب hosam بشكل مانوال ..

الخلاصة :

The screenshot shows the 'Edit User Group' configuration page for 'Guest1'. The left sidebar is the same as the previous images. The main area is titled 'Guest1' and contains the following settings:

- Name: Guest1
- Type: Guest
- Batch Guest Account Creation:
- User ID: Email | Auto Generated | Specify
- Maximum Accounts:
- Guest Details:
 - Enable Name:
 - Enable Email:
 - Enable SMS:
 - Password: Auto Generated | Specify
 - Sponsor: Optional | Required
 - Company: Optional | Required
- Expiration:
 - Start Countdown: On Account Creation | After First Login
 - Time: Days 0 | Hours 4 | Minutes 0 | Seconds 0

: Start countdown

On Account creation: أي سيتم احتساب فتره الانتهاء (4 ساعات مثلا) منذ انشاء الحساب ..

After First Login: سيتم احتساب فتره انتهاء الحساب من بعد اول دخول للحساب من قبل الزائر..

نلاحظ عند انشاء الحساب

The screenshot shows the 'Create User' form in the FortiGate VM64 interface. The 'Expiration' field is highlighted with a red box and is set to '7' hours. The 'User ID' is 'Anwar' and the 'Password' is '123'. The 'Guest Management' option is selected in the left sidebar.

باننا قمنا بكتابه اسم اليوزر والباسورد بشكل مانول ...

The screenshot shows the 'User List' in the FortiGate VM64 interface. The 'User ID' column is highlighted with a red box, showing the user 'Anwar' with an expiration of '7 hour(s) and 0 minute(s) after first login'.

User ID	Expires	Comments
mohamed.marfadi@gmail.com	2020/03/02 21:25:01 / 3 hour(s) and 41 minute(s)	
Reda.Esal@gmail.com	2020/03/02 21:15:00 / 3 hour(s) and 31 minute(s)	
Ahmed.Nabeel@gmail.com	2020/03/02 21:19:00 / 3 hour(s) and 35 minute(s)	
user0022	2020/03/02 21:32:00 / 3 hour(s) and 48 minute(s)	
hosam	2020/03/02 21:36:00 / 3 hour(s) and 52 minute(s)	
Anwar	7 hour(s) and 0 minute(s) after first login	

لواردت انشاء حسابات بشكل اوتوماتيكي لعدد مثلا 50 يوزر.

The screenshot shows the 'Edit User Group' configuration page in FortiGate VM64. The left sidebar is expanded to 'User & Device' > 'User Groups'. The main content area shows the configuration for a user group named 'Guest1' of type 'Guest'. The 'Batch Guest Account Creation' checkbox is checked and highlighted with a red box. Below it, the 'Maximum Accounts' is set to 0. The 'Expiration' section shows 'Start Countdown' set to 'After First Login'. The 'Time' section is set to 0 Days, 4 Hours, 0 Minutes, and 0 Seconds. At the bottom, there are 'OK' and 'Cancel' buttons.

The screenshot shows the 'User' configuration page in FortiGate VM64. The left sidebar is expanded to 'User & Device' > 'User Groups'. The main content area shows a table with columns for 'User ID', 'Expires', and 'Comments'. The 'Create New' button is highlighted with a red box, and the 'Multiple Users' checkbox is also highlighted with a red box. Below the table, it says 'No results'.

The screenshot shows the 'Create User' configuration page in FortiGate VM64. The left sidebar is expanded to 'User & Device' > 'User Groups'. The main content area shows the 'Create User' form. The 'Number of Accounts' is set to 50, highlighted with a red box. The 'User ID' and 'Password' are set to 'Auto Generated'. The 'Expiration' is set to 4 Hours, highlighted with a red box. The 'Comments' field is empty.

أساسيات فورتي جيت

User ID	Expires	Comments
user0229	4 hour(s) and 0 minute(s) after first login	
user0230	4 hour(s) and 0 minute(s) after first login	
user0231	4 hour(s) and 0 minute(s) after first login	
user0232	4 hour(s) and 0 minute(s) after first login	
user0233	4 hour(s) and 0 minute(s) after first login	
user0234	4 hour(s) and 0 minute(s) after first login	
user0235	4 hour(s) and 0 minute(s) after first login	
user0236	4 hour(s) and 0 minute(s) after first login	
user0237	4 hour(s) and 0 minute(s) after first login	
user0238	4 hour(s) and 0 minute(s) after first login	
user0239	4 hour(s) and 0 minute(s) after first login	
user0240	4 hour(s) and 0 minute(s) after first login	
user0241	4 hour(s) and 0 minute(s) after first login	
user0242	4 hour(s) and 0 minute(s) after first login	
user0243	4 hour(s) and 0 minute(s) after first login	
user0244	4 hour(s) and 0 minute(s) after first login	
user0245	4 hour(s) and 0 minute(s) after first login	

تم انشاء 50 حساب بشكل اوتوماتيكي فيمكنك طباعتها او ارسالها للزوار باي طريقة ..

➤ ثم بعد ذلك سنقوم بإنشاء بوليسي ونحدد بها الجروب المسماة (Guest1) في الSource.

لو تريد مثلا احدى موظفي الايتي عندك لا تريد ان تعطيه صلاحية كامله على الفورتي جيت وتريد فقط ان يدير حسابات الزوار (Guest users) نقوم بالخطوات التالية :

Administrator	Trusted Hosts	Profile	Type	Two-factor Authentication
admin		super_admin	Local	Disabled
hosam		SHOW_ONLY	Local	Disabled
yasser	192.168.2.140/32	Yasser-it	Local	Disabled

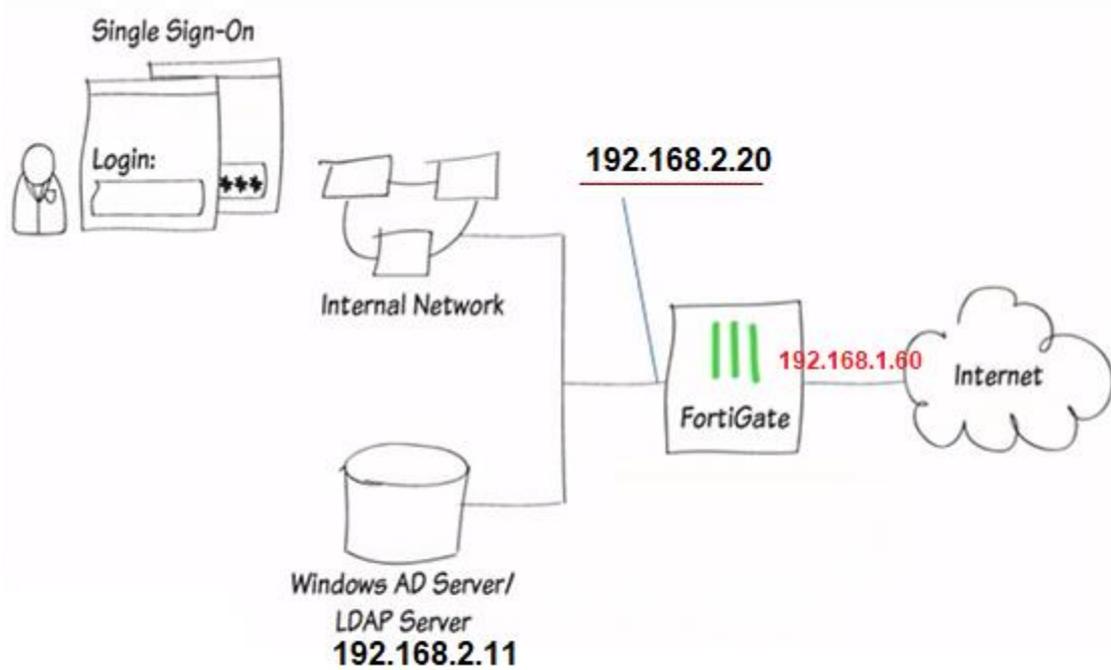
أساسيات فورتني جيت

كما بالصورة أعلاه تم انشاء يوزر باسم `guest_admin` يقوم بإدارة الجروب المسماة `Guest1`.

User ID	Expires	Comments
user0280	2020/03/05 01:12:00 / 3 hour(s) and 20 minute(s)	
user0281	2020/03/05 01:12:00 / 3 hour(s) and 20 minute(s)	

الآن اليوزر `guest_admin` يمكنه إدارة الجروب المسماة `Guest1` من انشاء يوزر والتعديل عليه وحذف اليوزرات التابعة للجروب `Guest1` وأيضا عمل `Purge` وطباعه اليوزرات.. الخ..

FSSO(fortinet single sign on)



نحن في الدروس السابقة لكي نصل الى الانترنت عبر الفورتني يجب ان يكون لدينا يوزر في الفورتني جيت لذا لكي افتح الانترنت على أي جهاز يوجد لدينا خطوتين

١- ادخال اليوزرنيم والباسورد للويندوز (للجهاز اول مره) أي login to computer

٢- ادخال اليوزرنيم والباسورد (local account) الموجود بالفورتني جيت

وبهذا استطيع الوصول الى الانترنت

اذا لدينا خطوتين لكي يتمكن الجهاز من الوصول الى الانترنت ...

ولتخفيض العمليتين السابقتين الى عمليه واحده فقط

أي الاعتماد على اليوزرنيم والباسورد الموجودين في AD فقط .

وذلك لتعريف كل اليوزرات والجروبات الموجودة في AD على الفورتني جيت .

وبذلك يمكنني التحكم بكل اليوزرات والجروبات عبر الفورتني جيت كأنهم local users وذلك عبر عمل

AD integration مع fortigate .

AD server in windows LDAP server ممكن يكون

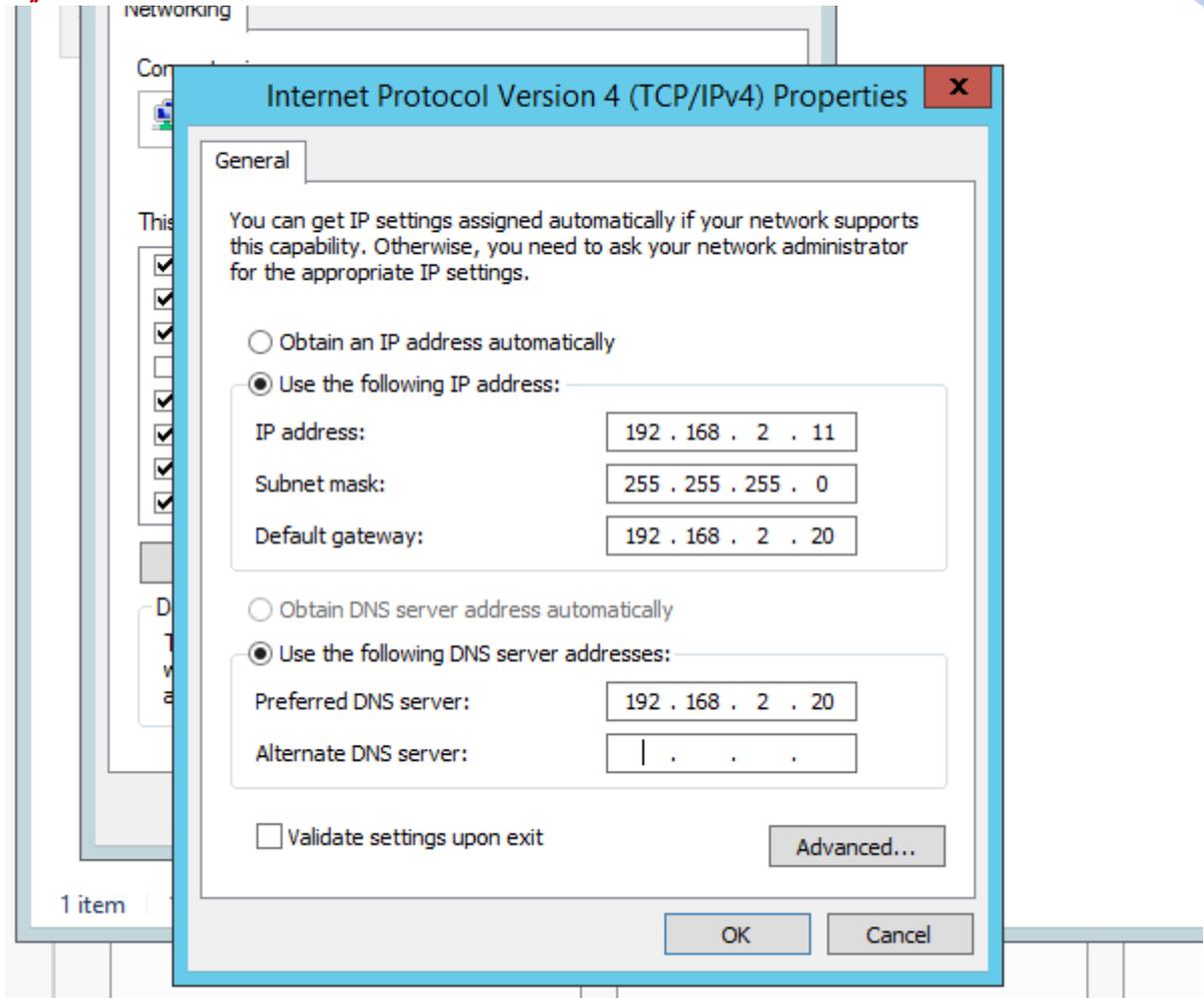
اولينكس اونوفل... الخ .

Ldap هي DB الخاصة بالحسابات

نحن سوف نتعامل مع ldap server in Microsoft وهو AD server

ولكي نقوم بعمل integrate للفورتى جيت مع الAD يجب ان تقوم بالخطوات التالية :

- ١- تحديد الLdap server للفورتى جيت أي من هو الAD server
 - ٢- عمل اعدادات للLdap server لكي يعمل single sign on أي يجب تفعل خاصيه single sign on على الفورتى جيت .
 - ٣- سنقوم بإنشاء FSSO group تحتوي بداخلها على اليوزرات او الجروبات الموجودة على الAD
 - ٤- انشاء بوليسي ونختار الجروب التي قمنا بإنشائها بالخطوة رقم 3 والتي تحتوي على المستخدمين الذي سوف نطبق عليهم فكره Single sign on .
- حيث أي شخص ليس لديه حساب في الAD لن يستطيع الوصول الى الانترنت عبر الفورتى جيت لأنك في البوليسي قمت بتخصيص FSSO group الالوانت سمحت بذلك .
- الان سنقوم بعمل AD server بالايبي 192.168.2.11 ونقوم بإنشاء يوزرات على الAD

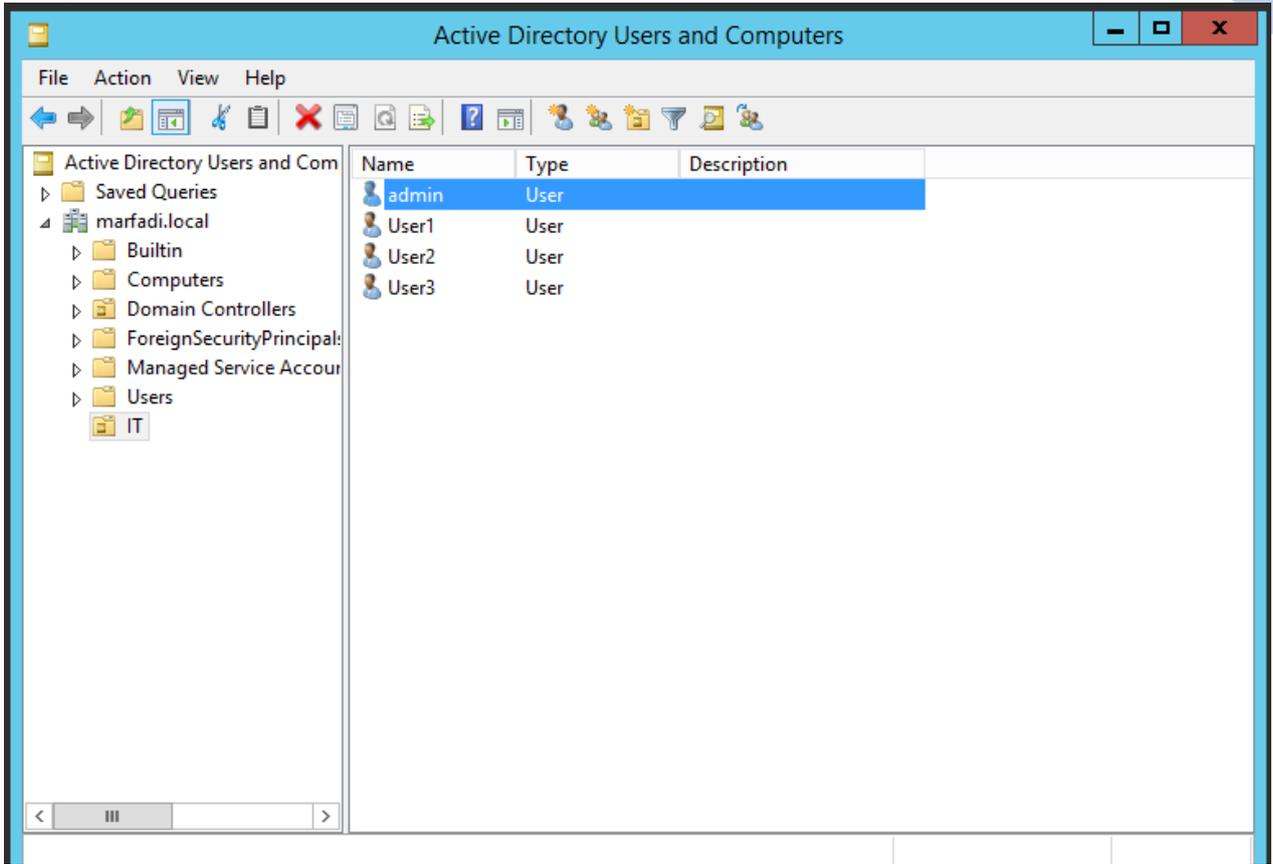


ملاحظة: قم باغلاق الفايرول للويندوز سيرفر 2012 (Active directory)

نقوم بإنشاء يوزرات على الAD كالتالي :

Admin ونوعه domain admins

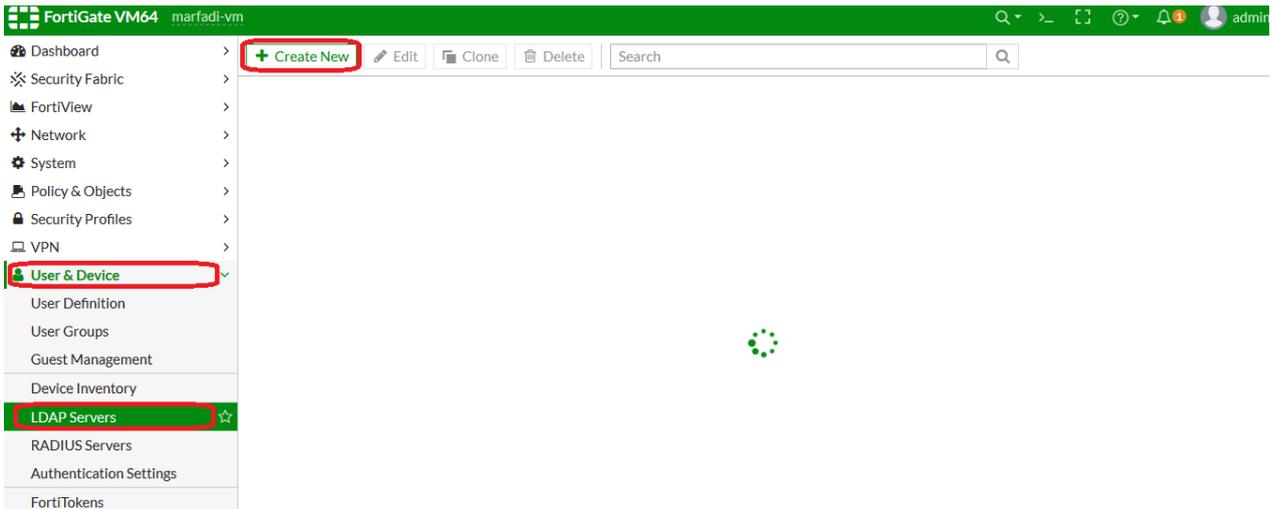
User3، User2، User1 ونوعه domain users

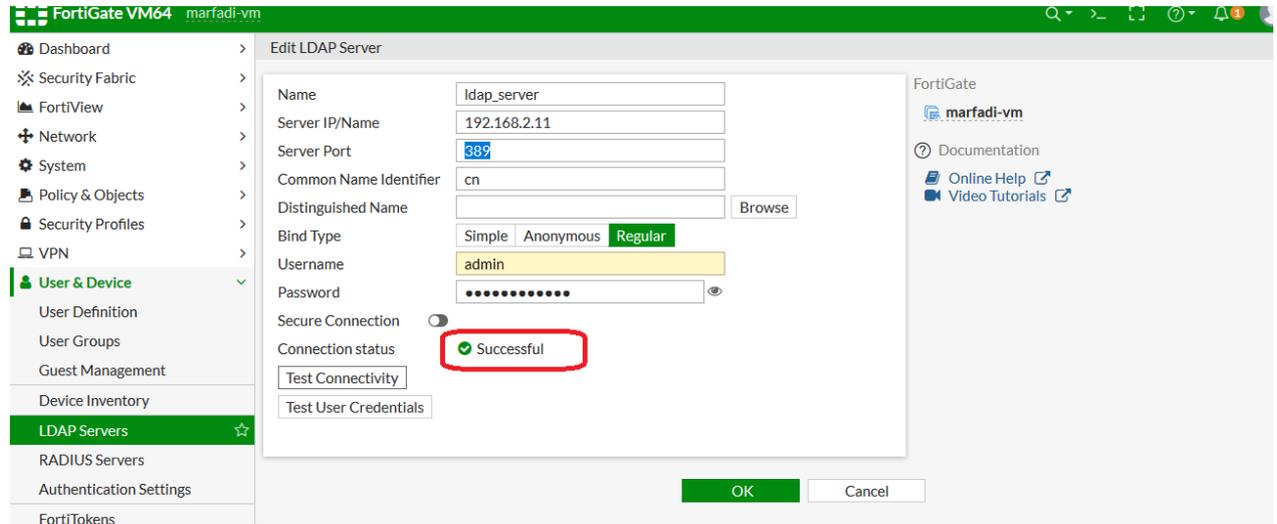
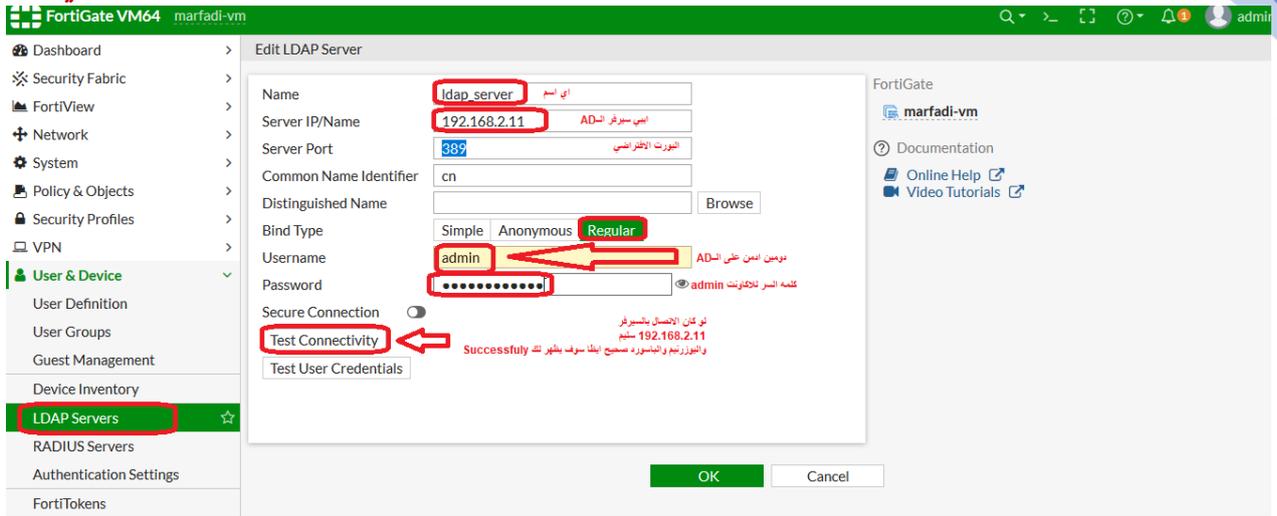


نتأكد من جهاز الكلاينت (Win 8.1) معمول له Joined للدومين وان السيرفر AD

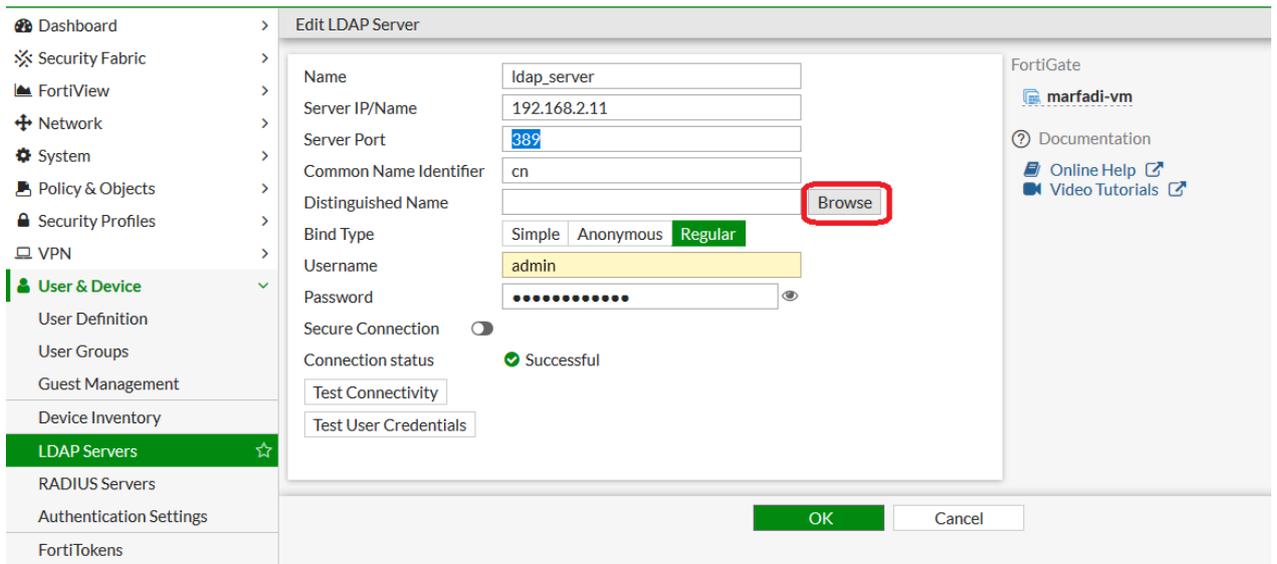
بيقدروا يوصلوا لبعض (موصلين على سويتش واحد Vnet1) وبيقدروا يعملوا ping بينهم البعض ..

الان سنقوم بأضافه الـ ldap server الذي هو AD (192.168.2.11) الى الفورتى جيت

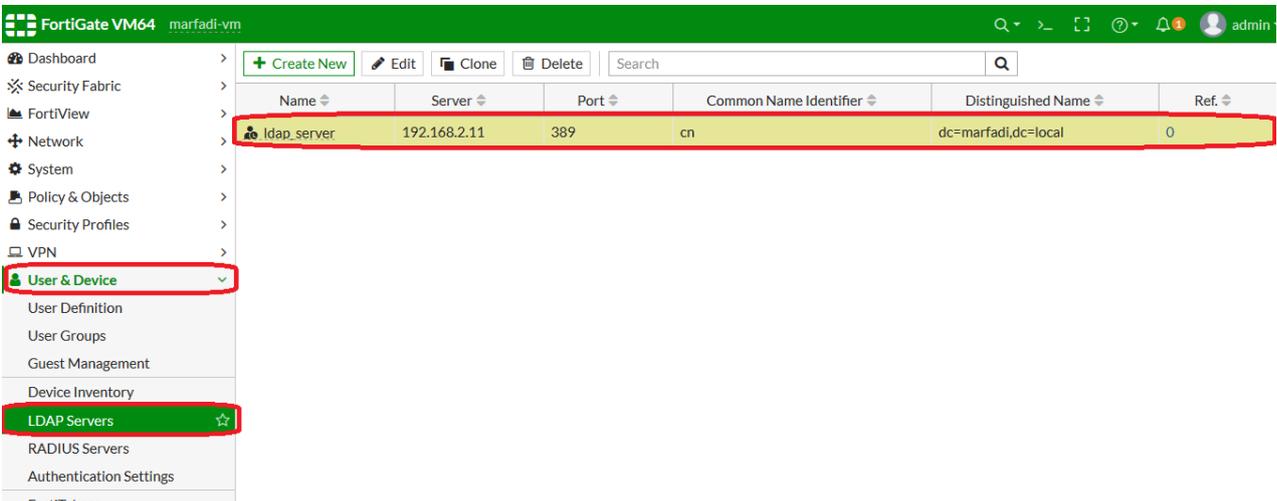
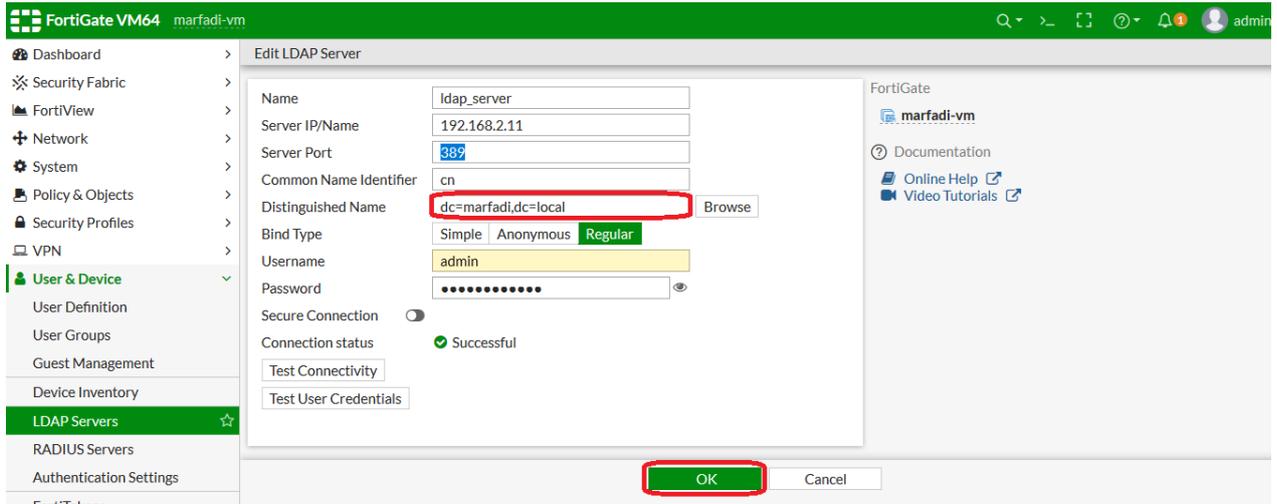
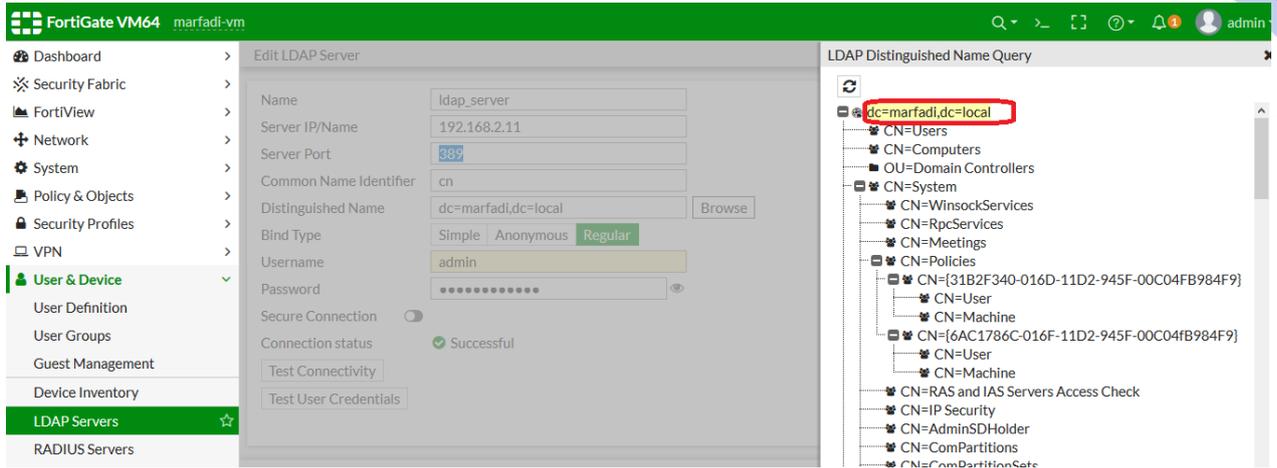




كما بالصورة أعلاه تبين بأن الاتصال بسيرفر الـ ldap سليم ..

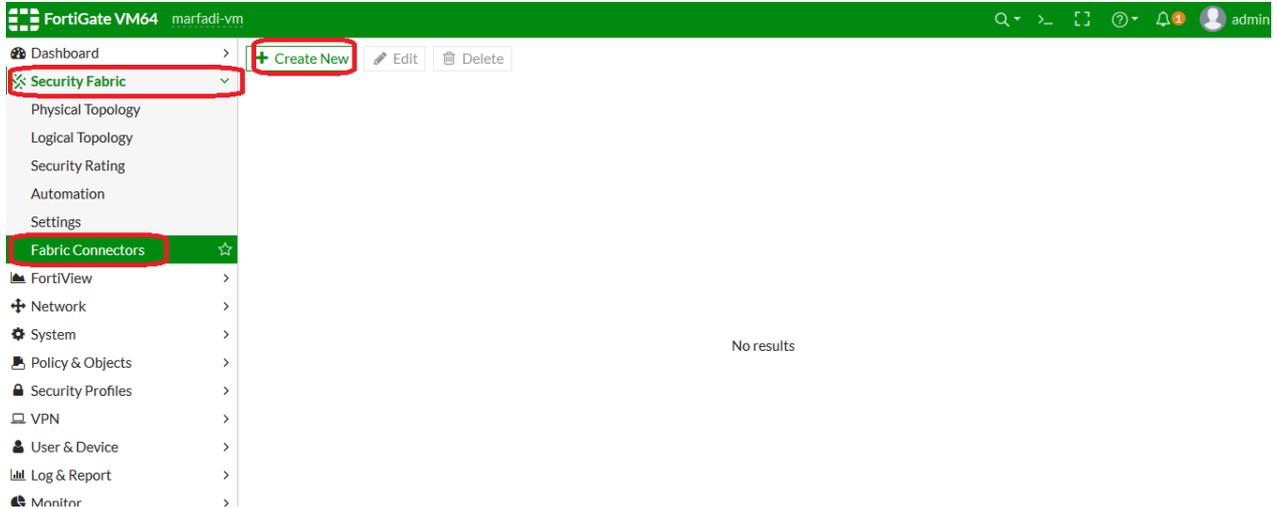


بعد النقر على الزر browse نقوم باختيار الدومين كما بالصورة ادناه

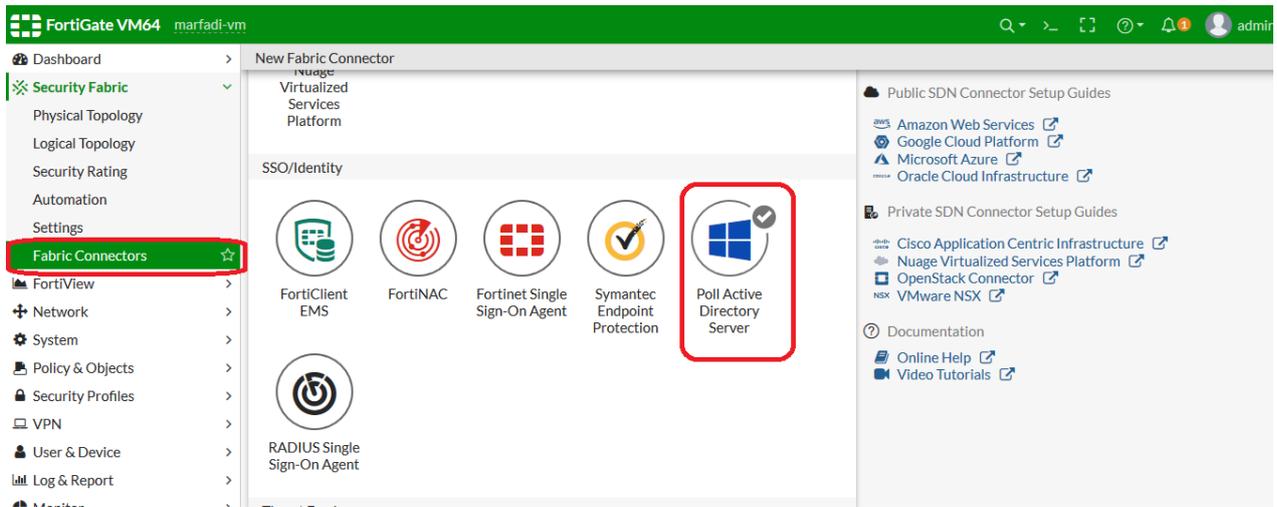


كما بالصورة أعلاه تم أضافه ال ldap server بنجاح ...

نقوم بضبط الاعدادات لتفعيل خاصية FSSO



هناك طريقتين لعمل ذلك وهما



الطريقة الأولى Poll Active Directory server

وهي الطريقة التي سنعمل عليها الآن

والطريقة الأخرى هي Fortinet Single Sign-on Agent

وسوف يتم شرحها لاحقاً ..

أساسيات فورتي جيت

قمنا باختيار الوحده التنظيميه (OU) المسماة IT والتي تحتوي على اليوزرات User1، User2، User3 من قائمه اليوزرات التي موجوده في الـ AD لكي أتمكن من رؤيتها على الفورتي جيت حيث بعد التحديد ننقر بالزر الأيمن ثم Add Selected ..

تم أضافه الـ OU من الـ AD الى الفورتي جيت لكي أتمكن من ان اتحكم فيها لاحقا عبر الفورتي جيت

SSO/Identity

Poll Active Directory Server

Connector Settings

Server IP/Name: 192.168.2.11

User: admin@marfadi.local

Password:

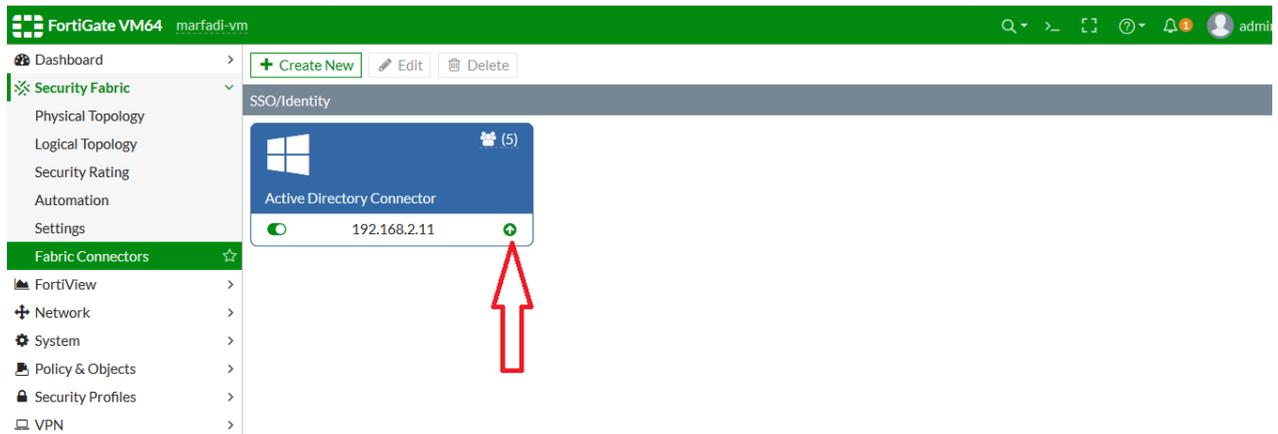
LDAP server: ldap_server

Enable polling:

Users/Groups: 5 Edit

OK Cancel

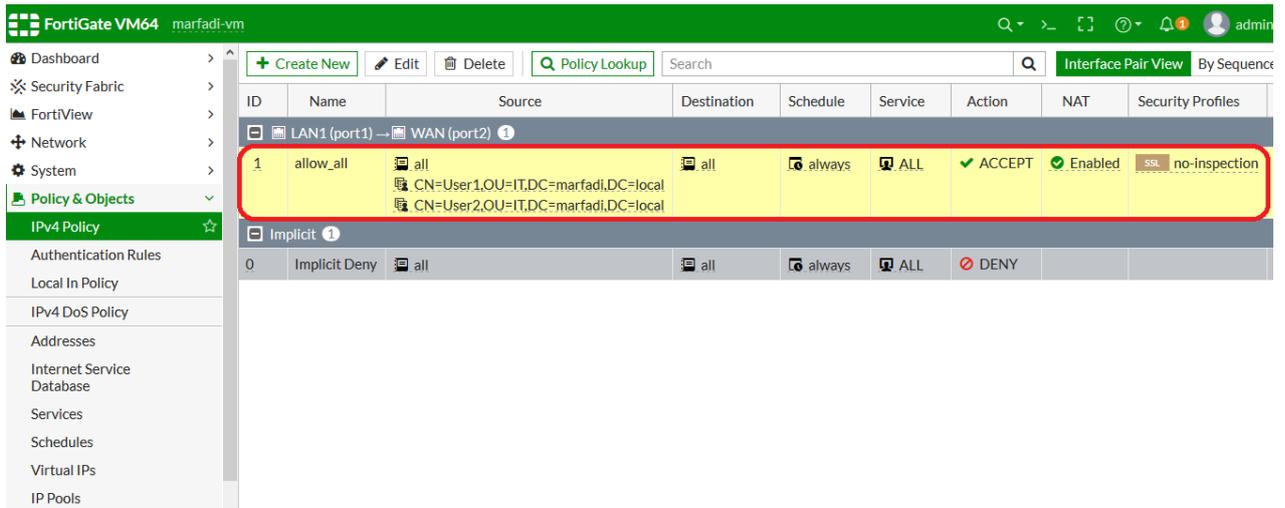
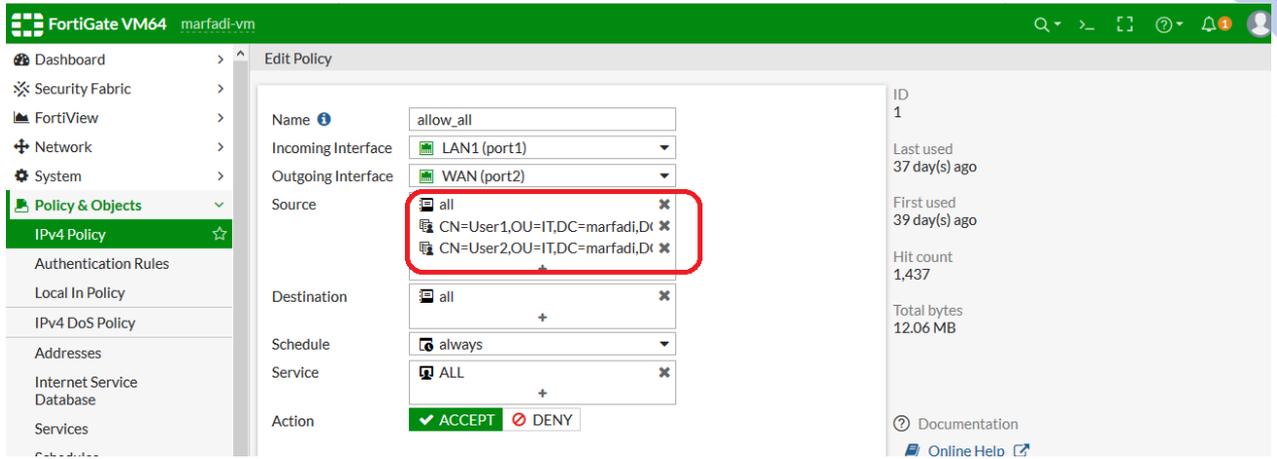
تمت بنجاح كما بالصور ادناه توجد علامه صح خضراء



لو كانت العملية لم تتم بنجاح فيكون السهم باللون الأحمر ليديل على فشل العملية ..

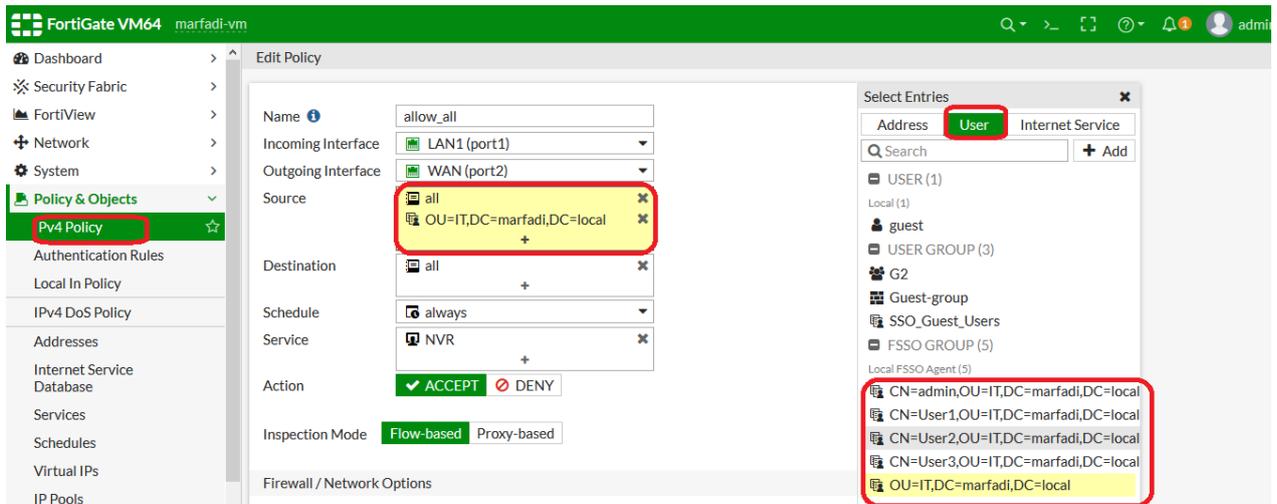
الآن سنقوم بإنشاء يوليبي ونختار منها اليوزرات مثلا User1 و User2 فقط ..

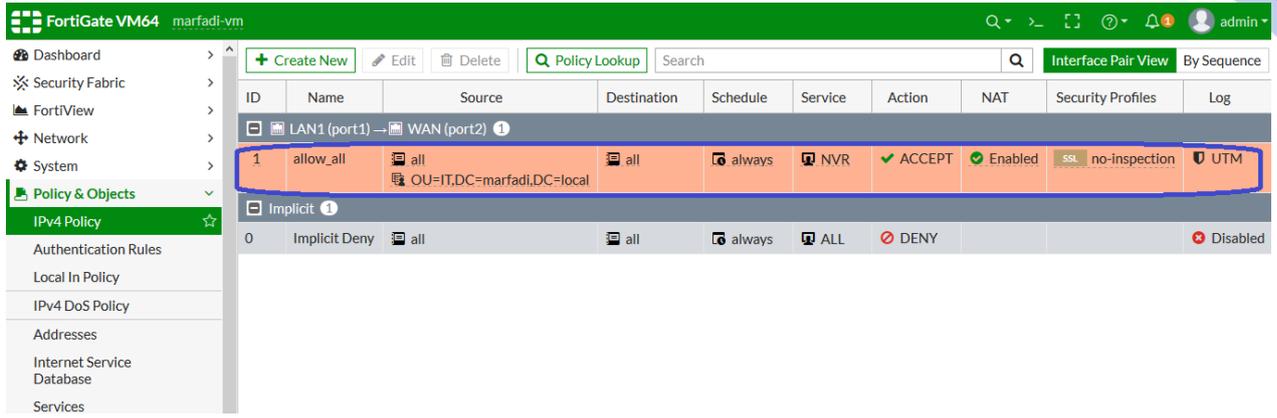
حيث هما فقط لهما الحق بالوصول الى الانترنت ..



ملاحظة:

لوقمنا باختيار الOU كامله كما بالصورة ادناه فأن اليوزرات التي بداخل تلك الOU لن تستطيع الوصول الى الانترنت وكأن الفورتى جيت لا يتعرف على الOU ..





البولييسي أعلاه لن تجعل اليوزرات التي بداخل الOU المسماة IT يحصلوا على الانترنت ..

الخطوة الثالثة :

لذا من الأفضل انشاء جروبات من نوع FSSO لكي تتمكن من استخدامها في البولييسي كما بالخطوات ادناه



حيث انشاءنا جروب باسم FSSO-IT-G وهي من نوع FSSO وستحتوي على كل اليوزرات التي بداخل الOU الموجودة على الAD والمسماة IT .

Group Name	Group Type	Members	Ref.
FSSO-IT-G	Fortinet Single Sign-On (FSSO)	OU=IT,DC=marfadi,DC=local	0
G2	Guest		0
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

الآن سنقوم بالتعديل على البوليسي السابقة لنقوم باختيار الجروب المسماة FSSO-IT-G كما بالصورة ادناه

Edit Policy

Name: allow_all

Incoming Interface: LAN1 (port1)

Outgoing Interface: WAN (port2)

Source: all, FSSO-IT-G

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

Inspection Mode: Flow-based

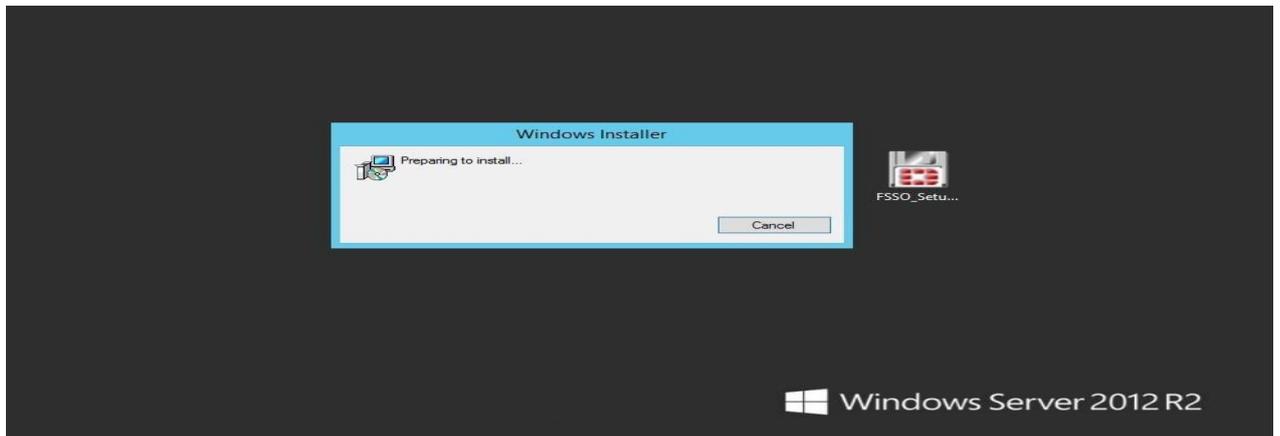
Firewall / Network Options: NAT (ON)

Select Entries dialog: User, FSSO-IT-G

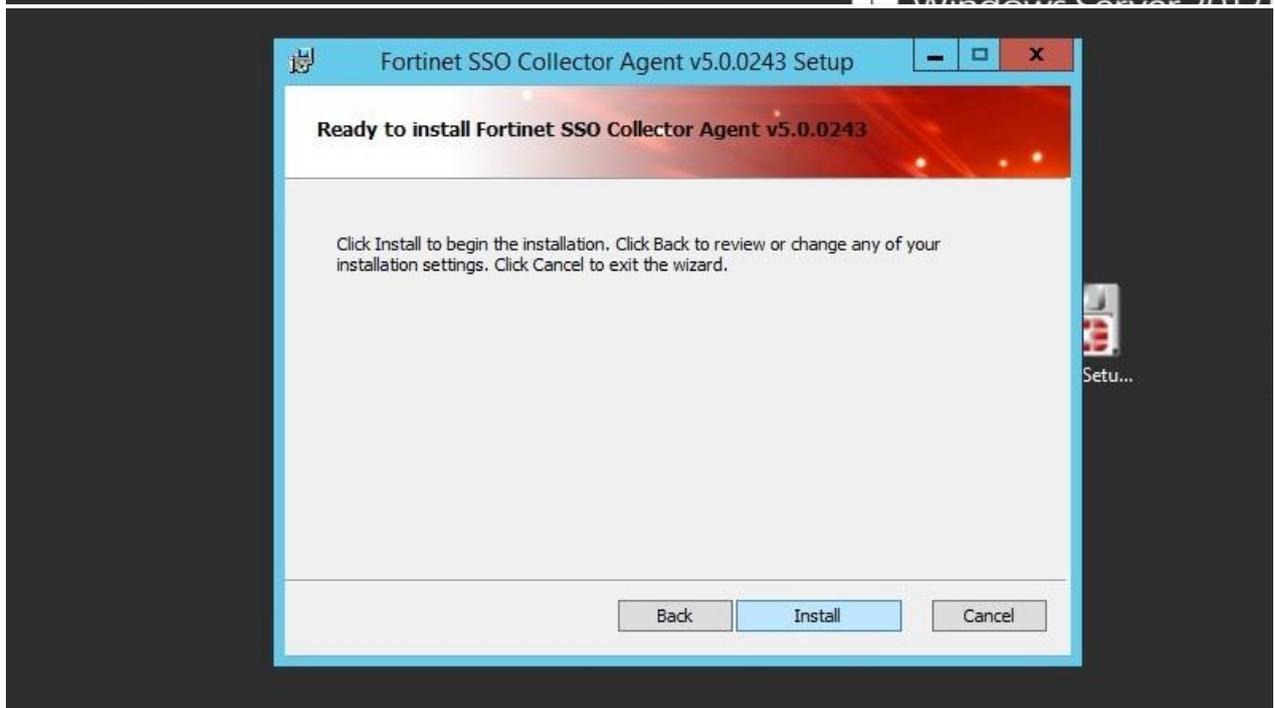
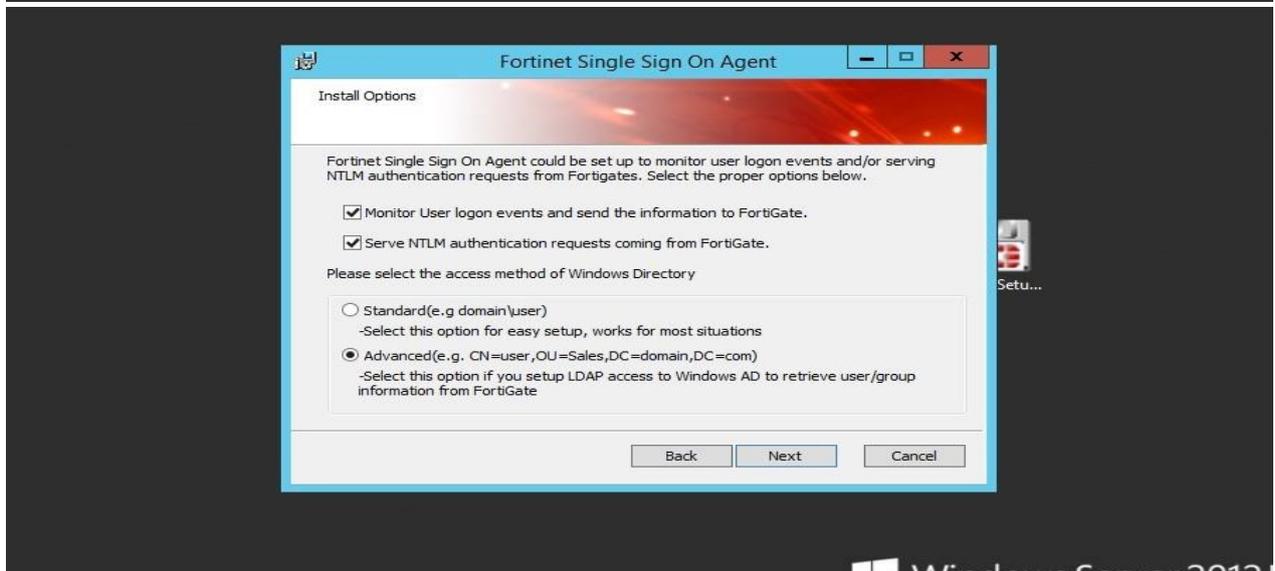
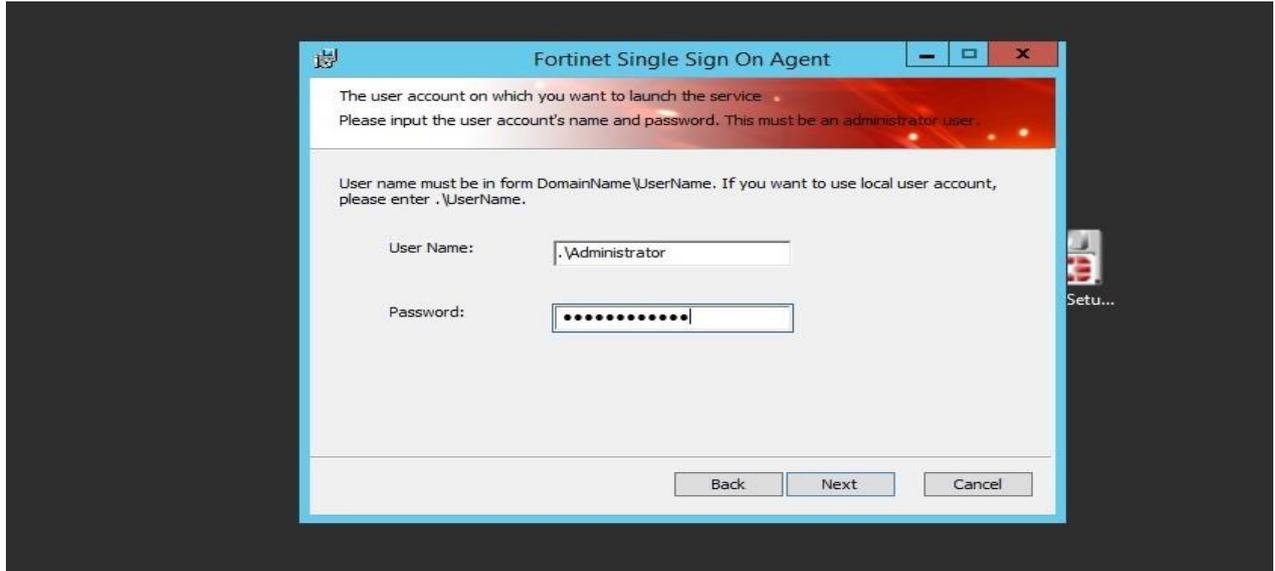
❖ الطريقة الثانية لعمل ال integration بين الفورتني جيت والـ AD تسمى

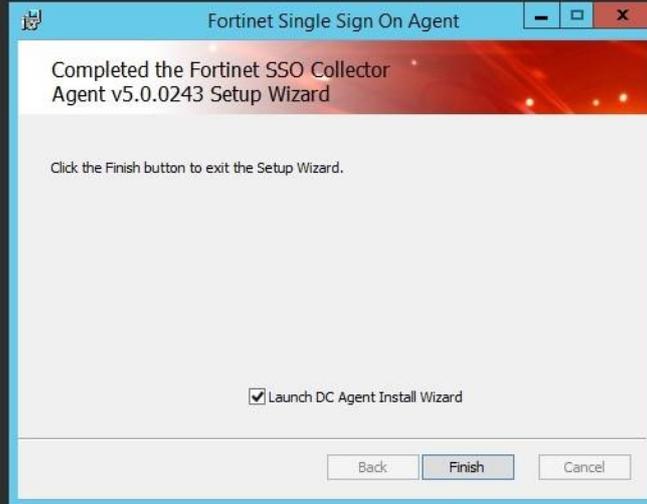
Fortinet Single Sign-on Agent

يتم تنزيل برنامج اسمه FSSO على سيرفر الدومين (AD)

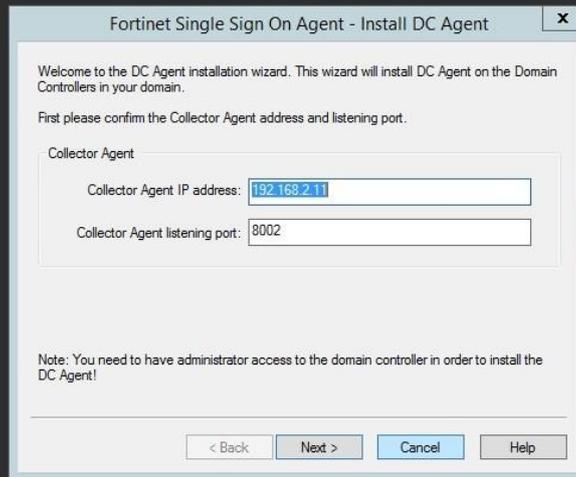


قم بكتابه كلمه السر التابعه للدومين ادمن للـAD

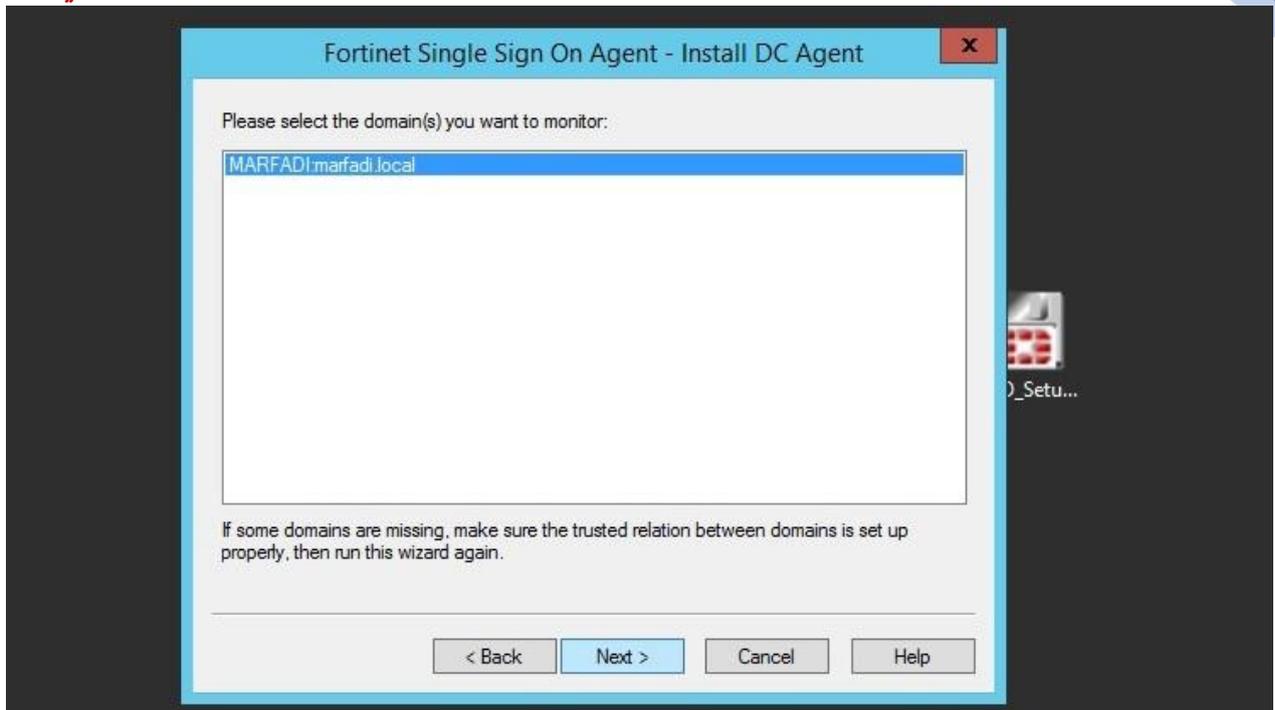




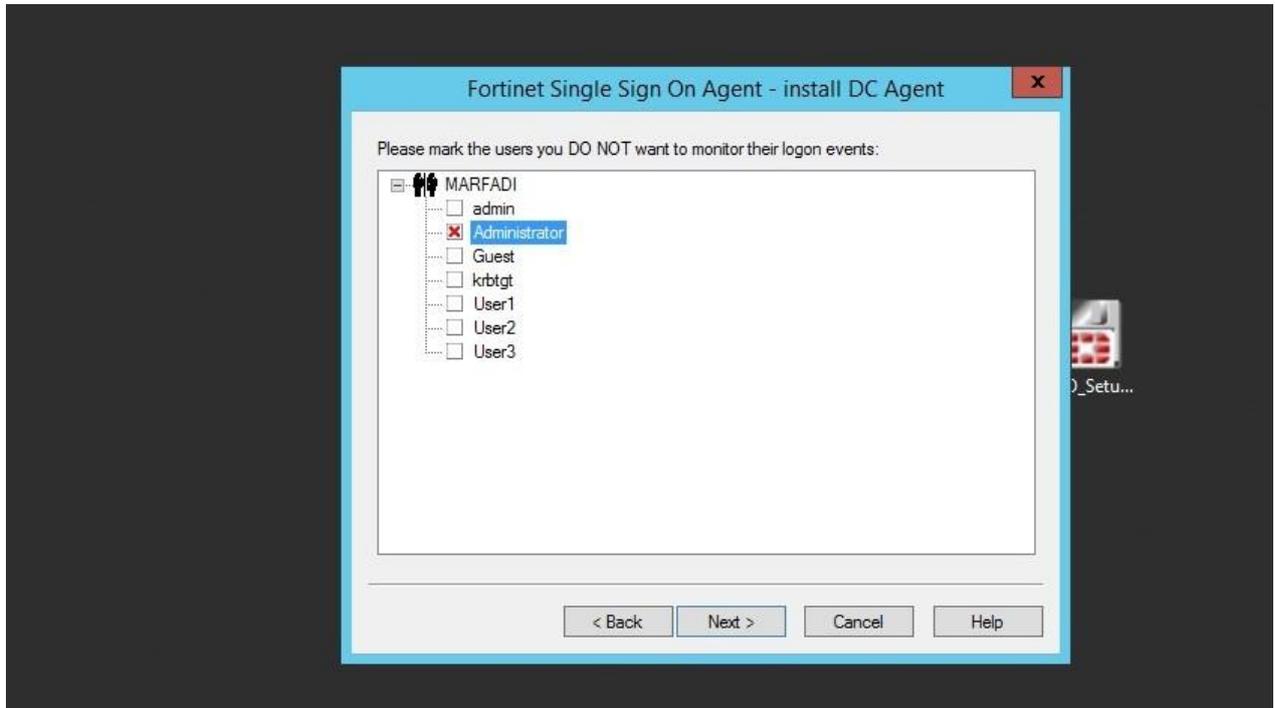
Windows Server 2012 R2

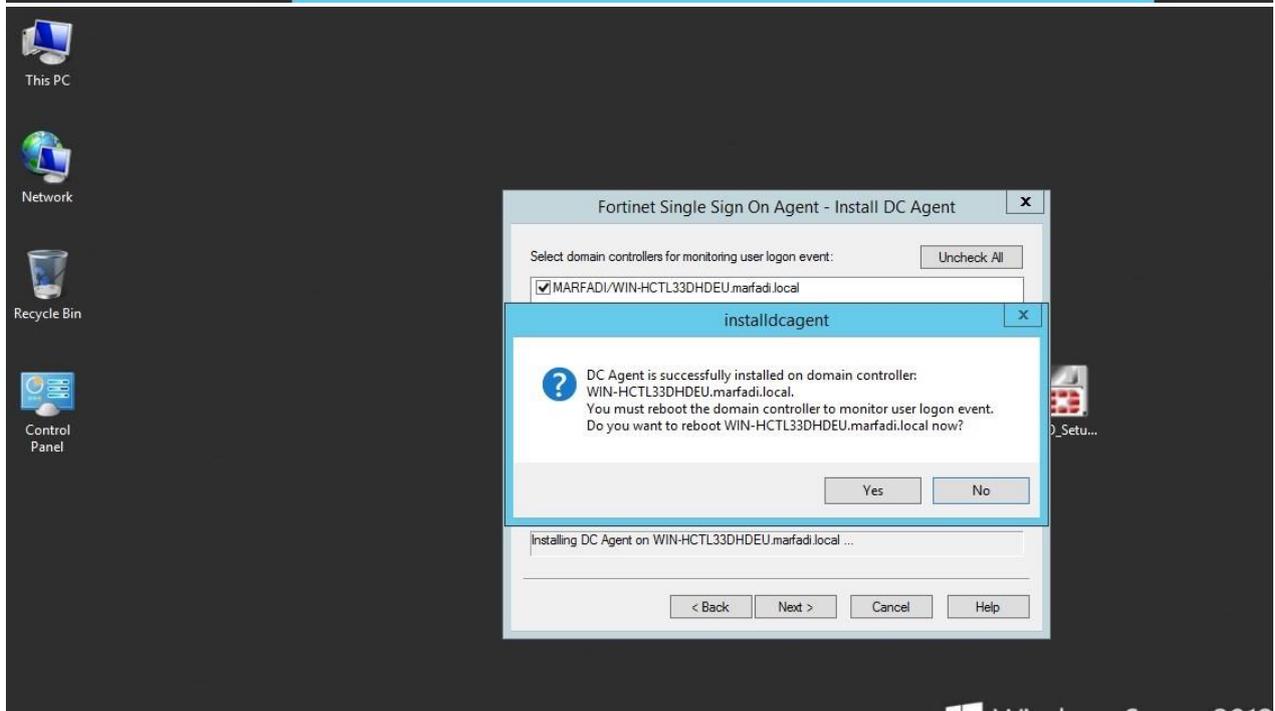
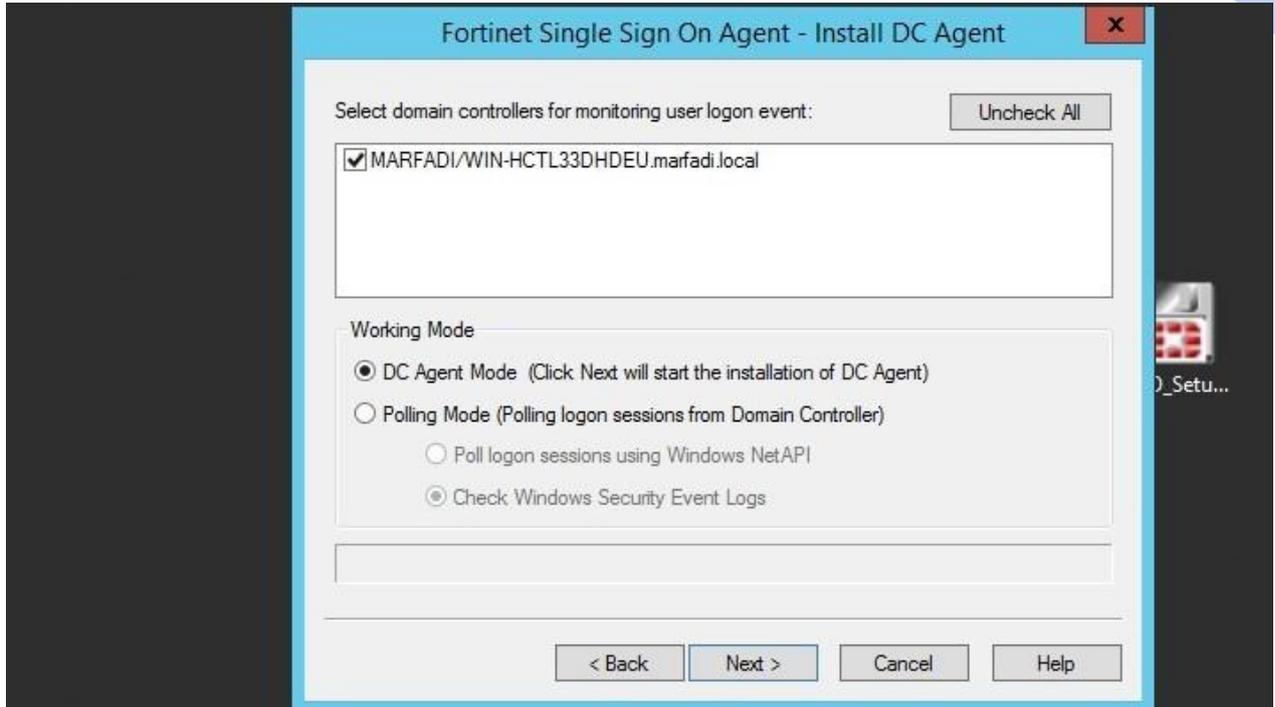


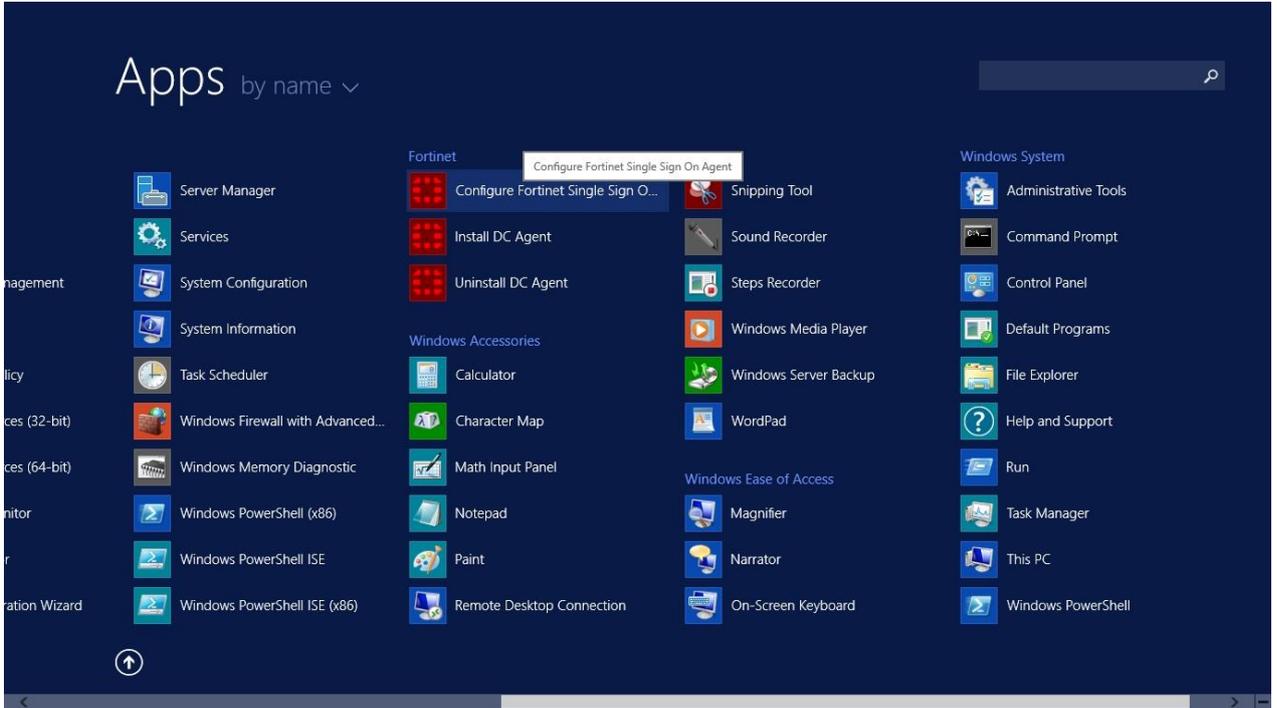
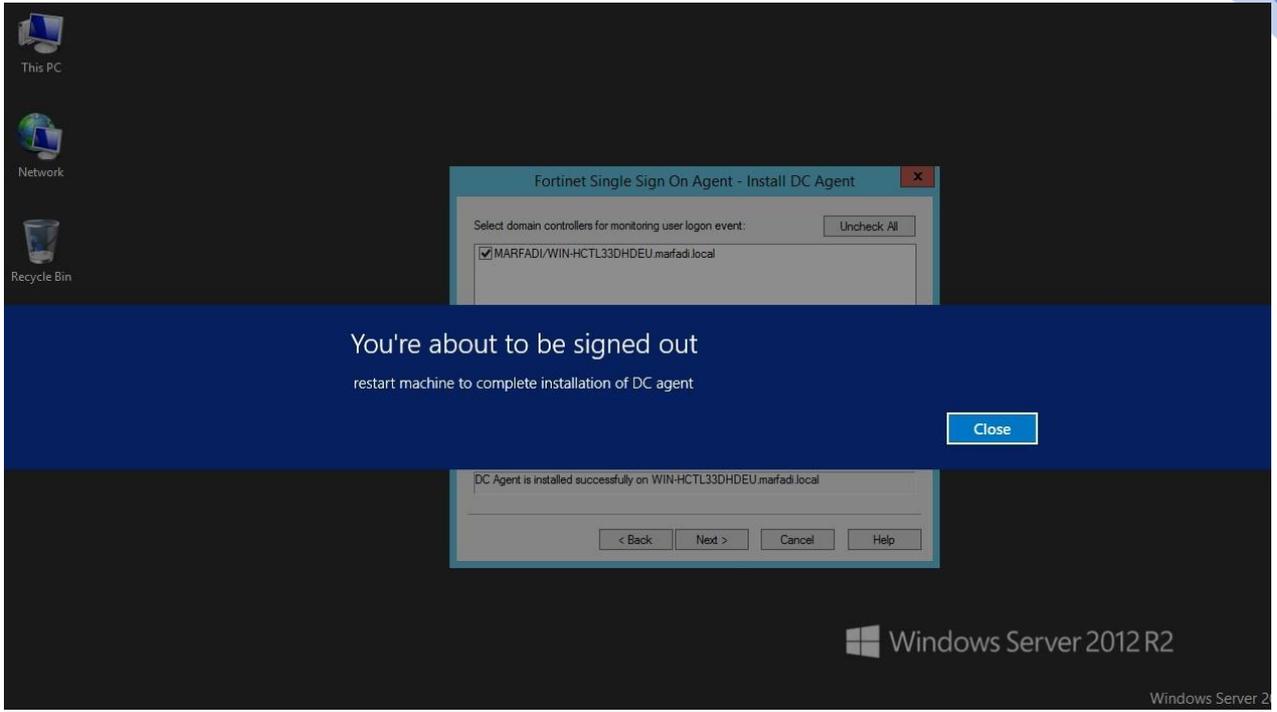
Windows Server 2012 R2

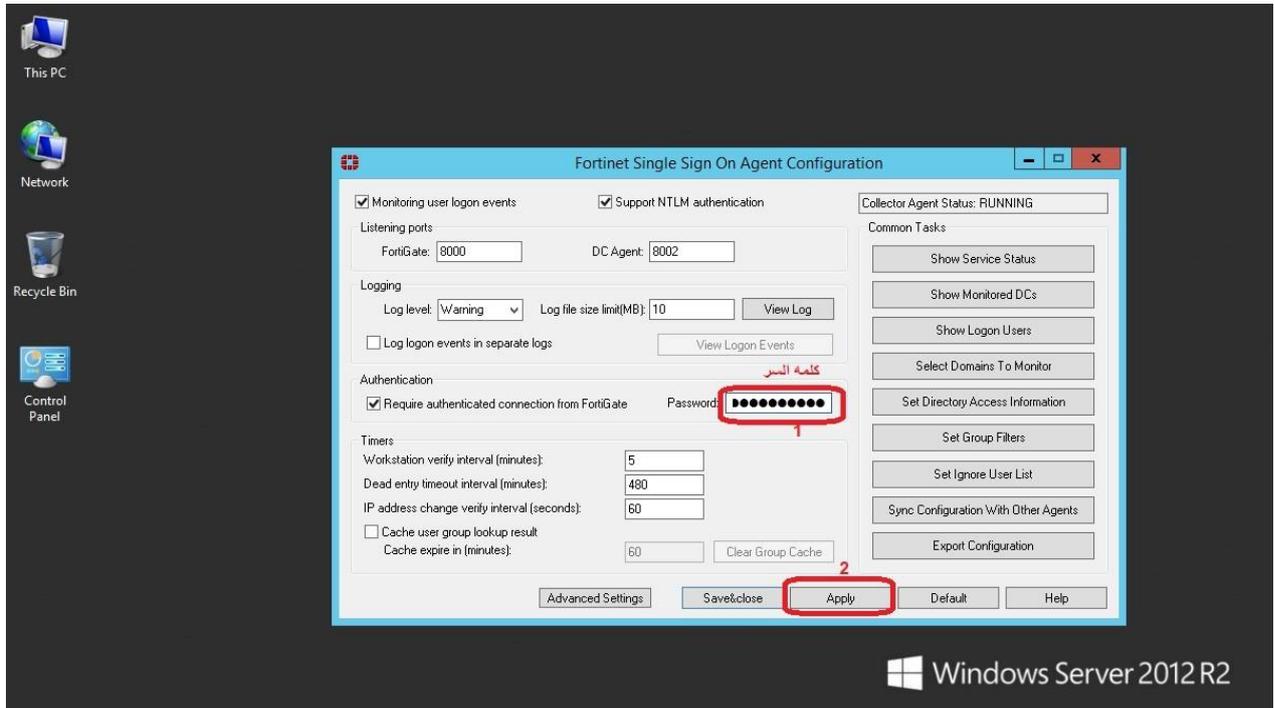
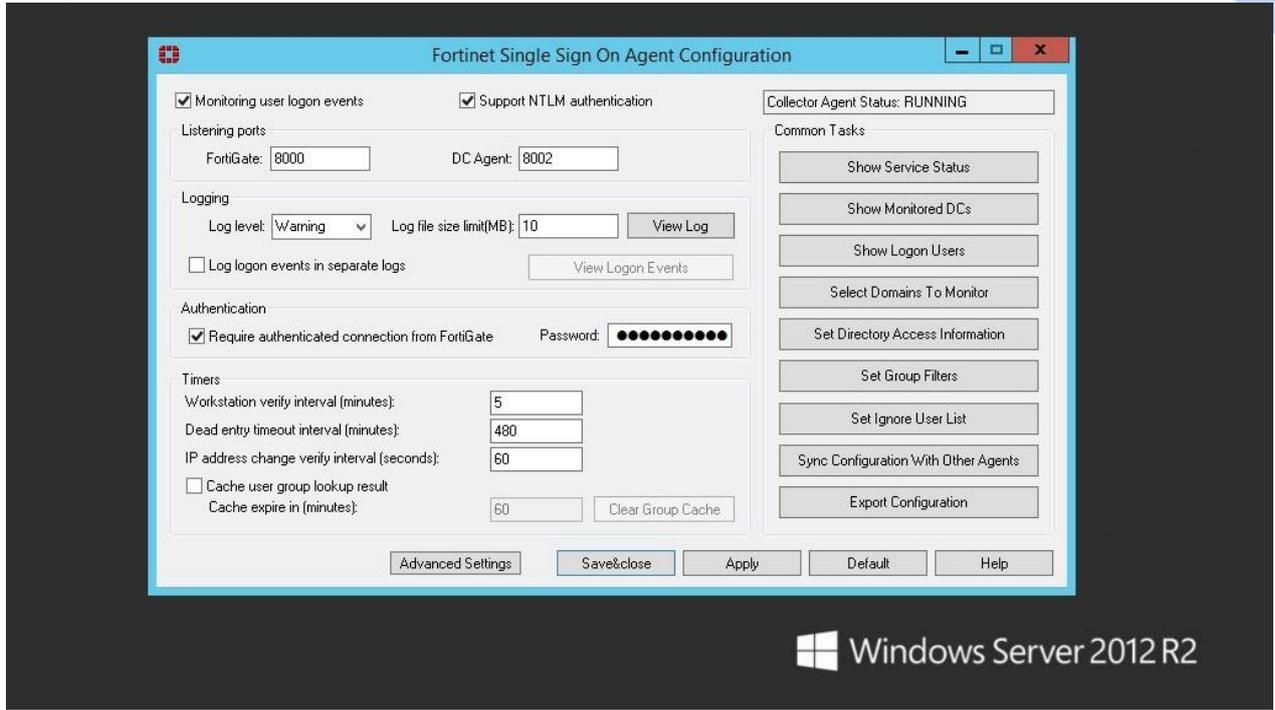


نقوم بتحديد اليوزرات المراد استثنائها من عمليه ال monitoring عبر برنامج FSSO Agent حيث تم استثناء اليوزر Administrator

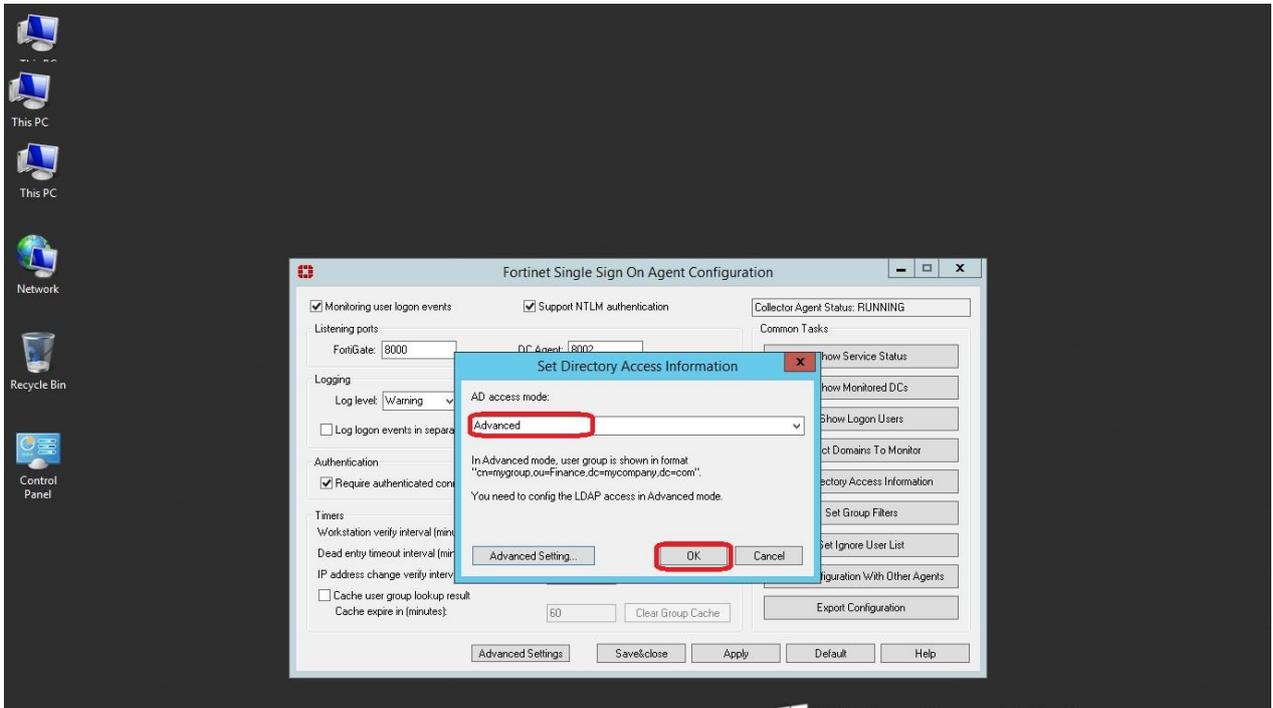
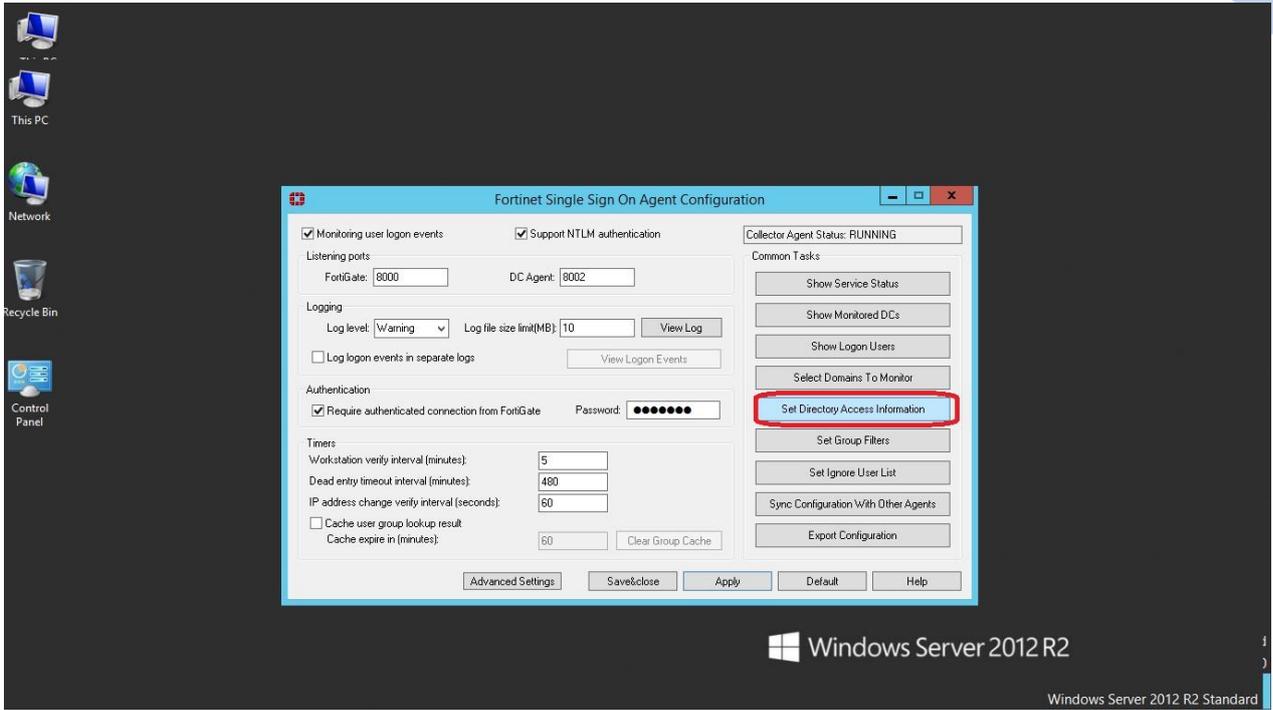








كما بالصورة أعلاه قم بكتابه باسورد (ليش شرط ان يكون نفس باسورد الدومين ادمن) حيث ستحتاج لها لعملية الاتصال بين الفورتني جيت وبرنامج FSSO ويفضل ان يكون معقد



سنقوم بإنشاء LDAP SERVER كما بالصورة ادناه

The screenshot shows the FortiGate VM64 management console for 'marfadi-vm'. The left sidebar contains a navigation menu with 'LDAP Servers' highlighted. The main content area displays a table with columns for Name, Server, Port, and Common Name Identifier. The table is currently empty, showing 'No results'.

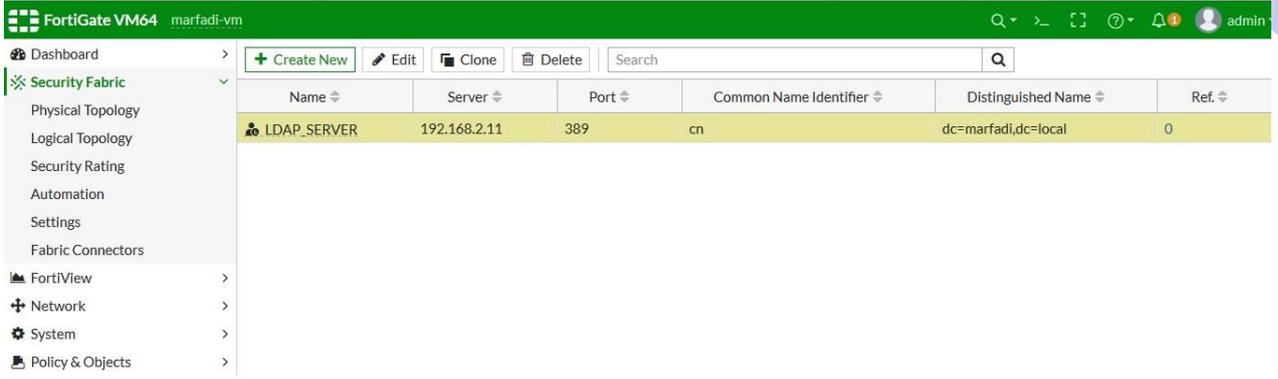
The screenshot shows the 'Edit LDAP Server' configuration dialog in the FortiGate VM64 management console. The dialog contains the following fields and options:

- Name: LDAP_SERVER
- Server IP/Name: 192.168.2.11
- Server Port: 389
- Common Name Identifier: cn
- Distinguished Name: (empty field with a 'Browse' button)
- Bind Type: Simple, Anonymous, Regular (Regular is selected)
- Username: admin@marfadi.local
- Password: (masked with dots)
- Secure Connection: (disabled)
- Connection status: Successful (with a green checkmark)
- Buttons: Test Connectivity (highlighted with a red box), Test User Credentials

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

The screenshot shows the FortiGate configuration page for an LDAP server. The configuration fields are: Name: LDAP_SERVER, Server IP/Name: 192.168.2.11, Server Port: 389, Common Name Identifier: cn, Distinguished Name: dc=marfadi,dc=local, Bind Type: Regular, Username: admin@marfadi.local, Password: [masked]. A green checkmark and the word "Successful" indicate the connection test passed. A "Browse" button next to the Distinguished Name field is circled in red and labeled with a red "1". To the right, the LDAP Distinguished Name Query tree is visible, with "DC=marfadi,DC=local" selected and circled in red and labeled with a red "2".

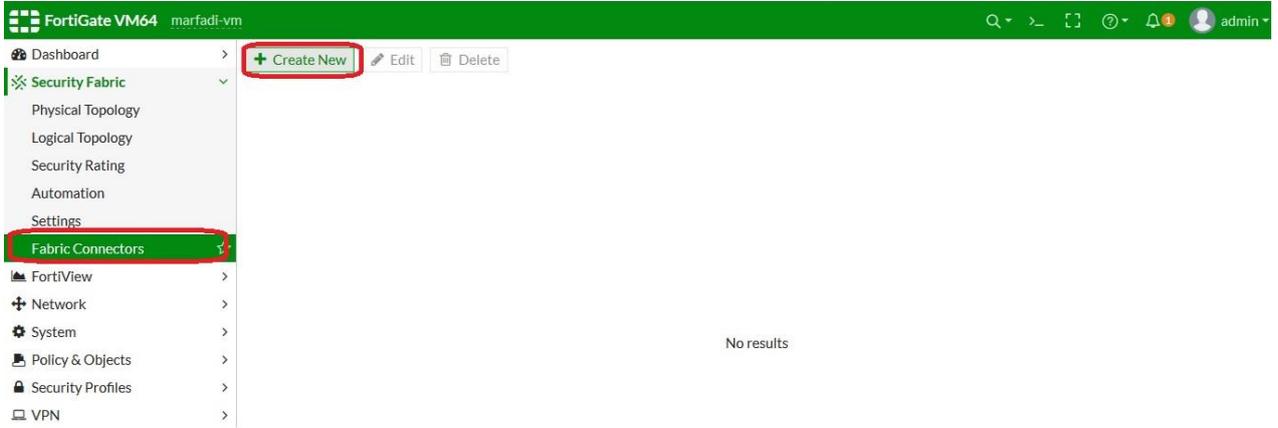
This screenshot shows the configuration details for the LDAP server. The fields are: Name: LDAP_SERVER, Server IP/Name: 192.168.2.11, Server Port: 389, Common Name Identifier: cn, Distinguished Name: dc=marfadi,dc=local, Bind Type: Regular, Username: admin@marfadi.local, Password: [masked]. The "Secure Connection" toggle is off, and the "Connection status" is "Successful". There are two buttons: "Test Connectivity" and "Test User Credentials", both circled in red. The "Test User Credentials" button is also labeled with a red "1". At the bottom right, there is a green "OK" button circled in red.

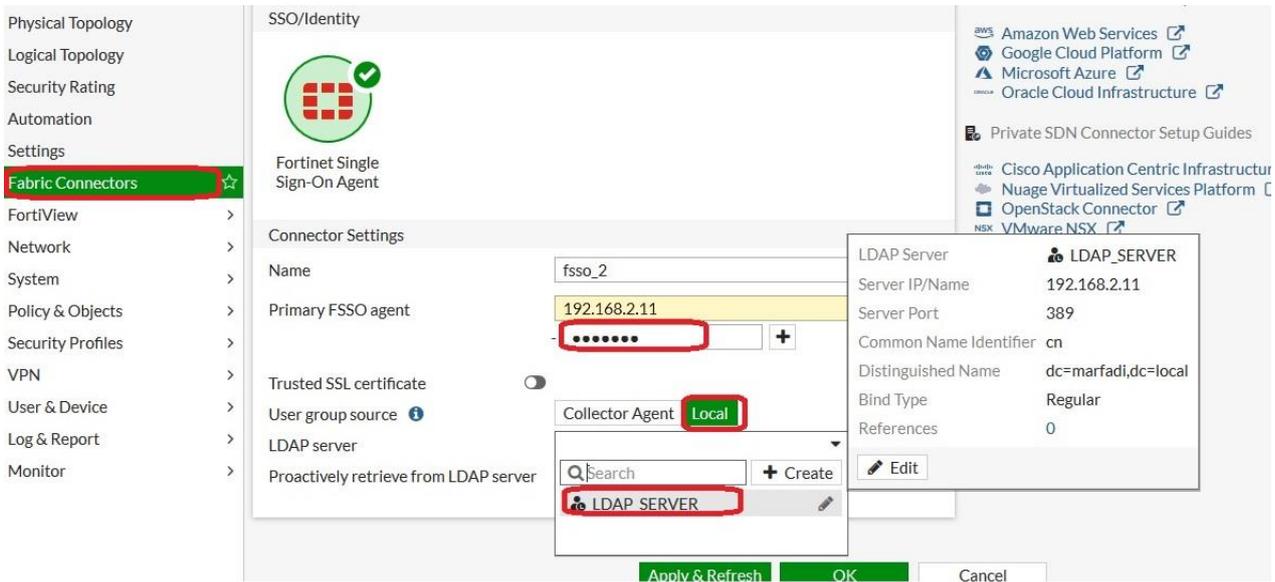
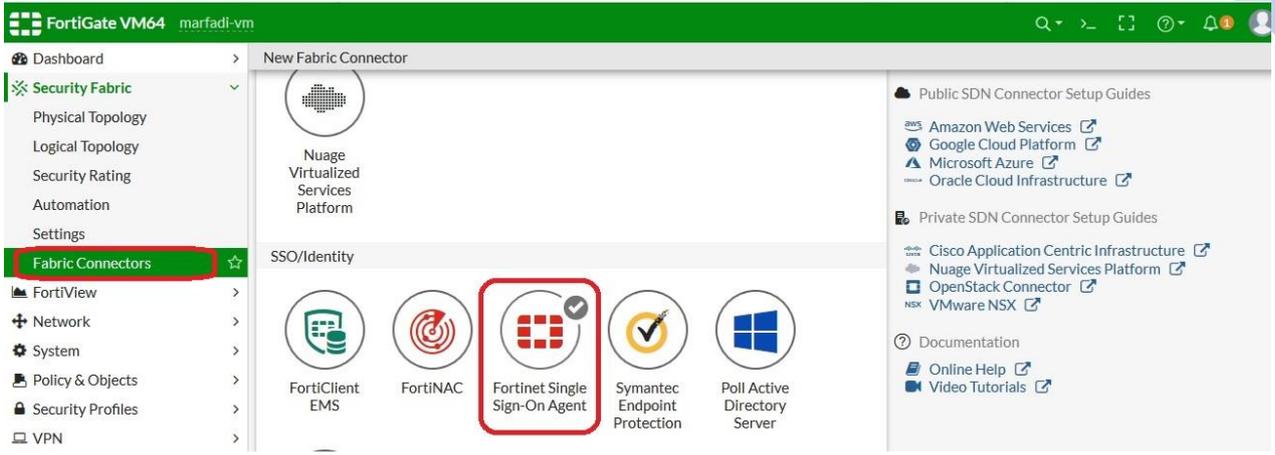


The screenshot shows the FortiGate VM64 interface for 'marfadi-vm'. The left sidebar is expanded to 'Security Fabric' > 'Fabric Connectors'. The main area displays a table with one entry:

Name	Server	Port	Common Name Identifier	Distinguished Name	Ref.
LDAP_SERVER	192.168.2.11	389	cn	dc=marfadi,dc=local	0

تم انشاء LDAP SERVER بنجاح باسم LDAP_SERVER والذي سنستخدمه لاحقا ..





هنا الباسورد هي نفسها التي قمنا بإنشائها في برنامج FSSO على سيرفر الدومين (AD) وهناك طريقتين للحصول على اليوزرات والجروبات التي موجودة على سيرفر الAD اما نقوم باختيار الخيار Local كما بالصورة أعلاه ومن ثم نختار الLDAP SERVER الذي قمنا بإنشاءه سابقا ..

أساسيات فورتني جيت

تم اختيار الجروب المسماه IT-FROUp

ID	Name
IIS_IUSRS	IIS_IUSRS
Incoming Forest Trust Builders	Incoming Forest Trust Builders
IT-GROUP	IT-GROUP
Network Configuration Operators	Network Configuration Operators
Performance Log Users	Performance Log Users
Performance Monitor Users	Performance Monitor Users
Pre-Windows 2000 Compatible Access	Pre-Windows 2000 Compatible Access
Print Operators	Print Operators
Protected Users	Protected Users
RAS and IAS Servers	RAS and IAS Servers
RDS Endpoint Servers	RDS Endpoint Servers
RDS Management Servers	RDS Management Servers

كما بالصورة أعلاه سنقوم بتحديد الجروبات واليوزرات الموجودة في الAD والتي تريد إضافتها (intergrated) مع الفورتني جيت

تم تحديد اليوزرات ادناه

ID	Name
admin	admin
Administrator	Administrator
amar	amar
Guest	Guest
hani	hani
krbtgt	krbtgt
User1	User1
User2	User2
User3	User3
user4	user4

بعد تحديد اليوزرات المطلوب إضافتها الى الفورتني جيت

كل ماتم اختياره الى الFSSO

ID	Name
IT-GROUP	IT-GROUP
hr-g	hr-g
User1	User1
User2	User2
User3	User3
user4	user4

كما بالصورة أعلاه تبين بأن عدد العناصر التي تم إضافتها هي 6

أساسيات فورتى جيت

تلاحظ العدد هنا 4 عناصر تم إضافتها ومن ثم نختار OK

لو كان السهم باللون الأحمر فذلك يعني بأن الاتصال بين الفورتى جيت والـ AD غير سليم نتأكد بأن لفايروول على سيرفر الـ AD مقفول ..

الآن سنقوم بإنشاء جروب من نوع FSSO ونقوم بإضافه اليوزرات او الجروبات التي قمنا باختيارها سابقا (selected) في الخطوات السابقة حيث هذه الجروب سيتم تطبيق بوليسي معينه عليها لاحقا ..

The screenshot shows the FortiGate VM64 management console. The left sidebar contains a navigation menu with 'User & Device' expanded. Under 'User & Device', 'User Groups' is highlighted with a red box. The main content area shows a table of existing user groups:

Group Name	Group Type	Members	Ref.
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

The screenshot shows the 'New User Group' configuration page. The 'Name' field is set to 'FSSO-GROUP-IT', the 'Type' is 'Fortinet Single Sign-On (FSSO)', and the 'Members' field has a '+' button. The 'Select Entries' panel on the right shows a list of entries, with 'CN=IT-GROUP,OU=IT,DC=marfadi,DC=local' selected. The 'OK' button is highlighted with a red arrow.

اختيار الجروب المسماة IT-GROUP والموجودة على AD

FortiGate VM64 marfadi-vm

Group Name	Group Type	Members	Ref.
FSSO-GROUP-IT	Fortinet Single Sign-On (FSSO)	CN=IT-GROUP,OU=IT,DC=marfadi,DC=local	0
Guest-group	Firewall	guest	0
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1

FortiGate VM64 marfadi-vm

Edit Policy

Name: private

Incoming Interface: LAN1 (port1)

Outgoing Interface: WAN (port2)

Source: all, FSSO-GROUP-IT

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT, DENY

Inspection Mode: Flow-based, Proxy-based

Firewall / Network Options: NAT

Select Entries

Address: User

Internet Service

USER (1)

Local (1)

guest

USER GROUP (3)

FSSO-GROUP-IT

Guest-group

SSO_Guest_Users

FSSO GROUP (5)

ssso20 (1)

CN=IT-G,OU=IT,DC=marfadi,DC=loca

ssso_2 (4)

CN=IT-GROUP,OU=IT,DC=marfadi,DC

CN=User1,OU=IT,DC=marfadi,DC=lo

CN=User2,OU=IT,DC=marfadi,DC=lo

CN=User3,OU=IT,DC=marfadi,DC=lo

تم تطبيق البوليسي على الجروب من نوع FSSO واسمها FSSO-GROUP-IT والتي قمنا بإنشائها سابقا ...

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

VPN

User & Device

Log & Report

Monitor

Routing Monitor

DHCP Monitor

SD-WAN Monitor

FortiGuard Quota

IPsec Monitor

SSL-VPN Monitor

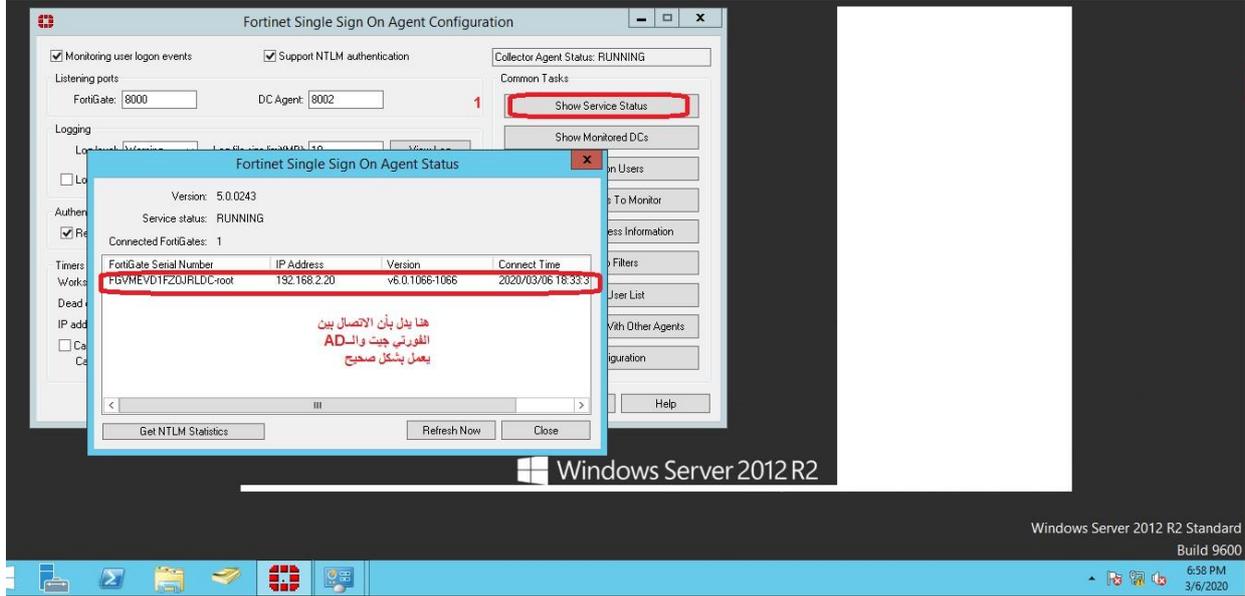
Firewall User Monitor

Quarantine Monitor

Refresh Deauthenticate Show all FSSO Logons Search

User Name	User Group	Duration	IP Address	Traffic Volume	Method
ADMIN		12 minute(s) and 15 second(s)	192.168.2.11	0 B	Fortinet Single Sign-On

كما بالصورة ادناه يتبين بأن الاتصال بين الفورتى جيت والـ AD سليم ..



كما قلنا سابقا لو تريد مراقبه اليوزرات التي ضمن FSSO من حيث المده التي يعمل عليها والايبي وحجم الترافيك كما بالصورة ادناه ...

أساسيات فورتني جيت

Dashboard Refresh Deauthenticate **Show all FSSO Logons** Search

User Name	User Group	Duration	IP Address	Traffic Volume	Method
ADMIN		31 minute(s) and 29 second(s)	192.168.2.11	3.35 kB	Fortinet Single Sig
USER2	CN=User2,OU=IT,DC=marfadi,DC=local CN=IT-GROUP,OU=IT,DC=marfadi,DC=local	11 minute(s) and 24 second(s)	192.168.2.121	11.79 MB	Fortinet Single Sig

Dashboard Refresh Add Filter

Dashboard Refresh Add Filter

Source	Device	Bytes	Sessions	Bandwidth
USER3 192.168.2.121		4.08 kB	1	896 bps

Dashboard Refresh Add Filter

يظهر لك كل الجلسات المستخدمة وحجم الترافيك والمدته ..

FortiGate VM64 marfadi-vm admin

Source	Device	Destination	Application	Protocol	Source Port	Destination Port	Bytes	Packets	Duration (s)
192.168.2.121		152.199.19.161	TCP/443	TCP	49362	443	50.55 kB	77	25s
192.168.2.121		93.184.220.29	TCP/80	TCP	49363	80	2.42 kB	8	24s
192.168.2.121		8.8.8.8	ICMP/8	ICMP	1	8	23.04 kB	384	3m 29s
192.168.2.121		152.199.19.161	TCP/443	TCP	49361	443	10.51 kB	22	25s

❖ هذه هي الطريقة الثانية (خيار آخر) لعمل integration عبر اختيار

الـ Collector Agent

The image shows two screenshots from the Fortinet management console. The top screenshot displays the configuration for a Fortinet Single Sign-On Agent. The 'Connector Settings' section includes: Name: sso3; Primary FSSO agent: 192.168.2.11; Trusted SSL certificate: (disabled); User group source: Collector Agent (Local); Users/Groups: 0. A red arrow points to the password field, with a note: 'هذا الباسورد الذي تم كتابته في FSSO Agent على سيرفر الـ AD'. The bottom screenshot shows the 'SSO/Identity' list with a new entry for 'Fortinet Single Sign-On' (sso3) highlighted. A red arrow points to the entry, with a note: 'تم اضافه كل شي بشكل اوتوماتيكي موجود على الـ AD من يوزرات وجروبات و OU و ووالخ'. Another red arrow points to the 'sso3' name, with a note: 'اسم FSSO'. A third red arrow points to the '(48)' notification, with a note: 'الاتصال بين الـ AD و الفورتني جيت سليم'.

كما بالصورة أعلاه تم أضافه كل الجروبات والـ OU الموجودة على الاكثف دايركتوري الى الفورتني جيت (عددها 48 عنصر)...

ماهي أنواع الـ antivirus DataBase ؟

١. **Normal antivirus signatures Database**: هذا النوع موجود في أي جهاز فورتى جيت أنت تشتريه بغض النظر عن نوعه حيث الداتا ييز الموجودة فيه بيتم اعدادها من قبل الفورتى جارد (FortiGuard) من قبل فريق البحث لشركة الفورتى نت حيث تحتوي الـ database لهذا النوع على أشهر أنواع الفيروسات حيث الجهاز عندما يقوم بالفحص يقوم بعمل مقارنة ما بين الملفات التي تصل اليه من خارج الشبكة وبين الـ signatures الموجودة في الداتا ييز فلو وجد بأن الملف له signature متشابه مع التي موجودة لديه في الـ DB فيقوم الجهاز باعتبار هذا الملف على انه فايروس وبيعمل له الـ action المناسب .

٢. **Extended**: هذا النوع متوفر في اغلب موديلات فورتى جيت (ليس جميعها) حيث بتحتوي على النوع الأول (Normal)+DB على الفيروسات الغير فعالة او غير نشطة حيث ممكن هذا الفيروسات ممكن تتنشط ويعاد نشاطها مره أخرى فهذا يكون الفورتى جيت لديه معلومة عن هذا النوع من الفيروسات ..

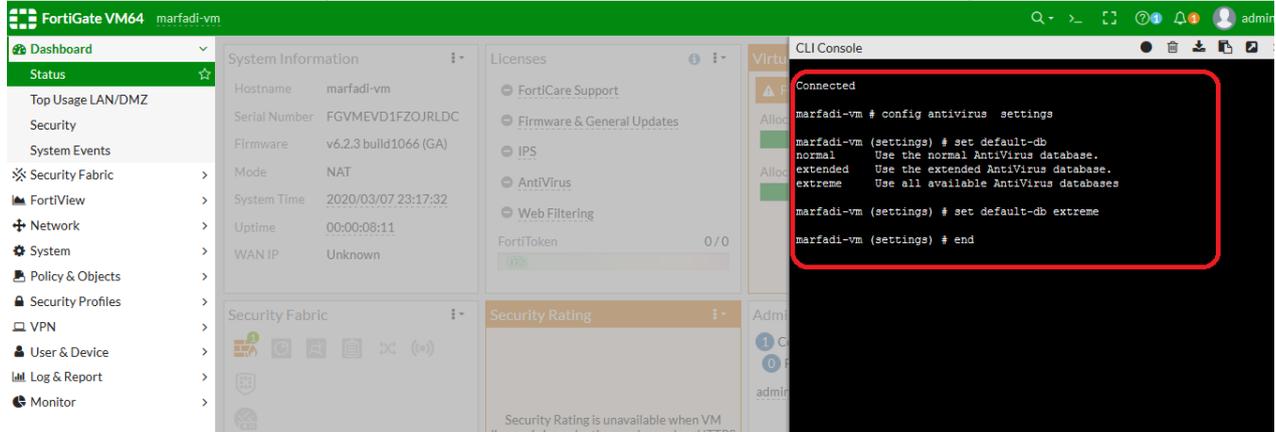
٣. **Extreme**: موجود هذا النوع من قواعد البيانات على بعض اجهزه الفورتى جيت حيث هي قاعده بيانات ضخمة وبتحتوي على DB النوعين السابقين +قاعده كبيره من الفيروسات حيث تكون مساحه هذا النوع كبيره جدا ولكنها توفر اكرامان وحمايه للشبكة .

حيث أي جهاز قبل ماتشتريه يمكنك معرفة ماذا يدعم من قاعده بيانات من الفيروسات من الأنواع السابقة ..

➤ ملاحظة: نسخه fortigate VM لا يوجد بها licence للـ Antivirus .

كيف تفرق بين قواعد بيانات الفيروسات على جهاز الفورتى جيت ؟

بيتم ذلك عبر ال cli ويجب ان يكون على جهاز حقيقي



كما بالصورة أعلاه تبين بأن الجهاز يدعم جميع الأنواع الثلاثة حيث

بعد كتابه الامر

#set default-db ?

ثم تكتب ؟ سيقوم بإظهار لك كل انواع القواعد الذي يدعمها الجهاز ويمكنك اختيار النوع المناسب لك

مثلا extreme

حيث ال extreme هو النوع الأفضل والاقوى ..

كيف بيتم عمليه التحديث للAntivirus DB ؟

(a) Manual: ستقوم بتحميل ملف من الملفات عبر (fortiGuard service update) وتعمل لهذا

الملف upload للجهاز ويقوم بتحديث الAntivirus DB

The screenshot shows the Fortinet support website. The URL in the browser is <https://support.fortinet.com/Main.aspx>. The page has a navigation bar with 'Home', 'Asset', 'Assistance', 'Download', and 'Feedback'. The 'Download' button is highlighted in red. A dropdown menu is open under 'Download', showing 'FortiGuard Service Updates' (highlighted in red), 'Firmware Images', 'Firmware Image Checksums', and 'HQIP Images'. Below this is a 'Customer Support Bulletin' section with three items and a 'More' button. The 'Asset' section is active, showing 'Download FortiGuard Service Updates'. A table lists the download links for 'Virus Definition' and 'Attack Definition' for 'FortiGate 80C'. The 'Virus Definition' link is '055.2.0_25.428.ETDB (MD5)' and the 'Attack Definition' link is '5.20_000_6.636 (MD5)'. Both links are highlighted in red and have green arrows pointing to them with the numbers '1' and '2' respectively. The footer contains links for 'Corporate', 'How to Buy', 'Products', and 'Services & Support'.

ثم نقوم بتحميل الـ 2 ملفات المشار اليهم بالون الأخضر ومن ثم نقوم بعمل لهم Upload من الفورتني جيت فايروول .

(b) **Automatic** : جعل الفورتني جيت يعمل على تنزيل التحديثات من FDN(fortiGuard) بمجرد وجود تحديثات جديدة. وبهذا يصبح الـ DB UP to Date .

أساسيات فورتى جيت

Dashboard > FortiGuard Distribution Network

Security Fabric >

FortiView >

Network >

System >

Administrators

Admin Profiles

Firmware

Settings

HA

SNMP

Replacement Messages

FortiGuard ☆

Feature Visibility

Certificates

Policy & Objects >

Security Profiles >

VPN >

User & Device >

Log & Report >

Monitor >

AntiVirus & IPS Updates

Accept push updates **On**

Use override push **Off**

Scheduled Updates **Off**

Improve IPS quality **Off**

Use extended IPS signature package **Off**

Update AV & IPS Definitions

Update Server Location

US only Lowest latency locations

Filtering

Web Filter Cache **On** Clear cache after 60 Minutes

Anti-Spam Cache **On** Clear cache after 30 Minutes

FortiGuard Filtering Protocol **HTTPS** **UDP**

FortiGuard Filtering Port 443 53 **8888**

Filtering Services Availability **Check Again**

Web Filtering **Down Arrow**

Anti-Spam **Down Arrow**

Request re-evaluation of a URL's category

حيث تقوم بتفعيل للخيار Accept push updates بحيث أي تحديث جديد موجود على FDN سيتم تنزيلها تلقائيا الى الفورتى جيت فايروول بدون تدخل منك .

او يمكنك عبر خيار اخر بأنك تعمل schedule updates وتحدد الأيام الذي يقوم فيها الفورتى جيت بتنزيل التحديثات من FDN .

أساسيات فورتى جيت

FortiGuard Distribution Network

AntiVirus & IPS Updates

Accept push updates

Use override push

Scheduled Updates Every 2 Hours

Improve IPS quality

Use extended IPS signature package

Update AV & IPS Definitions

Update Server Location

US only Lowest latency locations

Filtering

Web Filter Cache Clear cache after 60 Minutes

Anti-Spam Cache Clear cache after 30 Minutes

FortiGuard Filtering Protocol HTTPS UDP

FortiGuard Filtering Port 443 53 8888

Filtering Services Availability Check Again

Web Filtering ↓

Anti-Spam ↓

Request re-evaluation of a URL's category

Apply

مثلا يمكنك تحديد أيام واوقات معينه لعمل التحديث (اوقات خارج الدوام)

حيث ان ال antivirus بدون تحديث ليس له أي قيمه ...

لمعرفة ال licenses التابع لجهاز الفورتى جيت ككل

License Information

Entitlement	Status
FortiCare Support	Not Supported
Virtual Machine	Evaluation License - expires on 2020/03/19 FortiGate VM License
Allocated vCPUs	100% 1/1
Allocated RAM	49% 1002 MIB/ 2 GIB
Firmware & General Updates	Not Supported
Application Control Signatures	Version 6.00741
Device & OS Identification	Version 1.00085
Internet Service Database Definitions	Version 6.00076
Intrusion Prevention	Not Supported
IPS Definitions	Version 6.00741
IPS Engine	Version 5.00043
Malicious URLs	Version 1.00001
Botnet IPs	Version 1.00000
Botnet Domains	Version 0.00000
AntiVirus	Not Supported

View List

View List

Apply

أساسيات فورتى جيت

FortiGuard Distribution Network	
IPS Engine	Version 5.00043
Malicious URLs	Version 1.00001
Botnet IPs	Version 1.00000
Botnet Domains	Version 0.00000
AntiVirus	Not Supported
AV Definitions	Version 1.00000
AV Engine	Version 6.00132
Mobile Malware	Version 0.00000
Outbreak Prevention	Not Supported
Industrial DB	Not Supported
Industrial Attack Definitions	Version 6.00741
Security Rating	Not Supported
Security Rating Package	Version 2.00032
Web Filtering	Not Supported
Blacklisted Certificates	Version 0.00000
FortiGate Cloud	Not Supported

كما بالصورة أعلاه تبين بأن الترخيص لـ Antivirus غير موجود نظرا لأن نسخه عبارة عن VM تجريبي ...

حيث يحتوي الـ Antivirus على

Mobile Malware و AV Engine و AV Definitions

أي شيء قام جهاز الفورتى جيت بعمل له Detection سيتم تسجيله كما بالصورة ادناه

Date/Time	Service	Source	File Name	Virus/Botnet	User	Details	Action
No results							

الوقت والتاريخ لعملية اكتشاف الفيروس ويحدد له المصدر واسم الملف المعمول له detected وما هو اسم الفيروس ومن هو اليوزر الذي حصل عنده الـ detection وبعض التفاصيل وماه والـ action الذي حصل لهذا الفيروس ..

❖ طريقة تفعيل الـ antivirus على الفورتى جيت وعمل حمايه للشبكة من أي تهديدات :

The screenshot shows the FortiGate VM64 interface with the Security Profiles section selected. The table below lists the existing profiles:

Name	Comments	Ref
AV default	Scan files and block viruses.	0
AV wifi-default	Default configuration for offloading WiFi traffic.	1

كما بالصورة أعلاه يتبين بأن 2 بروفایل موجود بشكل افتراضي ولا يمكن حذفهما ..
ويمكنك انشاء بروفایلات جديد وتخصصها كما تشاء ومن ثم سيتم اختيارها لاحقا في البوليسي ...

➤ طريقة انشاء بروفایل جديد لـ antivirus :

The screenshot shows the FortiGate VM64 interface with the 'Create New' button highlighted in the Security Profiles section. The table below lists the existing profiles:

Name	Comments	Ref
AV default	Scan files and block viruses.	0
AV wifi-default	Default configuration for offloading WiFi traffic.	1

أساسيات فورتني جيت

Dashboard >
Security Fabric >
FortiView >
Network >
System >
Policy & Objects >
Security Profiles >
AntiVirus >
Web Filter >
DNS Filter >
Application Control >
Intrusion Prevention >
SSL/SSH Inspection >
Web Rating Overrides >
Web Profile Overrides >
Custom Signatures >
VPN >
User & Device >
Log & Report >
Monitor >

New AntiVirus Profile

Name: AV-FOR-Network
Comments: Write a comment... 0/255
Detect Viruses: Block Monitor
Inspected Protocols:
HTTP:
SMTP:
POP3:
IMAP:
MAPI:
FTP:
CIFS:
APT Protection Options:
Content Disarm and Reconstruction:
Treat Windows Executables in Email Attachments as Viruses:
Include Mobile Malware Protection:
OK Cancel

حيث تقوم بكتابه اسم البروفايل وفي حالة اكتشاف فايروس هل تقوم بعمل block أي سيمنع الملفات المصابه بالفايروس من الدخول الى الشبكة او Monitor وبهذا سيتم السماح للملفات المصابه بالمرور الى الشبكة بالإضافة الى قيامه بتسجيل logs على الفورتني جيت بان هذا الملف مصاب

ومن ثم تحدد البرتوكولات التي سيتم عمل لها فحص من قبل AV

FortiGate VM64 marfadi-vm

+ Create New Edit Clone Delete Search

Name	Comments	Ref.
AV-FOR-Network		0
AV default	Scan files and block viruses.	0
AV wifi-default	Default configuration for offloading WIFI traffic.	1

كما بالصورة أعلاه تم انشاء بروفايل جديد باسم AV-FOR-Network حيث يمكنك حذف او نسخ او التعديل عليه كما هي الأسمه المشار اليها في الصورة أعلاه ..

طريقة اختيار البروفایل مخصص في البوليسي :

The image displays two screenshots of the FortiGate VM64 web interface, specifically the 'Edit Policy' page for an IPv4 Policy. The left sidebar shows the navigation menu with 'Policy & Objects' and 'IPv4 Policy' selected. The main content area is divided into sections: Firewall / Network Options, Security Profiles, and Logging Options. In the Security Profiles section, the 'AntiVirus' profile is set to 'default'. A dropdown menu is open, showing a list of profiles: 'AV default', 'AV-FOR-Network', 'AV default', and 'AV wifi-default'. The 'AV-FOR-Network' profile is highlighted in yellow. In the bottom screenshot, the 'AV-FOR-Network' profile is selected as the AntiVirus profile.

تم تحديد البروفایل المسمى AV-FOR-Network والذي قمنا بإنشائه مسبقا ..

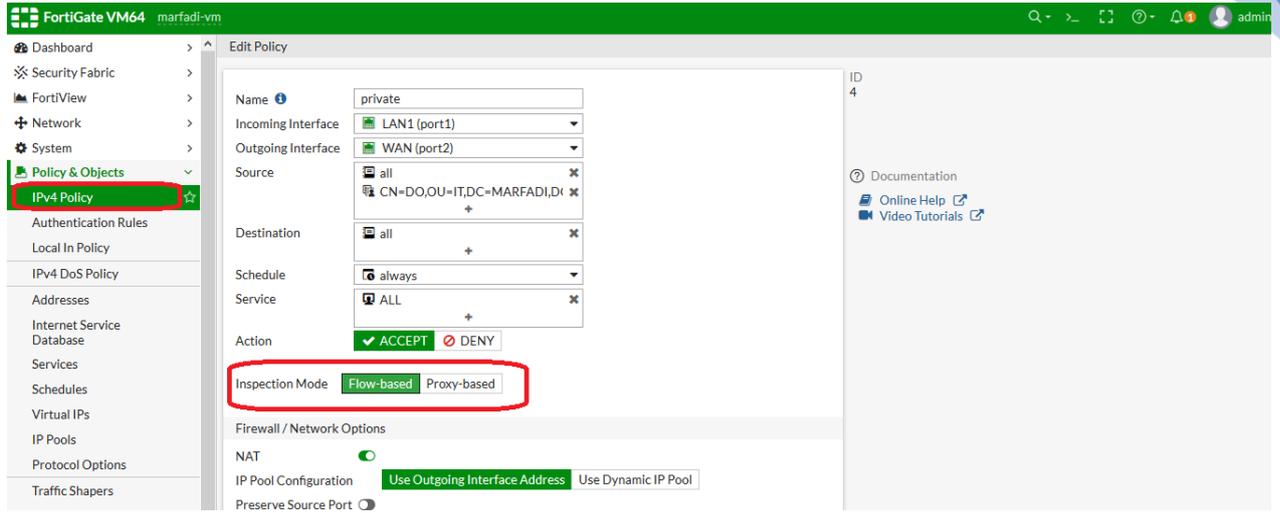
يجب ان تقوم بتفعيل الـ antivirus في كل بوليسي وذلك للأهمية ..

في حالة اردت تعمل حمايه للفورتى جيت بحيث لا يستطيع احد انشاء بروفائلات جديده مثل app control او AV او web filter.. الخ

لو قمت بالغاء تمكين هذا الخيار فانك لن تستطيع انشاء اي بروفائل جديد سواء لـ Antivirus او web application filtering او control حيث تستخدم كنوع من الامان من قبل مدير الفورتى جيت لكي لا يقوم اي احد باتشاء بروفائلات جديد

تلاحظ كما بالصورة أعلاه بأن خيار الحذف والتعديل والإضافة غير متاح بعد قيام بالغاء تفعيل الخاصية التالية: Multiple security profiles ..

: Antivirus Mode ➤



Proxy base mode	Flow base mode
<p>الفحص الأكثر شمولاً والأعمق والأطول وقت حيث يتم تقسيم الملفات (للباكت) إلى أجزاء</p>	
<p>يعتمد على مبدأ الـ buffering أي التخزين المؤقت أي أن كل الباكت والملفات التي تصل للفورتى جيت لا يتم تخزينها بشكل مؤقت على جهاز الفورتى جيت</p>	<p>يأخذ نسخه من الملفات ويحصل لها caching على الفورتى جيت قبل تسليمه إلى الكلاينت حيث لا يوجد عملية تقسيم للباكت ثم يقوم بإرسالها إلى محرك مكافحة الفيروسات ليتم عمل فحص لها ففي حالة كانت سليمه فإنه يتم تسليمها إلى المستلم أما لو كانت مصابه فيتم حذف الملف المصاب</p>
<p>في حالة لم يجد أي أصابه للملف بعد عملية الفحص يتم إرساله إلى الهدف أما في حالة وجود أصابه في الملفات يأخذ action معين ويعمل رساله للهدف كنوع من التحذير بأن الملف مصاب</p>	
<p>Default buffering=10 m لأي</p>	

<p>جهاز فورتى جيت . فلوكان الملف حجمه اكبر من 10 ميغا فأن هناك حالتين اما يتم عمليه تمرير الملف الى الهدف بدون فحص او ان يتم عمل له Block . يمكن التعديل على قيمه buffering size</p>	
--	--

❖ متى يتم استخدام flow base ومتى يتم استخدام proxy base ؟

هذا يعتمد على شكل الشبكة ..

مثلا لو هناك هجمات كثيره فالأفضل ان تختار proxy base

اما لو كان لدي شبكتين داخلية فيمكن استخدام ال flow base لأنه أسرع وبنفس الوقت الهجمات التي تكون في الشبكات الداخلية اقل بكثير من الهجمات التي تأتي من خارج الشبكة (الانترنت) .

ممكن تستخدم flow base لو كان سرعه الانترنت لديك بسيطة فالأفضل تستخدم ال flow base لأن عمليه الفحص تكون اقل بعكس عمليه ال proxy التي تكون عمليه الفحص ادق ولهذا يتم استهلاك الانترنت ..

❖ ماهي طريقة عمل مكافح الفيروسات في الفورتى جيت (يتعامل المكافح

بالفورتى جيت مع أي ملف على شكل مراحل)؟

المرحلة الأولى Antivirus protection ويسمى بالتهديدات الصريحه:

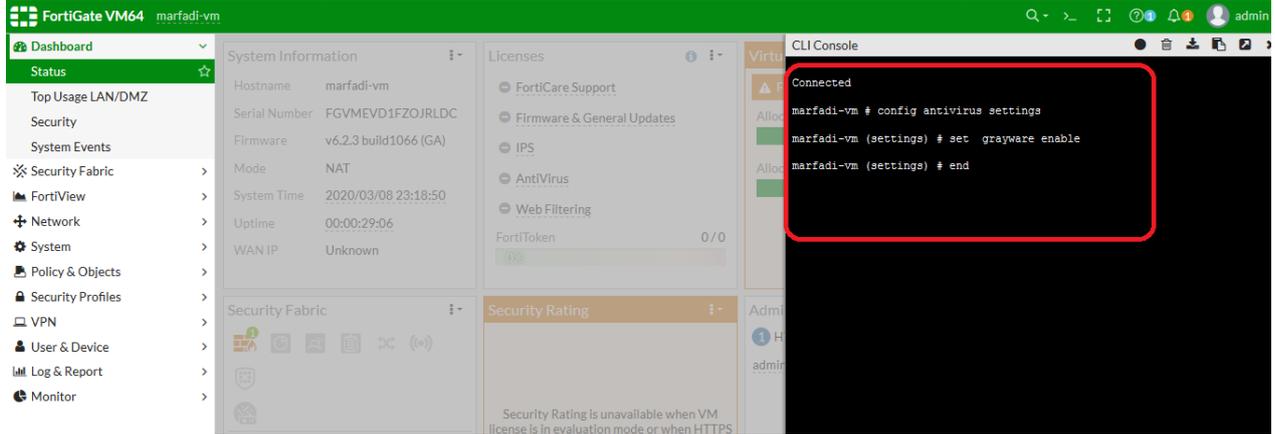
محرك البحث (DB) لدى مكافح الفيروسات أولا يقوم بالبحث على التهديدات الصريحه حيث لو قمت باستلام ملفات وهذه الملفات بتحتوي على تهديد صريح (malware) فيتم عمل action مناسب .

المرحلة الثانية (Grayware) specific function:

أساسيات فورتى جيت

تعتبر هذه المرحلة الثانية من مراحل تعامل مكافح الفيروسات التابع لفورتى جيت ، في هذه المرحلة يتم البحث عن البرمجيات التي تعتبر (Grayware) حيث الملفات او البرمجيات في هذه الحالة لا تعتبر مؤذيه أي انها غير صريحه بالتهديد ولا امنه .

هذه الخاصية بشكل افتراضي غير مفعله باجهزه الفورتى جيت فلو تريد تفعيلها لزياده نسبه الأمان فيكون ذلك عبر CLI كما بالصورة ادناه ..

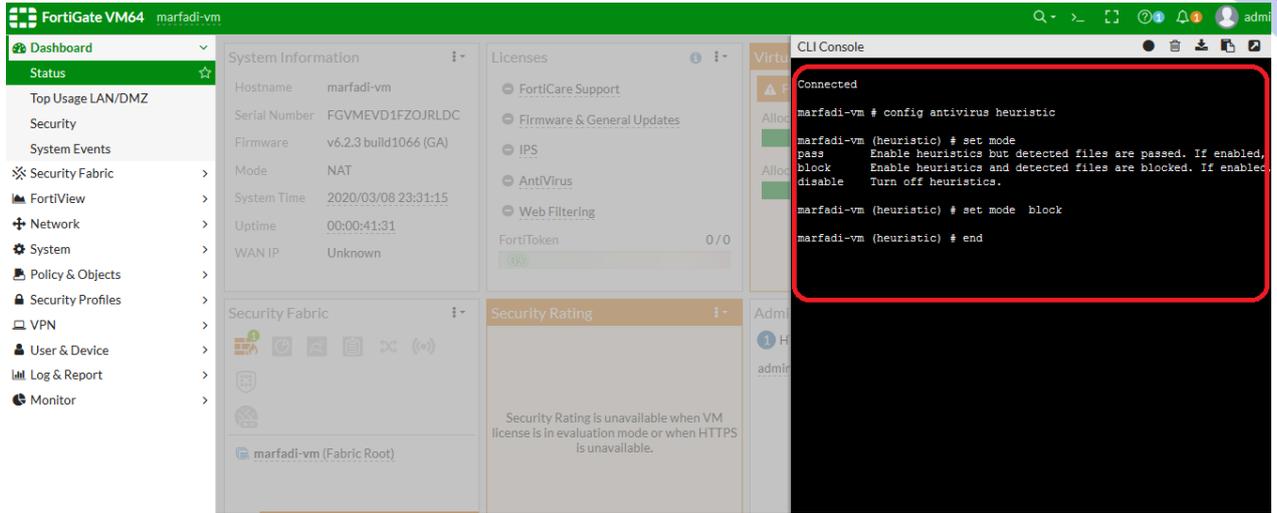


المرحلة الثالثة (الاستدلال) Heuristics :

لتم تفعيل هذه الخاصية فإن AV لووجد أي مؤشر (اشتباه) بأن الملف يحتوي على فايروس سوف يقوم بعمل action لهذه الملفات ..

حيث هذه الخاصية بشكل افتراضي غير مفعله ويوجد لهذه الخاصية أيضا pass أي في حالة الاشتباه قم بالسماح لها بالمرور الى الشبكة الداخليه وأيضا في خاصيه Block حيث في حالة الاشتباه اعمل لها Block ولا تجعل الملفات تمر الى الشبكة الداخليه ...

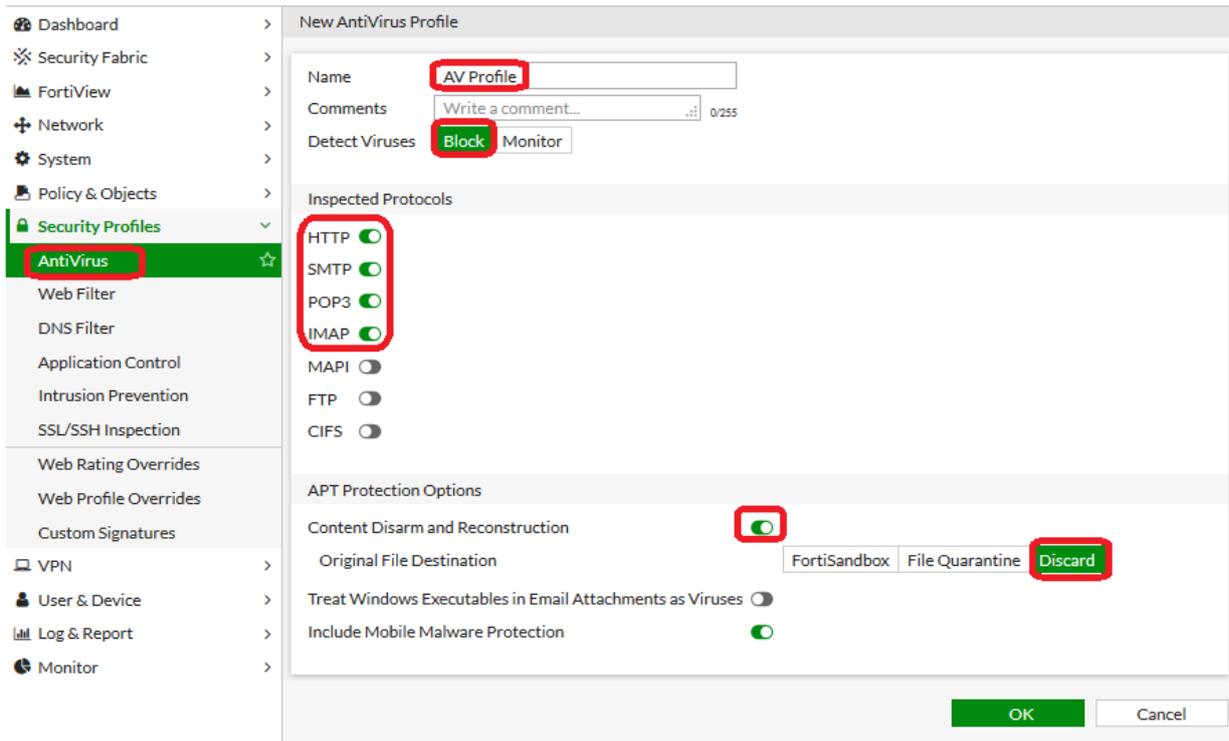
ولتفعيل هذه الخاصية عبر CLI



حيث هذه الخاصية بشكل افتراضي تكون disabled

ونحن جعلناها الان Block أي في حالة الاشتباه قم بعمل Block للملفات ..

: Antivirus Profile configuration ➤



يقوم بعمل فحص للترافيك http, smtp, pop3, imap ويعمل لها Block في حالة يحتوي على فايروس .

Content Disarm and Reconstruction: يجعل الفورتي جيت يأخذ أي ملف (pdf, doc, ...))

أساسيات فورتى جيت

وفحصه والتأكد من احتوائه على الهايبرلينك ، حيث فكره **الهايبرلينك** هي ملف ضار داخل ملف عادي وعند تمكين هذا الخيار يتم التعامل مع هذا الملف ، حيث يقوم الفورتى جيت بحذف الهايبرلينك واصبح لديك الملف الحقيقي فقط فهو حسب الخيارات أعلاه يقول لك هل تريد ان اطبق على الملف الحقيقي - السليم - **Original File Destination** احدى الخيارات ادناه :

FortiSandbox : في حالة كان عندك ترخيص fortisandbox

File Quarantine : حيث يقوم بالاحتفاظ بالملف الحقيقي في الفورتى جيت وفي هذه الحالة يجب ان يكون لديك هارد داخل الفورتى جيت .

Discard : حذف الملف الأصلي .

Treat Windows Executables in Email Attachments as Viruses : هذا الخيار يقوم بحذف

الملفات المرفقة التي تصل عبر الايميل فيها exe او msi او أي ملف تنفيذي .

Web filtering ➤

عبارة عن التحكم في المحتوى الذي يصل الى المستخدم او الذي يصل اليه المستخدم .

او بمعنى أوضح عبارة عن فلترة الـ **http** و **http** لكي يصل للمستخدم المحتوى الآمن والمسموح به ..

أسباب التحكم في Web filtering :

- ١- فقدان الإنتاجية بسبب ان الموظفين يهدرون اوقاتهم بالتصفح لأن له الحق بالوصول الى كل المواقع .
- ٢- بطئ الانترنت بسبب اهدار الترافيك في فتح المواقع مثل اليوتيوب والألعاب.
- ٣- تسريب المعلومات الهامة خارج الشركة
- ٤- التعرض للهجمات عبر المواقع
- ٥- تجنب أي مسؤليه قانونيه بسبب تنزيل احد الموظفين لبرمجيات غير مصرحه .

الجهات التي تصل عبر الويب :

- البرامج التجسسية والبرمجيات الضارة .
- التصيد عبر الايميلات وغيرها .
- استخدام موقع مزيف رغم انه مشابه للموقع الحقيقي .
- مواقع التحميل (peer to peer) حيث ممكن الموظف يقوم بتنزيل ملفات تحتوي على فايروسات .
- استهلاك الانترنت عبر مواقع streaming media (audio+video)

Web filtering mode

يوجد لدى فورتى جيت 3 أنماط مختلفه :

(١) **Proxy**: يعتمد على ال Buffering أي عملية تخزين البيانات لفترة محددة لحين إتمام عملية الفحص ثم تمرير البيانات الى الهدف (اليوزر) دقيق في عملية الفحص ولكنه بطئ بسبب عملية buffering. اعداداته كثيره .

(٢) **Flow**: لا يعتمد على ال Buffering حيث يمرر البيانات الى الهدف بدون تخزين حيث انه اقل دقه من البروكسي ويعتبر اسرع نمط .

(٣) **DNS**: لا يعتمد على ال Buffering حيث يقوم بعملية تحويل من اسم الى ايبي حيث شركه فورتى نت لديها dns server ويمكن الاعتماد عليه لعملية فلترة المواقع ، حيث يعتبر هذا النمط دقيق لأنه يعتمد على ال dns server التابع لفورتى نت حيث يتعبسريع ولكن ليس اسرع من ال flow mode

حيث يعتبر اقل اعدادات .

- ملاحظة: عملية الفحص تكون على ايبي الموقع واسم الموقع حيث ستقوم بإنشاء بروفایل خاص ب web filtering وتخصه لناس معينين.

The screenshot shows the FortiGate VM64 interface. In the top left, the 'Security Profiles' menu is highlighted. A table lists the profiles:

Name	Comments	Ref
Web-sites		0
default	Default web filtering.	0
monitor-all	Monitor and log all visited URLs, flow-based.	0
wifi-default	Default configuration for offloading WIFI traffic.	1

In the 'Edit Policy' window, the 'Security Profiles' section shows 'Web Filter' enabled. A dropdown menu is open, showing the selected profile 'default' and other options: 'monitor-all', 'Web-sites', and 'wifi-default'.

تم تطبيق بروفایل معين في الـ web filter على بوليسي معينه ..

➤ ماهي الخيارات المتاحة على الفورتى جيت بخصوص الـ web filtering

- ١) **Static URL Web filter**: عمليه التحكم في موقع معين بالضبط او التحكم على دومين كامل .
حيث بهذا النوع ستقوم بكتابه الموقع بنفسك .
- ٢) **Web content filter**: يمكنك من فلاتره المحتوى المطلوب بناء على كلمات محددده على صفحة الويب او أنماط معينه او جمل معينه
- ٣) **fortiGuard web filter**: يمكنك بوساطتها ان تتحكم بملايين المواقع من خلال التصنيفات التي معموله عبر شركه فورتى جيت

➤ شرح مفصل للأنواع المذكورة أعلاه :

١) fortiGuard web filter :

عبارة عن حل يتم ادارته من قبل شركة فورتى نت حيث لا يمكنك الاستفادة منه الا لوقمت بعملية تجديد الاشتراك كل سنة ..

حيث لو لم تكن مشترك بهذه الخدمة فانك لن تقدر التحكم بالمواقع بحسب التصنيف.

حيث ال vm لا تكون مفعلة ولذا لا يمكننا استخدام النوع fortiGuard web filter .

فمثلا لو تريد اغلاق مواقع ال social networking التي تقدر بمئات المواقع فإنه من الصعب اغلقها عبر الطريقة Static Url web filter اما عبر FortiGuard web filter فستكون سهله جدا حيث بخيار واحد يمكنك اغلاق كل مواقع التواصل الاجتماعي (categoring) ..

٢) rating أي تقييم المواقع مثل (موقع خبيث،....)

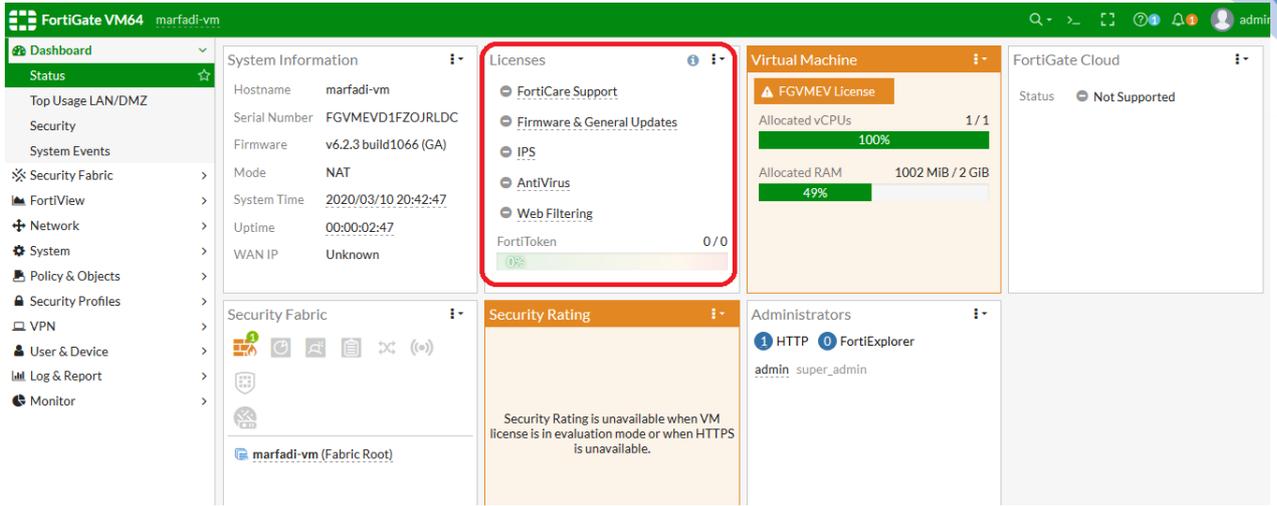
➤ ماهي علاقه فورتى جار بالفورتى جيت :

اليوزر عندما يطلب أي موقع فأن الفورتى جيت يأخذ الطلب ويرسله لأقرب سيرفر لفورتى جار بشرط ان يكون جهاز الفورتى جيت مشترك (License).

فلو كان الطلب (الموقع) الذي طلبه اليوزر ممنوع (Block) فيقوم سيرفر فورتى جار بإرسال رساله الى جهاز الفورتى جيت بأن الموقع محجوب والذي بدوره يقوم بإظهار رساله لليوزر بأن الموقع مغلق .

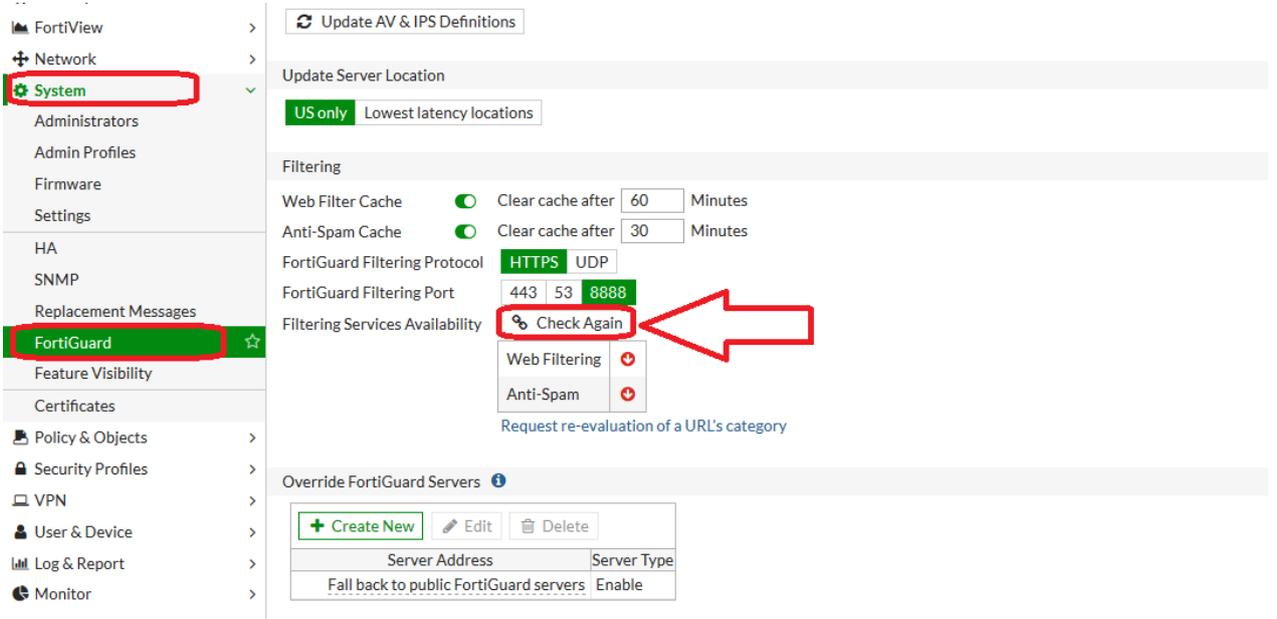
حيث يعتبر الفورتى جيت وسيط بين اليوزر والفورتى جار سيرفر

يجب ان تتأكد بان الفورتى جيت متوصل بشكل سليم مع الفورتى جار وأيضا لديك ترخيص (license).

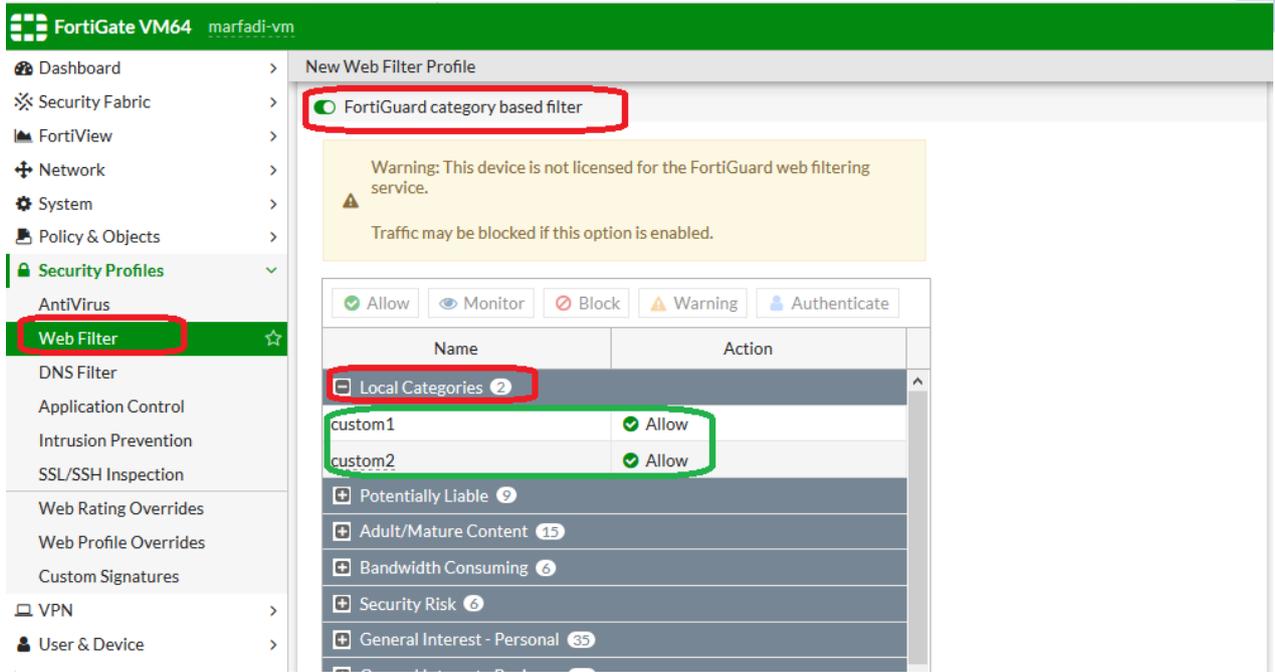


يجب ان تتأكد بأن ال licenses شغال بشكل سليم كما بالصورة أعلاه

وأیضا تتأكد من ال connectivity بين الفورتى جيت والفورتى جارد كما بالصورة ادناه



➤ كيفية التعامل مع ال fortiguard category في ال web filter :



نلاحظ بأن رساله الخطأ توضح بأن الفورتى جارد ليس متاح على ال fortigate vm حيث يجب ان تكون مشترك بخدمه الفورتى جارد لكي تتمكن من استخدامها ولكننا سوف نشرحها بشكل نظري ...

توجد عده تصنيفات عامه وتحت كل تصنيف عام تكون عده تصنيفات فرعيه وكل تصنيف فرعي يحتوي على مئات من المواقع

مثلا التصنيف المسمى security Risk يحتوي على 6 تصنيفات فرعيه (Sub categories) وهي كالتالي

Malicious Websites

Phishing

Spam

Spam URL

Dynamic DNS

New observed Domain

New Registered Domain

أساسيات فورتني جيت

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
 - AntiVirus
 - Web Filter
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - SSL/SSH Inspection
 - Web Rating Overrides
 - Web Profile Overrides
 - Custom Signatures
- VPN
- User & Device
- Log & Report
- Monitor

NEW WEB FILTER PROFILE

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow
 Monitor
 Block
 Warning
 Authenticate

Name	Action
Security Risk 6	
Malicious Websites	Block
Phishing	Block
Spam URLs	Block
Dynamic DNS	Block
Newly Observed Domain	Block
Newly Registered Domain	Block
General Interest - Personal 35	
General Interest - Business 15	

Category Usage Quota

فلوتريد اغلاق كل مواقع phishing فإنه يجلب عليك ان تقوم بإغلاق التصنيف المسي phishing وهكذا كما بالصورة ادناه

- System
- Policy & Objects
- Security Profiles
 - AntiVirus
 - Web Filter
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - SSL/SSH Inspection
 - Web Rating Overrides
 - Web Profile Overrides
 - Custom Signatures
- VPN
- User & Device
- Log & Report
- Monitor

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow
 Monitor
 Block
 Warning
 Authenticate

Name	Action
Security Risk 6	
Malicious Websites	Allow
Phishing	Block
Spam URLs	Allow
Dynamic DNS	Allow
Newly Observed Domain	Allow
Newly Registered Domain	Allow
General Interest - Personal 35	

حيث بمجرد النقر على sub categories بالزر الأيمن يظهر لك ال actions المراد اختياره مثل Allow, Monitor, Block, Warning, Authenticate

FortiGate v1004

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > AntiVirus > Web Filter

Local Categories 2

Name	Action
Local Categories 2	
Potentially Liable 9	
Adult/Mature Content 15	
Bandwidth Consuming 6	
Security Risk 6	
Malicious Websites	Block
Phishing	Allow
Spam URLs	Block
Dynamic DNS	Block

Category Usage

+ Create New Edit Delete

Category	Total quota
No results	

مثلا التصنيف (35) General Interest-Personal يحتوي على 35 تصنيف فرعي كما بالمرجع البرتقالي

General Interest - Personal 35

Advertising	Allow
Brokerage and Trading	Allow
Games	Allow
Web-based Email	Allow
Entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow

Category Usage Quota

+ Create New Edit Delete

Category	Total quota
No results	

أساسيات فورتني جيت

- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
 - AntiVirus
 - Web Filter ☆
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - SSL/SSH Inspection
- Web Rating Overrides
- Web Profile Overrides
- Custom Signatures
- VPN >
- User & Device >
- Log & Report >
- Monitor >

Name	Action
Job Search	✓ Allow
Medicine	✓ Allow
News and Media	✓ Allow
Social Networking	✓ Allow
Political Organizations	✓ Allow
Reference	✓ Allow
Global Religion	✓ Allow
Shopping	✓ Allow
Society and Lifestyles	✓ Allow

Category Usage Quota ⓘ

[+ Create New](#) [Edit](#) [Delete](#)

Category	Total quota
No results	

- Dashboard >
- Security Fabric >
- FortiView >
- Network >
- System >
- Policy & Objects >
- Security Profiles >
 - AntiVirus
 - Web Filter ☆
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - SSL/SSH Inspection
- Web Rating Overrides
- Web Profile Overrides
- Custom Signatures
- VPN >
- User & Device >
- Log & Report >
- Monitor >

edit web filter profile

Allow
 Monitor
 Block
 Warning
 Authenticate

Name	Action
Sports	✓ Allow
Travel	✓ Allow
Personal Vehicles	✓ Allow
Dynamic Content	✓ Allow
Meaningless Content	✓ Allow
Folklore	✓ Allow
Web Chat	✓ Allow
Instant Messaging	✓ Allow
Newsgroups and Message Boards	✓ Allow

Category Usage Quota ⓘ

[+ Create New](#) [Edit](#) [Delete](#)

Category	Total quota
No results	

أساسيات فورتني جيت

Dashboard	>
Security Fabric	>
FortiView	>
Network	>
System	>
Policy & Objects	>
Security Profiles	>
AntiVirus	>
Web Filter	☆
DNS Filter	>
Application Control	>
Intrusion Prevention	>
SSL/SSH Inspection	>
Web Rating Overrides	>
Web Profile Overrides	>
Custom Signatures	>
VPN	>
User & Device	>
Log & Report	>
Monitor	>

Name	Action
Digital Postcards	✓ Allow
Child Education	✓ Allow
Real Estate	✓ Allow
Restaurant and Dining	✓ Allow
Personal Websites and Blogs	✓ Allow
Content Servers	✓ Allow
Domain Parking	✓ Allow
Personal Privacy	✓ Allow
Auction	✓ Allow

85% 89

Category Usage Quota ⓘ

+ Create New Edit Delete

Category	Total quota
No results	

Advertising: تحتوي على كل المواقع الإعلانية .

Education: يحتوي على كل المواقع التعليميه(المدارس والجامعات ..الخ) .

Health and Wellness: يحتوي على كل مواقع الصحة .

News and Media: يحتوي على مواقع الاخبار .

Personal Vehicles: يحتوي على مواقع الشاحنات والسيارات

Personal Privacy: يحتوي على المواقع الشخصيه

Sports: مواقع الرياضه

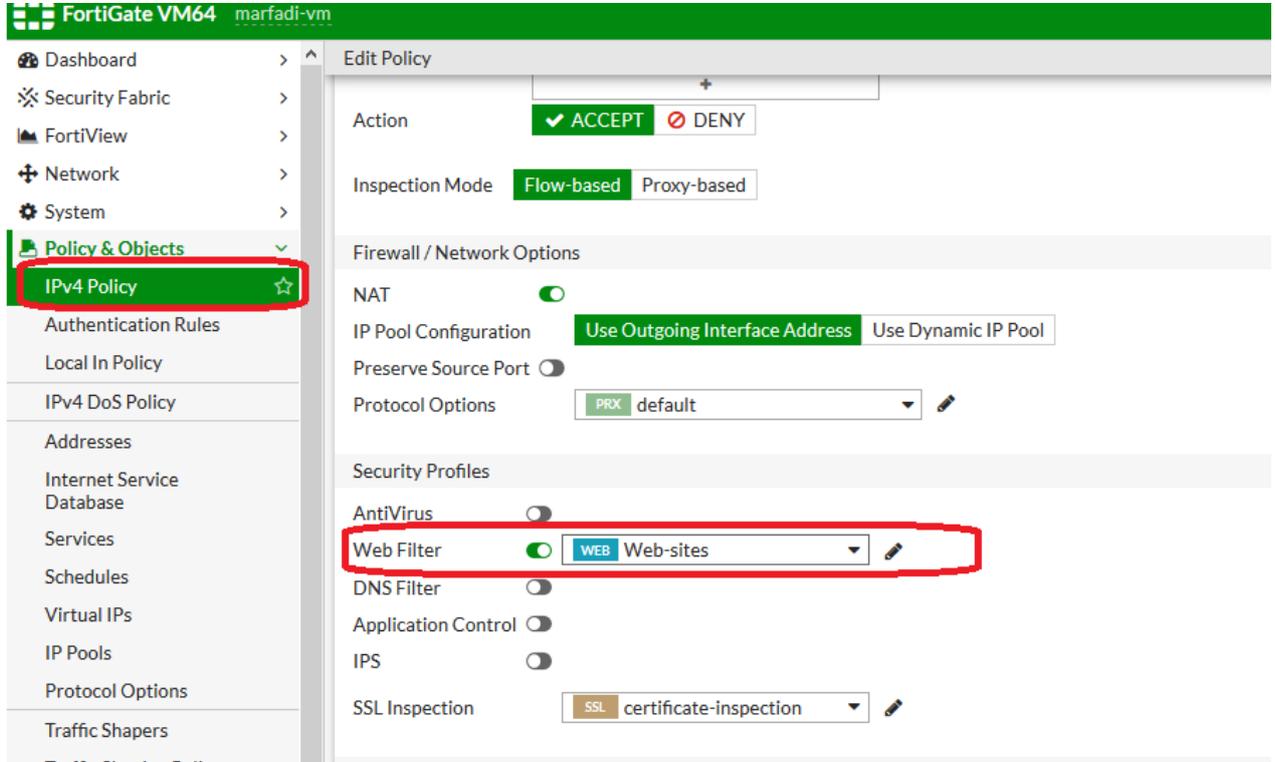
Shopping: مواقع التسويق

Social Networking: الشبكات الاجتماعية مثل الفيسبوك والتويتروال جوجل بلاس

Games: مواقع الالعاب

Web Chat: مواقع الشات حيث يختلف عن app chat

حيث تقوم باختيار ال actions المناسب ثم تقوم بإعطاء اسم للبروفایل ومن ثم تنشئ بوليسي وتختار هذا البروفایل لهذا البوليسي لكي يتم تطبيقه ..



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles
4	private	all CN=DO,OU=IT,DC=MARFADI,DC=LOCAL	all	always	ALL	ACCEPT	Enabled	WEB Web-sites SSL certificate-inspection
3	public	Subnet1	all	always	ALL	DENY	Enabled	SSL no-inspection
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection
5	3	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection
0	Implicit Deny	all	all	always	ALL	DENY	Enabled	SSL no-inspection

مقال

لوتريد اغلاق مواقع التواصل الاجتماعية مثل الفيسبوك وتويتر وأيضا اغلاق مواقع الاخبار مثل صحافه 24 وموقع bbc.com وغيرها ..

فأننا سنقوم أولا بإنشاء بروفایل باسم Block social networking&News

أساسيات فورتى جيت

وستقوم بالسماح لكل ال categories ماعدا ال social networking و New and media سوف نقوم بإغلاقها كما بالصورة ادناه ..

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > Web Filter

New Web Filter Profile

Name: Block Social networking&News

Comments: Write a comment... 0/255

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow Monitor Block Warning Authenticate

Name	Action
Job Search	Allow
Medicine	Allow
News and Media	Block
Social Networking	Block
Political Organizations	Allow

فعند محاوله فتح أي موقع اخباري مثل BBC فإنه ستظهر لك رساله بان الموقع مغلق بالإضافة الى المعلومات بايى الجهاز 192.168.2.121 الذي حاول يفتح الموقع وأيضا ال category الذي ينتهي لها هذا الموقع هو News and Media والذي تم اغلاقه بواسطتها ..



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: www.google.com.sa/url?sa=t&rc=t=j&q=&esrc=s&source=web&cd=1&ved=0CCMQJAA&url=http%3A%2F%2Fwww.bbc.co.uk%2FArabic&ei=qn1LVdjjD6faywOGu4HoCg&usq=AFQJcNETWo6CBteDfhs16nqipWTM3i8Mfw
Category: News and Media
Client IP: 192.168.2.121
Server IP: 173.194.113.23
User name:
Group name:

To have the rating of this web page re-evaluated [please click here](#).

فلو قمت بفتح موقع الفيسبوك <https://facebook.com> فإنه سوف يفتح معك بشكل طبيعي بالرغم انه مصنف تحت Social network وذلك لأنك طلبت الموقع ب https وليس http ولتفادي هذه المشكله يجب ان تقوم بتفعيل خاصيه

أساسيات فورتى جيت

https وبذلك تجعل الفورتى جيت يقوم بفحص أي موقع ssl inspection=certificates-inspection وبهذا سوف غلق المواقع الاجتماعية،

اي ان أي شخص يريد الوصول الى موقع ضمن تصنيف الشبكات الاجتماعية او المواقع الإخبارية سواء كان http او https فانه سوف يتم اغلاقها ..

The screenshot shows the FortiGate configuration interface. The left sidebar is expanded to 'Policy & Objects', with 'IPv4 Policy' selected. The main area shows the 'Edit Policy' configuration for 'Flow-based' inspection mode. Under 'Security Profiles', 'Web Filter' is enabled and set to 'WEB Block Social networking&News', and 'SSL Inspection' is enabled and set to 'SSL certificate-inspection'. Both are highlighted with red boxes.

ملاحظة :

لوكان الموقع المراد الوصول اليه http وهو ضمن التصنيف المعمول له Block فسوف تظهر رساله الغلق (Web page Blocked) من فورتى جيت كما بالصورة ادناه

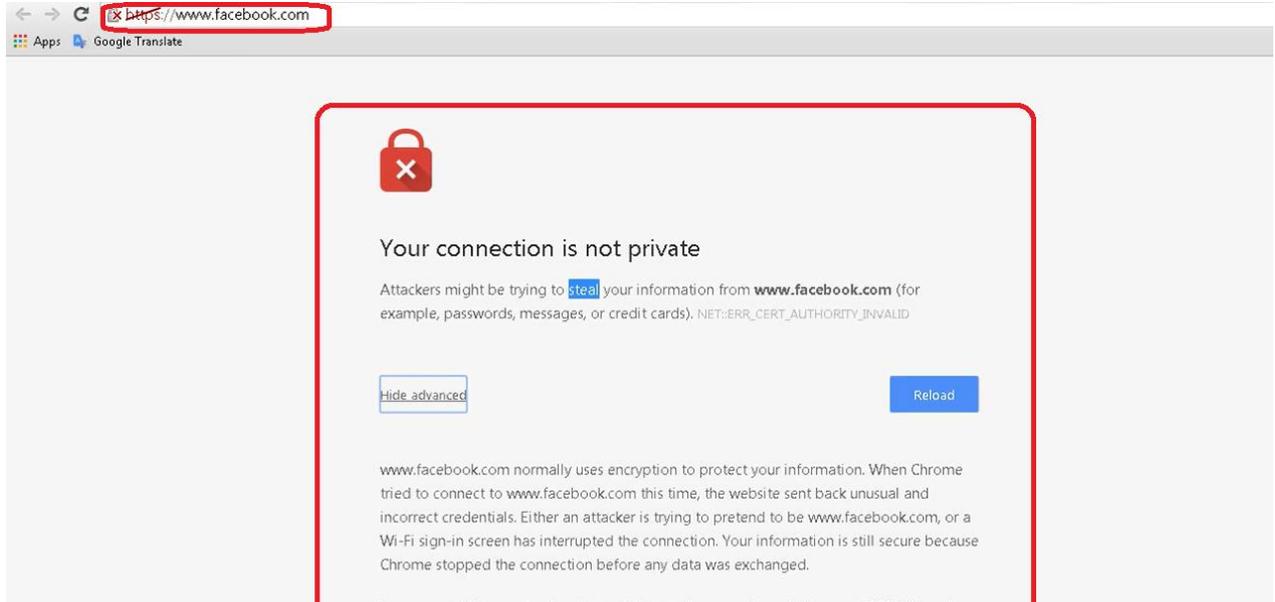
The screenshot shows a FortiGuard Web Filtering error message. The message is titled 'Web Page Blocked!' and contains the following information:

- You have tried to access a web page which is in violation of your internet usage policy.
- URL: www.google.com.sa?url?sa=t&rc=t=j&q=&esrc=s&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Fwww.bbc.co.uk%2Farabic&ei=qn1LVdjjD6faywOGu4HoCg&usq=AFQjCNETWocBteDfhs16nqipWTM3i8Mfw
- Category: News and Media
- Client IP: 192.168.1.100
- Server IP: 173.194.113.23
- User name:
- Group name:

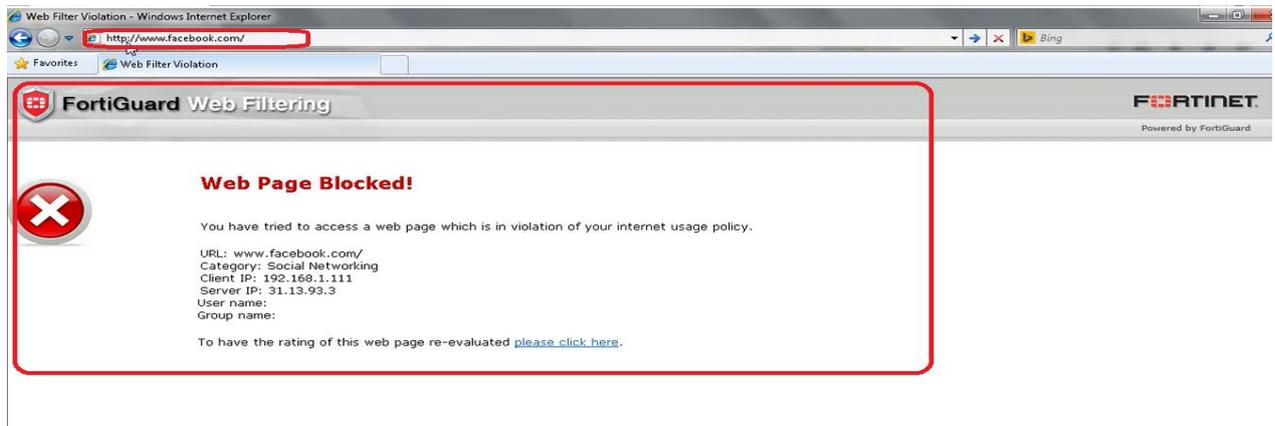
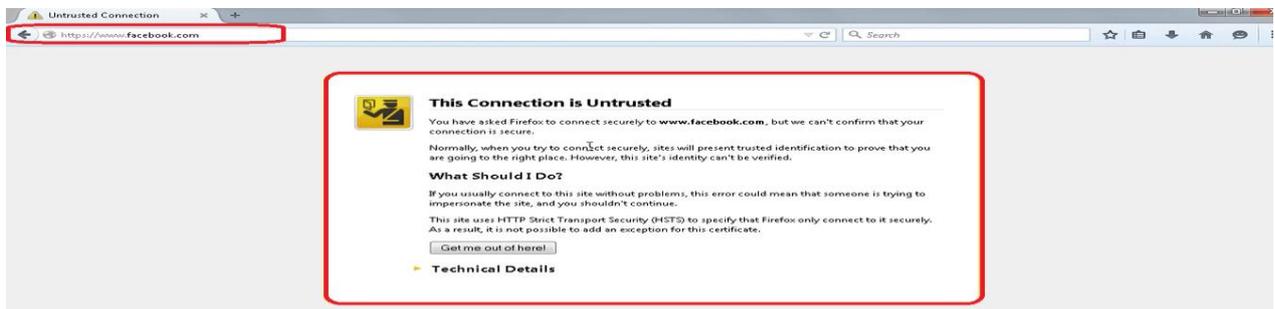
To have the rating of this web page re-evaluated [please click here](#).

أساسيات فورتى جيت

اما لو قمت بتفعيل خاصية ssl inspection فأن رساله الغلق Web page Blocked لن تظهر بهذا الشكل (باغلب المتصفحات) مع مواقع الـ https بل تظهر لك رساله الخطأ كما بالتالي وذلك بحسب المتصفح



وهذا عن طريق متصفح اخر لنفس الموقع



اما عن طريق متصفح Internet explorer ظهر لك رساله الـ Web Page Blocked كما بالصورة أعلاه ..

وفي جميع الأحوال لن تستطيع الوصول الى تلك المواقع سواء http او https

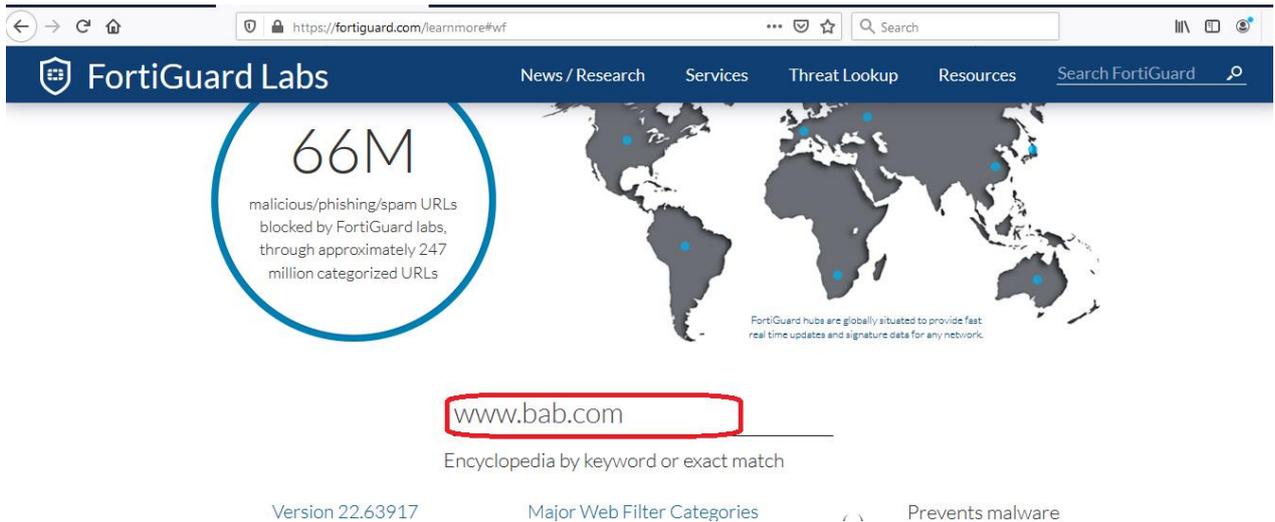
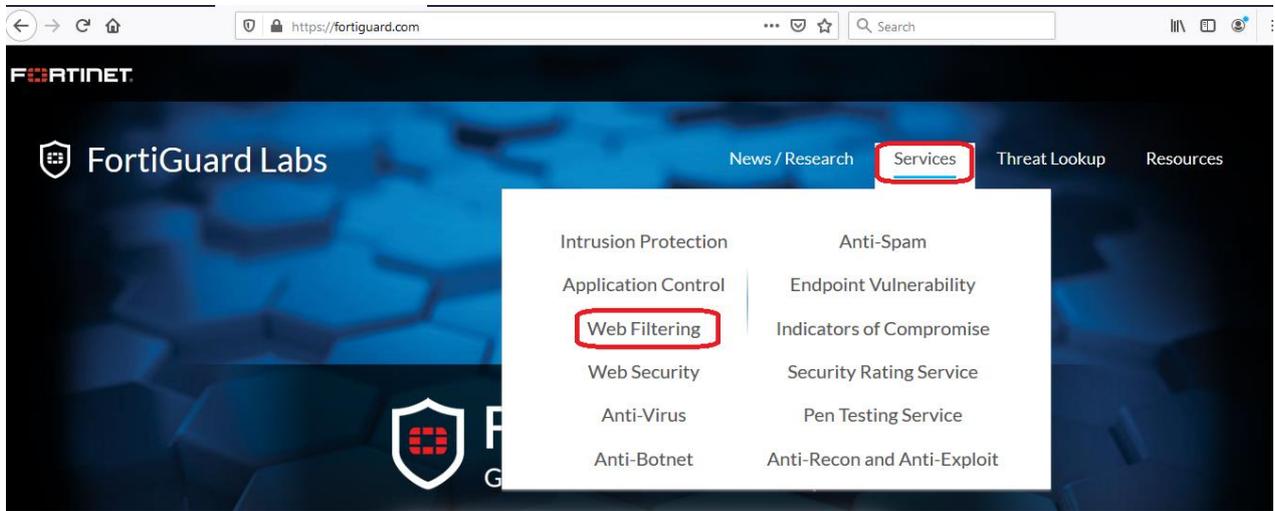
بواسطة fortiguard categories سوف تستطيع اغلاق ألف المواقع بحسب تصنيفها بنقر زر واحد بدون الحاجة الى كتابه المواقع يدويا ...

طريقة معرفة تصنيف أي موقع ..

مثلا موقع www.bab.com لو تريد معرفة تصنيفه

نقوم بالدخول الى الموقع التالي <https://fortiguard.com>

ثم كما بالصورة التالية



نكتب المواقع المراد معرفة ال category التابع له ثم enter

سوف يظهر لك التصنيف للموقع كما بالصورة ادناه

FortiGuard Labs News / Research Services Threat Lookup Resources www.bab.com

At a glance:

WF Rating History
Jun 19th, 2015 @ 11:05:20 PDT removed as Not Rated
Jul 21st, 2009 @ 13:10:26 PDT added as News and Media

DOWNLOAD FortiClient

Web Filter Lookup

www.bab.com 5.6+

Submit a URL to check its Rating FortiOS Version

Category: News and Media

Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media. This category includes TV and Radio sites, as long as they are not exclusively for entertainment purpose, but excludes academic journals. Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.

إذا الموقع www.bab.com يقع ضمن التصنيف news and Media .

أنواع الـ action :

Allow Monitor Block Warning Authenticate

Name	Action
+ Local Categories 2	
- Potentially Liable 9	
Drug Abuse	Allow
Hacking	Allow
Illegal or Unethical	Block
Discrimination	Warning
Explicit Violence	Authenticate
Extremist Groups	Warning
Proxy Avoidance	Allow

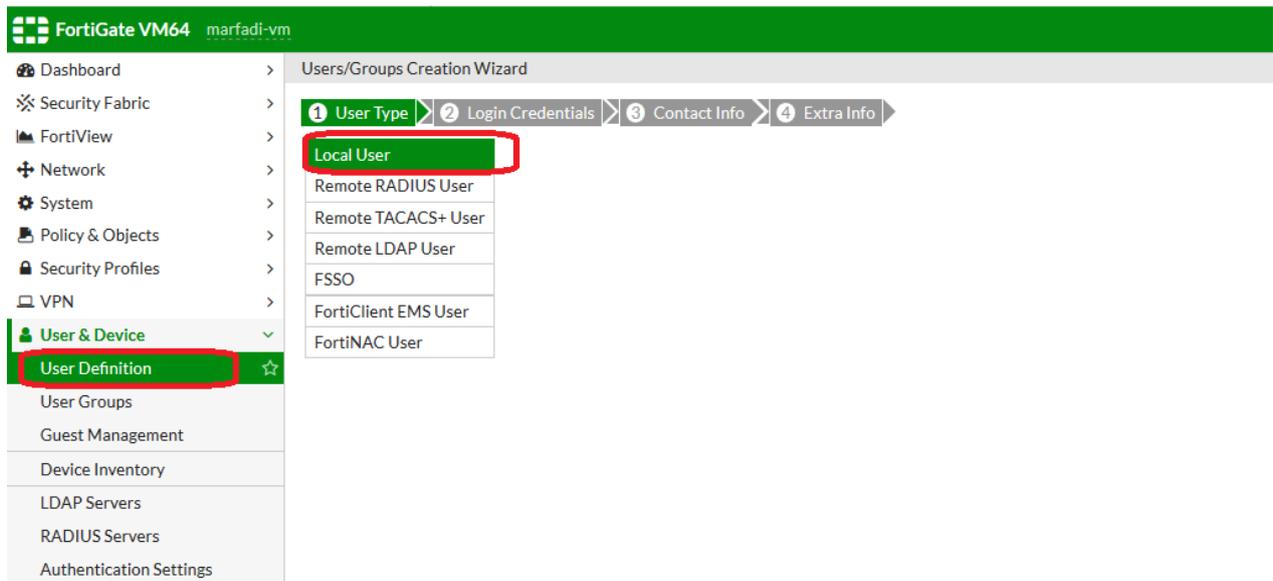
OK

- ١- Allow: السماح للوصول لأي موقع يندرج تحت الـ category التي عملت لها allow
- ٢- Block: منع الوصول لأي موقع يندرج تحت الـ category التي عملت لها block
- ٣- Monitor: مراقبه أي شخص من الوصول الى أي موقع يندرج تحت category قمت بعمل لها monitor ..

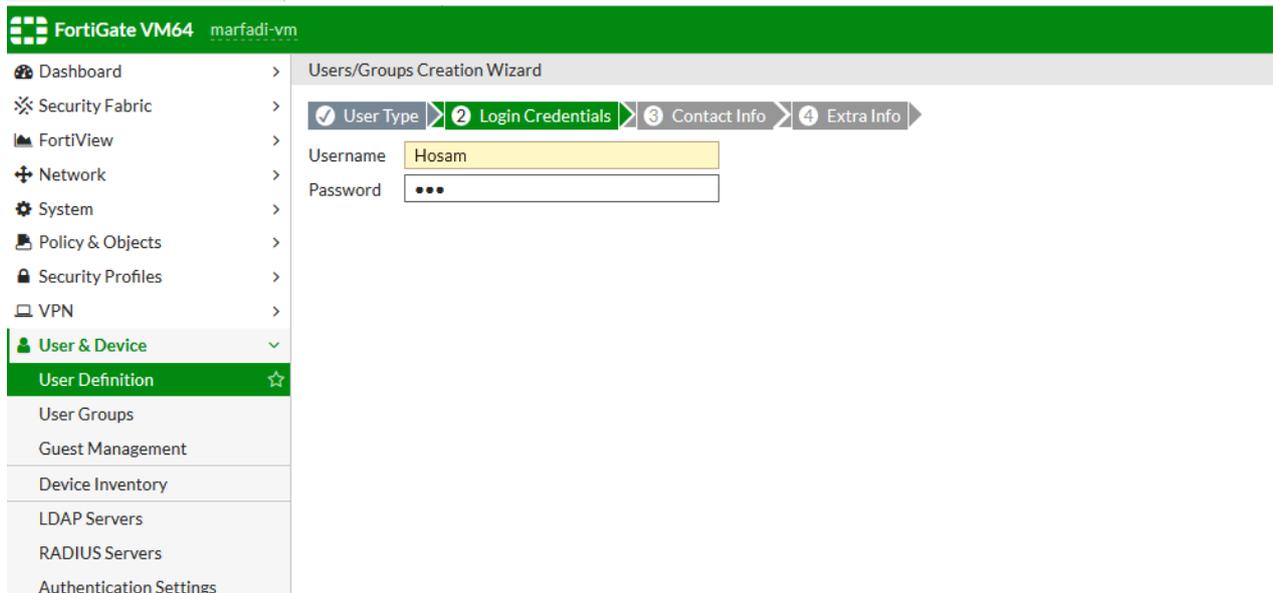
أساسيات فورتى جيت

حيث المراقبة سوف تكون في ال logs حيث سيظهر لك ماذا فتح من موقع ومتى ومن الشخص الذي فتح الموقع ولكن بشرط يجب ان يكون اليوزر موجود في local users (حسابات محليه) التابع للفورتى جيت أي ان اليوزر لو أراد الوصول الى الانترنت يجب ان يقوم بإدخال اليوزر ينم وباسورد حيث سيتم عمل Monitor لهذا اليوزرات فقط .

فاذا قمت بإنشاء يوزر محلي باسم Hosam وباسورد 123 على الفورتى جيت وأريد مراقبه ال category المسماة social networking سوف نقوم بالتالي :



The screenshot shows the FortiGate VM64 interface for the 'Users/Groups Creation Wizard'. The 'User Type' step is selected, and a dropdown menu is open, showing 'Local User' as the selected option. The 'User Definition' menu item is also highlighted in the left sidebar.



The screenshot shows the 'Login Credentials' step of the 'Users/Groups Creation Wizard'. The 'Username' field is filled with 'Hosam' and the 'Password' field is masked with dots. The 'User Type' step is now completed and marked with a checkmark.

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

User Type | Login Credentials | Contact Info | **4 Extra Info**

User Account Status: **Enabled** Disabled

User Group: LOCAL

FortiGate VM64 marfadi-vm

Name	Type	Two-factor Authentication	Ref.
Hosam	LOCAL	0	
guest	LOCAL	1	

FortiGate VM64 marfadi-vm

Edit Web Filter Profile

Name: **Monitor Social networking&News**

Comments: Write a comment... 0/255

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Allow | Monitor | Block | Warning | Authenticate

Name	Action
News and Media	Monitor
Social Networking	Monitor
Political Organizations	Allow
Reference	Allow
Global Religion	Allow
Shopping	Allow

تم عمل مراقبه New and Media و Social Networking كما بالصورة أعلاه

FortiGate VM64 marfadi-vm

Name	Comments	Ref.
WEB Monitor Social networking&News		0
WEB Web-sites		0
WEB default	Default web filtering.	0
WEB monitor-all	Monitor and log all visited URLs, flow-based.	0
WEB wifi-default	Default configuration for offloading WIFI traffic.	1

Edit Policy

Name: private

Incoming Interface: LAN1 (port1)

Outgoing Interface: WAN (port2)

Source: all, Hosam

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT, DENY

Inspection Mode: Flow-based, Proxy-based

Firewall / Network Options

NAT: ON

IP Pool Configuration: Use Outgoing Interface Address, Use Dynamic IP Pool

Preserve Source Port: ON

Protocol Options: PRX, default

Security Profiles

AntiVirus: OFF

Web Filter: ON, WEB Monitor Social networking&News

DNS Filter: OFF

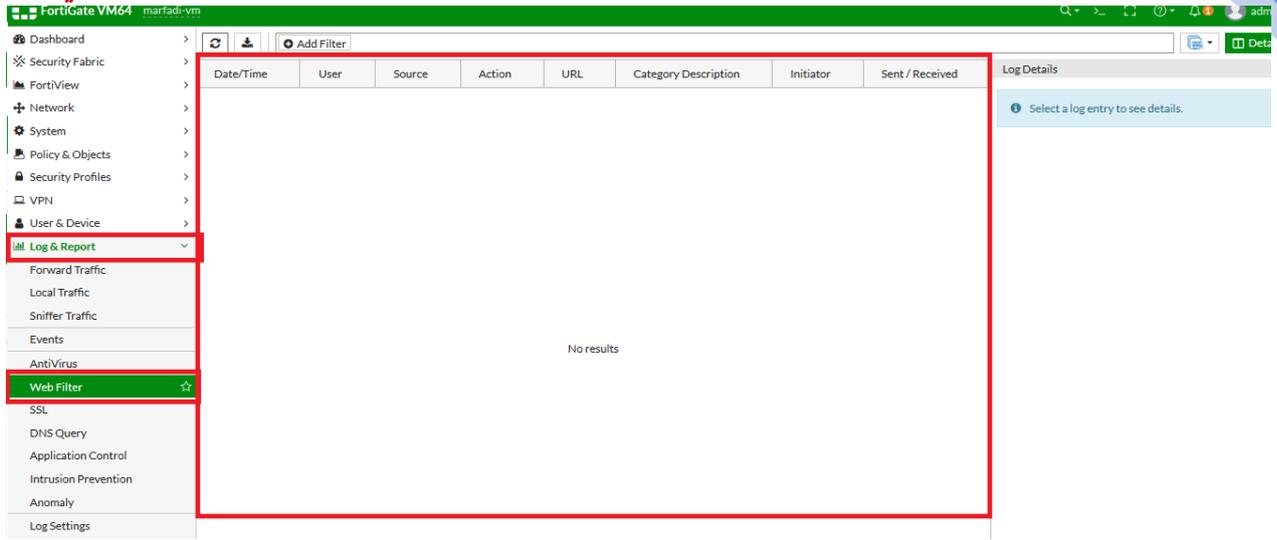
Application Control: OFF

IPS: OFF

كما بالصورة أعلاه تم انشاء بوليسي بحيث يتم مراقبه اليوزر المسى Hosam عند الوصول الى Social networking & new and Media

حيث المفترض عندما يقوم اليوزر Hosam بفتح موقع مثل فيسبوك او صحافه نت او غيرها من المواقع ضمن التصنيف ال Social networking & new and Media

فانه سوف يطلب منه يوزرنيم وباسورد وبد إدخالها من قبل hosam فان الموقع سوف يفتح طبيعي ولمراجعته ال logs لليوزر



حيث يظهر لك الوقت واسم اليوزر وال action والموقع الذي تم الوصول اليه من قبل اليوزر وال category المندرج تحتها هذا الموقع وغيرها من المعلومات ..

أي ان يوزر معمول له Monitor فاني ممكن اطالع على ال logs كما بالصورة أعلاه ..

لو كنت تريد فتح مثلا مواقع معينه مثل الفيسبوك وتويتر لفتره محدده ولكن بدون تحديد الوقت (مثلا 15 دقيقه في اليوم لكل يوزر) ليس محدد الوقت المسموح، بل أي وقت سوف يستخدمه اليوزر سوف يتم اعطائه 15 دقيقه فقط بغض النظر عن الوقت وبعدها سوف يتم عمل block لتلك المواقع .. فمثلا بعض الموظفين سوف يفتحوا المواقع صباحا لمدة ربع ساعه والبعض الاخر ظهرا والخ وهكذا حيث سيتم حساب وقت كل يوزر على حده وبعد انتهاء الوقت سوف يتم عمل Block لهذه ال category .

➤ يوجد في الفورتى جيت خاصيه جميله جدا اسمها ال Quota حيث يتم تطبيق ال quota على ال category التي ال action لها Monitor او authenticate او warning فقط

أساسيات فورتني جيت

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

Name	Action
Entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow
Job Search	Allow
Medicine	Allow
News and Media	Monitor
Social Networking	Monitor
Political Organizations	Allow
Reference	Allow

Category Usage Quota

+ Create New Edit Delete

Category	Total quota

عندما اريد انشاء Quota وذلك بالنقر على الخيار Create New فإنه يجب ان تكون ال category من احدى الأنواع الثلاثة التي ذكرت سابقا لكي أتمكن من انشاء ال quota

FortiGate VM64 marfadi-vm

Edit Web Filter Profile

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web filtering service.
Traffic may be blocked if this option is enabled.

New/Edit Quota

Category: [] +

Quota Type: Time Traffic

Total quota: 0 hour(s) 5 minute(s) 0 second(s)

OK Cancel

نقوم بتحديد نوع ال Quota هل بالوقت ام بالترافيك (بالحجم)

ونقوم بتحديد ال category المراد تطبيق quota عليها .

أساسيات فورتى جيت

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web service.
Traffic may be blocked if this option is enabled.

Name	Action
entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow
Job Search	Allow
Medicine	Allow
News and Media	Monitor
Social Networking	Monitor
Political Organizations	Allow
Reference	Allow

Category Usage Quota

Create New Edit Delete

Category Total quota

Category

Quota Type: Time Traffic

Total quota: 0 hour(s) 5 minute(s) 0

OK Cancel

Category: News and Media
Rating: G
Group: General Interest - Personal
Description: Sites that offer current news and opinion, including those sponsored by newspapers, general-circulation magazines, or other media. This category includes TV and Radio sites, as long as they are not exclusively for entertainment purpose, but excludes academic journals. Alternative Journals: Online equivalents to supermarket tabloids and other fringe publications.
Examples: cnn.com, gmw.cn, ifeng.com, bbc.co.uk

Search

FORTIGUARD WEB FILTER CATEGORY

- Adult/Feature Content (15)
- Abortion
- Advocacy Organizations
- Alcohol
- Alternative Beliefs
- Dating
- Gambling
- Lingerie and Swimsuit
- Marijuana
- Nudity and Risque
- Other Adult Materials
- Pornography
- Sex Education
- Sports Hunting and War Games
- Tobacco
- Weapons (Sales)
- General Interest - Personal (2)
- News and Media
- Social Networking
- Potentially Liable (1)
- Extremist Groups
- Unrated (1)
- Unrated

FortiGate VM64 maradi-vm

Edit Web Filter Profile

FortiGuard category based filter

Warning: This device is not licensed for the FortiGuard web service.
Traffic may be blocked if this option is enabled.

Category: News and Media Social Networking

Quota Type: Time Traffic

Total quota: 0 hour(s) 15 minute(s) 0 second(s)

OK Cancel

تم السماح 15 دقيقة لليوزر من الوصول الى مواقع الاخبار ومواقع التواصل الاجتماعي فقط ...
حيث بمجرد انتهاء الـ 15 دقيق للموظف فانه سيتم عمل Block لتلك المواقع مباشرة ..

أساسيات فورتني جيت

- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
 - AntiVirus
 - Web Filter
 - DNS Filter
 - Application Control
 - Intrusion Prevention
 - SSL/SSH Inspection
 - Web Rating Overrides
 - Web Profile Overrides
 - Custom Signatures
- VPN
- User & Device
- Log & Report
- Monitor

Traffic may be blocked if this option is enabled.

Allow Monitor Block Warning Authenticate

Name	Action
Entertainment	Allow
Arts and Culture	Allow
Education	Allow
Health and Wellness	Allow
Job Search	Allow
Medicine	Allow
News and Media	Monitor
Social Networking	Monitor
Political Organizations	Allow
Reference	Allow

Category Usage Quota

Create New Edit Delete

Category	Total quota
News and Media Social Networking	15 minute(s)

Warning: معناها بأنه تم اغلاق الموقع في الشبكة حيث ستظهر لك رساله تحذيره لليوزر توضح بان الموقع الذي قمت بطلبه محجوب لو تريد فتحه سوف تفتحه على مسؤوليتك وستصبح متراقب من قبل الفورتني جيت

حيث سيظهر رساله تحذيره كل فتره تحددها انت بأن الموقع متراقب من قبل مدير الشبكة لأنك فتحن موقع مندرج تحت category معمول لها Warning .

حيث مثلا سوف نعمل warning للـ category المسماة Alcohol فمجرد تنقر بالزر الأيمن على الـ Alcohol وتختار الـ action=warning فإنه سوف تفتح لك نافذه كم بالتالي

حيث كل 5 دقائق يظهر لك رساله تحذيره لو انت لا زلت فاتح أي موقع ضمن التصنيف المحدد سابقا (Alchol).

حيث لو قام المستخدم بفتح أي موقع ينتهي لهذا التصنيف سوف تظهر له رساله ال Block كما بالصورة التالية



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy.

URL: almokhtsar.com/
Category: News and Media
Client IP: 192.168.1.111
Server IP: 174.128.176.156
User name: tamer
Group name: WF

To have the rating of this web page re-evaluated [please click here](#).



فلو تريد ان تفتح الموقع فقم باختيار الخيار Proceed .

فبعد 5 دقائق سوف يتم اغلاق الصفحة ثم ظهور رساله ال Web Page Blocked فلو تريد ان تفتح

الموقع على مسؤوليتك فثم باختيار Proceed.

حيث يصبح كل المواقع المندرجه متراقبه عبر الفورتني جيت ويمكن استعراض كل ال logs كما بالتالي :

Authenticate : متى تريد ان تجعل البورتال يطلب يوزرنيم وباسورد ؟

حيث أي احد يحاول يفتح أي موقع يندرج تحت ال category المعمول لها Authenticate فإنه سوف

يطلب منه يوزرنيم وباسورد .

أساسيات فورتى جيت

The screenshot shows the 'Edit Web Filter Profile' interface. The left sidebar has 'Web Filter' selected. The main area shows a profile named 'Monitor Social networking&News'. A warning message is present. Below, a table lists categories and their actions:

Name	Action
Security Risk	Allow
General Interest - Personal	Allow
Advertising	Allow
Brokerage and Trading	Allow
Games	Authenticate
Web-based Email	Monitor
Entertainment	Block
Arts and Culture	Warning
Education	Authenticate
Health and Wellness	Allow

قمنا بإنشاء action نوعها Authenticate على الـ category المسماة Games

The screenshot shows the 'Edit Filter' dialog box. The 'Warning Interval' is set to 5 minutes. The 'Selected User Groups' field is empty, and a red arrow points to it. A dialog box is open, asking for user groups to select from.

حيث أي يوزر من الجروب المختاره سوف يفتح موقع من مواقع الألعاب سوف يظهر له نافذه البورتال (يوزرنيم وباسورد).. الخ

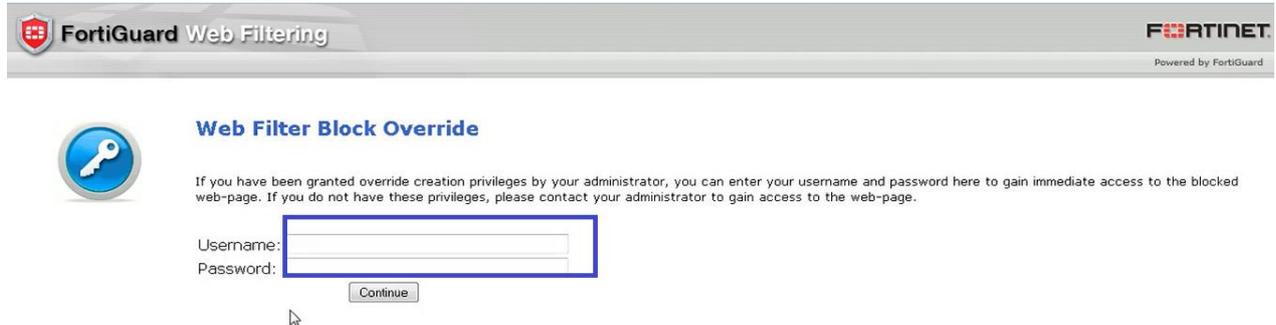
الخلاصة :

أساسيات فورتى جيت

أي احد يحاول يوصل للمواقع المدرجه تحت تصنيف الألعاب الذي انت عامل عليها authenticate فانه سوف يطلب منه يوزرنيم وباسورد. اي كل 5 دقائق وف يظهر له البورتال اللي بيطلب منه اليوزرنيم والباسورد لكي يعمل reauthentication ويستطيع الوصول الى تلك المواقع ...



ثم بعد النقر على الزر proceed فإنه سوف تظهر لك الشاشة التالية



فيجب عليك ادخال اليوزرنيم والباسورد لأحد اليوزرات التي تنتهي للجروب المحدده.

ملاحظة :

ال warning يعتبر نفس ال authenticate الا انه في حالة ال authenticate يطلب منك يوزرنيم وباسورد

..

أساسيات فورتني جيت

أحيانا لا يعمل معي الـ web filter by category وخصوصا الـ warning لذا يجب عليك التأكد بأنك قمت بالأشياء التالية لكي تعمل معك بشكل صحيح :

➤ توجد اعدادات معينة لـ ssl أي للمواقع التي تكون https وليس http يجب ان تكون مضبوط الاعدادات بشكل سليم لكي يعمل معك الـ web filtering أيضا يجب ان تكون عامل الشهادة certificate بشكل سليم ومستوردها على متصفحات واجهزه الكلايننت ..

The screenshot shows the 'Edit SSL/SSH Inspection Profile' configuration page. The 'Name' field is set to 'deep-inspection'. The 'Inspection method' is set to 'Full SSL Inspection'. The 'CA certificate' is set to 'Fortinet_CA_SSL'. The 'Protocol Port Mapping' section shows ports for HTTPS (443), SMTPS (465), POP3S (995), IMAPS (993), and FTPS (990) all enabled. The 'Exempt from SSL Inspection' section has 'Reputable websites' disabled.

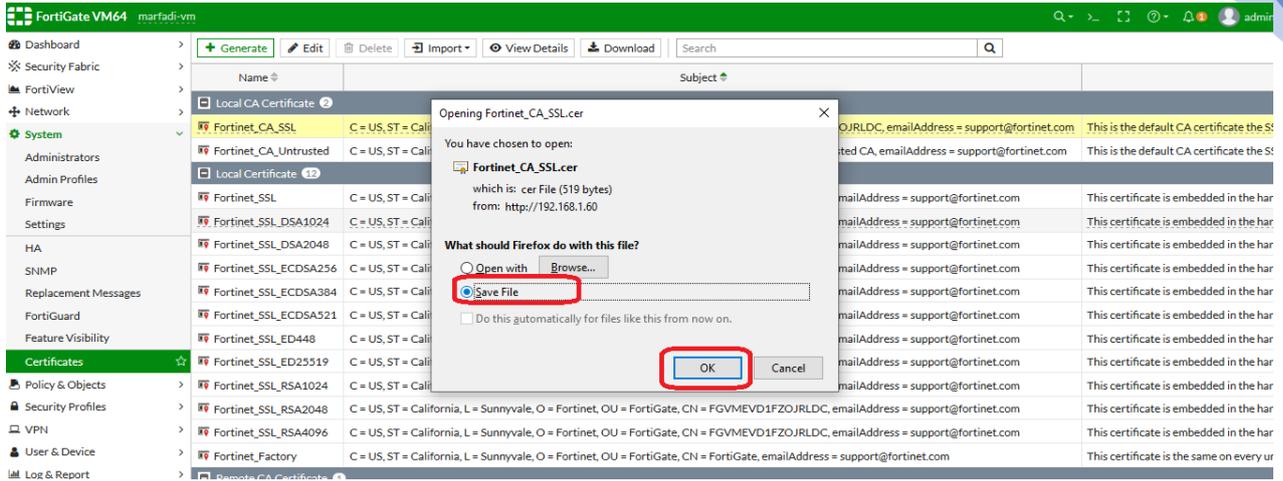
ننشئ ssl/ssh inspection ونجعلها Full SSL Inspection ثم نختارها في البوليسي كما بالصورة التالية :

The screenshot shows the 'Edit Policy' configuration for a Fortinet device. The 'Service' is set to 'ALL', 'Action' is 'ACCEPT', and 'Inspection Mode' is 'Flow-based'. Under 'Security Profiles', 'Web Filter' is set to 'WEB default' and 'SSL Inspection' is set to 'SSL deep-inspection'. A red arrow points to the 'SSL deep-inspection' dropdown, and a text box explains: 'This SSL profile uses full SSL inspection. End users will likely see certificate warnings unless the certificate is installed in their browser.'

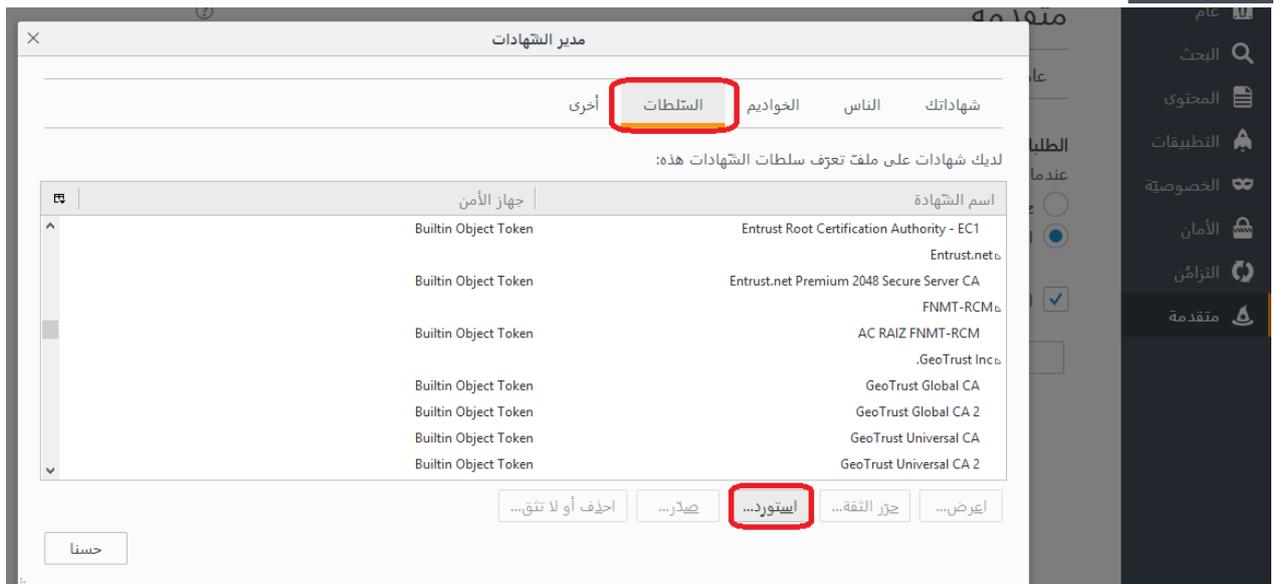
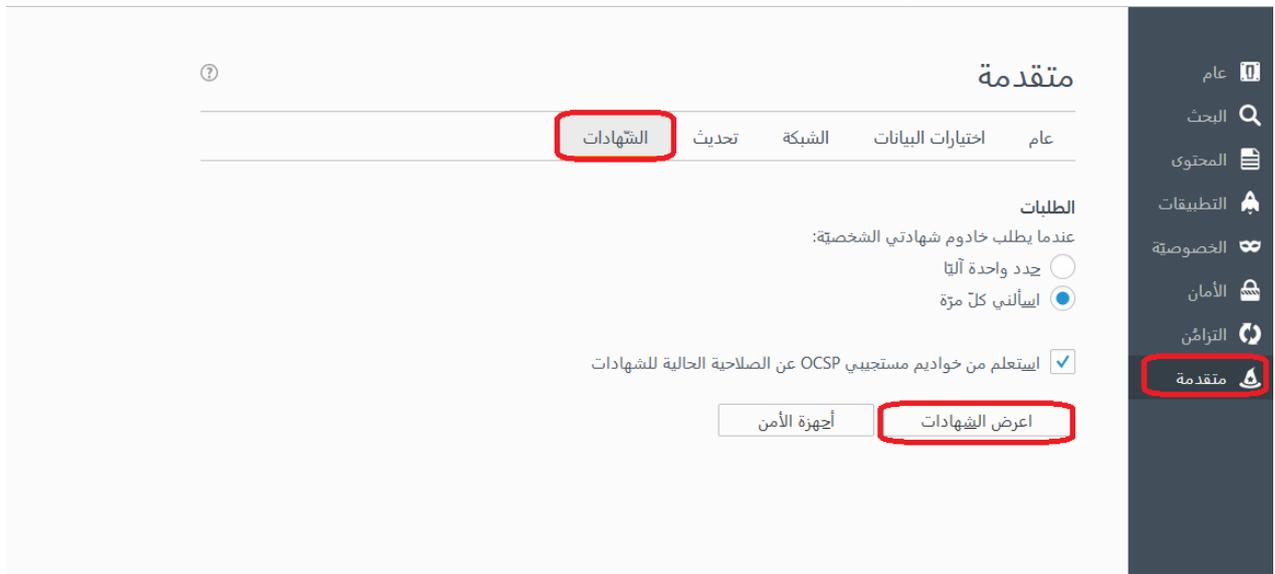
نلاحظ بأننا اخترنا البروفایل المسمی deep-inspection والذي تم تجهيزه سابقا ونلاحظ بأن هناك hint يقول فيها عند اختيار full SSL inspection فان اليوزرات سوف يحتاجوا ان تقوم باستيراد تلك الشهادة على متصفحاتهم ..

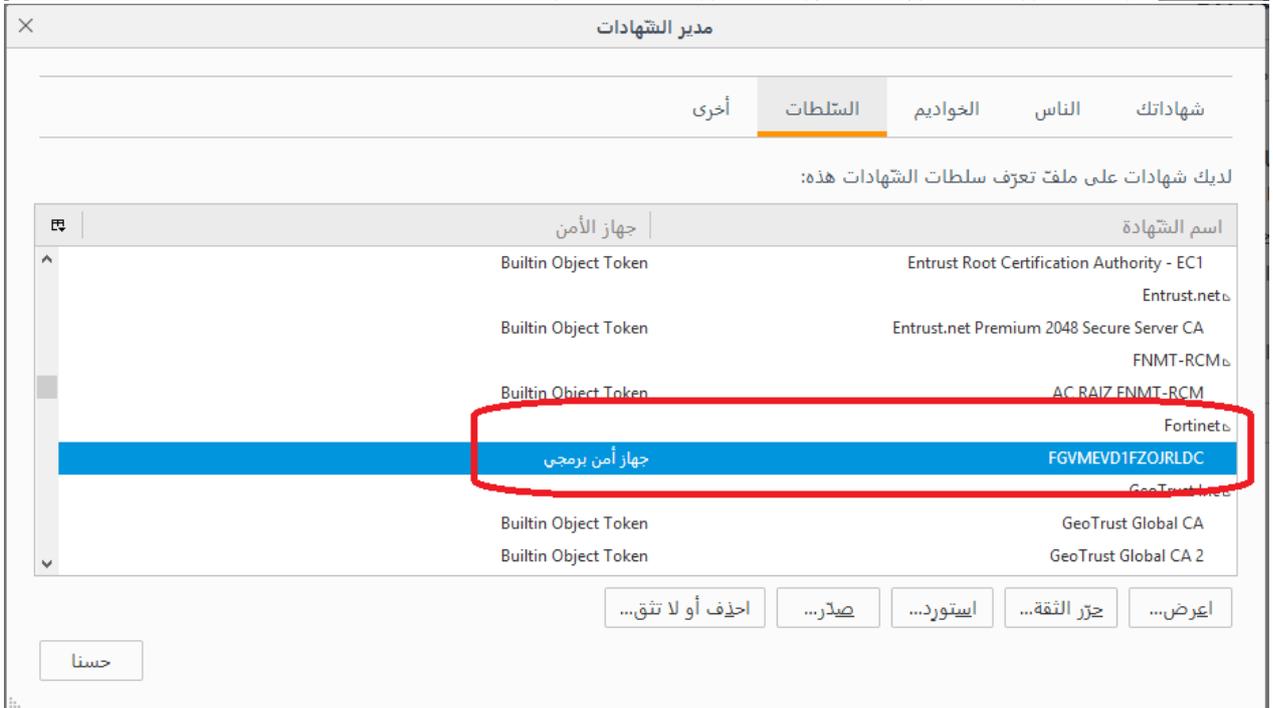
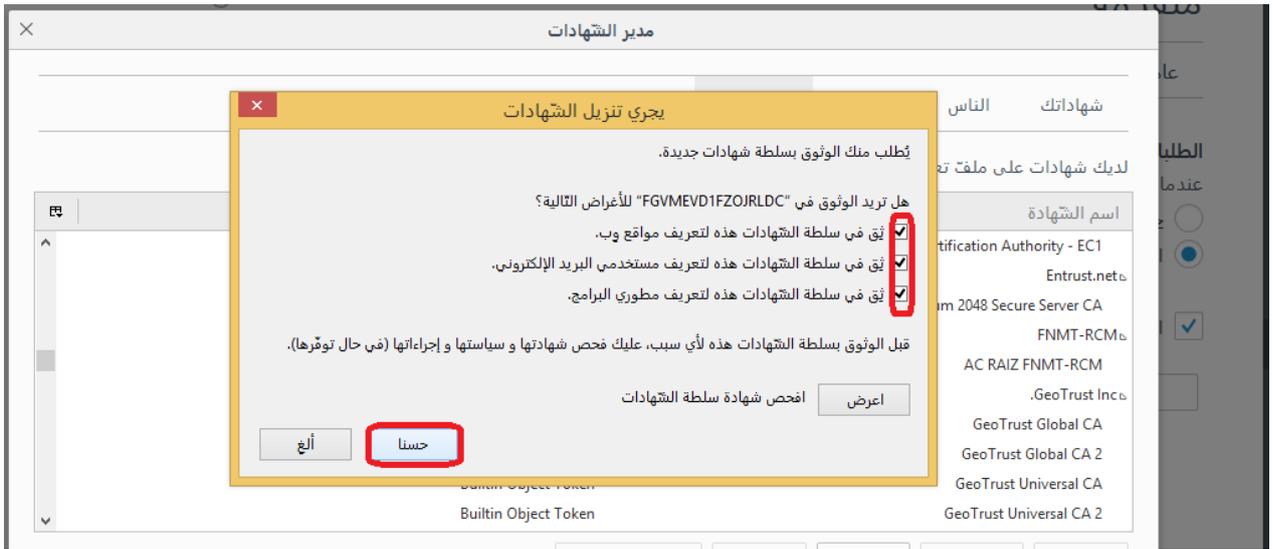
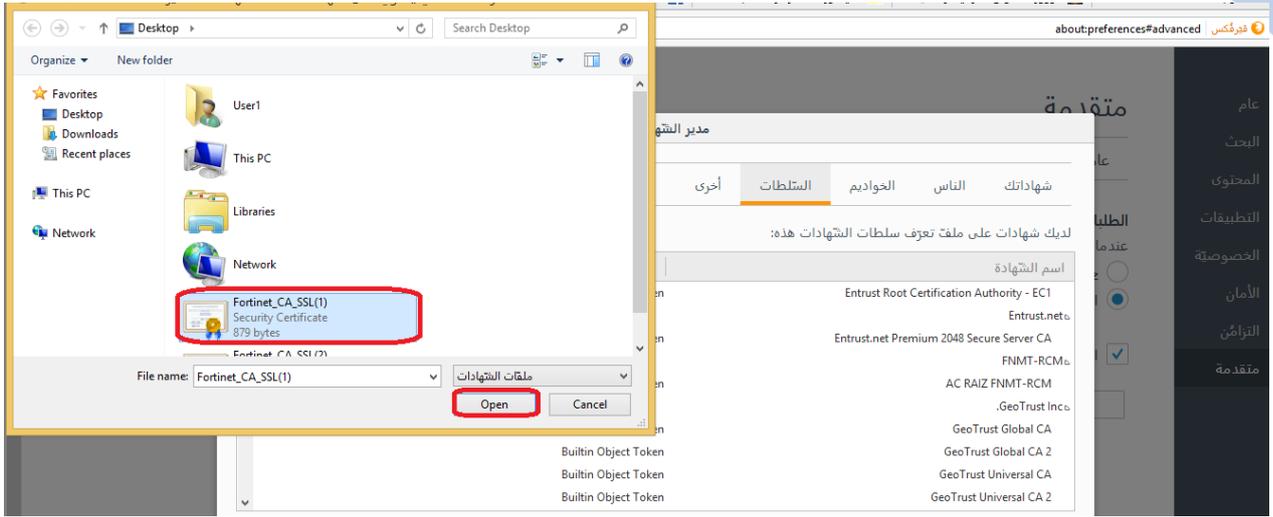
الآن سوف نقوم بتصدير الشهادة من الفورتني جيت كالتالي :

The screenshot shows the 'Certificates' management interface. The 'Certificates' section is highlighted in green. A table lists various certificates, with 'Fortinet_CA_SSL' highlighted in red. The 'Download' button for this certificate is also highlighted in red. The table columns are 'Name' and 'Subject'. The 'Fortinet_CA_SSL' row shows the subject: 'C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Authority, CN = FGVMEVD1FZOJRLDC, emailAddress = support@fortinet.com'. A note next to it says: 'This is the default CA certificate the SSL'.



نقوم بنسخها على اجهزه الموظفين ثم نستوردها على متصفحاتهم كما بالخطوات التالية



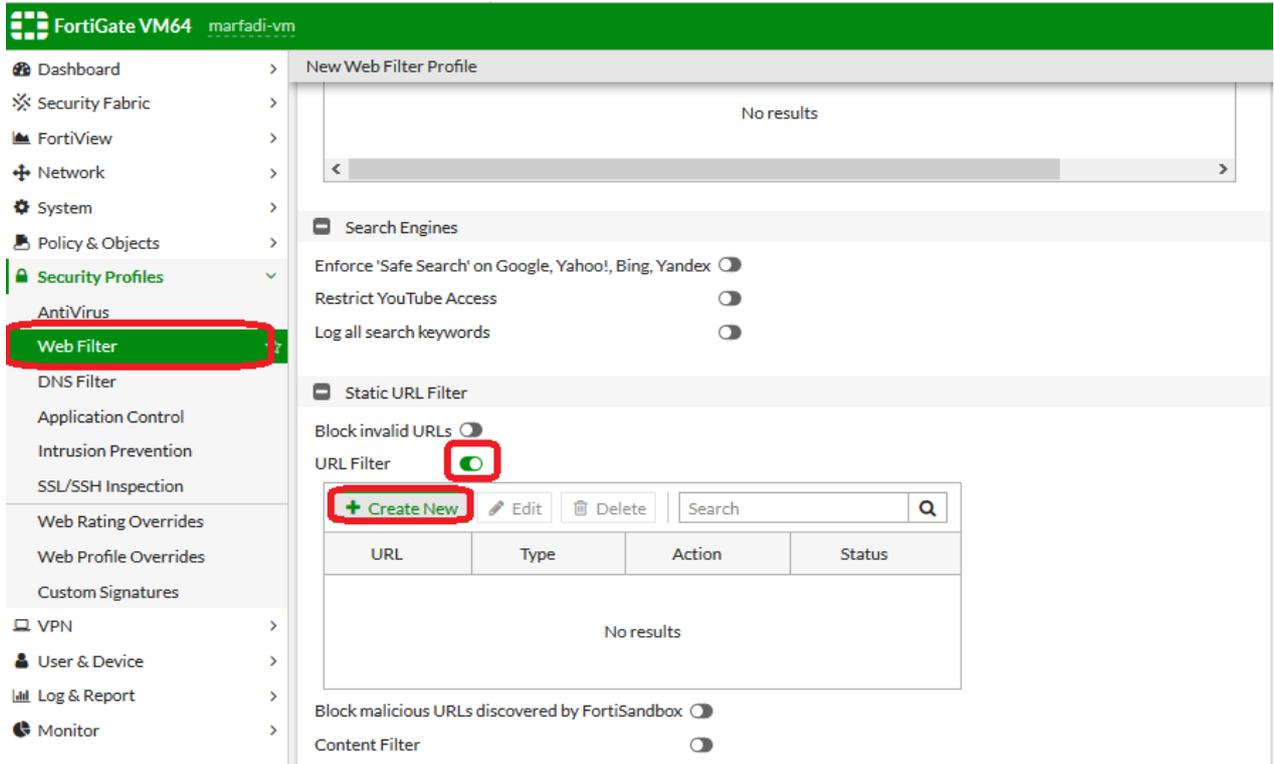


نلاحظ بالصورة أعلاه بأن الشهادة تم استيرادها بنجاح وعند النقر عليها نقرتين تظهر لك تفاصيل الشهادة..

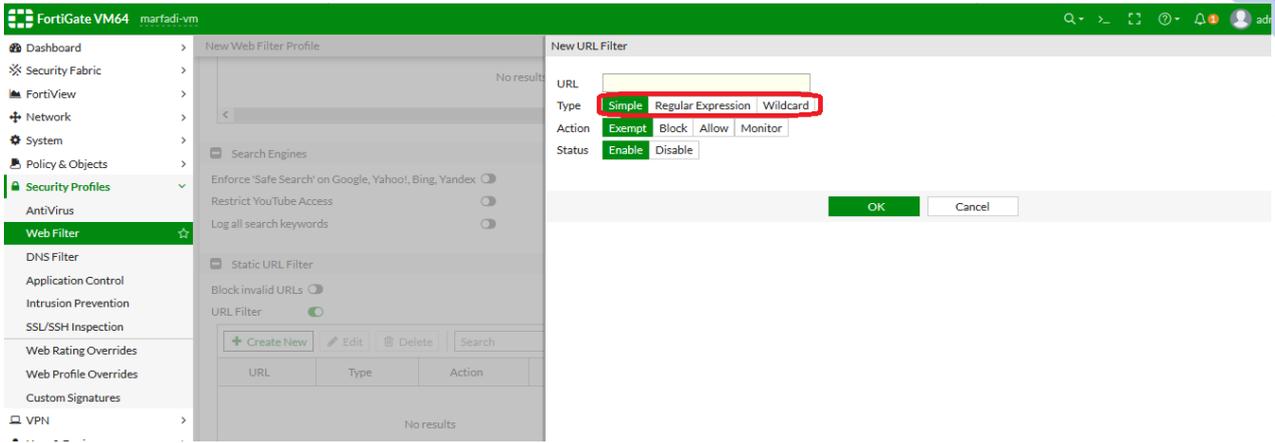


Web URL filtering ❖

توجد 4 أنواع مهمه في web URL filter



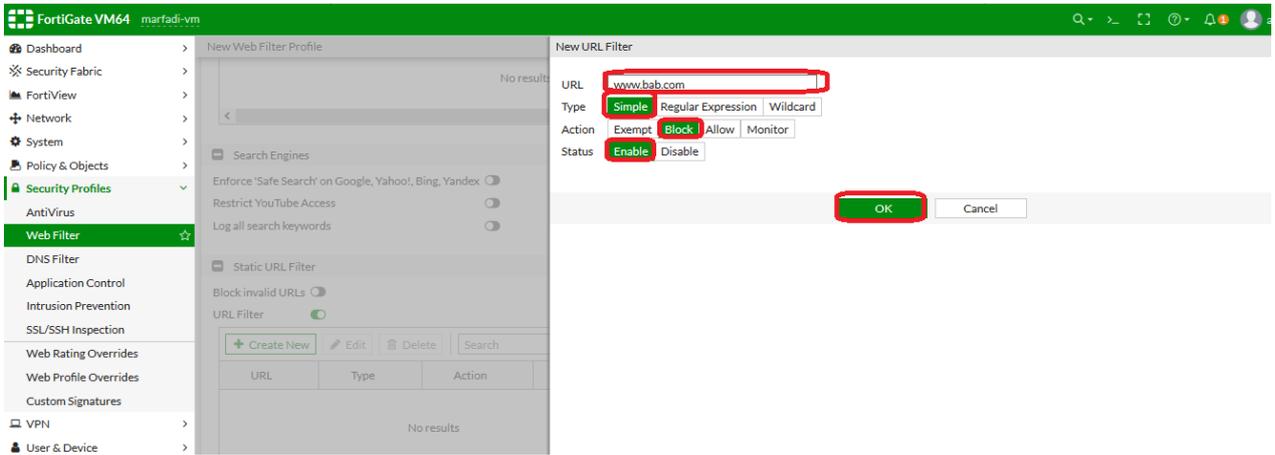
قمنا بإنشاء بروفایل جديد وتم تفعيل الخيار URL Filter ثم نقوم بإنشاء ال static url كما بالصورة ادناه



يوجد لدينا عدة أنماط (أنواع-اشكال-طرق) تكتب فيها المواقع لكي تطبق عليها action معين .

(١) Simple : تكتب ال url لموقع صراحة كالتالي

www.bab.com او bab.com كل يؤدي نفس الغرض ..



أساسيات فورتى جيت

The screenshot displays the FortiGate VM64 configuration interface. The left sidebar shows the navigation menu with 'Web Filter' highlighted in green. The main content area shows the 'Static URL Filter' configuration. The 'URL Filter' section is active, and a table lists the filtered URLs:

URL	Type	Action	Status
www.bab.com	Simple	Block	Enable

Below the table, the 'Rating Options' section is visible, with 'Allow websites when a rating error occurs' and 'Rate URLs by domain and IP Address' options.

The bottom screenshot shows the 'Web Filter' configuration table with 'profile.1' highlighted in yellow:

Name	Comments	Ref.
Web-sites		0
default	Default web filtering.	0
monitor-all	Monitor and log all visited URLs, flow-based.	0
profile.1		0
wifi-default	Default configuration for offloading WiFi traffic.	1

كما

بالصورة أعلاه تم انشاء البروفايل باسم 1 profile

أساسيات فورتى جيت

The screenshot shows the 'Edit Policy' configuration for an IPv4 Policy. The 'Action' is set to 'ACCEPT'. The 'Inspection Mode' is 'Flow-based'. Under 'Firewall / Network Options', 'NAT' is disabled, and 'IP Pool Configuration' is set to 'Use Outgoing Interface Address'. Under 'Security Profiles', 'Web Filter' is enabled and set to 'WEB profile 1'. 'SSL Inspection' is set to 'deep-inspection'. 'Logging Options' are set to 'Security Events' and 'All Sessions'.

تطبيق البوليسي وتم اختيار البروفايل 1 في Web Filter

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
4	private	all	all	always	ALL	ACCEPT	Enabled	WEB profile 1 SSL deep-inspection	UTM	249.13 MB
3	public	Subnet1	all	always	ALL	DENY			Disabled	269.52 KB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

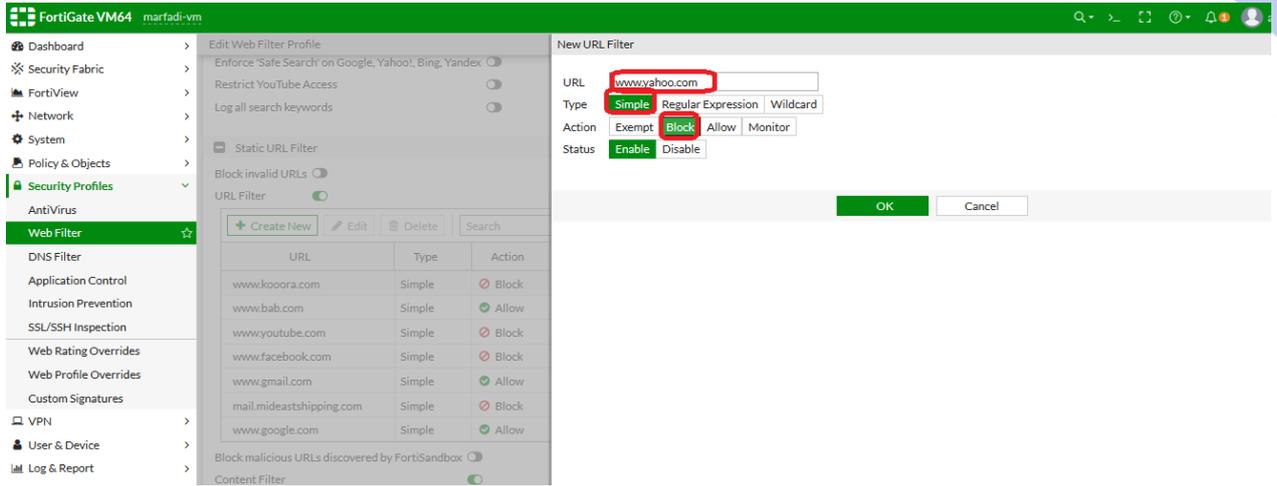
توجد عدة طرق للتحكم بالويب بواسطة Static Url :

الطريقة الأولى :

ملاحظة :

لوقمت بإغلاق للموقع www.yahoo.com

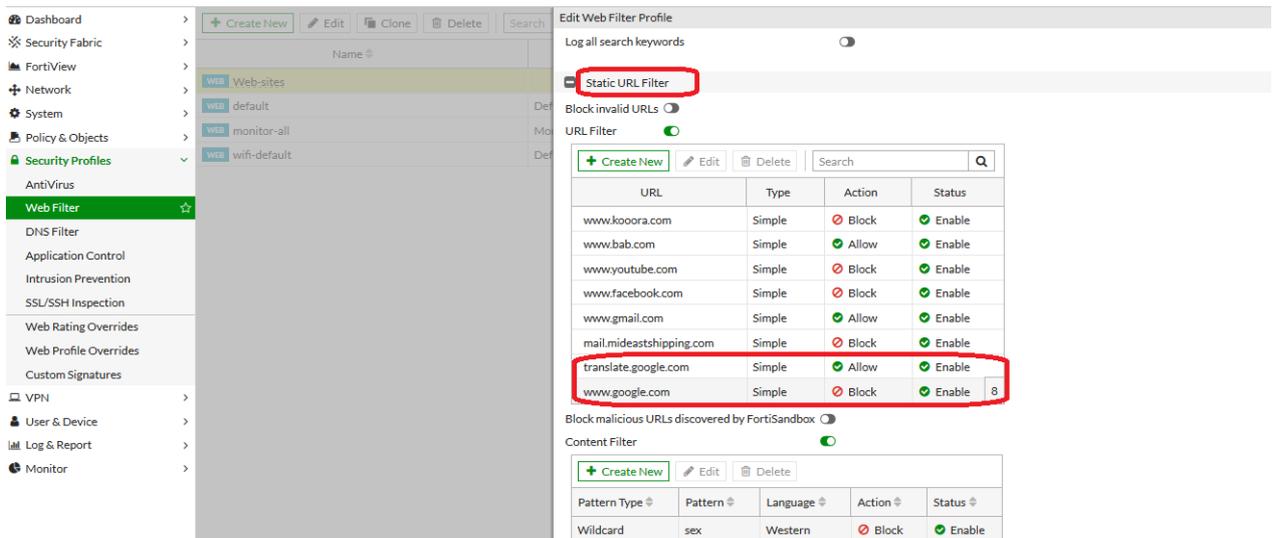
فإن أي موقع يندرج تحت هذا الموقع سيتم اغلاقه أيضا كما بالصورة ادناه



الطريقة الثانية :

اما في حالة تريد بالتحكم بموقع معين (صفحة معينة) في الموقع عن طريق المسار او ما يسمى الـ URL مثلا السماح فقط بصفحة معينة مثلا translate.google.com وهو مترجم جوجل ومنع جوجل بشكل كامل

..

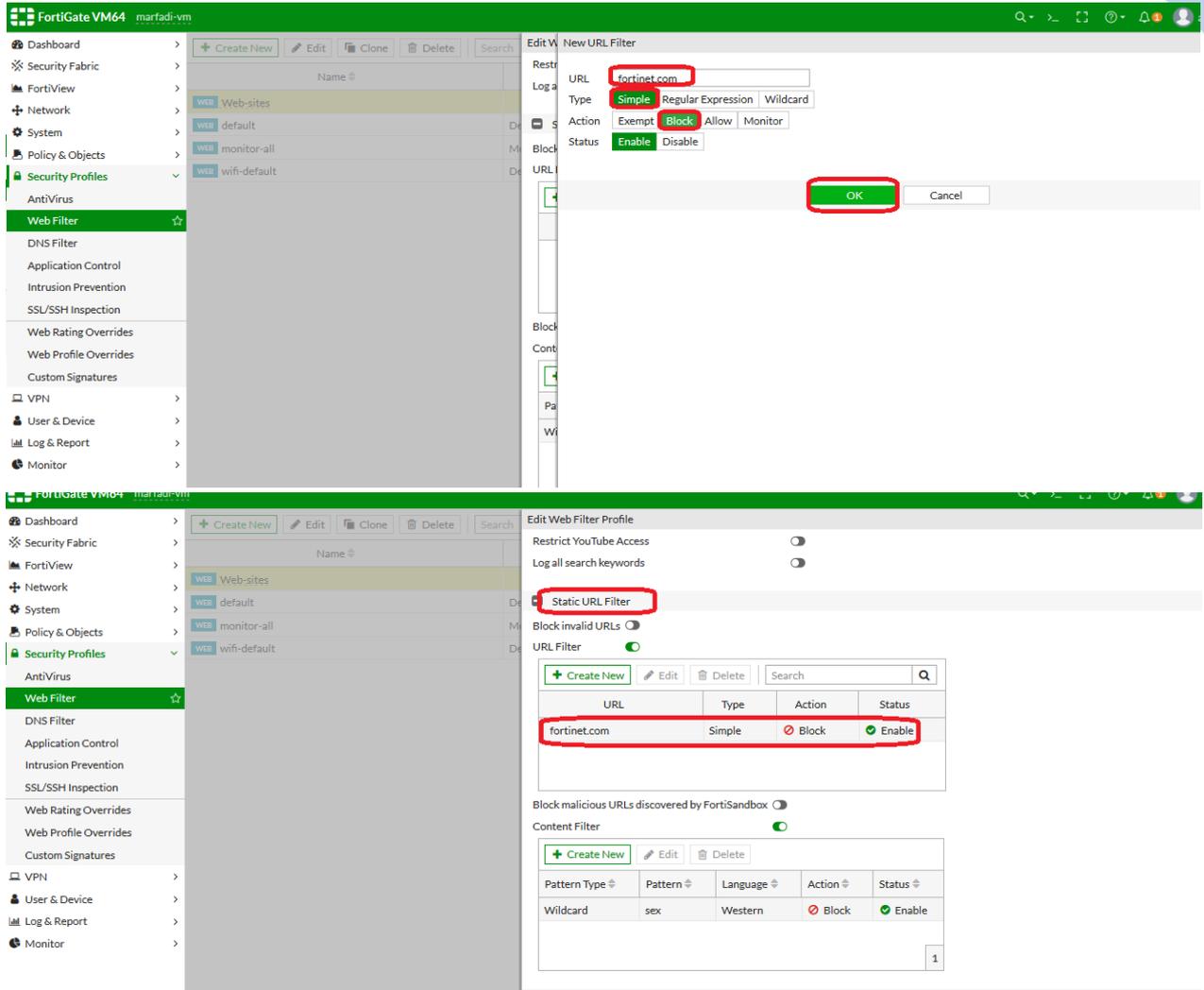


حيث قمنا بالسماح لمترجم جوجل فقط واغلاق كل شي في جوجل ...

الطريقة الثالثة :

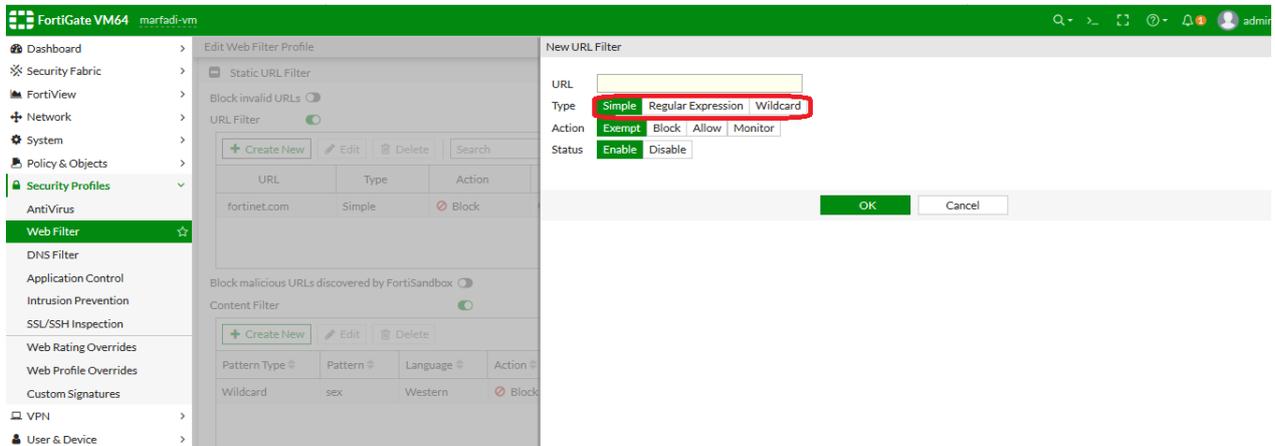
اما في حالة تريد ان تقوم بالتحكم باي موقع ينتهي مثل www.fortinet.com بغض النظر عن أي صفحة تحت هذا الموقع (Sub domain) لهذا الموقع مثل support.fortinet.com حيث انه يندرج تحت

- الموقع www.fortinet.com



حيث أي sub domain يندرج تحت الموقع Fortinet.com مثل support.fortinet.com او غيرها سيتم اغلاقه بغض النظر عن اسم الموقع ...

توجد 3 أنماط تستطيع ان اتحكم باي موقع في الويب فلتر:



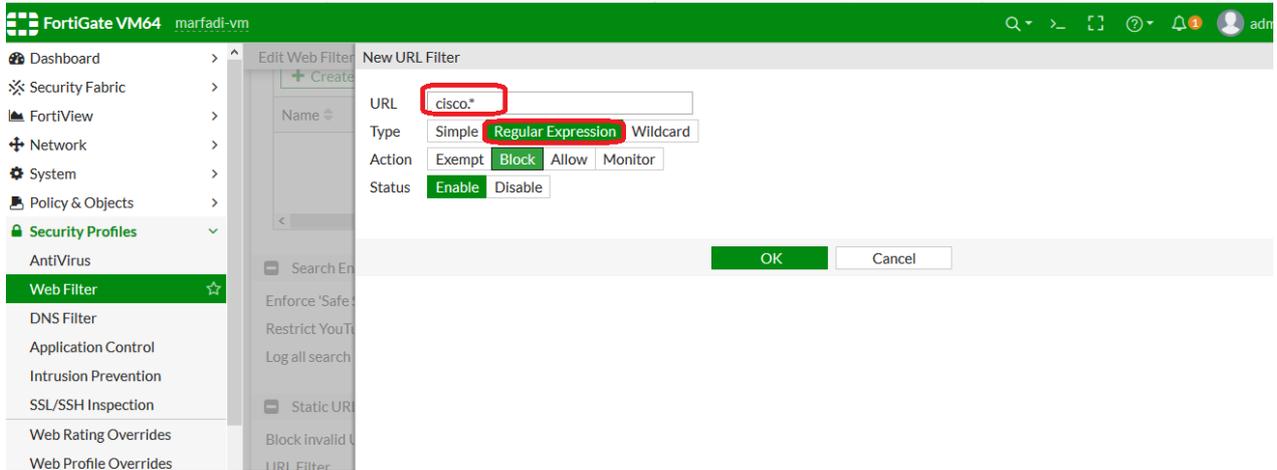
وهي Simple -Regular Expression-Wildcard

اما نكتب بالصيغه www.bab.com او bab.com مباشرة

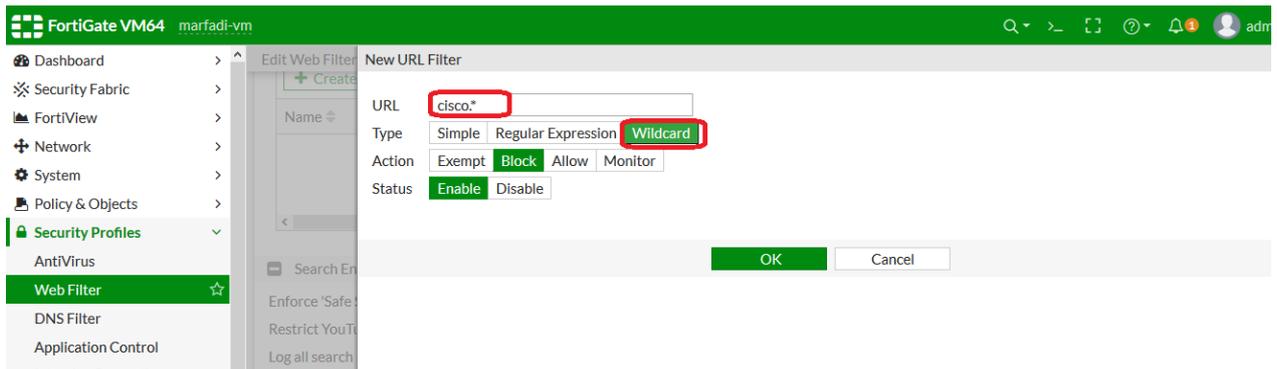
اما الأنواع **Regular Expression** و **Wildcard** فإنه تستخدم عندما تريد استخدام رموز

مثلا لو اردت التحكم بالدومين المسمى **cisco** بغض النظر هل هو cisco.com او cisco.net حيث كليهما ييفتح لك نفس الموقع ..

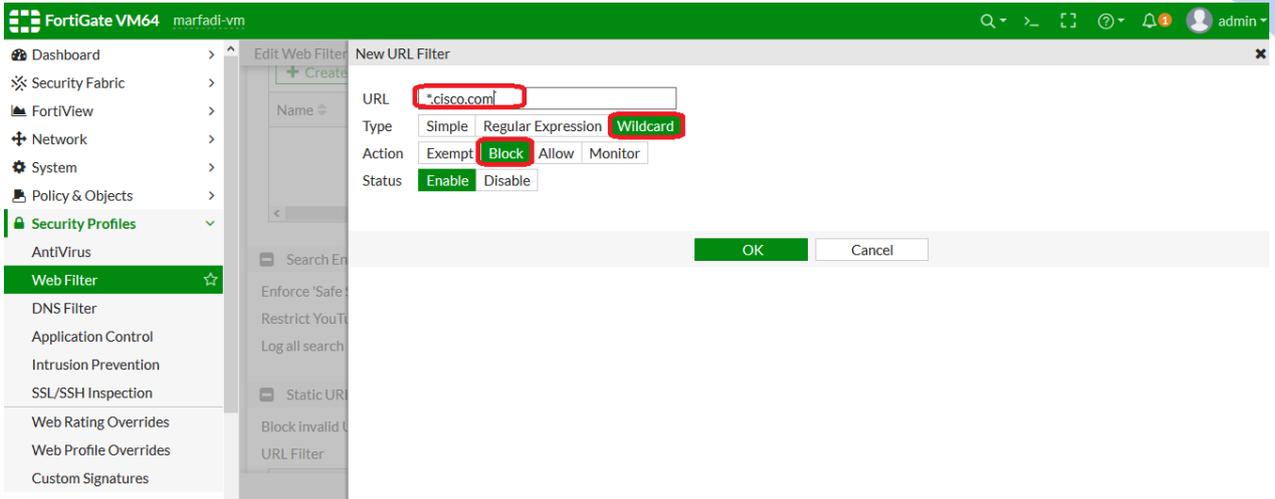
فبواسطة **Regular Expression** او **Wildcard** يمكنك التحكم بالدومين المسمى **cisco** بغض النظر هل هو .com او .net او .org كما بالصورة ادناه



او

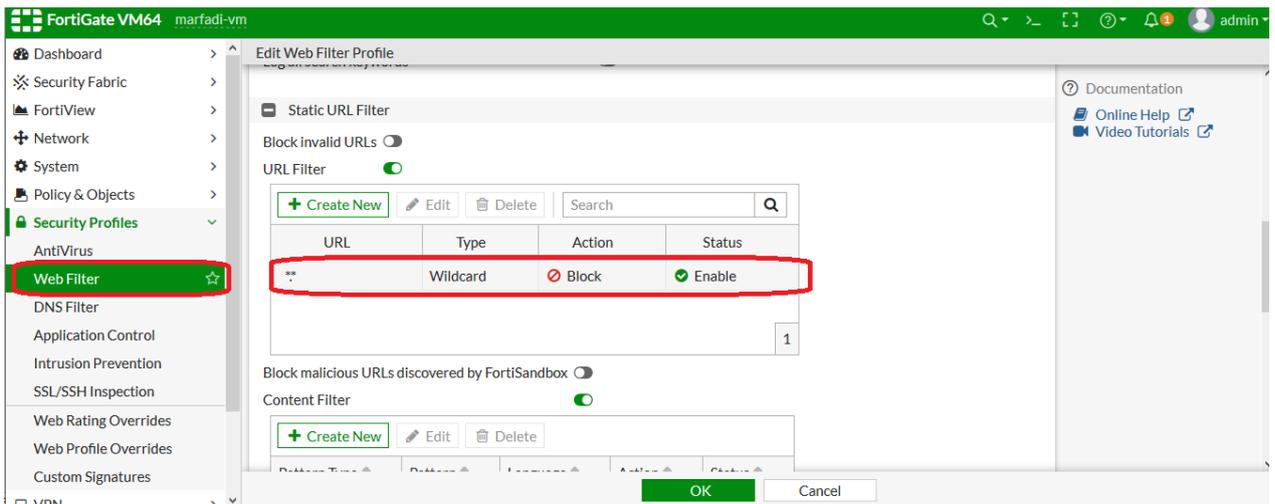
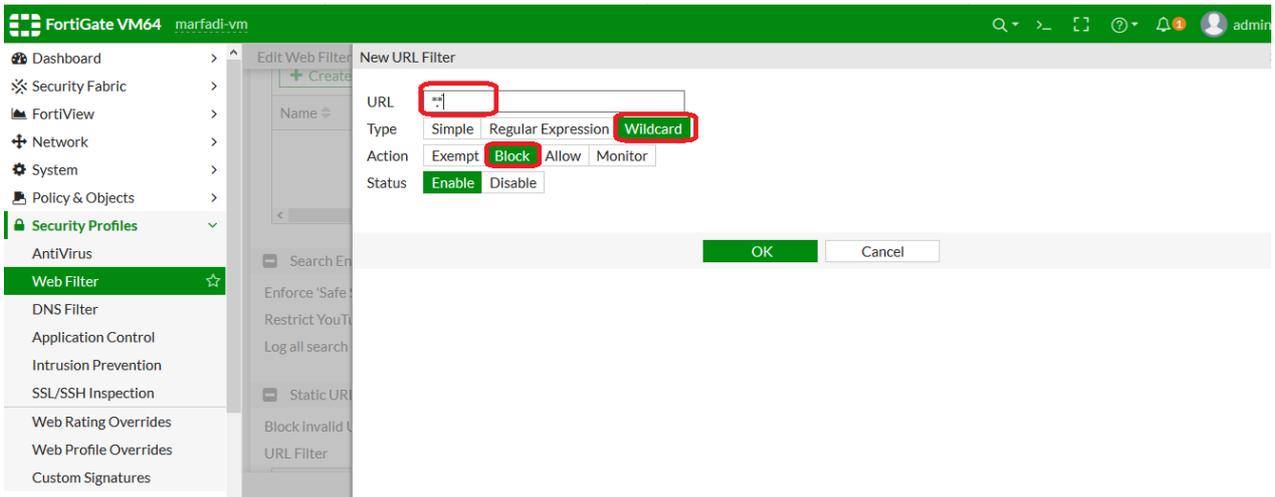


يمكن استخدام الرموز بالطريقة التالية
***.cisco.com** أي ان أي sub domain سوف يتم التحكم به ..
كما بالصورة التالية



فلو اردت ان تقوم بإغلاق كل المواقع

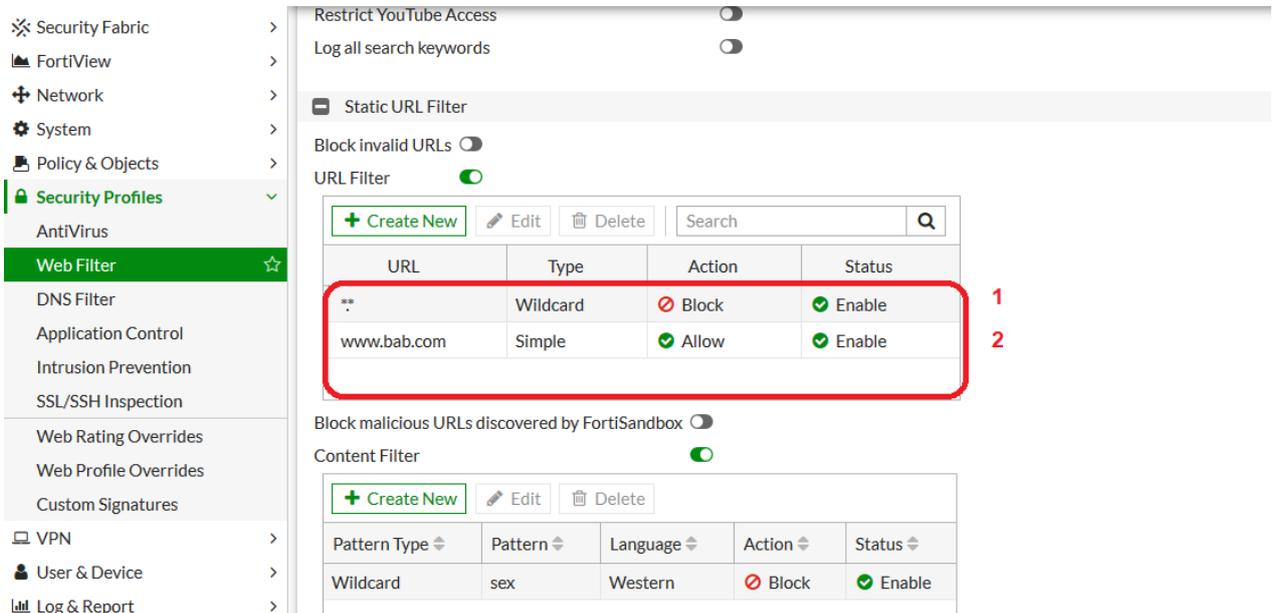
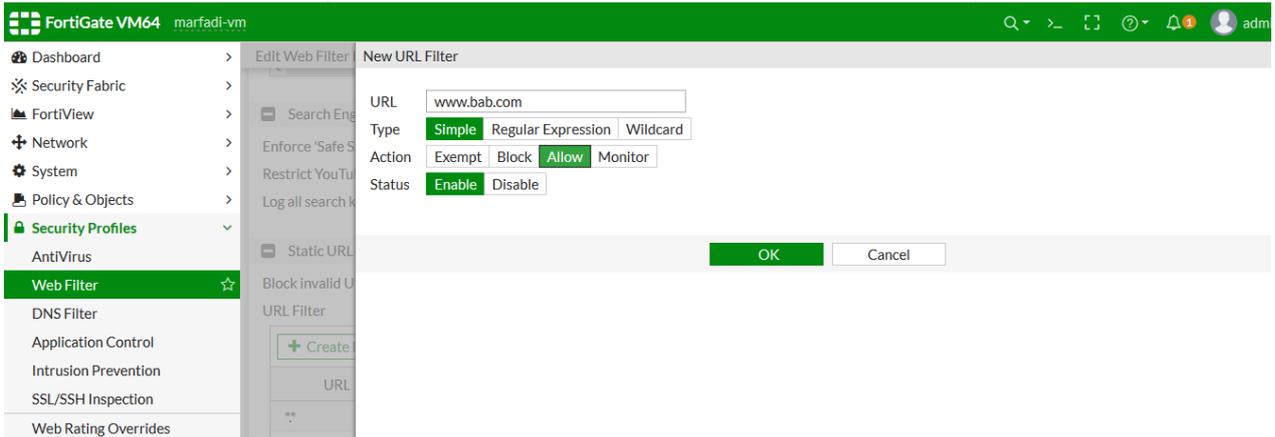
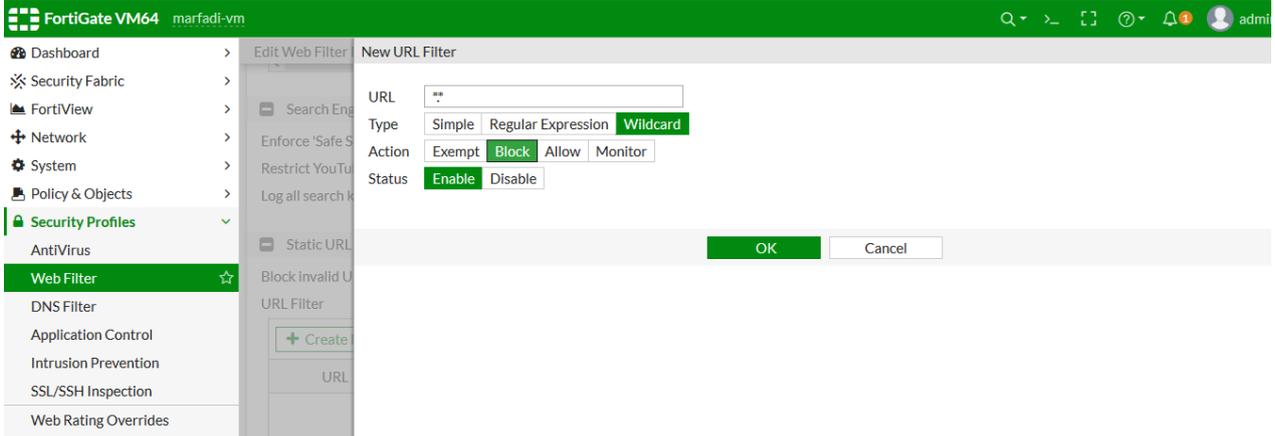
.* أي قم بالتحكم باي موقع تحت أي شي ..



ترتيب ال URL لها اهميه ..

حيث يتم تطبيق ال URL من الأعلى الى اسفل (يبدأ بتطبيق المواقع من الأعلى وهكذا) ..

مثال لو اردت اغلاق كل المواقع ماعدا صفحة www.bab.com



فبحسب الترتيب أعلاه فإنه سوف يتم اغلاق كل المواقع بما فيها الموقع www.bab.com اما لوقمنا بإعادة ترتيب ال URL Filter كما بالصورة التالية

URL	Type	Action	Status
www.bab.com	Simple	Allow	Enable
*	Wildcard	Block	Enable

فأن الموقع www.bab.com سوف يكون متاح وسيتم اغلاق باقي المواقع كامله ..
لذا ترتيب ال URL مهم جدا جدا وهو نفس فكره ال Policy حيث يتم تطبيقها من اعلى الى اسفل ..

Web content filter

عبارة عن عملية التحكم بمحتوى الموقع (صفحات الانترنت) بناء على الكلمات او الجمل او الرموز التي تكون داخل الصفحة .

مثلا لو كانت الصفحة تحتوي على كلمة sex اعمل لها Block حيث ان جهاز الفورتى جيت يعمل scan للصفحة بحيث لو وجد الكلمة التي يبحث عنها فإنه يقوم بتطبيق action معين .
بشرط ان عملية الفحص تصل الى score معين حيث يعرف ال score بانها قيمه او رقم معين لكل كلمة او جملة او رمزا داخل الفورتى جيت فلتر ..
بحيث لو وصل مجموع ال score الى ال threshold فان الفورتى جيت سيقوم بتطبيق ال action المعين س واء allow او block اما اذا لم يصل ال score لهذا الموقع الى قيمه ال threshold فإن ال action لا يطبق ابدا على هذه الصفحة ...

ملاحظة :

أساسيات فورتى جيت

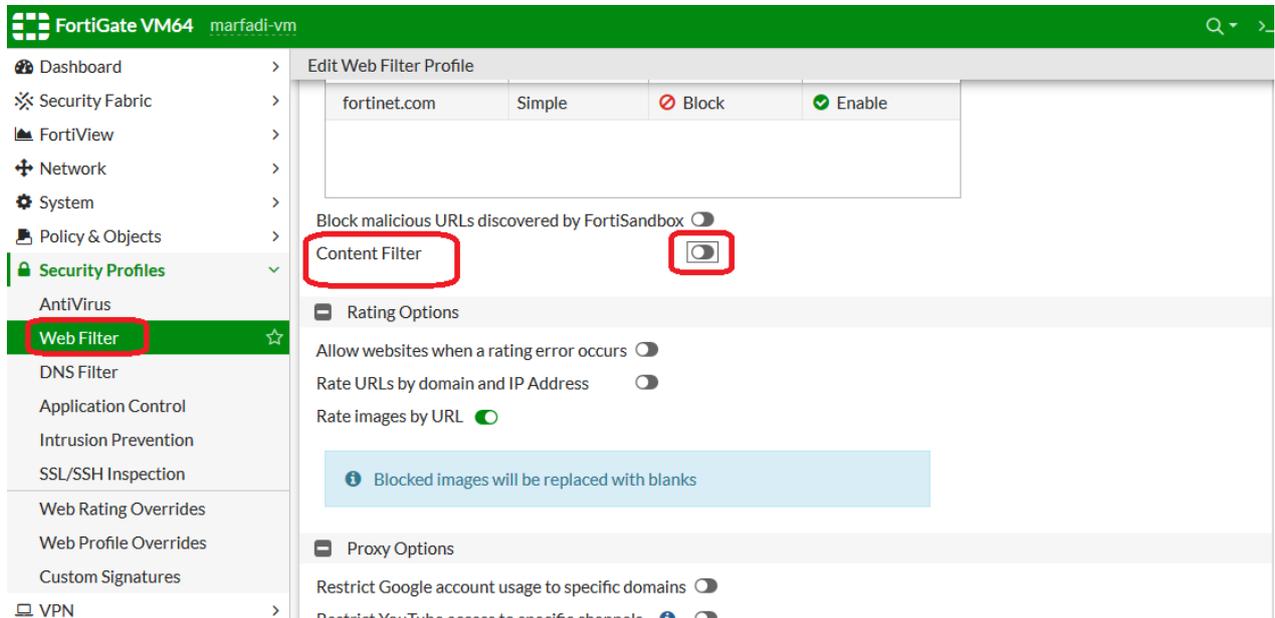
حيث ال threshold هو الحد وهي نتيجته جمع ال score للكلمات او الجمل او الرموز المفلتره على الفورتى جيت الى ان تصل للحد ..

حيث ال threshold يساوي 10

وال score لأي جملة او كلمه او رمز هو الرقم 10 .

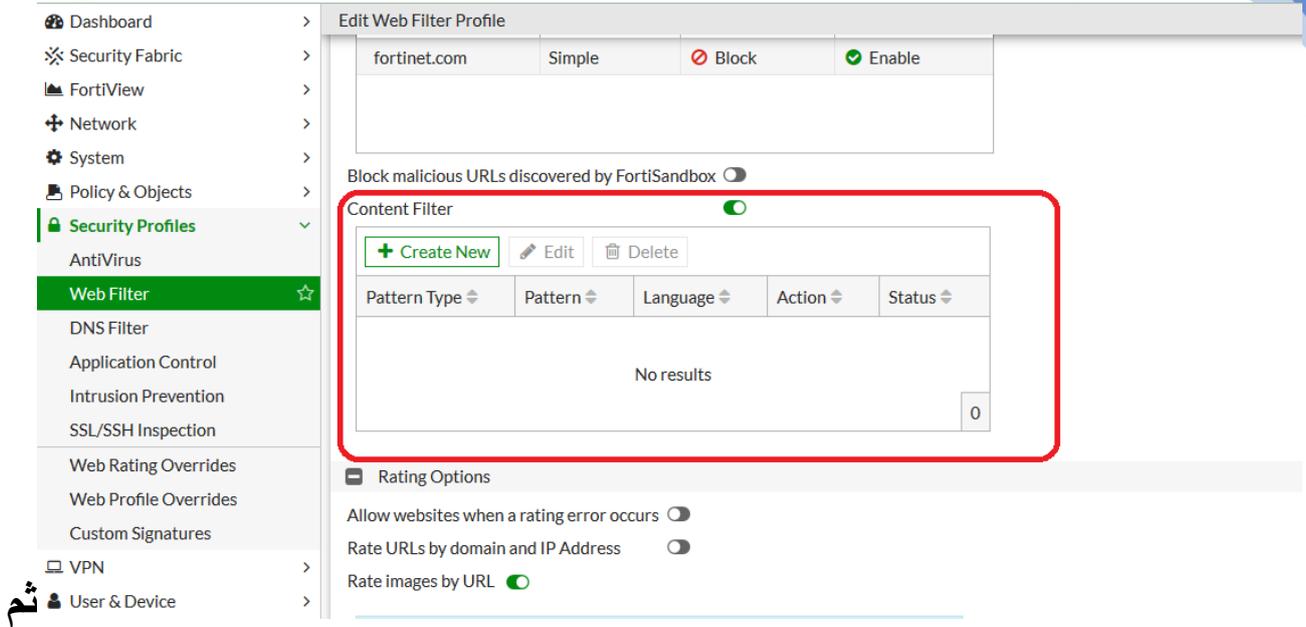
حيث أي كلمه انا عامل لها فلتر على الفورتى جيت مثلا (sex) فلوجودها فأن ال score سيكون 10 ولذا يتم الوصول الى قيمه ال threehold وبهذا سيتم تطبيق ال action على هذا الموقع .

ملاحظة: ال score موجود فقط على CLI وليس بواسطة ال GUI حيث يمكنك تعديل قيمه ال score حيث القيمة الافتراضية هي 10 ويمكنك تغييرها ..



نقوم بتفعيل الخيار Content Filter

أساسيات فورتى جيت



Dashboard > Edit Web Filter Profile

fortinet.com Simple Block Enable

Block malicious URLs discovered by FortiSandbox

Content Filter

+ Create New Edit Delete

Pattern Type	Pattern	Language	Action	Status
No results				

0

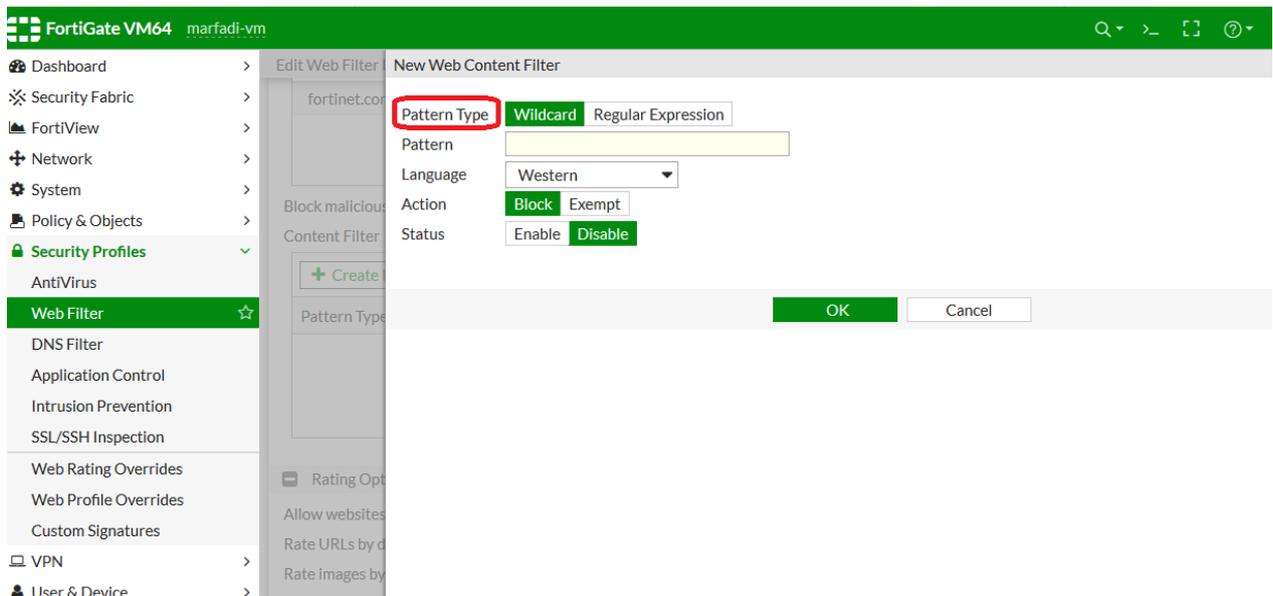
Rating Options

Allow websites when a rating error occurs

Rate URLs by domain and IP Address

Rate images by URL

create New



FortiGate VM64 marfadi-vm

Edit Web Filter New Web Content Filter

fortinet.com

Pattern Type Wildcard Regular Expression

Pattern

Language Western

Action Block Exempt

Status Enable Disable

OK Cancel

حيث **pattern Type** نحدد النمط الذي سوف اكتب فيها الكلمة التي سنقوم بعمل لها فلتره هل **Wildcard** ام **Regular Expression**

Wildcard : للتحكم بكلمه او جمله اورمزولديك الى حد 80 حرف فقط .

Regular Expression : حيث هنا يتم استخدام تعبيرات معينه في بعض لغات البرمجه ونحن في اغلب الأوقات نستخدم النمط الأول (**Wildcard**)

حيث ال **Pattern**: هي الكلمة او الجملة او الرمز الذي سوف تعمل لها فلتره .

Language: اللغة التي كاتب فيها الكلمة او الجملة ولا توجد اللغة العربية

Action: الحدث الذي سنقوم به عندما تصل ال score الى قيمه ال **threshold** .

Status: هل تريد تطبيقها ام لا

The screenshot shows the FortiGate VM64 web interface. The left sidebar is expanded to 'Security Profiles' > 'Web Filter'. The main area shows the 'New Web Content Filter' configuration page. The 'Pattern Type' is set to 'Wildcard', the 'Pattern' is 'sex', the 'Language' is 'Western', the 'Action' is 'Block', and the 'Status' is 'Enable'. Below the configuration form, there is a table showing the filter configuration for 'fortinet.com'.

Pattern Type	Pattern	Language	Action	Status
Wildcard	sex	Western	Block	Enable

أي صفحة تحتوي على كلمة sex سيتم عمل Block لها ..

طريقة تعديل قيمه ال score بوسطه ال **command line**

```
Connected

marfadi-vm # config webfilter content

marfadi-vm (content) # edit 1

marfadi-vm (1) # set name default

marfadi-vm (1) # config entries

marfadi-vm (entries) # edit sex

marfadi-vm (sex) # set
*pattern-type Banned word pattern type: wildcard pattern or Perl reg
*status Enable/disable banned word.
*lang Language of banned word.
*score Score, to be applied every time the word appears on a
*action Block or exempt word when a match is found.

marfadi-vm (sex) # show full-configuration
config entries
  edit "sex"
    set pattern-type wildcard
    set status enable
    set lang western
    set score 10
    set action block
  next
```

```
marfadi-vm (sex) # set score 9

marfadi-vm (sex) # show full-configuration
config entries
  edit "sex"
    set pattern-type wildcard
    set status enable
    set lang western
    set score 9
    set action block
  next
end

marfadi-vm (sex) # end
```

حيث تم الدخول الى وضع webfilter حيث سيتم التعديل على البروفايل المسمى Default وبالتحديد الكلمة sex والتي تم انشائها مسبقا في web filter content . حيث قمنا بإظهار الاعدادات السابقة عبر الامر show full-configuration للكلمة sex حيث نلاحظ بأن score=10 ثم نقوم بتعديل القيمة الى 9 ..

Application controller

عبارة عن التحكم بالتطبيقات (السوفتوير)(البرامج)على الشبكة .
حيث الفورتى جيت لديه الامكانيه بأنه يكتشف ويحلل أي ترافيك موجود في الشبكة اعتماد على
التطبيقات ويقوم باخذ action معين .

التطبيقات مثل أي برامج الدردشه او الرسائل الفوريه (Instant message) مثل سكايب ياهو
ماسنجر واتساب

او تطبيقات browser based او التطبيقات التي تعتمد على المتصفح مثل فيسبوك او تويتر
حيث الفورتى جيت له القدرة بالتحكم بالتطبيق وايضا خصائص التطبيق نفسه.

فالسؤال هو ما الفرق بين الويب فلتر والابلكيشن كنترول ؟؟
حيث لو قمت باغلاق موقع فيسبوك عبر ال web filter فهذا انا قفلت الموقع فما الحاجه الى اغلاق
الفيسبوك أيضا من ال application control !!!

الاجابة بأنى ممكن اسمح للفيسبوك عبر ال web filer ولكنى اريد اغلاق خاصيه معينه في الفيسبوك
مثل منع التعليق او like... الخ في الفيسبوك او منع فتح الفيديوهات على الفيسبوك بالرغم ان
الفيسبوك بشكل عام مفتوح
حيث هذا لا يتم الا عبر ال application controller ..

حيث في application controller اقدر التحكم في سلوكيات او خصائص التطبيق .

حيث ال application controller يستطيع التحكم بالتطبيقات اعتماد على IPS ..
حيث ips لديه اقدره على تحليل الترافيك ويكتشف أي تطبيق حتى ان كان هذا التطبيق لا يستخدم
البورتات القياسيه (Non standard protocols).

أساسيات فورتى جيت

الفورتى جيت يعتمد على ال application control database والتي تكون على شكل قائمه موجودة على الفورتى جيت حيث يتم تحديث تلك القائمة بشكل مستمر عبر FortiGuard App control License .

Forigate's signature هو الشئ الذي يعتمد عليه ال app control في التحكم بالتطبيقات حيث يحتوي ال signature على port التطبيق و services و ip's و URL لكل تطبيق .

:Application control action

يوجد لدى الفورتى جيت 4 أنواع من ال action :

- (١) Allow :اسمح لكل شيء
- (٢) Monitor :اسمح مع تسجيل الاحداث (logs)
- (٣) Block :منع مع تسجيل الاحداث (logs)
- (٤) Quarantine :عند الدخول على هذا التطبيق فأفورتى جيت سيقوم بعمل ban لايي اليوزر الذي حاول الوصول لهذا التطبيق .

ماهو ال Traffic shape :

Traffic shape : تخصيص ترافيك معين لطبق معين حيث ال traffic shaper يحتوي على 5 اشكال :

Gurantee(80k) : اضمن بأن الترافيك سوف يأخذ 80 كيلو لتطبيق معين على الأقل .

High priority : اضمن بأن لدي اعلى اولويه لترافيك بالمرور..

Low priority : اخذ اقل اولويه للترافيك

Medium priority : اخذ اولويه متوسطه

Shared : تخصيص مثلا 1 ميغا لترافيك معين حيث الناس تتشارك فيه .

مثلا تخصيص 1 ميغا مثلا لتطبيق الفيسبوك حيث ان جميع الأشخاص في الشركة الذين سيتخدمو الفيسبوك سوف يتشاركوا ب 1 ميغا .

Name	Comments	Ref.
APP allow gmail		0
APP block remote access app		0
APP block-high-risk		0
APP default	Monitor all applications.	0
APP wifi-default	Default configuration for offloading WiFi traffic.	1

حيث نقوم بإنشاء بروفایل معين للapp control ولسكن اسمه Block Social app

حيث سنقوم باغلاق كل التطبيقات التي تستخدم مواقع التواصل الاجتماعي مثل فيسبوك او تويتر او الخ..

Name: Block Social app

Comments: 0/255

Categories:

- All Categories
- Business (179, 6)
- Cloud.IT (31)
- Collaboration (293, 6)
- Email (87, 12)
- Game (124)
- General.Interest (241, 9)
- Mobile (3)
- Network.Service (332)
- P2P (85)
- Proxy (106)
- Remote.Access (91)
- Social.Media (150, 31)
- Storage.Backup (296, 16)
- Update (48)
- Video/Audio (206, 13)
- VoIP (31)
- Web.Client (18)
- Unknown Applications

Network Protocol Enforcement:

Application and Filter Overrides:

Name	Comments	Ref.
APP Block Social app		0
APP allow gmail		0
APP block remote access app		0
APP block-high-risk		0
APP default	Monitor all applications.	0
APP lwifi-default	Default configuration for offloading WiFi traffic.	1

تم الانشاء ...

ثم عند تطبيق البوليسي نقوم بتفعيل app control واختيار البروفايل الذي أنشأناه مسبقا ..

Edit Policy

NAT

IP Pool Configuration **Use Outgoing Interface Address** Use Dynamic IP Pool

Preserve Source Port

Protocol Options **PRX** default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control **APP** Block Social app

IPS

SSL Inspection **SSL** deep-inspection

Mirror SSL Traffic to Interfaces

Logging Options

Log Allowed Traffic **Security Events** All Sessions

Generate Logs when Session Starts

مع التأكيد من تفعيل الخاصية SSL Inspection=deep-inspection لكي يتمكن من التحكم باي تطبيق او موقع يستخدم ssl protocol (https) ..

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
4	private	all	all	always	ALL	ACCEPT	Enabled	APP Block Social app deep-inspection UTM	
3	public	Subnet1	all	always	ALL	DENY		SSL no-inspection UTM	Disabled
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	SSL no-inspection UTM	
1	allow_internet	Subnet1	all	work_time	ALL	ACCEPT	Enabled	SSL no-inspection UTM	
5	3	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection UTM	
0	Implicit Deny	all	all	always	ALL	DENY			Disabled

كما نلاحظ بالصورة ادناه بأن ال app control يقسم الى categories

Categories

- All Categories
- Business (179, 6)
- Cloud.IT (31)
- Collaboration (293, 6)
- Email (87, 12)
- Game (124)
- General.Interest (241, 9)
- Mobile (3)
- Network.Service (332)
- P2P (85)
- Proxy (106)
- Remote.Access (91)
- Social.Media (150, 31)
- Storage.Backup (296, 16)
- Update (48)
- Video/Audio (206, 13)
- VoIP (31)
- Web.Client (18)
- Unknown Applications

Network Protocol Enforcement

بتحتوي على تصنيفات حيث تم تقسيم كل مجموعة من التطبيقات المتشابهة في الخصائص بتصنيف معين .

ملاحظة : تم السماح لكل التطبيقات الغير معروفة (Unknown Applications) (الفورتى جيت ليس لديه signature لهذا التطبيقات) ..

حيث بمجرد النقر على أي category يمكنك تطبيق أي action تريده كما بالصورة ادناه ..

أساسيات فورتى جيت

Categories

All Categories

Business (179, 6)

Monitor

Allow

Block

Quarantine

View Signatures (179)

View Cloud Signatures (6) 16

Video/Audio (206, 13)

Web.Client (18)

Cloud.IT (31)

Email (87, 12)

General.Interest (241, 9)

Network.Service (332)

Proxy (106)

Social.Media (150, 31)

Update (48)

VoIP (31)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

Create New Edit Delete

Priority	Details	Type	Action
----------	---------	------	--------

يمكن ان أقوم بتصفح كل الsignatures (التطبيقات) التي بيتحكم بها الفورتى جيت وذلك كالتالي :

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

Intrusion Prevention

SSL/SSH Inspection

Web Rating Overrides

Web Profile Overrides

Custom Signatures

VPN

User & Device

Edit Application Sensor

93 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: Block Social app

View Application Signatures

Comments: 0/255

Categories

All Categories

Business (179, 6)

Collaboration (293, 6)

Game (124)

Mobile (3)

P2P (85)

Remote.Access (91)

Storage.Backup (296, 16)

Video/Audio (206, 13)

Web.Client (18)

Cloud.IT (31)

Email (87, 12)

General.Interest (241, 9)

Network.Service (332)

Proxy (106)

Social.Media (150, 31)

Update (48)

VoIP (31)

Unknown Applications

كما يمكنني ان اظهر الsignatures لتصنيف معين كما بالصورة التالية :

أساسيات فورتني جيت

System
Policy & Objects
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Custom Signatures
VPN
User & Device
Log & Report

All Categories
Business (179, 6)
Collaboration (293, 6)
Game (124)
Mobile (3)
P2P (85)
Remote.Access (91)
Storage.Backup (296, 16)
Video/Audio (13)
Web.Cl...
Cloud.IT (31)
Email (87, 12)
General.Interest (241, 9)
Network.Service (332)
Proxy (106)
Social.Media (150, 31)
Update (48)
VoIP (31)
Unknown Applications

Monitor
Allow
Block
Quarantine
View Signatures (124)

Create New Edit Delete

حيث ستظهر لك كل التطبيقات التي تندرج تحت هذا التصنيف كما بالصورة ادناه

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Custom Signatures
VPN
User & Device

View Application Signatures
Create New Edit Delete Search All Cloud

Name	Category	Technology	Popularity	Risk
51.Com_Games	Game	Browser-Based	★★★★☆	Low
AIM.Game	Game	Browser-Based	★★★★☆	Low
Addicting.Games	Game	Browser-Based	★★★★☆	Low
Aion	Game	Client-Server	★★★★☆	Low
All.Slots.Casino	Game	Browser-Based	★★★★☆	Low
Apple.Game.Center	Game	Client-Server	★★★★☆	Low
Armagetron	Game	Client-Server	★★★★☆	Low
Armor.Games	Game	Browser-Based	★★★★☆	Low
Battle.Net	Game	Browser-Based	★★★★☆	Low
Battlefield.Game	Game	Client-Server	★★★★☆	Low
BnB	Game	Client-Server	★★★★☆	Low
Bnbpopo	Game	Client-Server	★★★★☆	Low
BomberClone	Game	Client-Server	★★★★☆	Low

حيث يمكن البحث عن أي تطبيق تريده للتأكد من وجوده في هذا التصنيف...

Name	Category	Technology	Popularity	Risk
Facebook	Social.Media	Browser-Based	★★★★★	High
Facebook.App	Social.Media	Browser-Based	★★★★☆	High
Facebook.App.CastleVille	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.CityVille	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Kongregate	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.MyTribe	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Name	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Ninja.Saga	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.RestaurantCity	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.SocialRSS	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Sorority.Life	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Typing.Maniac	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Wild.Ones	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.WordsWithFriends	Social.Media	Browser-Based	★☆☆☆☆	Low
Facebook.App.Yoville	Social.Media	Browser-Based	★☆☆☆☆	Low

كما بالصورة أعلاه تم البحث عن كلمه facebook داخل هذا التصنيف المسمى social networking حيث الفيسبوك يمكنك التحكم بكل خصائصه من هنا ...

حيث نلاحظ كما بالوصوره أعلاه عمود باسم **Name** يوضح اسم التطبيق وايضا عمود باسم **Category** يبين التصنيف المنتمي له هذه التطبيق (social Media-sports-news- p2p ...)

والعمود الثالث باسم **Technology** يوضح التقنيه التي بيشتغل فيها التطبيق .. هل يعمل عن طريق المتصفح (Browser-based) او تطبيق يعمل بتقنيه (Client-server) أي ان التطبيق يعمل ك client ومرتبط بserver مثل برنامج كاسبرسكاي حيث يأخذ التحديث من السيرفر التابع لموقع كاسبر.. او تطبيق يعمل بتقنيه (peer-to-peer)

والعمود الرابع باسم **popularity** بمعني الشعبيه (الشهره) حيث يظهر لك نجوم بعدد شهره التطبيق ..

العمود الخامس باسم **Risk** ويوضح مدى خطوره التطبيق (خطر **critical** ، مرتفع **elevated** ، منخفض **low** ، متوسط **Medium** ، ليس خطر **None** ..)

❖ طريقة التحكم في التطبيقات عبر الـ Application control :

مثلا لو اريد اغلاق كل مواقع التواصل الاجتماعي (فيسبوك، تويتر، انستجرام....).

The screenshot shows the FortiGate VM64 web interface for editing an application sensor. The left sidebar shows the navigation menu with 'Application Control' selected. The main content area is titled 'Edit Application Sensor' and displays a list of categories. The 'Social.Media' category is selected, and its configuration options are shown in a dropdown menu. The 'Block' option is highlighted in green.

Category	Count
Business	179 (6)
Collaboration	293 (6)
Game	124
Mobile	3
P2P	85
Remote.Access	91
Storage.Backup	296 (16)
Video/Audio	206 (13)
Web.Client	18
Cloud.IT	31
Email	87 (12)
General.Interest	241 (9)
Network.Service	332
Proxy	106
Social.Media	150 (31)

Network Protocol Enforcement:

Application and Filter Overrides:

- Monitor
- Allow
- Block
- Quarantine
- View Signatures (150)
- View Cloud Signatures (31)

Dashboard > Edit Application Sensor

Security Fabric >

FortiView >

Network >

System >

Policy & Objects >

Security Profiles >

AntiVirus

Web Filter

DNS Filter

Application Control ☆

Intrusion Prevention

SSL/SSH Inspection

Web Rating Overrides

Web Profile Overrides

Custom Signatures

VPN >

User & Device >

Categories

All Categories

Business (179, 6)

Collaboration (293, 6)

Game (124)

Mobile (3)

P2P (85)

Remote.Access (91)

Storage.Backup (296, 16)

Video/Audio (206, 13)

Web.Client (18)

Cloud.IT (31)

Email (87, 12)

General.Interest (241, 9)

Network.Service (332)

Proxy (106)

Social.Media (150, 31)

Update (48)

VolP (31)

Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New Edit Delete

بهذه الطريقة سيتم اغلاق كل مواقع التواصل الاجتماعي ويظهر للمستخدم الرسالة التالية :

https://www.facebook.com/?_rd= Search

Application Blocked!

You have attempted to use an application which is in violation of your internet usage policy.

Facebook

Category: Social.Media
URL: https://www.facebook.com/
Client IP: 192.168.1.110
Server IP: 31.13.93.3
User name:
Group name:
Policy:
FortiGate Hostname: FGT80C3911605533

كما بالصورة أعلاه يظهر لنا اسم التصنيف الذي ينتمي اليه موقع الفيسبوك (Social Media) والurl الذي حاول الوصول اليه اليوزر صاحب الايبي المحدد بالصورة ...

➤ لمعرفة ماهي البرامج (signatures) التي بتكون مندرجه تحت الـ category :

Name: Block Social app View Application Signatures

Comments: 0/255

Categories

All Categories

- Business (179, ☁ 6)
- Collaboration (293, ☁ 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, ☁ 16)
- Video/Audio (206, ☁ 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, ☁ 12)
- General.Interest (241, ☁ 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, ☁ 31)
 - Monitor
 - Allow
 - Block
 - Quarantine
 - View Signatures (150)
 - View Cloud Signatures (31)

Network Protocol Enforcement

Application and Filter Overrides

Name	Category	Technology	Popularity	Risk
Drupal	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Dudu	Social.Media	Network-Protocol	☆☆☆☆☆	■■■■■
Engadge	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Eyejot	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_CastleVille	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_CityVille	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_Kongregate	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_MyTribe	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_Name	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_Ninja.Saga	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_RestaurantCity	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_SocialRSS	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■
Facebook.App_Sorority.Life	Social.Media	Browser-Based	☆☆☆☆☆	■■■■■

طريقة التحكم بخاصية معينه داخل الموقع وليس كل الموقع :

التحديد لتطبيق معين او لخاصية معينه داخل التطبيق يكون من الخيار

Application and Filter Overrides

مثلا اريد افتح الفيسبوك ولكن اقفل خاصيه اعجبني :

The screenshot shows the FortiGate configuration interface. On the left, the 'Policy & Objects' menu is expanded. The main area displays 'Application and Filter Overrides' with a table of categories and their counts. The 'Social.Media' category is highlighted with a red box. Below this, the 'Add New Override' dialog is open, showing a search for 'facebook'. The search results table is also highlighted with a red box, listing various Facebook-related applications and their categories, popularity, and risk levels.

Name	Category	Technology	Popularity	Risk
Facebook	Social.Media	Browser-Based	★★★★★	Low
Facebook.App	Social.Media	Browser-Based	★★★★☆	Low
Facebook.App_AngryBirds	Game	Browser-Based	★★★★☆	Low
Facebook.App_AvengersAlliar	Game	Browser-Based	★★★★☆	Low
Facebook.App_BubbleFairyla	Game	Browser-Based	★★★★☆	Low
Facebook.App_BubbleSafari	Game	Browser-Based	★★★★☆	Low
Facebook.App_CandyCrushSa	Game	Browser-Based	★★★★☆	Low
Facebook.App_CastleVille	Social.Media	Browser-Based	★★★★☆	Low
Facebook.App_CityVille	Social.Media	Browser-Based	★★★★☆	Low
Facebook.App_Criminalcase	Game	Browser-Based	★★★★☆	Low
Facebook.App_EmpiresAndAl	Game	Browser-Based	★★★★☆	Low

كما بالصورة أعلاه تم البحث عن التطبيق facebook في خانه البحث وظهرت كل التطبيقات التي باسم facebook

حيث اول تطبيق يظهر لك مثلا facebook بدون أي اضافات يعتبر التطبيق العام (موقع الفيسبوك كامل مع الخصائص المدرجة تحته)...

فمثلا facebook.app هذا يعني التطبيق نفسه وليس ال URL

أساسيات فورتني جيت

حيث action هو Block التي سوف نحدده للتطبيقات التي سوف نختارها كما بالصورة التالية :
مثلا اريد اغلاق خاصيه معينه في الفيسبوك وليكن اغلاق النشر والدخول وزراعجيني

Type **Application** Filter

Action Block

Add All Results + Add Selected facebook Selected 0 All Cloud

Name	Category	Technology	Popularity	Risk
Facebook.Messenger.Image.U	Collaboration	Client-Server	★★★★☆	█
Facebook.Messenger.Video.Tr	Collaboration	Client-Server	★★★★☆	█
Facebook.Messenger.VoIP.Cal	Collaboration	Client-Server	★★★★☆	█
Facebook.Messenger.Voice.M	Collaboration	Client-Server	★★★★☆	█
Facebook.Chat	Social.Media	Browser-Based	★★★★☆	█
Facebook.File.Download	Social.Media	Browser-Based	★★★★☆	█
Facebook.File.Upload	Social.Media	Browser-Based	★★★★☆	█
Facebook.Like.Button	Social.Media	Browser-Based	★★★★☆	█
Facebook.Login	Social.Media	Browser-Based	★★★★☆	█
Facebook.Plugins	Social.Media	Browser-Based	★★★★☆	█
Facebook.Post	Social.Media	Browser-Based	★★★★☆	█
Facebook.Search	Social.Media	Browser-Based	★★★★☆	█
Facebook.Video.Play	Social.Media	Browser-Based	★★★★☆	█

Action Block

Add All Results + Add Selected facebook Selected 0 All Cloud

Name	Category	Technology	Popularity	Risk
Facebook.Messenger.Image.U	Collaboration	Client-server	★★★★☆	█
Facebook.Messenger.Video.Tr	Collaboration	Client-Server	★★★★☆	█
Facebook.Messenger.VoIP.Cal	Collaboration	Client-Server	★★★★☆	█
Facebook.Messenger.Voice.M	Collaboration	Client-Server	★★★★☆	█
Facebook.Chat	Social.Media	Browser-Based	★★★★☆	█
Facebook.File.Download	Social.Media	Browser-Based	★★★★☆	█
Facebook.File.Upload	Social.Media	Browser-Based	★★★★☆	█
Facebook.Like.Button	Social.Media	Browser-Based	★★★★☆	█
Facebook.Login	Social.Media	Browser-Based	★★★★☆	█
Facebook.Plugins	Social.Media	Browser-Based	★★★★☆	█
Facebook.Post	Social.Media	Browser-Based	★★★★☆	█
Facebook.Search	Social.Media	Browser-Based	★★★★☆	█
Facebook.Video.Play	Social.Media	Browser-Based	★★★★☆	█

حيث نحدد بالزر الأيمن للخاصية وليكن منع زر اعجبنى بالفيسبوك ثم نختار الخيار Add Selected

أساسيات فورتني جيت

Name	Category	Technology	Popularity	Risk
Facebook.Messenger.Image.I	Collaboration	Client-Server	★★★★☆	🟢
Facebook.Messenger.Video.Tr	Collaboration	Client-Server	★★★★☆	🟢
Facebook.Messenger.VoIP.Cal	Collaboration	Client-Server	★★★★☆	🟢
Facebook.Messenger.Voice.M	Collaboration	Client-Server	★★★★☆	🟢
Facebook.Chat	Social.Media	Browser-Based	★★★★☆	🟢
Facebook.File.Download	Social.Media	Browser-Based	★★★★☆	🟡
Facebook.File.Upload	Social.Media	Browser-Based	★★★★☆	🟡
Facebook.Like.Button	Social.Media	Browser-Based	★★★★★	🟡
Facebook.Login	Social.Media	Browser-Based	★★★★☆	🟡
Facebook.Plugins	Social.Media	Browser-Based	★★★★★	🟡
Facebook.Post	Social.Media	Browser-Based	★★★★☆	🟡
Facebook.Search	Social.Media	Browser-Based	★★★★☆	🟡
Facebook.Video.Play	Social.Media	Browser-Based	★★★★☆	🟡

تم تحديد الخصائص التالية بالفيديوك (Like ,Login,post)

Edit Application Sensor

Game (124) | Mobile (3) | P2P (85) | Remote.Access (91) | Storage.Backup (296, ☁ 16) | Video/Audio (206, ☁ 13) | Web.Client (18)

General.Interest (241, ☁ 9) | Network.Service (332) | Proxy (106) | Social.Media (150, ☁ 31) | Update (48) | VoIP (31) | Unknown Applications

Network Protocol Enforcement

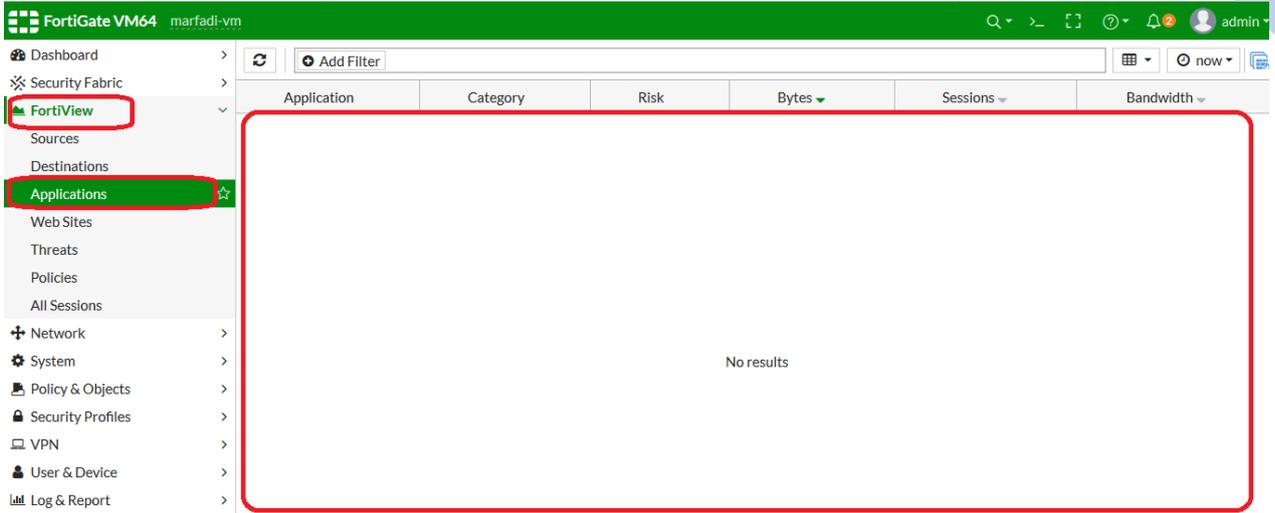
Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	Facebook.Like.Button Facebook.Login ☁ Facebook.Post ☁	Application	<input checked="" type="radio"/> Block

Options

لو تريد متابعه ومراقبه الـ logs كما بالصورة التالية

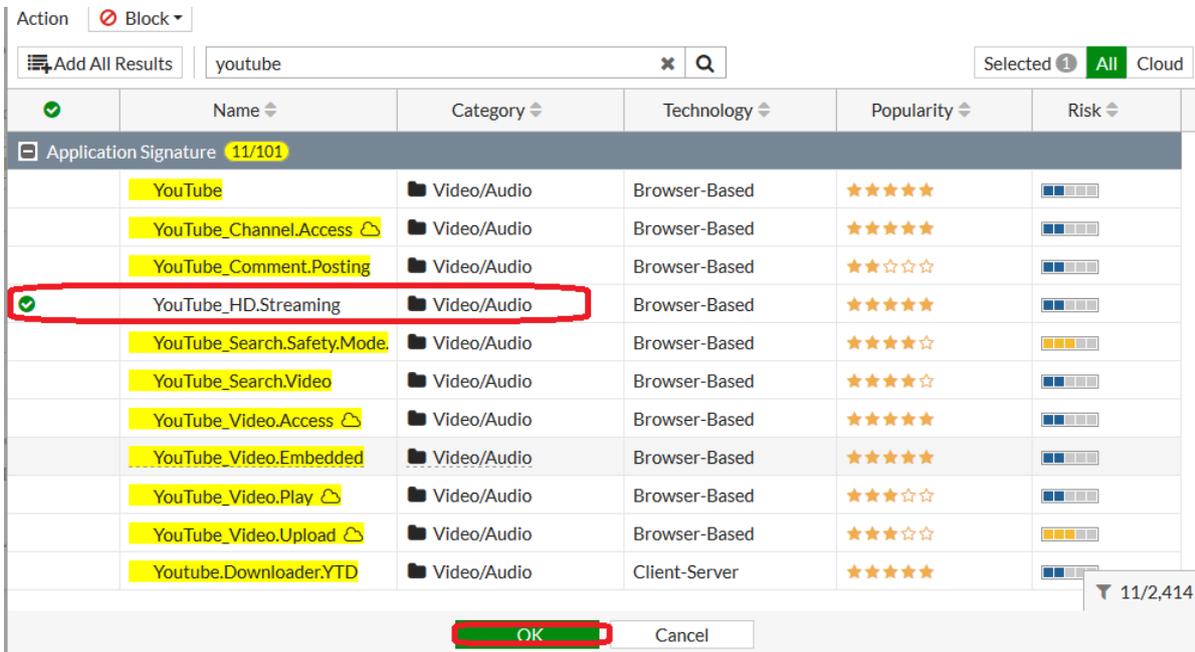


حيث يظهر لك كل التطبيقات التي حاول اليوزر الوصول اليها والتي في الأصل معمول لها Block او Monitor ...

حيث سيوضح لك اسم التطبيق والتصنيف الذي ينتهي له التطبيق ودرجه خطوره وحجم استهلاك الانترنت... الخ

مثال اخر:

اريد اغلاق قط الفيديوهات عاليه الدقه (HD) فقط من على اليوتيوب ...



أساسيات فورتى جيت

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > Application Control

AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Custom Signatures

VPN > User & Device >

Edit Application Sensor

Video/Audio (206, 13) | VoIP (31)

Web.Client (18) | Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

+ Create New | Edit | Delete

Priority	Details	Type	Action
1	Facebook_Like.Button Facebook_Login Facebook_Post	Application	Block
2	YouTube_HD.Streaming	Application	Block

Options

Block applications detected on non-default ports

Allow and Log DNS Traffic

QUIC Allow Block

Replacement Messages for HTTP-based Applications

طبعا توجد تصنيف (Category) اسمها Update والأفضل ان تتركها مثلا تحديث مكافحة الفيروسات او تحديث ويندوز.. الخ

FortiView > Network > System > Policy & Objects > Security Profiles > Application Control

AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Custom Signatures

VPN > User & Device > Log & Report > Monitor >

93 Cloud Applications require deep inspection.
1 policies are using this profile.

Name: Block Social app | View Application Signatures

Comments: 0/255

Categories

All Categories

- Business (179, 6)
- Collaboration (293, 6)
- Game (124)
- Mobile (3)
- P2P (85)
- Remote.Access (91)
- Storage.Backup (296, 16)
- Video/Audio (206, 13)
- Web.Client (18)
- Cloud.IT (31)
- Email (87, 12)
- General.Interest (241, 9)
- Network.Service (332)
- Proxy (106)
- Social.Media (150, 31)
- Update (48)

Allow Block Quarantine

View Signatures (48) | Apply

أساسيات فورتني جيت

Name	Category	Technology	Popularity	Risk
Avira.Update	Update	Client-Server	★★★★★	Low
BitDefender.Update	Update	Client-Server	★★★★☆	Low
Chrome.Update	Update	Browser-Based	★★★★★	Low
Dell.Update	Update	Client-Server	★★★☆☆	Low
Driver.Booster.Update	Update	Client-Server	★★★★☆	Low
Duba.Update	Update	Client-Server	★★★★☆	Low
Firefox.Update	Update	Client-Server	★★★★★	Low
FortiClient	Update	Client-Server	★★★★☆	Low
Google.Update	Update	Client-Server	★★★★☆	Low
InstallAnywhere.Update	Update	Client-Server	★★★☆☆	Low
Java.Update	Update	Client-Server	★★★★☆	Low
Kaspersky.Update	Update	Client-Server	★★★★★	Low
MS.Windows.Activation	Update	Client-Server	★★★☆☆	Low
MS.Windows.Update	Update	Client-Server	★★★★★	Low
Malwarebytes	Update	Client-Server	★★★★★	Low
McAfee.Update	Update	Client-Server	★★★★★	Low

فيمكنك السماح للتطبيق المناسب او منع التحديث لتطبيق ما ...

مثلا اريد السماح للكاسبرو والفيرفوكس ان يعملوا تحديث

Storage.Backup (296, 16) | Update (48)
 Video/Audio (206, 13) | VoIP (31)
 Web.Client (18) | Unknown Applications

Network Protocol Enforcement

Application and Filter Overrides

[+ Create New](#) [Edit](#) [Delete](#)

Priority	Details	Type	Action
1	Facebook_Like.Button Facebook_Login Facebook_Post	Application	Block
2	Firefox.Update Kaspersky.Update	Application	Allow

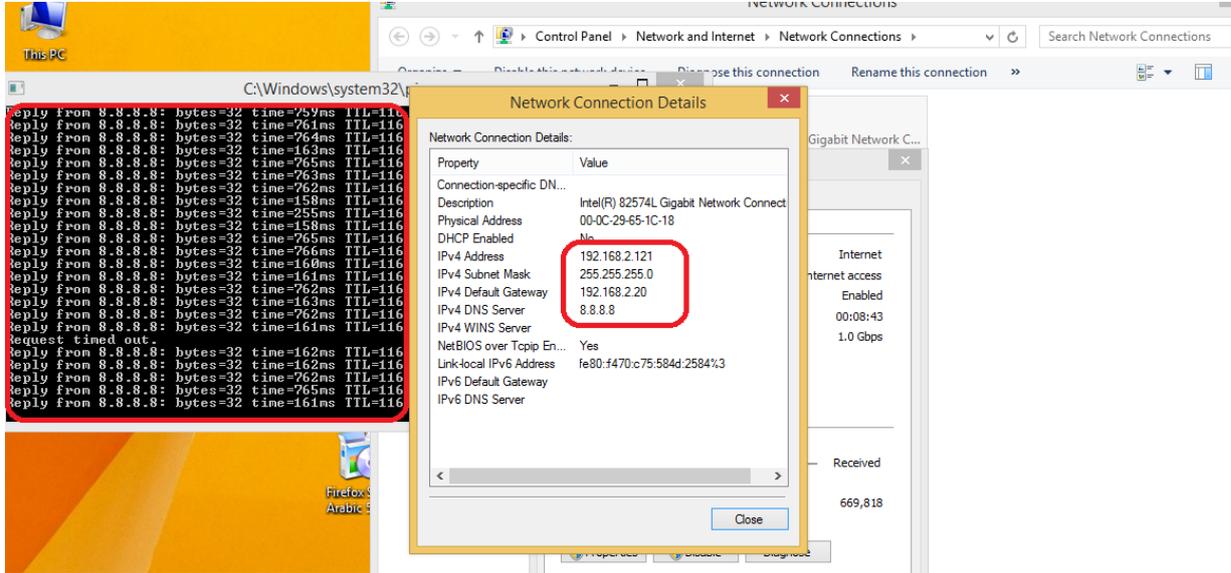
Options
 Block applications detected on non-default ports

[Apply](#)

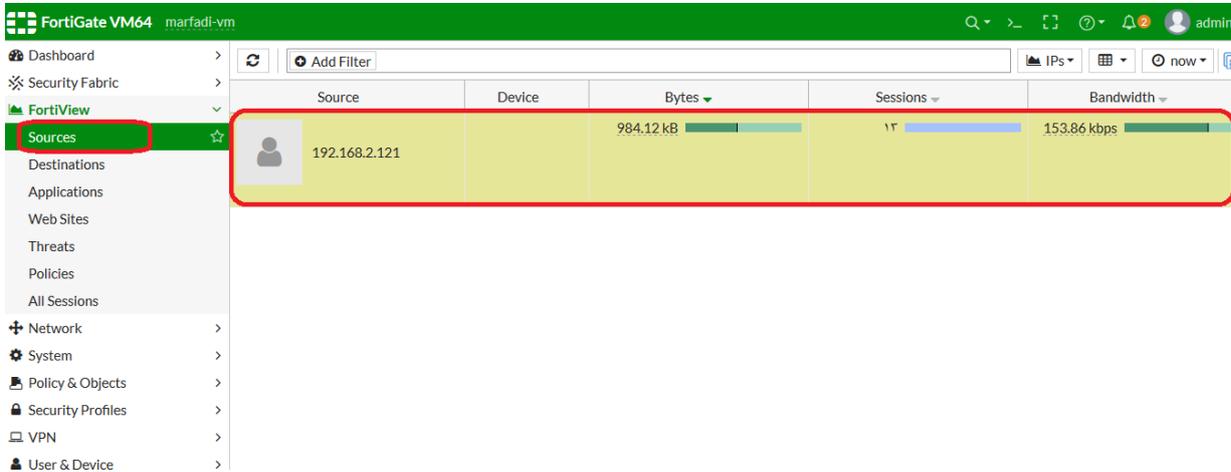
طريقة عمل حظر (ban) لجهاز معين ...

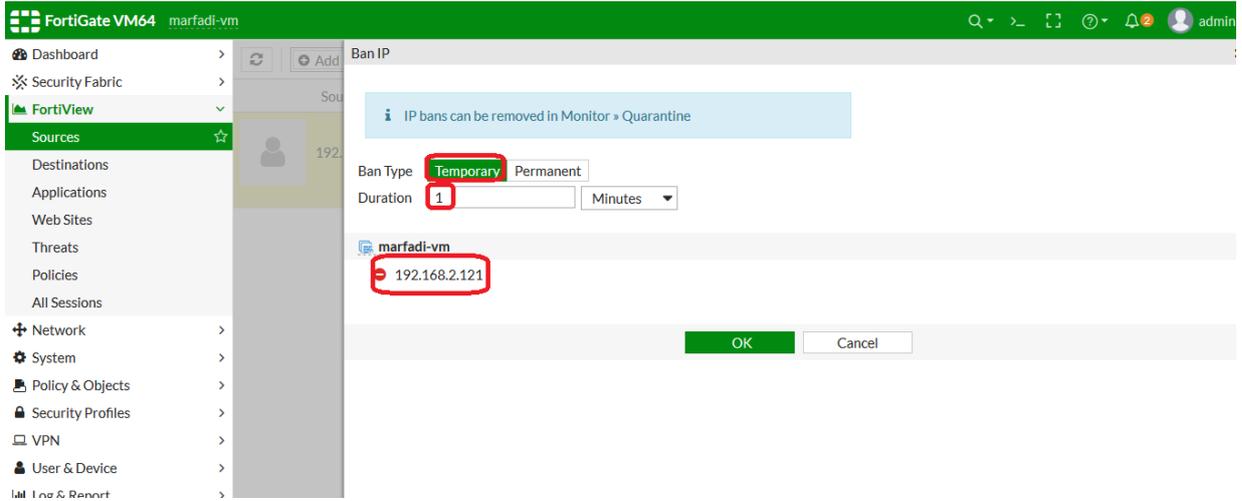
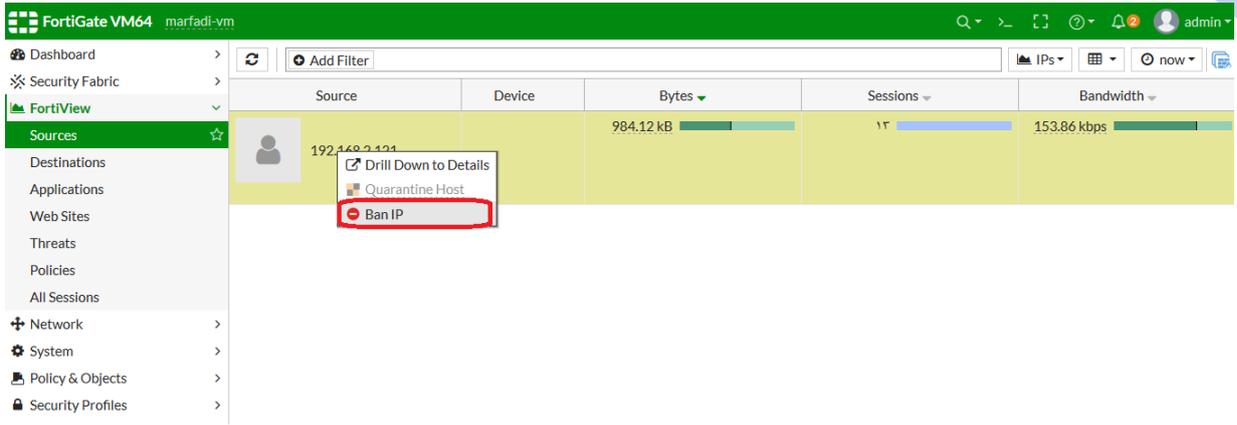
لنفترض بأن الجهاز صاحب الايبي 192.168.2.121 نريد عمل له حظر..

حيث نلاحظ بان الانترنت شغال قبل عمليه الحظر..



الآن سوف نعمل ban للجهاز كما بالخطوات التالية :





كما بالصورة أعلاه سوف يسالك هل تريد الحظر لهذا الجهاز Temporary: أي موقت ولفتره زمنيه محدده وليكم دقيقه واحده فقط وبعدها يتم فك الحظر بشكل تلقائي .

Permeant: سيتم حظر الايبي (الجهاز) بشكل دائم ولفك الحظر لهذا الجهاز يتم الدخول بحسب الخطوات التالية :

أساسيات فورتى جيت

The screenshot shows the FortiGate VM64 interface with the Quarantine Monitor selected in the left sidebar. The main area displays a table with the following data:

Details	Device	Source	Expires	Description
Banned IP				
192.168.2.121		Administrative	29 minute(s) and 49 second(s)	

The screenshot shows the same interface as above, but with the 'Delete' button highlighted in a red box. The table data remains the same:

Details	Device	Source	Expires	Description
Banned IP				
192.168.2.121		Administrative	29 minute(s) and 49 second(s)	

The screenshot shows the Quarantine Monitor interface after the entry has been deleted. The table is empty, displaying 'No results'. A confirmation message is shown at the bottom right: 'Entries removed from ban.'

Details	Device	Source	Expires	Description
No results				

: Network Protocol Enforcement

أساسيات فورتى جيت

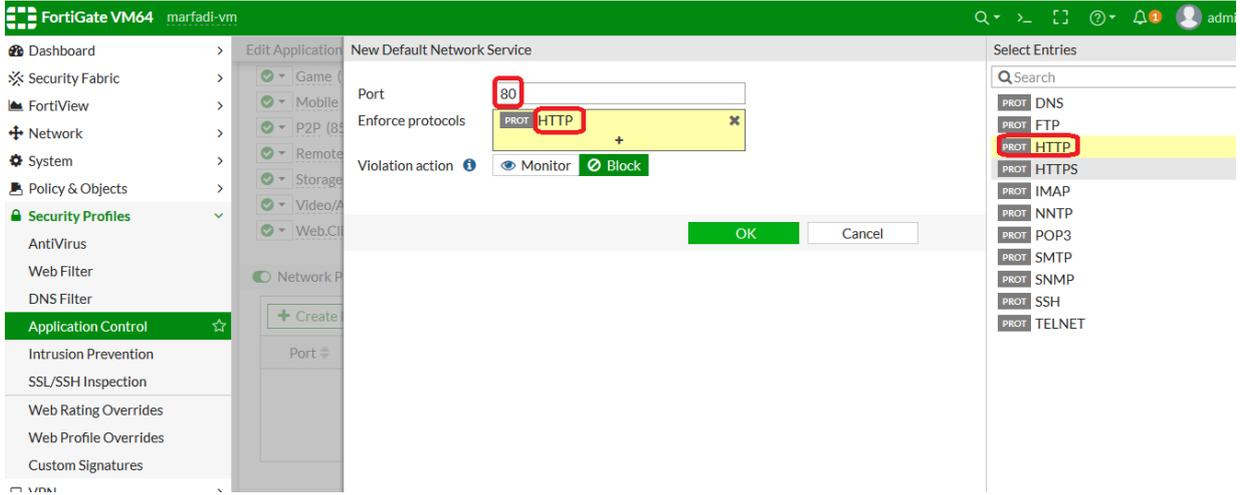
هذه الخاصية موجودة في ال Application control حيث كما نعلم توجد لكل بروتوكول بورت معين بشكل افتراضي كما بالتالي :

Default port Number	Protocol
80	http
443	https
22	Ssh
23	telnet
53	Dns

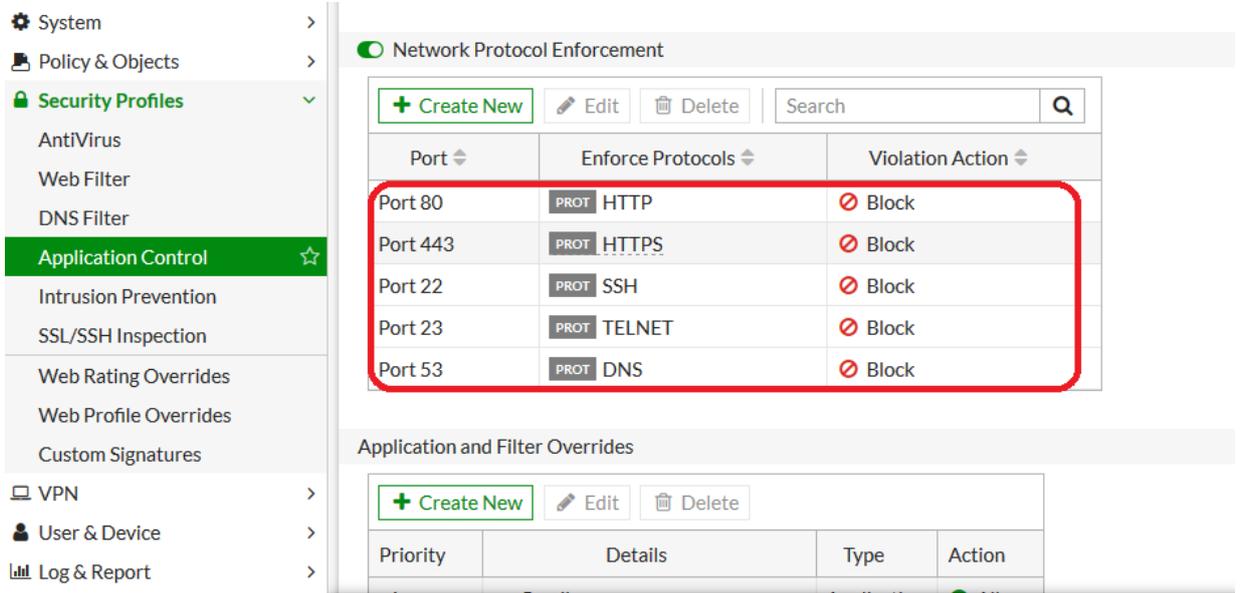
حيث يمكن ان يقوم اليوزر بتغيير رقم ال port للبروتوكول وهذا يتم التحايل على الفورتي جيت ..

فيمكن بواسطة الخاصية المذكورة أعلاه بأن امنع عملية تغيير رقم ال port لبروتوكول معين ..

The screenshot shows the FortiGate web interface. On the left, the 'Security Profiles' menu is expanded, and 'Application Control' is selected. The main content area is titled 'Edit Application Sensor'. Under the 'Network Protocol Enforcement' section, a checkbox is checked and highlighted with a red box. Below this, a '+ Create New' button is also highlighted with a red box. The main area displays a table with columns for 'Port', 'Enforce Protocols', and 'Violation Action'. The table is currently empty, showing 'No results'.



وهكذا..



حيث لو حاول احد تغيير رقم البورت لأحدى البروتوكولات أعلاه سيتم عمل Block .

Email filter ❖

كيفيه فلترة الايميلات على الفورتي جيت ..

أي عمليه اداره الايميلات الغير مرغوب فيها (spam email) عبر جهاز الفورتي جيت سواء وصل الايميل الى الـ Inbox او الـ Junk ..

حيث الفورتي جيت معتمد على خدمه من الفورتي جارد اسمها FortiGuard Anti spam services او Email filtering والتي تحتوي على قاعده بيانات والذي تحدد ما اذا كان الـ ip او الايميل او URL غير مرغوب ام لا ..

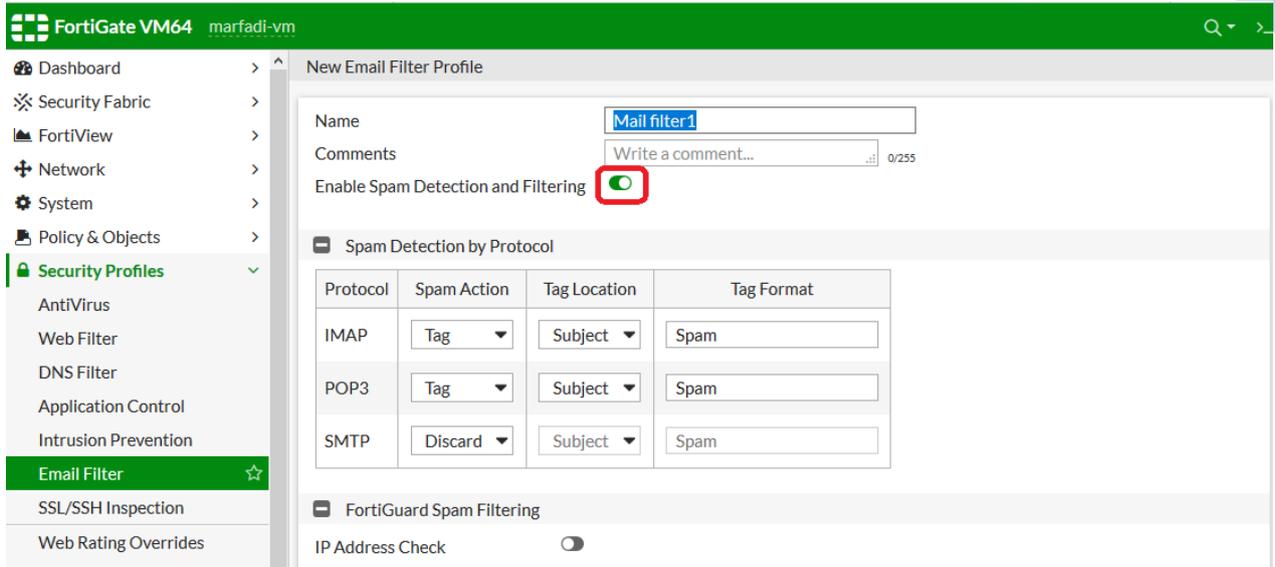
حيث اسم الاشتراك التي يجب ان تشترك بها هو Email filtering ويجب ان يكون معمول له License

License Information		
Support Contract	• Registration	Registered
FortiGuard	• IPS & Application Control	Licensed (Expires)
	• AntiVirus	Licensed (Expires)
	• Web Filtering	Licensed (Expires)
	• Vulnerability Scan	Licensed (Expires)
	• Email Filtering	Licensed (Expires)

نقوم باظهار خاصيه Email filter كما بالصورة ادناه لكي تظهر في security profiles .

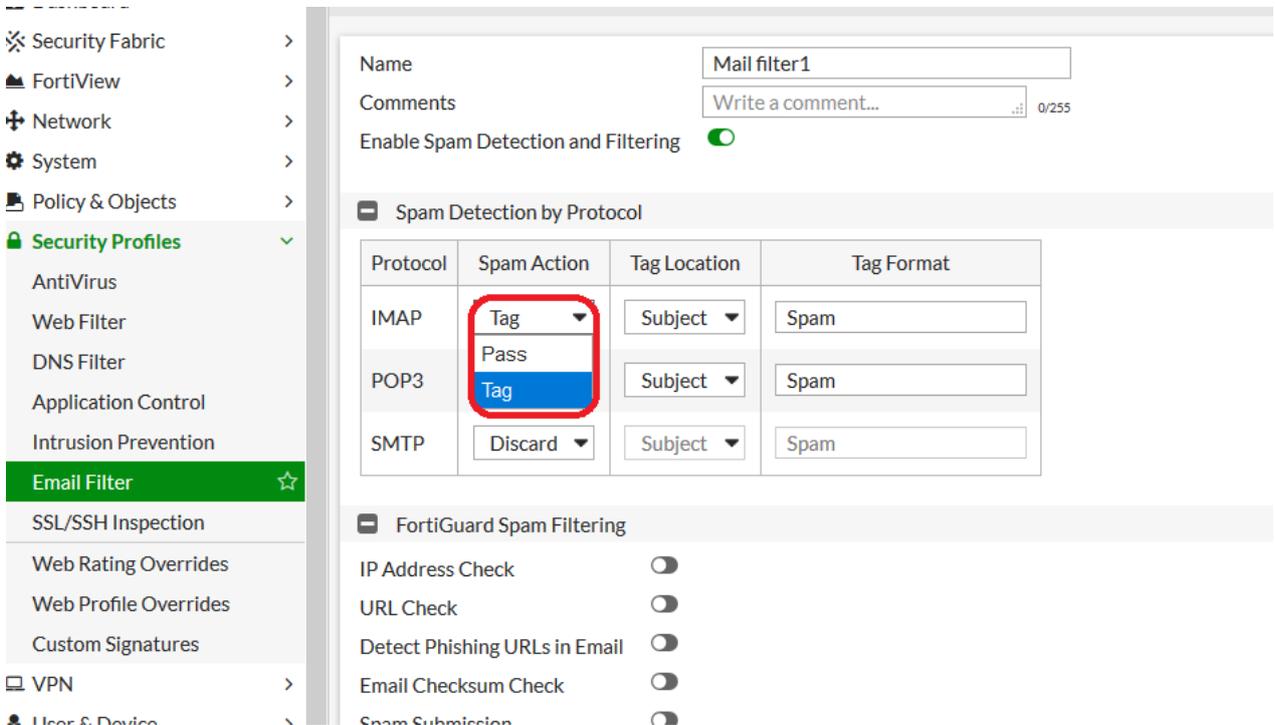
نلاحظ ظهور الخاصية الان ..

الان يمكنك أضافه بروفائل باسم Mail filter1 وذلك من خلال النقر على الزر Create New



حيث بمجرد تفعيل الخيار Enable Spam Detection and Filtering تظهر لك الجدول المسمى Spam Detection by protocol كما بالصورة أعلاه والذي يقصد به عملية كشف عن الاسبام ايميل واعمل لها فلتره ..

حيث يقصد بالجدول أعلاه بأن أي ايميل يستخدم ال IMAP او POP3 في الاستلام او يستخدم SMTP في الارسال فإن تم الكشف عليه بأنه spam فإن ال action الذي ستقوم به في الimap هو اما Tag او pass



Pass: معناها مرور الايميل بدون ماتعمل له أي action وهذا اجراء غير موصى به .

أساسيات فورتني جيت

Tag: أي تعمل علامه على الايميل سواء على Subject الخاص بالايميل او في headers وبهذا سيتم استلامه في ال spam folder او junk folder وبنفس الوقت معمول له في العنوان او ال header بانه spam او أي كلمه حددتها في الخانه tag format.

ونفس الكلام مع بروتوكول الاستقبال الpop3 ...

Protocol	Spam Action	Tag Location	Tag Format
IMAP	Tag	Subject	Spam
POP3	Tag	Subject	Spam
SMTP	Tag	Subject	Spam

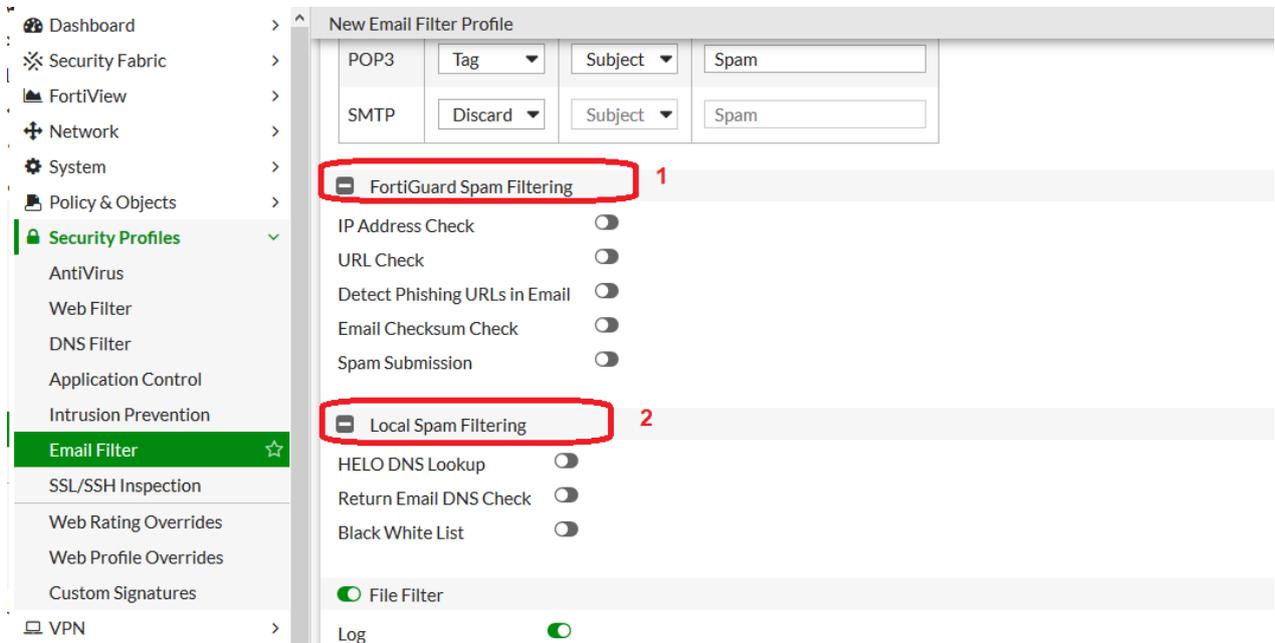
FortiGuard Spam Filtering

- IP Address Check
- URL Check
- Detect Phishing URLs in Email
- Email Checksum Check

اما الsmtp وهو البروتوكول المستخدم لعملية ارسال الايميل فإن ال action الافتراضي له هو Discard أي ان أي ايميل أقوم بإرساله (من داخل الشبكة الخاصة بي) فلا تعتبره على انه spam حتى وان كان كذلك، أي لا تقم بعمل له tag بانه spam لأنه من الغير منطقي بأن ترسل ايميل من شبكتك الداخليه ويظهر للمستلم في العنوان او ال Header بانه spam ..

➤ ماهي الطرق التي يستخدمها الفورتى جيت لكي يساعدك لاكتشاف الاسبام ايميل ؟

يعتمد على احدى الطرق :



(A) الاعتماد على الفورتى جارد (fortigurd spam filtering license) :

1. **Ip Address check** : أي ايميل اورساله تمر عبر جهاز الفورتى جيت ستخضع لفحص من خلال الفورتى جارد (سيتم ارسالها الى الفورتى جارد) فلو وجد بأن الايبي المرسل منه الايميل موجود بالقائمة السوداء فسيتم عمل اشاره على انه Spam ويتم وضعه في مجلد الاسبام للايميل اما في حالة كان الايميل سليم فسيتم تمريره الى الهدف بدون أي مشاكل ..

أساسيات فورتى جيت

٢. **URL Check**: أي URL (سواء عنوان البريد أو أي رابط في محتوى الرسالة نفسها) سيتم فحصه عبر الفورتى جارد فلو كان نظيف سيتم تمريره الى الهدف بدون أي مشاكل وان كان فيه مشكله فسيتم عمل عليه علامه بأنه اسبام وارساله الى مجلد الاسبام .

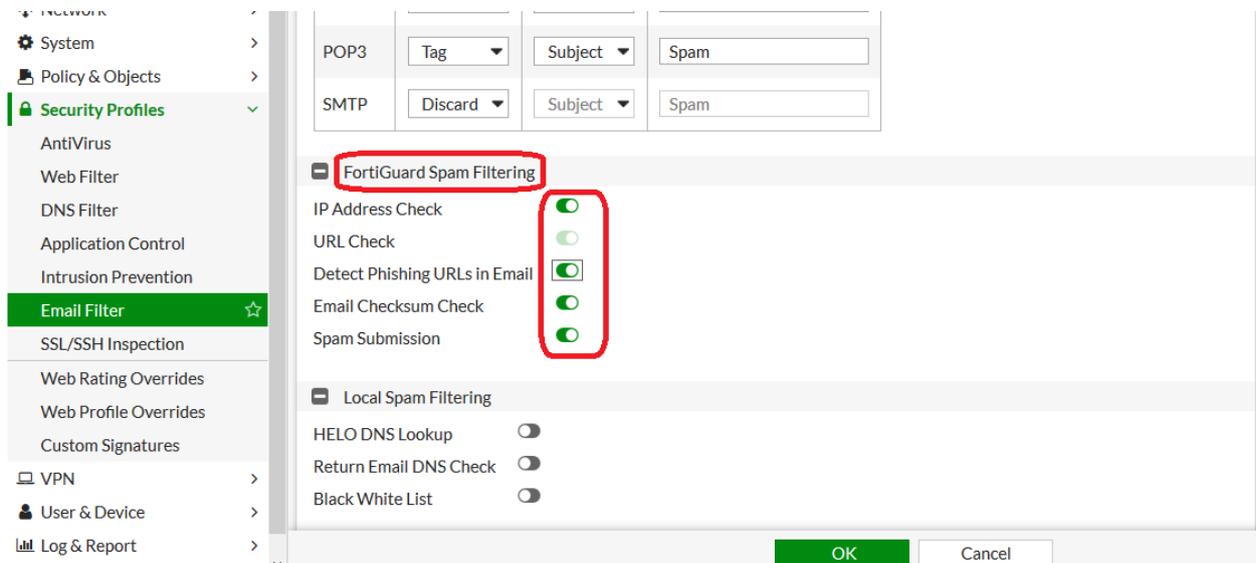
٣. **Detect Phishing URLs in emils**: سيتم الكشف عن روابط التصيد وسيتم اخضاع الروابط (URL) للفحص في URL Phising List فلو وجد هذا الرابط في تلك القائمة فأما سيقوم بحذف الرابط (URL) كاملاً او سيترك لك الرابط ولكن سيحذف منه الرابط المشبوه فحتى لو نقرت على الرابط لا يتم تحويلك الى phishing URL ..

٤. **Emil checksum Check**: يتم فحص طريقة كتابه الايميل نفسه (هل طريقة مفهومه ومكتوب بلغه معروفه ام لا). فلو كانت الطريقة معروفه فيتم تمرير الايميل ماعدا ذلك سيتم عمل له علامه بأنه spam mail .

٥. **Spam submission**: تجعل **fortiGurd antispam service** يعدل الايميل من اسبام الى ايميل عادي ..

حيث لو افترضنا بأن ايميل معين تم تصنيفه من قبل الفورتى جارد عن طريق الخطأ على انه اسبام فلو قمنا بتفعيل هذه الخاصية فأن أي ايميل سيتم وصوله الى spam folder فيمكنك تعديله ومعالجته بأن هذا الايميل سليم وليس اسبام وبهذا سيتم ارساله الى الفورتى جارد بحيث مره أخرى سيتم وصوله بشكل طبيعي.

حيث يتم تفعيل كل الخيارات الخمسه أعلاه كما بالصورة التالية :



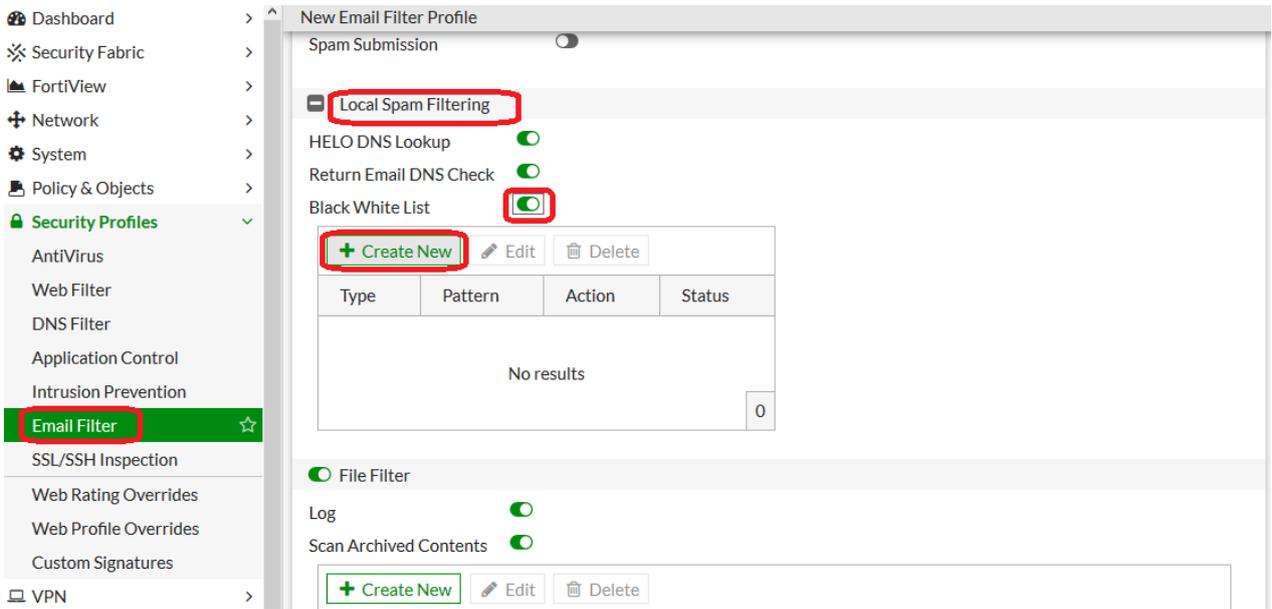
(B) الاعتماد على الفورتني جيت نفسه وبدون الحاجة الى لايسنز (Local Spam Filtering) .

١- Helo DNS Lookup: يتم التأكد هل domin التابع للإيميل موجود في Public

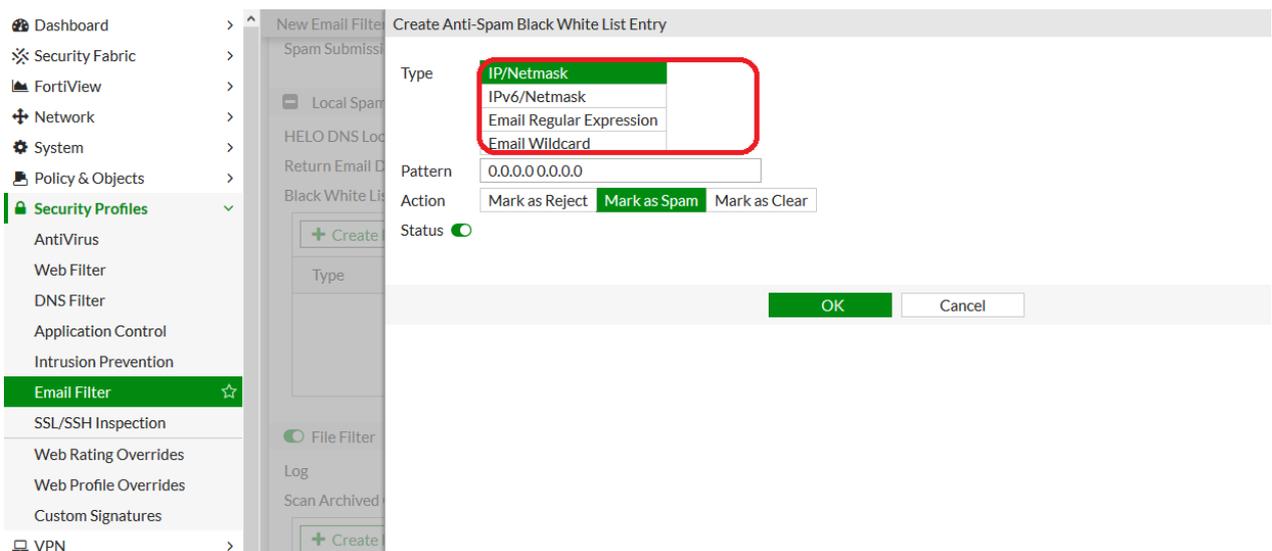
DNS فلولم يكن موجود فسيعتبر هذا الدومين اسبام .

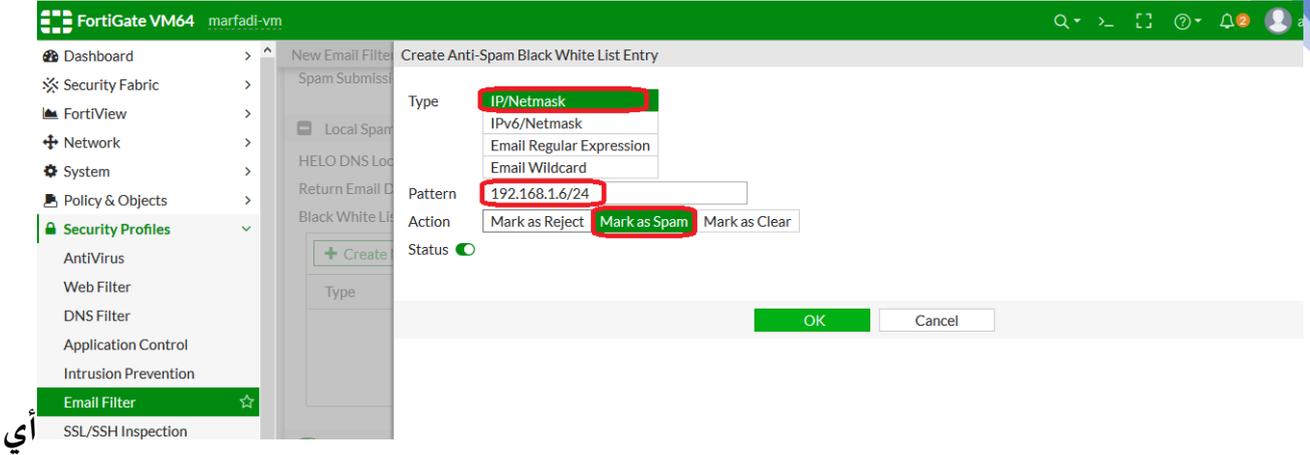
٢- Return Email DNS check

٣- Black white List: سيتم عمل قائمه سوداء وبيضاء بشكل يدوي كما بالتالي :



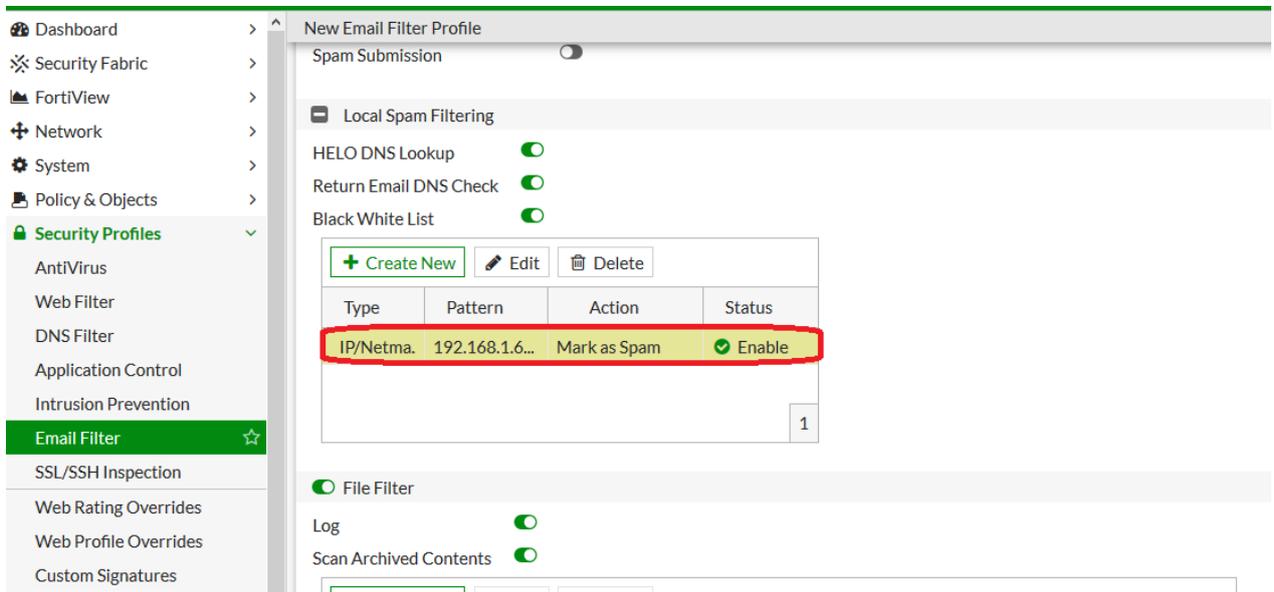
سيتم انشاء قائمه بيضاء او سوداء وذلك بالنقر على الزر Create New





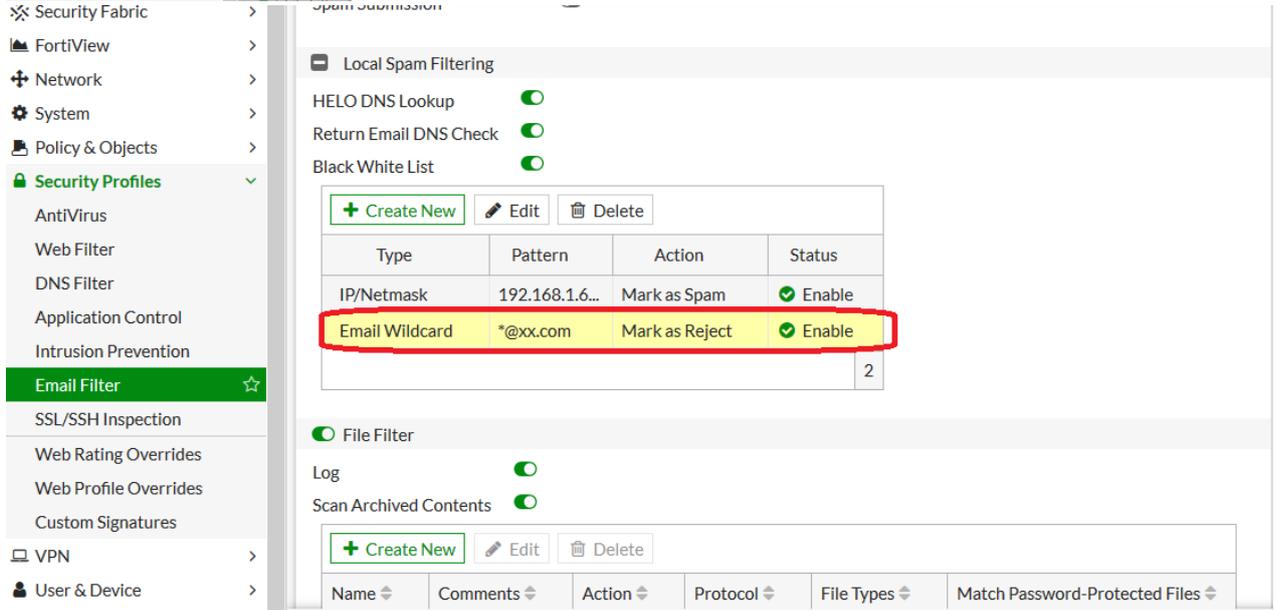
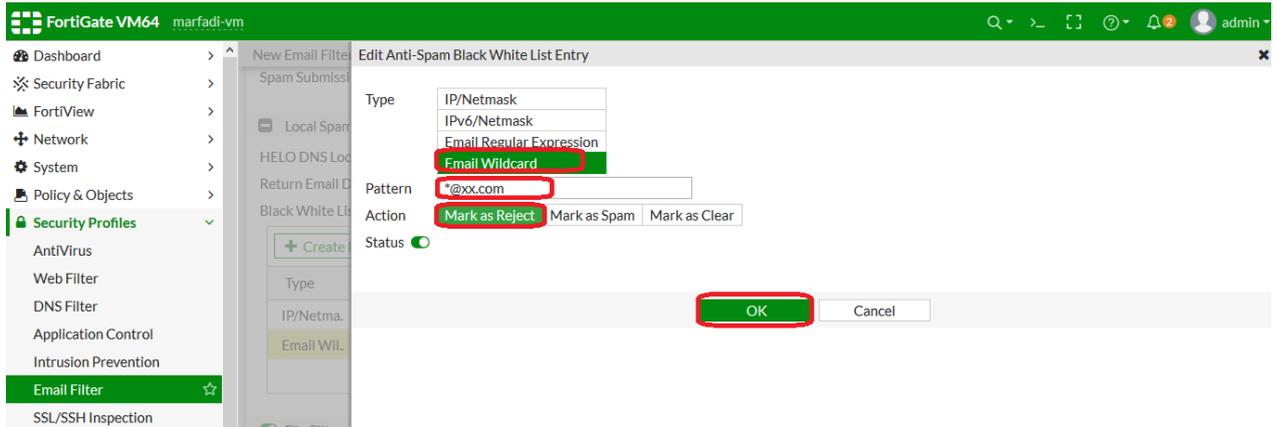
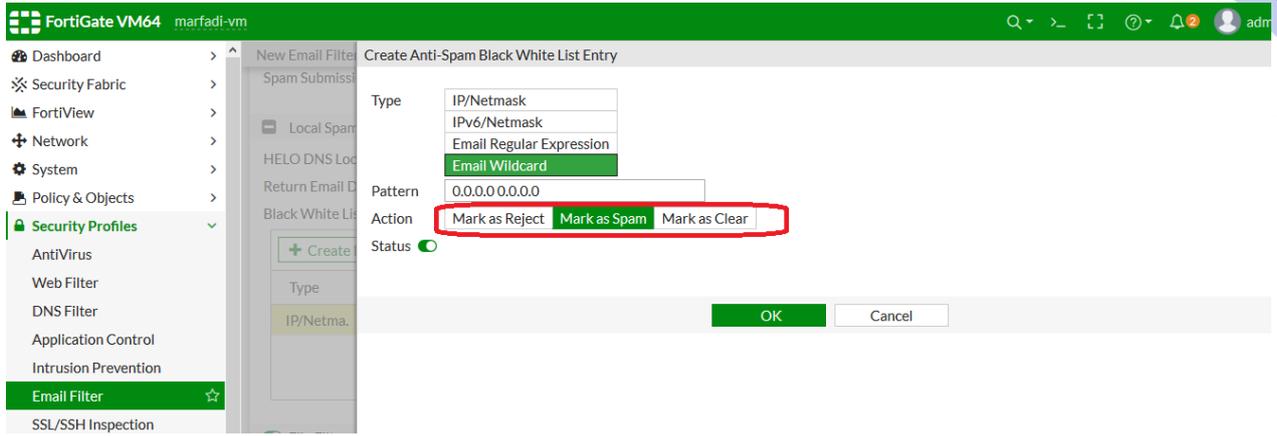
ايميل يأتي من الايبي 24/192.168.1.6 سيتم تطبيق عليه

الaction=mark as Spam أي علم عليه بأنه اسبام ايميل .



حيث الaction احدى الخيارات التالية :

- ١- Mark as Reject : ارفض الارسال والاستلام من هذا الايميل نهائيا مره أخرى .
- ٢- Mark as Spam : جعل الايميل ك اسبام
- ٣- Mark as Clear : مسح الايميل



طريقة الـ **Email Wildcard**: لوانت تستلم ايميلات مزعجه من دومين معين ايميل محدد فيمكنك

استخدام هذه الطريقة حيث هنا يمكن استخدام الرموز مثل *..

حيث أي ايميل من الدومين *@XX.COM سيتم رفضه ..

طريقة **Email Regular Expression**: نفس النوع السابق ولكن لا يمكن استخدام الرموز مثل *..



عبارة عن ارسال تنبيهات (alert) لمدراء الشبكة الذي يتحكموا بجهاز الفورتى جيت بالأحداث التي تحدث في الشبكة وذلك كنوع من التحذير والتنبيه والقيام بحدث معين.
حيث في حالة حدوث أي حدث (Event) فأن جهاز الفورتى جيت سوف يقوم بعملية التنبيه (alert) وذلك بالإرسال الى الايميل او الى الموبايل عبر SMS Getaway ..

شروط تنفيذ عملية logging and monitoring كالتالي :

1. ان يكون ال Fortigate device يستطيع الوصول الى الانترنت .
2. ان يكون لديك SMTP server مثل جوجل او ياهو او أي شركة استضافة مثل blue host او Hostator او غيرها حيث الذي يهيك هو الاعدادات الأساسية لعملية الارسال مثل رقم المنفذ مثلا smtp=25,26,465,587 والإعدادات تختلف من شركة الى أخرى mail.marfadi.com وأيضا تقوم بتحديد الايميل الذي سوف ترسل منه وأيضا الايميل الذي سوف يستقبل رسائل ال alert .
3. تفعيل عملية ال events حيث بشكل افتراضي تكون غير مفعلة (deactivate) على الفورتى جيت وأيضا تحدد الاحداث في حالة حدوثها يتم ارسال ايميل (alert) لأيميل يتم تحديده مسبقا ..

الآن سوف نقوم بتفعيل ال smtp server على الفورتى جيت مثلا smtp.gmail.com

حيث سيتم الارسال عبر الايميل الخيار Mohamed.marfadi@gmil.com Default Reply To

حيث بمجرد تمكين ال smtp server كما بالصورة أعلاه فأن خيار ال

Email Alert Settings تظهر لك كما بالصورة ادناه ...

الايمل المرسل حيث لو كان هناك تعارض بين الايمل هنا وبين الايمل المحدد ي smtp فان الايمل الذي سيتم الارسال منه هو الموجود في smtp server

تحدد الایميلات التي سو يصل لها التحذير عند حصول اي حدث

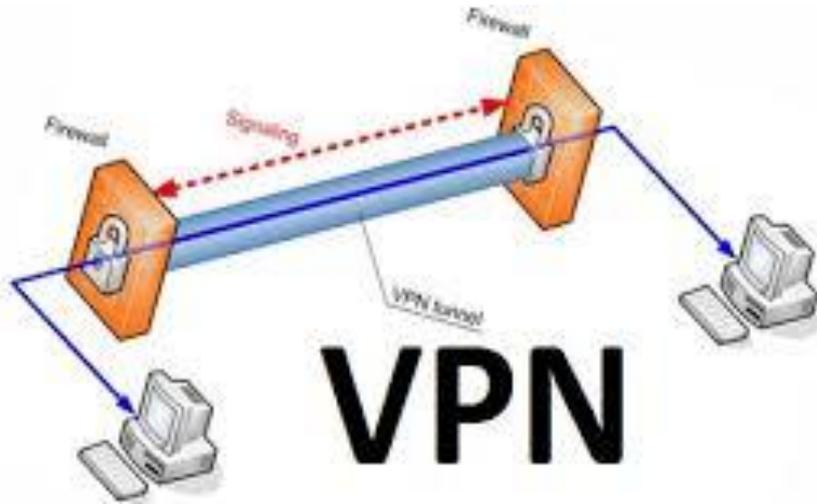
بعد 5 دقائق من حدوث الحدث (event) مثلا كما هو محدد ادناه (Configuration change) اي في حالة تم تعديل الاعدادات ي جهاز الفورتني جيت فأن جهاز الفورتني جيت سوف يقوم بعمل alert بارسال ايميل من mohamed.marfadi@gmail.com

هذا الاحداث التي سيتم تطبيقها مثلا الان تم تحديد Configuration chande

ما المقصود بـ VPN ؟

عبارة عن شبكة خاصة افتراضية أي عبارة عن تكوين شبكة بين عدة اطراف بواسطة الانترنت . حيث هدف الـ VPN هو السماح للوصول الى مصادر الشبكة (سيرفرات، طابعات، ملفات،....الخ) عن بعد بواسطة الانترنت حيث تصبح وكأنك موجود داخل الشبكة الداخلية (المحلية).

أي يمكنك عمل شبكة كاملة مكونه من عدة اجهزه (كمبيوترات، سيرفراتن IP PHONE، روترات ، سويتشات واكسس بوينت ... الخ حيث يتم ذلك عبر الانترنت بشكل آمن وبهذا يمكن ان أوصل الى السيرفرات .. الخ عن بعد عبر الانترنت وأيضا يمكنك الوصول الى الـ ERP من البيت عبر الانترنت .



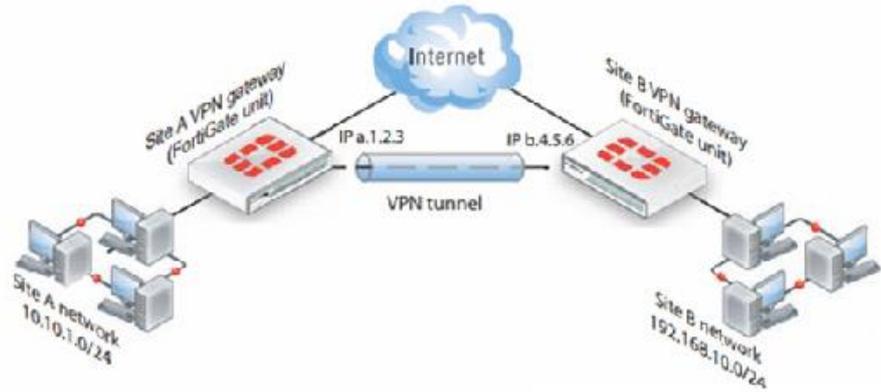
➤ أي بيانات تمر عبر الـ VPN تكون آمنة لأنها بتمر ب3 أشياء أساسيه (مميزات) :

1. توفيرقناه (Tunnel) تمر من خلالها البيانات من المصدر الى الهدف لذا تحقق الموثوقية والأمان .
2. البيانات بتمر بشكل مشفر خلال القناه من المصدر الى الهدف
3. يكون لها باسورد مشتركه تسمى (pre shared key) ما بين المصدر والهدف .

➤ اشكال الاتصال الـ VPN او يسمى (VPN Tunnel designs) :

1. Site-to-site VPN او peer to peer :

- The site-to-site VPN shown in this Figure is a peer-to-peer relationship



هذا النوع معناه بأن كل طرف لديه جهاز فورتى جيت يوجد ما بينهم قناه (tunnel). حيث كما بالصورة أعلاه يوضح بأنه يجب ان يكون لدى كل جهاز فورتى جيت Real ip كما موضح أعلاه الطرف الأول الايى هو (a.1.2.3) والطرف الاخر (b.4.5.6).

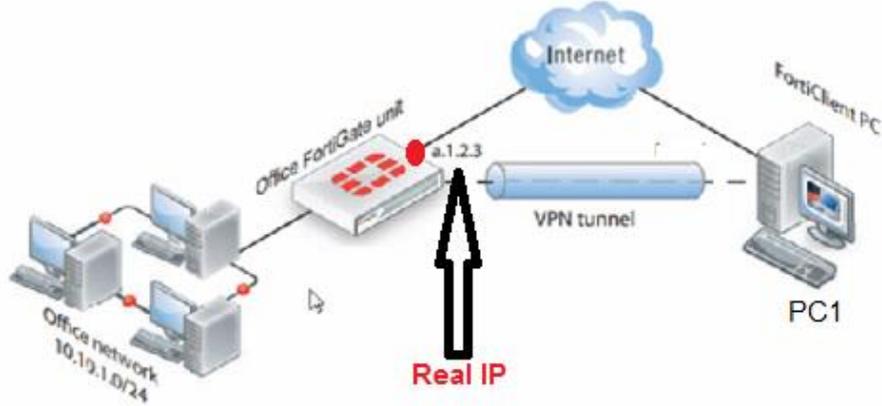
حيث يوجد لدينا كما بالصورة أعلاه 2 فروع (شبكتين محليتين) 24/10.10.1.0 والأخرى 24/192.168.10.0 مع العلم يمكن ان تربط اكثر من فرع (شبكة) بشرط توفر لديك في كل فرع جهاز فورتى جيت وأيضا real ip .

أساسيات فورتى جيت

حيث نلاحظ بأن كل شبكة داخلية لها PRIVATE IP مختلف عن الأخرى ولكن عن طريق الvpn فإن تلك الشبكات المختلفة تتصل مع بعض بشكل طبيعي .

٢. CLIENT-SERVER او يسمى FortiClient-to-Fortigate vpn :

➤ The FortiClient-to-FortiGate VPN shown in this Figure is a client-server relationship.



أي ان جهاز pc1 (يجب ان يكون منزل عليه برنامج forticlient) يستطيع الوصول الى الشبكة الداخلية 24/10.10.1.0 وليس العكس .

ملاحظة: pc1 يمكن ان يكون كمبيوتر او موبيل بمختلف انظمته التشغيل .

حيث يمكن للجهاز الوصول الى مصادر الشبكة الموجودة على الشبكة 24/10.10.1.0 وكأنك اخذت هذا الجهاز ووصلته بالسويتش الموجود بالفرع البعيد (24/10.10.1.0) .

٣. Another VPN vendors and fortigate unit .

حيث هذا النوع من الاشكال (site to site) أي ربط اكثر من فرع بحيث يكون احدى الأطراف هو جهاز الفورتى جيت والطرف الاخر أي جهاز فاير وول يتعامل مع بروتوكولات الvpn سواء كان من شركة سيسكو مثلا ASA او مثلا ايزا من مايكروسوفت او غيرها ..



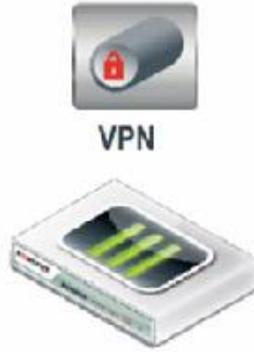
حيث هذا الشكل يعتبر نفس الشكل الأول (peer-to-peer) أي الند بالند .

➤ أنواع بروتوكولات الـ VPN :

☐ VPN Protocols

SSL VPN

- Typically used to secure web transactions
- HTTPS link created to securely transmit application data
- Client signs on through secure web page (SSL VPN portal) on the FortiGate device



IPSec VPN

- Well suited for network-based legacy applications
- Secure tunnel created between two host devices
- IPSec VPN can be configured between FortiGate unit and most third-party IPSec VPN devices or clients

حيث أي فايروول يجب ان يدعم هذه الأنواع من بروتوكولات الـ VPN وهما IPSec VPN و SSL VPN

IPSec VPN: تستخدم مع التطبيقات القديمة (windows application) بعكس الـ SSL VPN يعمل الـ tunnel مع http link ويستخدم الـ web application مع امكانيته استخدامه مع الـ windows application ولكن بشكل نادر..

حيث كليهما يحقق اعلى درجة من الأمان والموثوقية للبيانات ...

: VPN Encryption

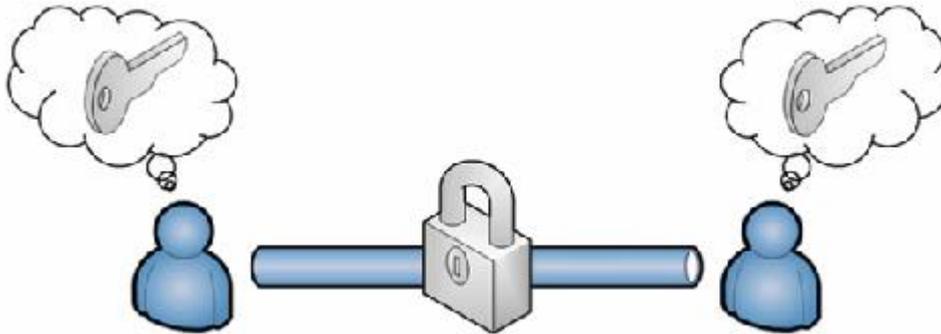
احدى اهم ميزات الـ VPN هي عملية تشفير البيانات التي بتمر من المصدر الى الهدف وذلك لزياده الأمان و الموثوقية .



حيث يتم عملية التشفير في المصدر (بأحدى خوارزميات التشفير) وعملية فك التشفير في الهدف ..

AES256	A 128-bit block algorithm that uses a 256-bit key.
AES192	A 128-bit block algorithm that uses a 192-bit key.
AES128	A 128-bit block algorithm that uses a 128-bit key.
3DES	Triple-DES, in which plain text is DES-encrypted three times by three keys.
DES	Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key

لزياده الأمان والموثوقية يقوم ال vpn بين طرفي الاتصال باستخدام باسورد متفق عليها بين الطرفين وتسمى بـ **preshared key** او **RSA certificate**



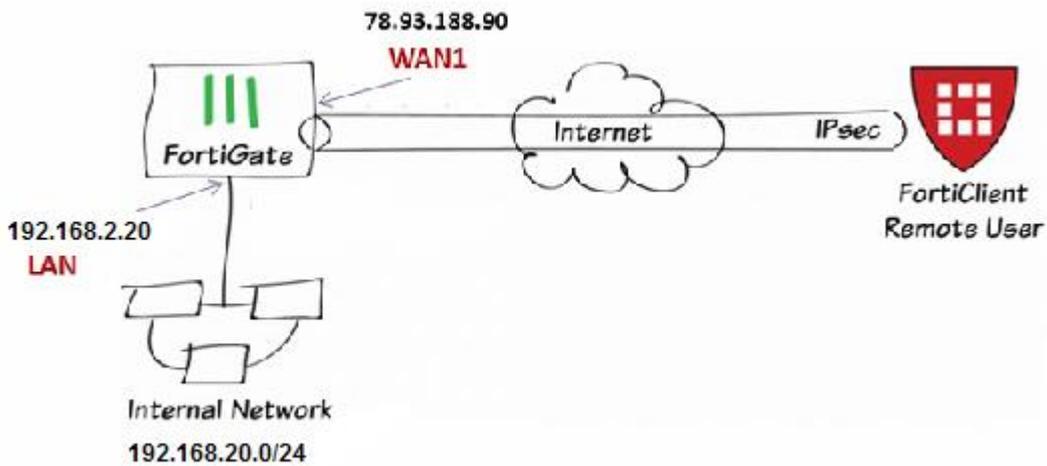
حيث يعتبر الفورتى جيت من اشهر الأشياء التي بتحقق لك VPN server والفورتى كلاينت من اشهر الأشياء التي بتحقق لك ان يكون لديك VPN client سواء على اجهزه موبايل او كمبيوتر وبغض النظر عن نوع نظام التشغيل ..

IPSec VPN : يمكن من خلاله ان تقوم بربط فرعين (site to site) او point to site .

أساسيات فورتى جيت

SSL vpn: لا يمكن استخدامه للربط بين الفروع بطريقة Site to site بل يستخدم في ربط point to site أي بين جهاز كمبيوتر وروتر مثلا يعني لازم تتصل ببيوزرنيم وباسورد ..

➤ التطبيق العملي لـ IPsec Client/server :



كما بالصورة أعلاه فأننا سوف نسمح لبيوزر (جهاز) بالوصول الى الشبكة الداخليه عبر IPsec vpn .

حيث يجب ان يكون لدي real ip للمنفذ Wan1 مثلا 78.93.188.90 حيث ان هذا الايبي متاح على الانترنت وأيضا متاح من داخل الشبكة الداخليه بعكس ال private ip للشبكة الداخليه 24/192.168.2.0 الذي يكون متاح فقط من داخل الشبكة الداخليه .

حيث wan1 هو الذي سيقوم باستلام الاتصال القادم من المستخدمين من برع الشبكة (Remote user) كما بالصورة الموضحة أعلاه .

حيث الجهاز سوف يتصل بالايبي 78.93.188.90 عبر برنامج الفورتى كلاينت

.fortiClient

أساسيات فورتى جيت

حيث الفكرة التي اريد ان احققها هي اني اسمح للجهاز المنزل عليه برنامج الفورتى كلاينت الوصول الى أي جهاز بالشبكة الداخلية وذلك بعد تأسيس الاتصال عبر IPsec بشرط يكون لديه اليوزرنيم والباسورد .

حيث يمكن لعدد كبير من Clients الوصول الى الفورتى جيت بنفس الوقت .

ويمكنك ان تقوم بعمل policy بحيث تحدد الشبكات او الاجهزه المراد الوصول اليها فقط ..

في هذه الطريقة اصبح الجهاز البعيد(remote user) مثله مثل أي جهاز داخل الشبكة الداخليه ..

ولتطبيق هذا العملية يجب ان تحقق المتطلبات التالية :

1. يكون لدي يوزر محلي على الفورتى جيت (user) حيث هذا اليوزر (الحساب) سوف يتم اعطاءه لليوزر البعيد (remote user) للسماح بالاتصال بالفورتى جيت ، كما يمكن انشاء جروبات لتصنيف مثلا جروب للمدراء وجروب للتسويق وجروب للاتي ... الخ حيث ان الجروب ليست شي أساسي ولكن كنوع من التنظيم .
2. ان يكون لدي عناوين (address) للشبكة الداخليه لتعريف الفورتى جيت بعنوان الشبكة الداخلية لكي اسمح بعد ذلك لأي شخص من خارج الشبكة (remote user) بالوصول اليها .
3. انشاء IPsec tunnel واحد فيها preshared key او الشهادة لكي اجعل الاخرين يتصلوا بها .
4. انشاء بولييسي لكي اسمح للترافيك من remote user الى الشبكة الداخليه حيث سيكون لدينا 2 بولييسي

البولييسي الأولى لكي اسمح بالترافيك الوصول من الفورتى جيت الى الشبكة الداخليه وهذه البولييسي يتم انشاءها جهاز الفورتى جيت بشكل اوتوماتيكي بمجرد انشاء tunnel

اما البولييسي الثانية سيتم انشاءها بحيث تسمح بوصول الترافيك من جهاز اليوزر (remote user) الى جهاز الفورتى جيت (الى wan1 interface)

5. سنقوم بعمل اعدادات معينه لبرنامج الفورتى كلاينت على اجهزه اليوزر (remote user).

التطبيق العملي :

الخطوة الأولى :

انشاء local user بعدد الأشخاص المراد السماح لهم كما بالتالي :

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

- Local User
- Remote RADIUS User
- Remote TACACS+ User
- Remote LDAP User
- FSSO
- FortiClient EMS User
- FortiNAC User

User & Device

- User Definition
- User Groups
- Guest Management
- Device Inventory
- LDAP Servers
- RADIUS Servers
- Authentication Settings
- FortiTokens

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Username marfadi1

Password ●●●

FortiGate VM64 marfadi-vm

Users/Groups Creation Wizard

1 User Type > 2 Login Credentials > 3 Contact Info > 4 Extra Info

Email Address

SMS

Two-factor Authentication

أساسيات فورتى جيت

- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device**
- User Definition**
- User Groups
- Guest Management
- Device Inventory
- LDAP Servers
- RADIUS Servers
- Authentication Settings
- FortiTokens
- Log & Report

Users/Groups Creation Wizard

✓ User Type > ✓ Login Credentials > ✓ Contact Info > **4 Extra Info**

User Account Status: Enabled Disabled

User Group:

FortiGate VM64 marfadi-vm

admin

+ Create New Edit Clone Delete Search

Name	Type	Two-factor Authentication	Ref.
guest	LOCAL	✘	1
marfadi1	LOCAL	✘	0
marfadi2	LOCAL	✘	0

كما بالصورة أعلاه تم إنشاء 2 يوزر.
ثم نقوم بإنشاء جروب باسم vpn_users ونضعهما فيه.

The screenshot shows the 'New User Group' configuration page in the FortiGate VM64 web interface. The left sidebar has 'User & Device' expanded, with 'User Groups' highlighted. The main form has the following fields:

- Name: vpn_users
- Type: Firewall
- Members: marfadi1, marfadi2
- Remote Groups: No results

 The 'Select Entries' panel on the right shows a list of users: guest, marfadi1, and marfadi2.

الخطوة الثانية:

انشاء العناوين للشبكة الداخليه

The screenshot shows the 'New Address' configuration page in the FortiGate VM64 web interface. The left sidebar has 'Policy & Objects' expanded, with 'Addresses' highlighted. The main form has the following fields:

- Name: INTERNAL_NETWORK
- Color: Change
- Type: Subnet
- IP/Netmask: 192.168.2.0/24
- Interface: LAN1 (port1)
- Show in address list:
- Static route configuration:
- Comments: Write a comment... (0/255)

 The 'OK' button is highlighted at the bottom right.

أساسيات فورتني جيت

Name	Type	Details	Interface
Address			
FABRIC_DEVICE	Subnet	0.0.0.0/0	
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0	
INTERNAL_NETWORK	Subnet	192.168.2.0/24	LAN1 (port1)
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interf
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VL
YEMEN	Geography	United States	
all	Subnet	0.0.0.0/0	
gmail.com	FQDN	gmail.com	
login.microsoft.com	FQDN	login.microsoft.com	
login.microsoftonline.com	FQDN	login.microsoftonline.com	
login.windows.net	FQDN	login.windows.net	
none	Subnet	0.0.0.0/32	
pc1	Subnet	192.168.2.144/32	LAN1 (port1)
server1	Subnet	192.168.2.122/32	LAN1 (port1)

الخطوة الثالثة :

انشاء IPSEC tunnel

FortiGate VM64 marfadi-vm

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > Security Profiles > VPN > IPsec Tunnels

+ Create New
IPsec Tunnel
IPsec Aggregate

Interface Binding Status Ref

No results

أساسيات فورتى جيت

VPN Creation Wizard

1 VPN Setup > 2 Authentication > 3 Policy & Routing > 4 Client Options

Name: **IPSec_tunnel**

100 concurrent user(s) will be supported

Template type: Site to Site | Hub-and-Spoke | **Remote Access**

Remote device type: Custom | **Client-based** | Native

FortiClient | Cisco

Dialup - FortiClient (Windows, Mac OS, Android)

This FortiGate | Internet | FortiClient

< Back | **Next >** | Cancel

حيث تم تحديد اسم لل tunnel باسم IPSec_tunnel ونوعها Remote Access وكما بالصورة أعلاه فأن
اجهزة اليوزر يمكن ان تكون ويندوز او ماك او اندرويد .

FortiGate VM64 marfadi-vm

VPN Creation Wizard

1 VPN Setup > **2 Authentication** > 3 Policy & Routing > 4 Client Options

Incoming Interface: **WAN (port2)**

Authentication method: **Pre-shared Key** | Signature

Pre-shared key: [Redacted]

User Group: **vpn_users**

IPSec_tunnel: Dialup - FortiClient (Windows, Mac OS, Android)

This FortiGate | Internet | FortiClient

< Back | **Next >** | Cancel

كما بالصورة أعلاه تم تحديد نوع ال incoming interface الذي سيتقبل الاتصال وهو كما شرحنا
سابقا سيكون wan1 الذي عليه ال real ip
وسوف نكتب ال preshared key التي سيتم إعطائها للمستخدمين الذي سوف يدخلوا من خارج
الشبكة (Remote users)

تم تختار الجروب المسموح لها توصل لـ tunnel المسماة IPsec_tunnel
مثلا vpn_users والتي بداخلها اليوزرات marfadi1 و marfadi2

كما بالصورة أعلاه تم تحدد local interface =lan1 وهي الشبكة الداخليه وبالتحديد local address=Internal_network التي تم تحديدها سابقا بـ 24/192.168.2.0 .

وتم تحديد الايبيهاث التي سوف يحصل عليها اجهزه الـ remote users من جهاز الفورتى جيت بمجرد الاتصال بـ vpn وهي 10.10.10.1 الى 10.10.10.5 أي خمسة اجهزه .

وتوجد لدينا خاصيتين :

Enable ipv4 SplitTunnel حيث عند تفعيلها فانت تسمح للـ remote users بالوصول الى شبكات

محدد ه ..

Allow Endpoint Registeration عند تفعيلها فانت بذلك تفعل عمليه الـ registration على برنامج

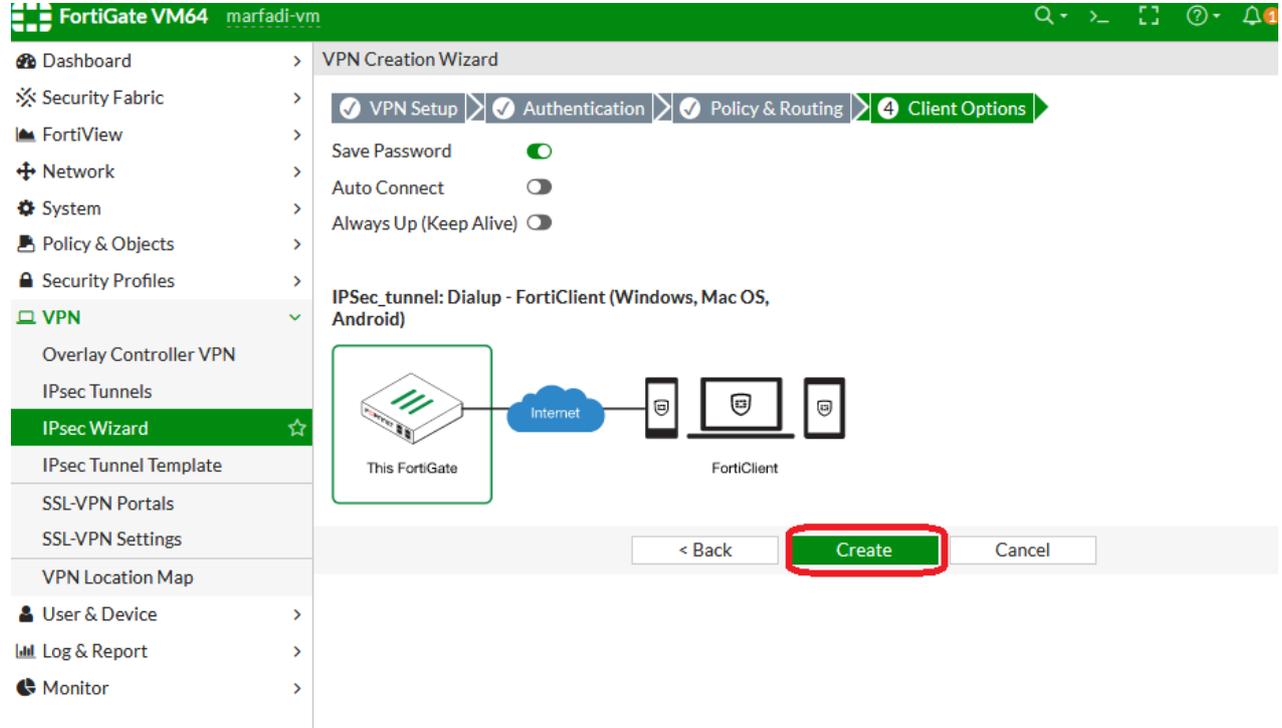
.. forticlient

حيث الكلاينث (remote user vpn) يمكن يعمل تسجيل على الفورتى جيت

أساسيات فورتى جيت

حيث هذه الخاصية يمكن من خلالها تطبيق بروفایل على هذا اليوزر(الكلاينت)

فهذا يمكن تطبيق على جهاز اليوزر أي بروفایل (web filter, app control, anti virus, ips) و كانه جهاز على الشبكة الداخليه وهذا أصبحت الاجهزه التي تعمل remote vpn مؤمنه أيضا ..



: Save Password

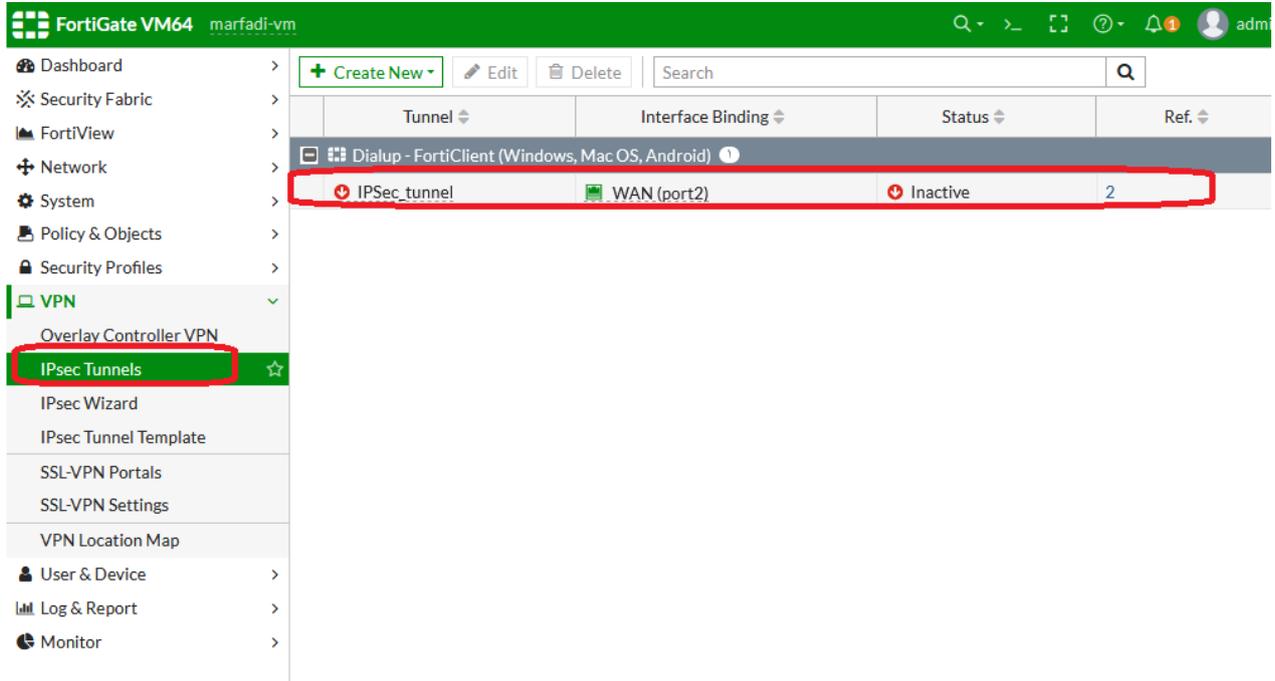
عندما تتم عمليه الاتصال للكلاينت مع الفورتى جيت فهل تريد السماح بعمل save للباسورد على جهازه ام لا !

: Auto Connect

هل تريد بأن تجعل الشخص (Remote user) يعمل Auto connect أي بمجرد ان نظام التشغيل يعمل فانه يتم الاتصال بالفورتى جيت عبر VPN بواسطة ال forticlient ام لا !!

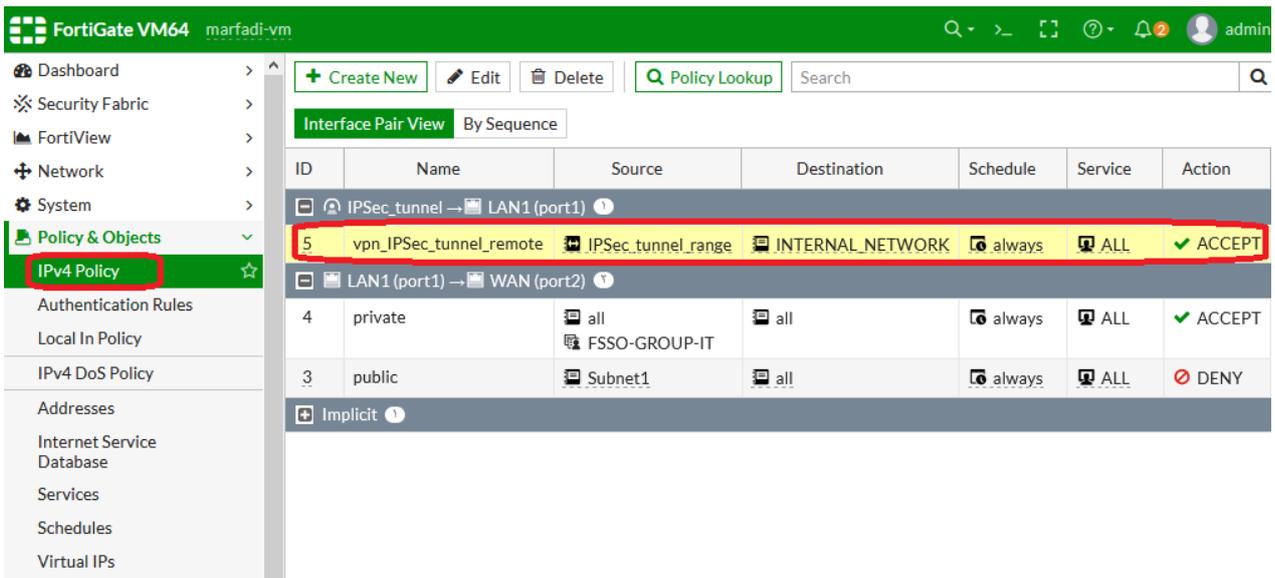
: Always Up (Keep Alive)

جعل الاتصال شغال على طول بحيث لو حصل مشكله او فصل بالإنترنت على جهاز اليوزر فإنه بمجرد ما يعود الانترنت للجهاز تتم عمليه الاتصال مباشره حيث كل 3 دقائق يقوم الفورتى كلاينت بعمل اعاده اتصال ..



تم انشاء الvpn tunnel وحالتها Inactive لأن لا يوجد أي اتصال حاليا عليها من أي يوزر فمجرد الاتصال يصبح الحالة active .

نلاحظ بأنه بمجرد انشاء ال tunnel تم انشاء بوليسي كما بالصورة ادناه



أساسيات فورتى جيت

بعد ذلك يجب ان تقوم بتوجيه الترافيك القادم من الخارج (remote users) الى الفورتى جيت وذلك بإنشاء البوليسى كالتالي :

بحيث نقول أي اتصال من ipsec_tunnel وهو الـ virtual interface بأي ايبى سأل على الـ WAN1 بأي ايبى اسمح له بالوصول كما بالصورة ادناه

The screenshot shows the 'New Policy' configuration page in FortiGate. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy'. The main configuration area is titled 'New Policy' and contains the following settings:

- Name: allow_remote_vpn
- Incoming Interface: IPSec_tunnel
- Outgoing Interface: WAN (port2)
- Source: all
- Destination: all
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (unchecked)
- Inspection Mode: Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:
 - NAT:
 - IP Pool Configuration: Use Outgoing Interface Address (selected), Use Dynamic IP Pool (unselected)
 - Preserve Source Port:
 - Protocol Options: PRX default
- Security Profiles: (empty)

أساسيات فورتني جيت

The screenshot shows the FortiGate VM64 configuration interface. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy'. The main area displays a table of policies under the 'Interface Pair View' tab. The policy 'allow_remote_vpn' is highlighted in yellow. The table has the following columns: ID, Name, Source, Destination, Schedule, Service, and Action.

ID	Name	Source	Destination	Schedule	Service	Action
5	vpn_IPSec_tunnel_remote	IPSec_tunnel_range	INTERNAL_NETWORK	always	ALL	ACCEPT
6	allow_remote_vpn	all	all	always	ALL	ACCEPT
4	private	all FSSO-GROUP-IT	all	always	ALL	ACCEPT
3	public	Subnet1	all	always	ALL	DENY
	Implicit					

تم

انشاء البوليسي وبهذا اصبح جهاز الفورتني جيت اصبح جاهز لاستقبال الاتصال عبر vpn connection
بعد ذلك سوف نقوم بعمل الإعدادات على برنامج الفورتني كلاينت ..

The screenshot shows the FortiClient VPN interface. The title bar reads 'FortiClient VPN'. Below the title bar, there is a message: 'Upgrade to the full version to access additional features and receive technical support.' The main area features a large blue icon of a globe with a laptop and a padlock, representing a VPN connection. At the bottom, there is a red-bordered button labeled 'Configure VPN'.

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

New VPN Connection

VPN: SSL-VPN IPsec VPN

Connection Name:

Description:

Remote Gateway: *
+Add Remote Gateway

Authentication Method:

Authentication (XAuth) Prompt on login Save login Disable

+ Advanced Settings

حيث تم تحديد نوع الاتصال هو IPsec VPN ثم أي اسم للاتصال وليكن Marfadi
و remote Getaway هو ايي WAN1 وهول real ip المحدد 78.93.188.90

FortiClient VPN

Upgrade to the full version to access additional features and receive technical support.

VPN Name:

Username:

Password:

ثم نقوم بإدخال اليوزرنيم والباسورد لليوزر مثلا marfadi1 والذي قمنا بإنشائه في اول الخطوات ثم
نقوم بعمل اتصال ..

أساسيات فورتى جيت

بحسب الصورة أعلاه فأننا سوف نقوم بعملية ربط فرعين ببعض (الحديده ،عدن) عبر الفورتى جيت بواسطة الانترنت بحيث الجهاز الذي بفرع الحديده يستطيع الوصول بالجهاز الموجود بعدن والعكس ...

نلاحظ بأن هنالك جهاز فورتى جيت في كل فرع وأيضا real ip لكل فرع .

قمنا بأعداد ال vm للفرع ADEN

```
FortiGate-UM64 login:
FortiGate-UM64 login: admn
Password: ***
^C
FortiGate-UM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:*****
Confirm Password:*****
Welcome !

FortiGate-UM64 # config system interface

FortiGate-UM64 (interface) # edit port1

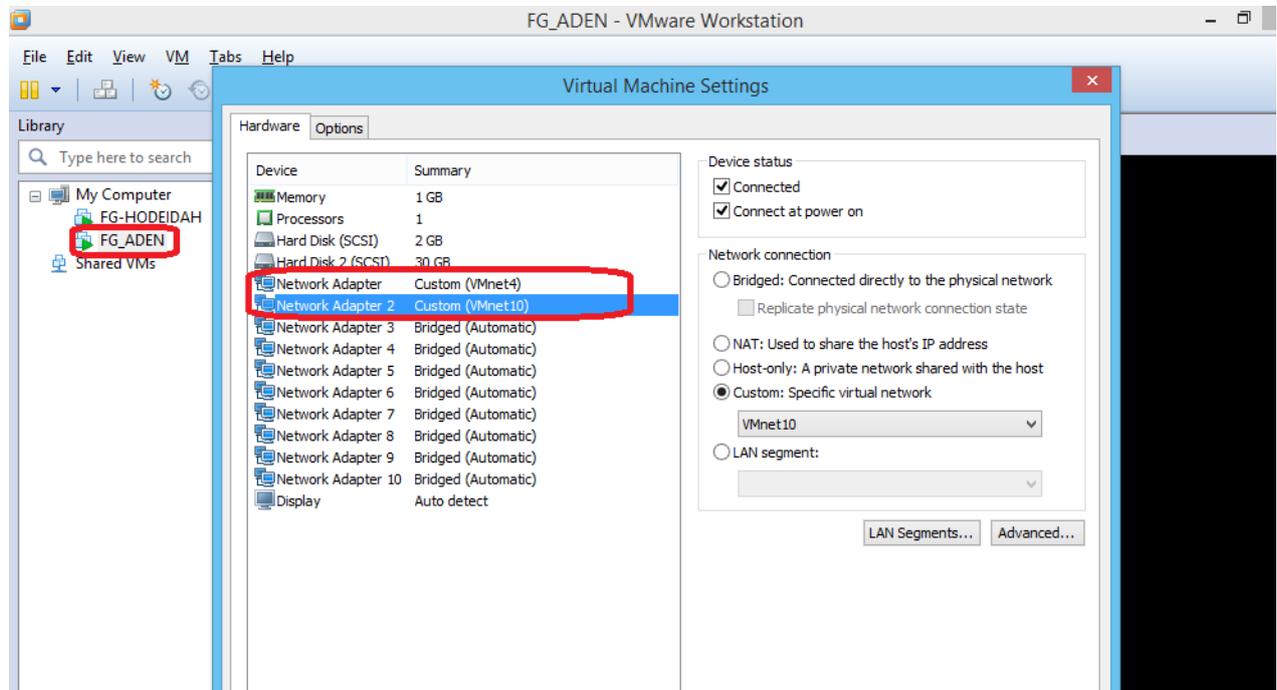
FortiGate-UM64 (port1) # set mode static

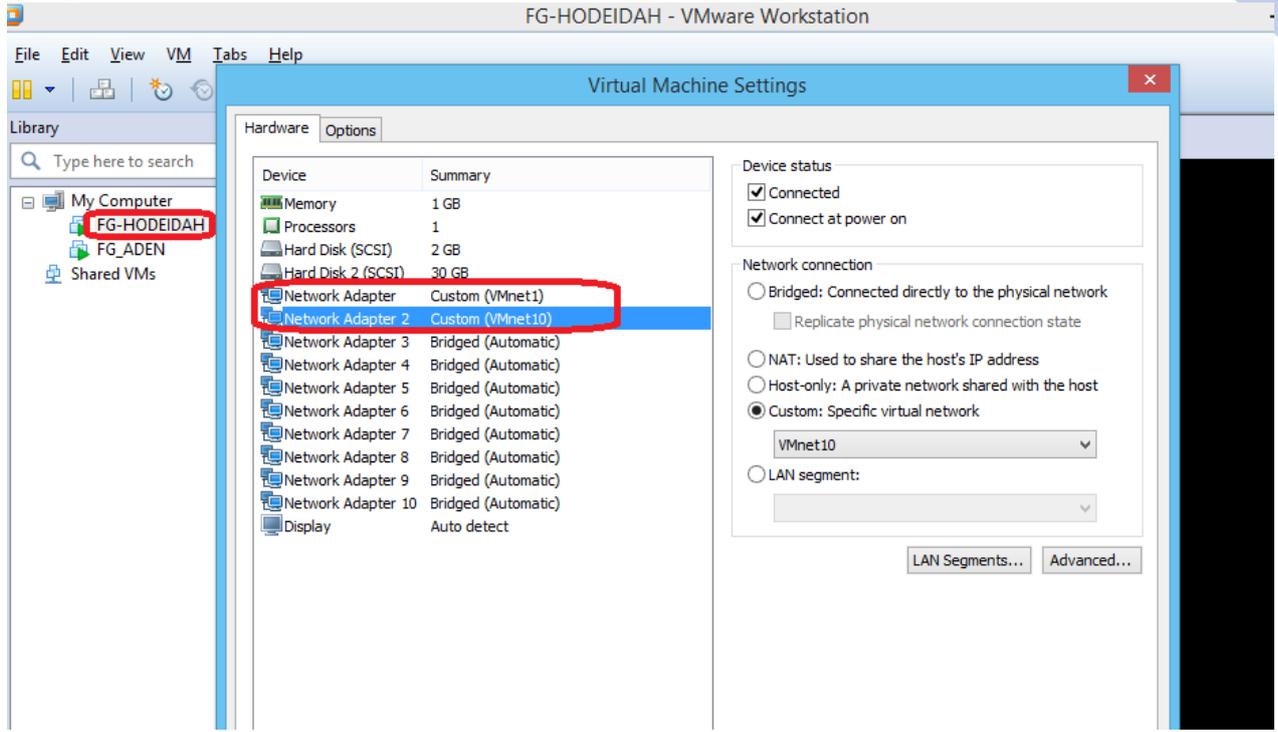
FortiGate-UM64 (port1) # set ip 10.0.0.99 255.255.255.0

FortiGate-UM64 (port1) # set allowaccess https http ping ssh

FortiGate-UM64 (port1) # end

FortiGate-UM64 # _
```





نلاحظ بأننا جعلنا كرت الشبكة (LAN) لفرع **الحديده** هو VMnet1

سوف نجعل كرت الشبكة لجهاز الكمبيوتر PC-HOD الموجود بفرع الحديده على السويتش VMnet1 ..

والكرت الاخر (WAN1) لفرع **الحديده** هو VMnet10

وسوف نجعل كرت الشبكة (LAN) لفرع **عدن** هو VMnet4

سوف نجعل كرت الشبكة لجهاز الكمبيوتر الموجود بفرع الحديده على السويتش VMnet4 ..

والكرت الاخر (WAN1) لفرع **عدن** هو VMnet10

وبهذا الطريقة وكأننا جعلنا الاثنين الـ Vm مربوطين على الانترنت لعمل محاكاة ..

فنلاحظ بأن جهاز الكمبيوتر الموجود في الفرع الحديده في شبكة مختلفه وأيضا على سويتش مختلف عن جهاز الكمبيوتر الموجود في الفرع عدن ..

نحن نريد تحقيق عمليه الاتصال فيما بين الجهازين PC-HOD مع PC-ADEN بواسطة IPsec vpn .

الـ VPN تعتبر من احدى الوسائل الأساسية للوصول الى INTERNAL NETWORK من أي مكان بالعالم
مثلا كما يحصل حاليا بسبب جائحه كورونا (work at home) عبر الانترنت .

حيث الفورتني جيت تقدم لنا اكثر من طريقة لعمل vpn :

١- vpn over IP SEC

٢- vpn over SSL

vpn over SSL

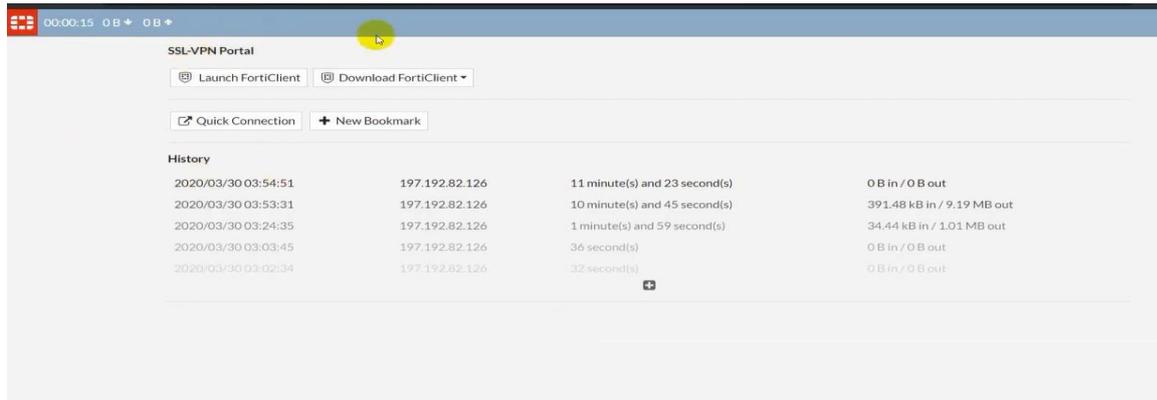
حيث ال vpn/ssl بيتم بطريقتين :

١- **web mode** : هي عبارة عن صفحة انترنت من خلالها يتم الوصول الى الشبكة الداخليه الخاصة بي

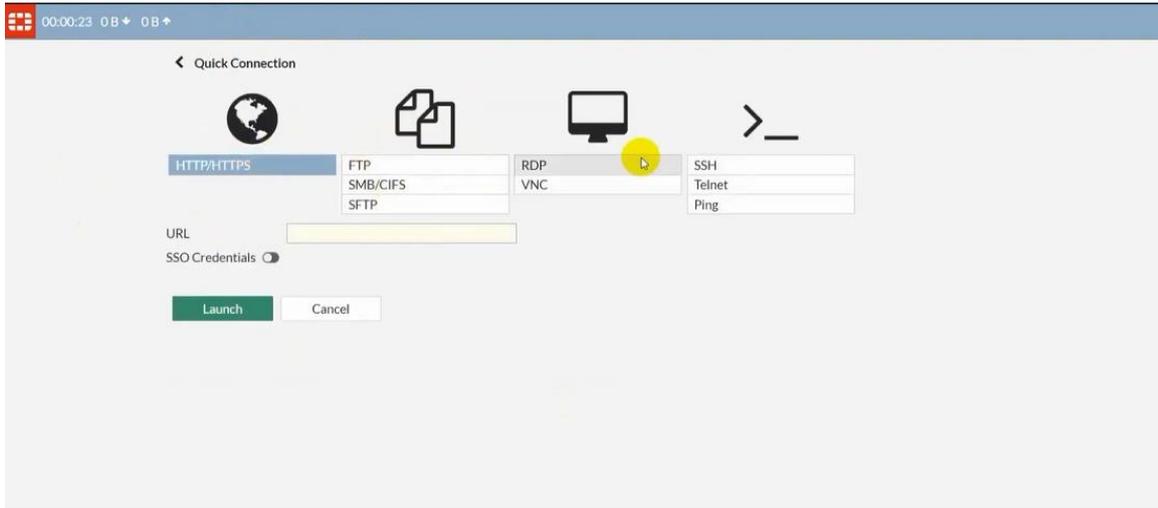
واقدر أوصل الى سيرفيس معينه انا محددتها مسبقا او الى كل ال services هذا حسب ما تريده وكل

هذا بيتم عبر web interface مثلا IE او Mozilla firefox .. الخ

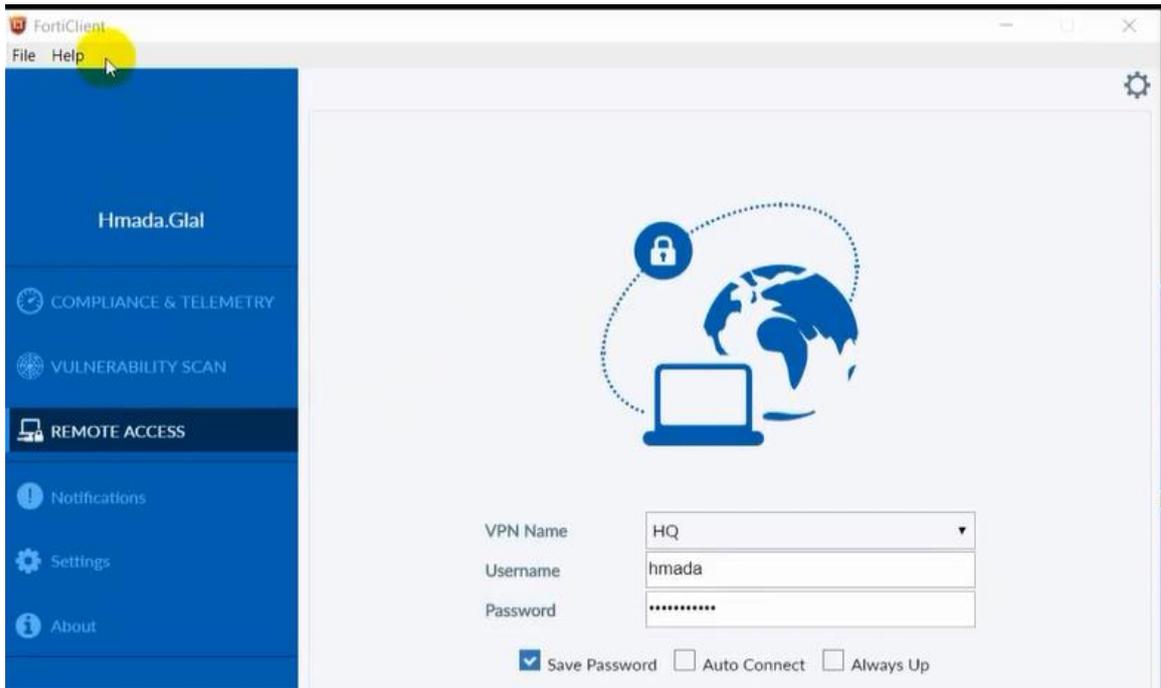
حيث شكل ال web mode كما بالصورة ادناه



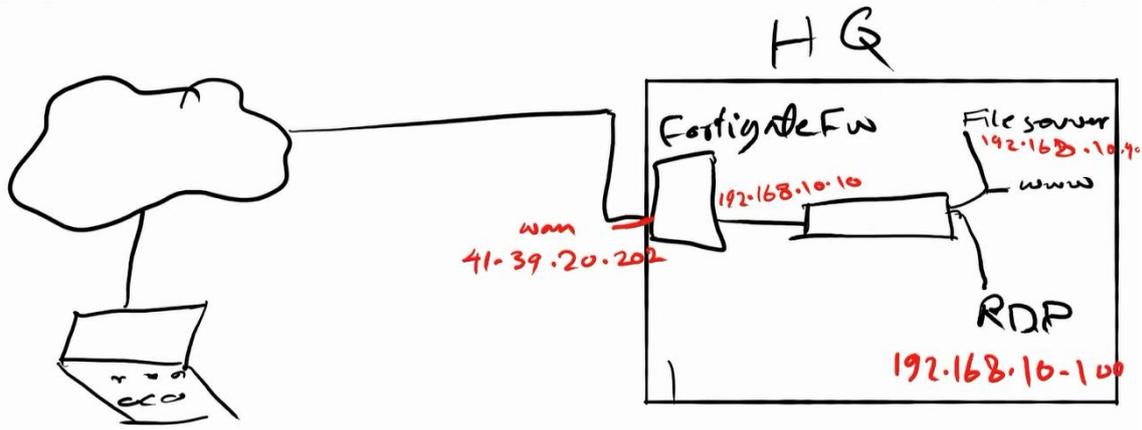
والذي من خلاله يمكنه الوصول الى ال services كما بالصورة ادناه



٢- *Tunneling mode* : هو الشكل المعتاد الذي من خلاله يعمل vpn حيث فورتى جيت بتستخدم برنامج تابع لها يسمى Forticlient ويتم تنزيله على الويندوز او الماك او اندرويد



كما بالصورة ادناه سوف نقوم بشرح التصميم لل lab :



حيث نريد الوصول عبر الالبتوب الى الفايل سيرفر وباقي السيرفرات الموجودة في الشبكة الداخليه كما بالصورة أعلاه ..

حيث ال ssl vpn يحتاج بعض الإعدادات على الفورتى جيت لكي يتم تنفيذه :

- 1- يحتاج الى انشاء local user و local Group لديهم صلاحية ال vpn
- 2- Listen interface وهو ال WAN يكون عليه ال real ip
- 3- Security policy تسمح بمرور الترافيك ما بين الشبكة الداخليه وال vpn وما بين ال vpn والانترنت لو اردت اجعل المستخدمين الي برع الشبكة مثلا جهاز (الالبتوب) يستخدم الانترنت من خلال الشبكة الداخليه الخاصة بي .

الان سوف نقوم بعملية التطبيق عمليا :



أساسيات فورتى جيت

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Username hmada.gal

Password

تم انشاء local user باسم hmada.gal

Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

Email Address

SMS

Two-factor Authentication

ثم نقوم بكتابه الايميل الخاص بي في حالة تم نسيان الباسورد سيقوم بإرساله الى الايميل في حالة قمت بعمل reset password

FortiGate 80E CarePharma-Fortinet

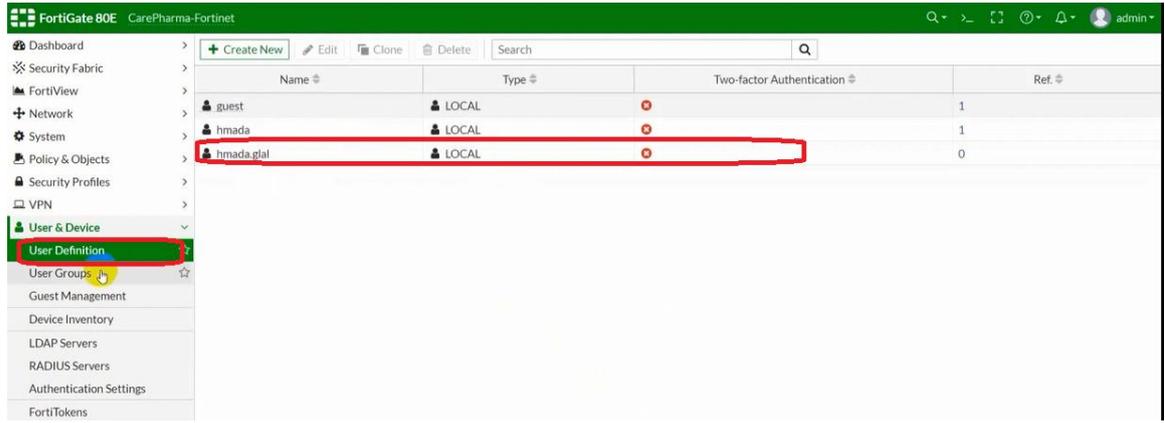
Users/Groups Creation Wizard

1 User Type 2 Login Credentials 3 Contact Info 4 Extra Info

User Account Status Enabled Disabled

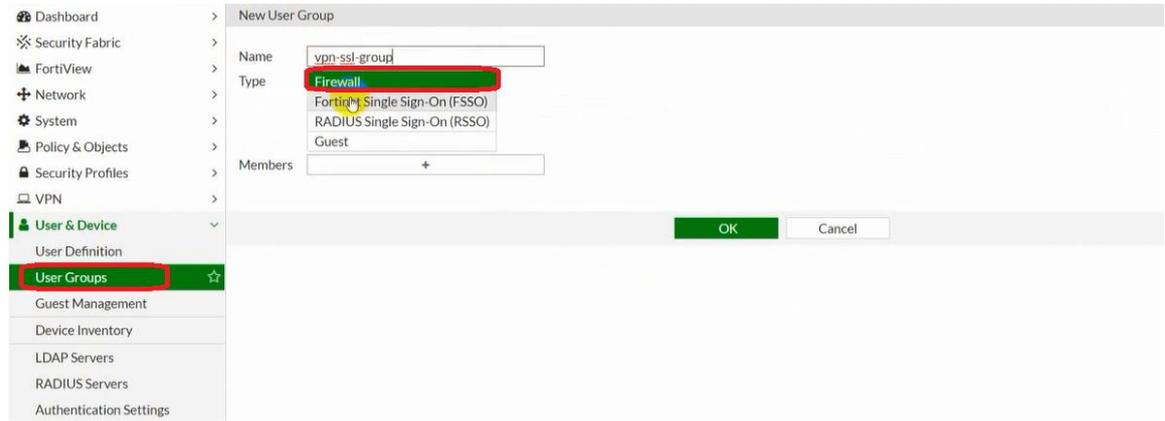
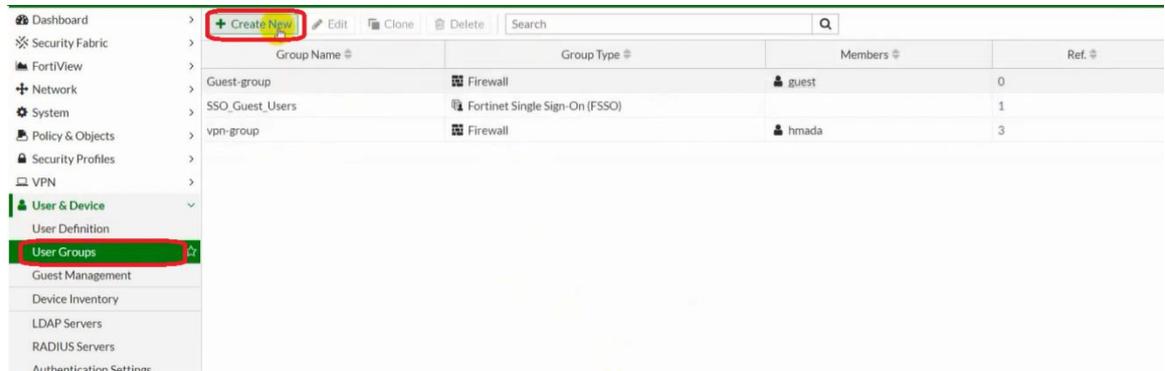
User Group

حيث حالة الحساب هي Enabled .



تمت عمليه الانشاء ..

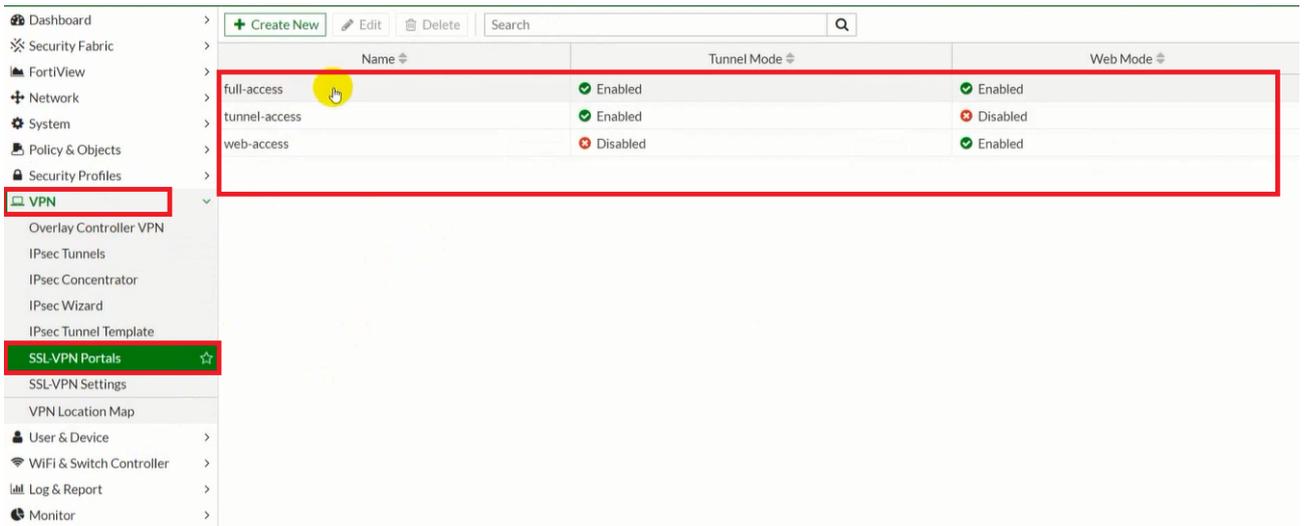
الآن سنقوم بإنشاء group كما بالصورة ادناه



اسمها VPN-SSL-group ونوعها لوكالي (Firewall)



ثم نقوم بإضافه اليوزرات اليها ..



نلاحظ كما بالصورة أعلاه بان الفورتني جيت بشكل افتراضي يوجد بداخله 3 portal كالتالي :

Full-access: هنا لهم صلاحيات بانهم يوصلوا الى vpn سواء عبر ال tunnel mode او web access

Tunnel-access: هذه صلاحيات خاصه ب tunnel mode

Web-access: هذه خاصه بالويب اكسس حيث اليوزرات التي سوف يتم وضعهم هنا سيتم اعطائهم صلاحيات بانهم يوصلوا الى vpn عبر الويب مود .

حيث سنقوم بالتعديل على full-access :

Name	Tunnel Mode	Web Mode
full-access	Enabled	Enabled
tunnel-access	Enabled	Disabled
web-access	Disabled	Enabled

FortiGate

CarePharma-Fortinet

Documentation

Online Help

Video Tutorials

Name: full-access

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode **Disabled**

Enable Split Tunneling

Routing Address: +

Source IP Pools: SSLVPN_TUNNEL_ADDR1

Tunnel Mode Client Options

Allow client to save password:

Allow client to connect automatically:

Allow client to keep connections alive:

DNS Split Tunneling:

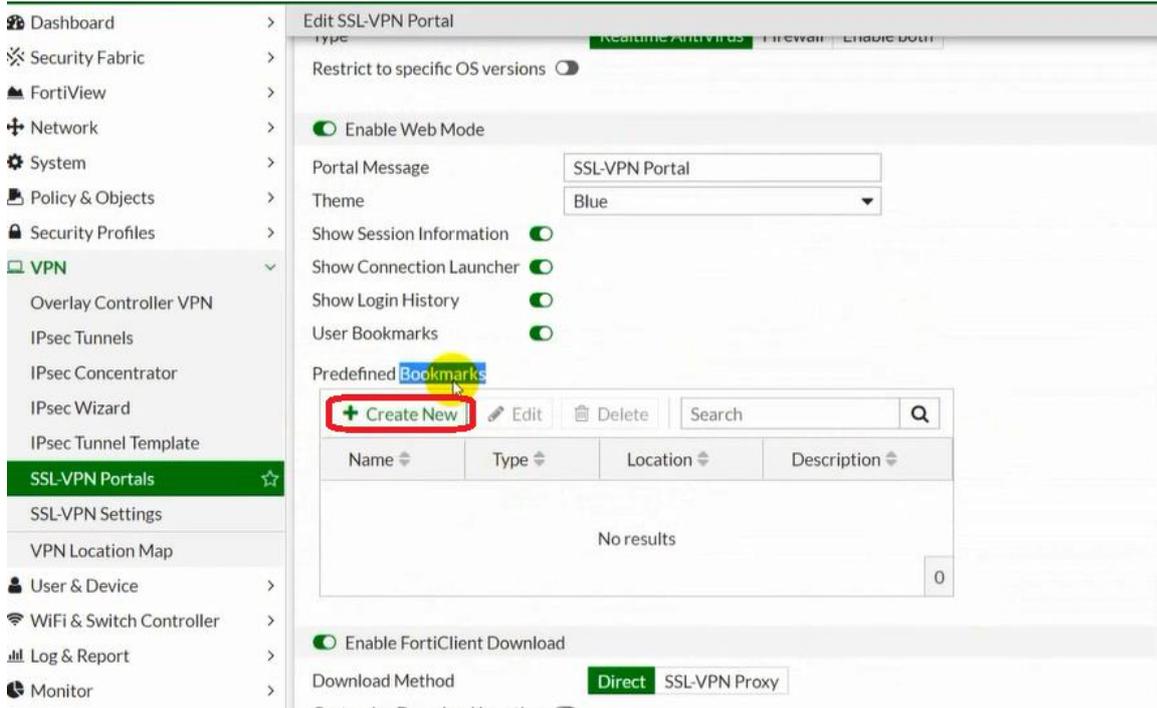
Host Check:

Type: Realtime AntiVirus Firewall Enable both

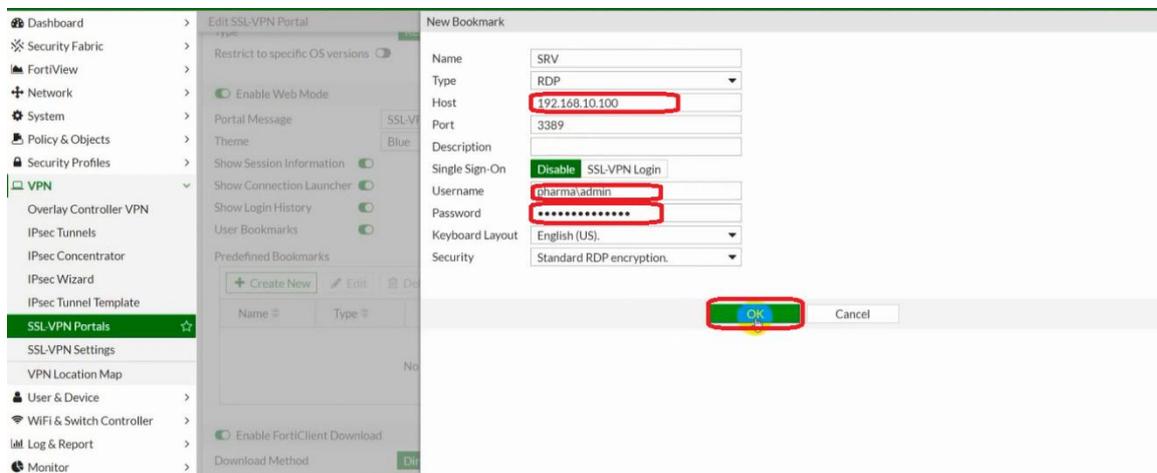
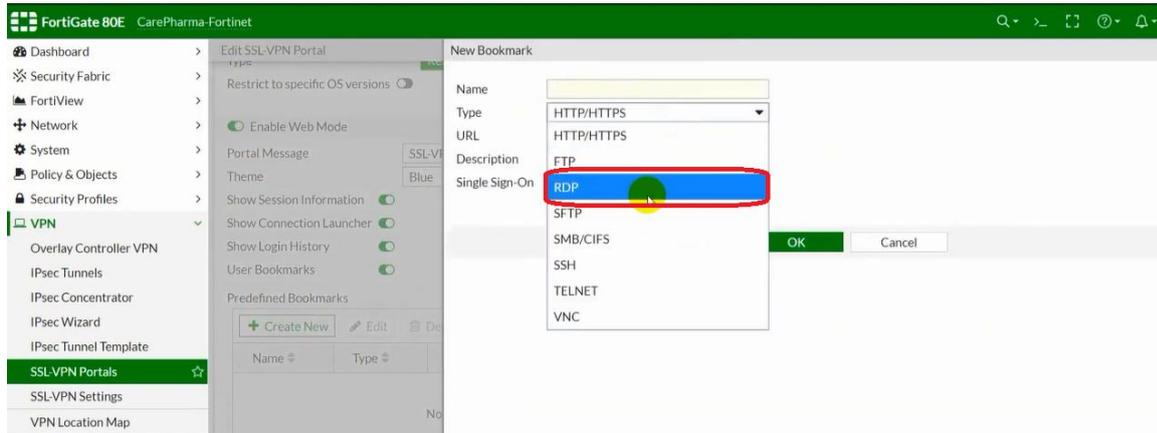
Restrict to specific OS versions:

Enable Web Mode:

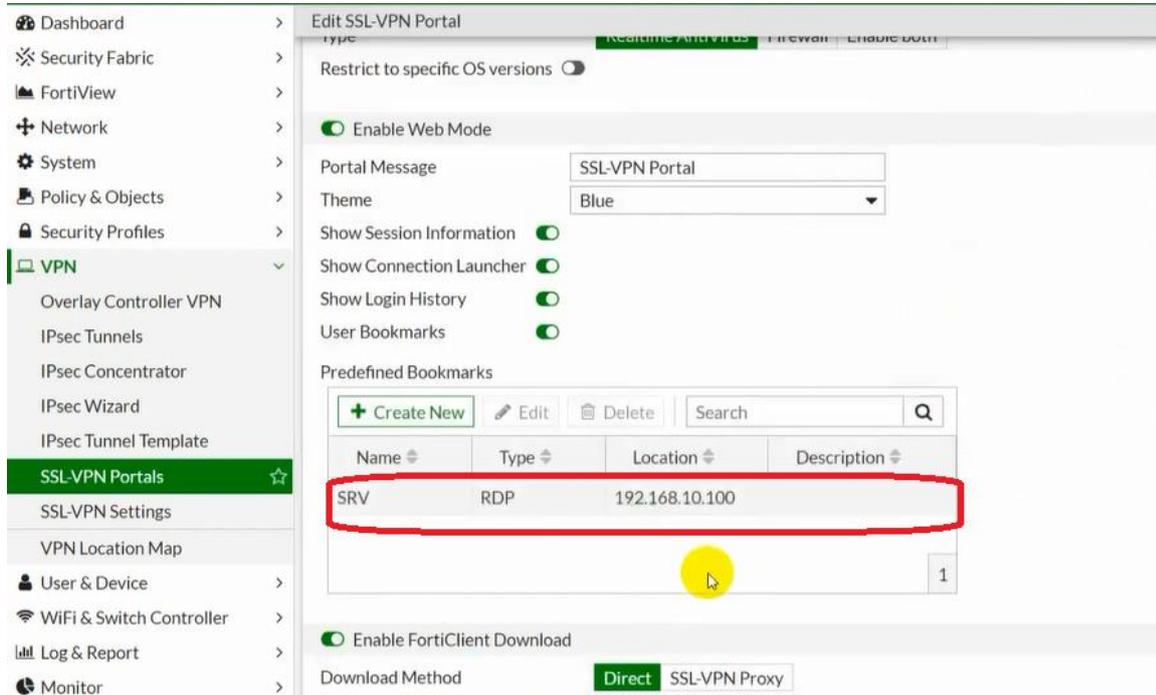
كما بالصورة أعلاه تم اغلاق الخيار Enable Split Tunneling



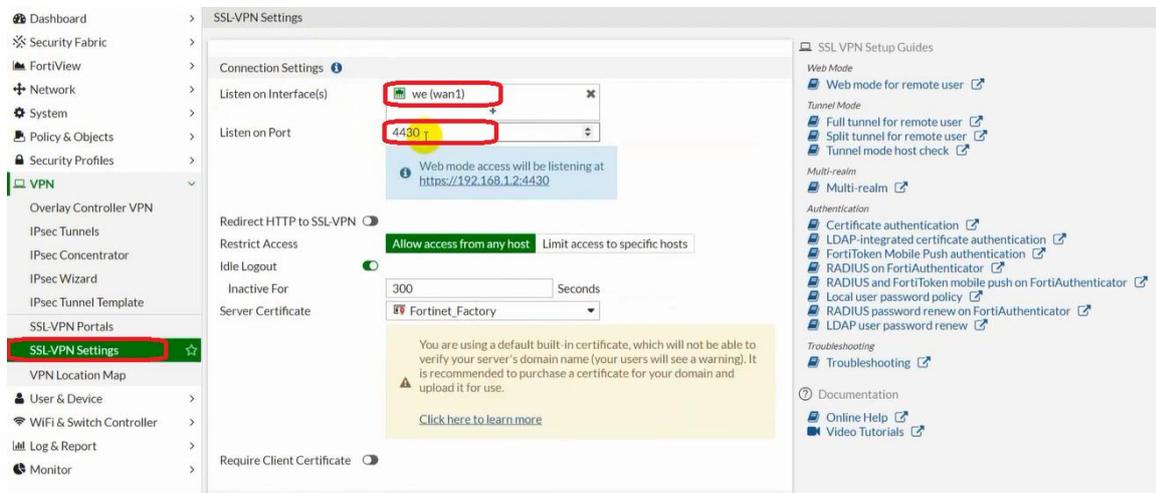
ولو اردت أضافه Bookmarks لـ web access mode



تم إضافة bookmark حيث سيتم الوصول الى السيرفر 192.168.10.100 عبر ال remote Desktop (RDP) حيث تم كتابه اليوزرنيم والباسورد التابع للسيرفر



بعد ذلك نقوم بالذهاب الى SSL-VPN-Settings



حيث قمنا بتحديد كرت الWAN والذي عليه ip real ويفضل تغيير ال listening port من 443 الى 4430 بحيث يمكن اداره الفورتى جيت نفسه عبر 443 (https) من خارج الشبكة عبر الانترنت وكما يمكن الوصول الى vpn web mode عبر البورت 4430.

أساسيات فورتي جيت

The screenshot shows the FortiGate web interface for SSL-VPN Settings. The left sidebar lists various configuration areas, with 'VPN' expanded and 'SSL-VPN Settings' selected. The main content area shows the following settings:

- Redirect HTTP to SSL-VPN:
- Restrict Access: **Allow access from any host** (highlighted in red) | Limit access to specific hosts
- Idle Logout:
- Inactive For: 300 Seconds
- Server Certificate: **Fortinet_Factory** (highlighted in red)
- Require Client Certificate:
- Tunnel Mode Client Settings: **Automatically assign addresses** (highlighted in green) | Specify custom IP ranges

A yellow warning box is visible, stating: "You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and upload it for use. [Click here to learn more](#)"

كما بالصورة أعلاه يمكن الوصول عبر ال vpn من أي جهاز وأيضا يفضل لا تقوم بتغيير الشهادة واتركها كما هي .

The screenshot shows the FortiGate web interface for SSL-VPN Settings, focusing on the Tunnel Mode Client Settings and Authentication/Portal Mapping sections.

- Require Client Certificate:
- Tunnel Mode Client Settings: **Automatically assign addresses** (highlighted in green) | Specify custom IP ranges
- DNS Server: **Same as client system DNS** (highlighted in red) | Specify
- Specify WINS Servers:
- Authentication/Portal Mapping: **Same as client system DNS** (highlighted in red)

A yellow warning box is visible, stating: "It is recommended to purchase a certificate for your domain and upload it for use. [Click here to learn more](#)"

The Authentication/Portal Mapping table is as follows:

Users/Groups	Portal
All Other Users/Groups	full-access

أيضا يتم ترك الاعدادات كما بالصورة أعلاه بحيث الفورتي جيت هو من يقوم بتعيين الايبي لليوزرات التابعه لل VPN .

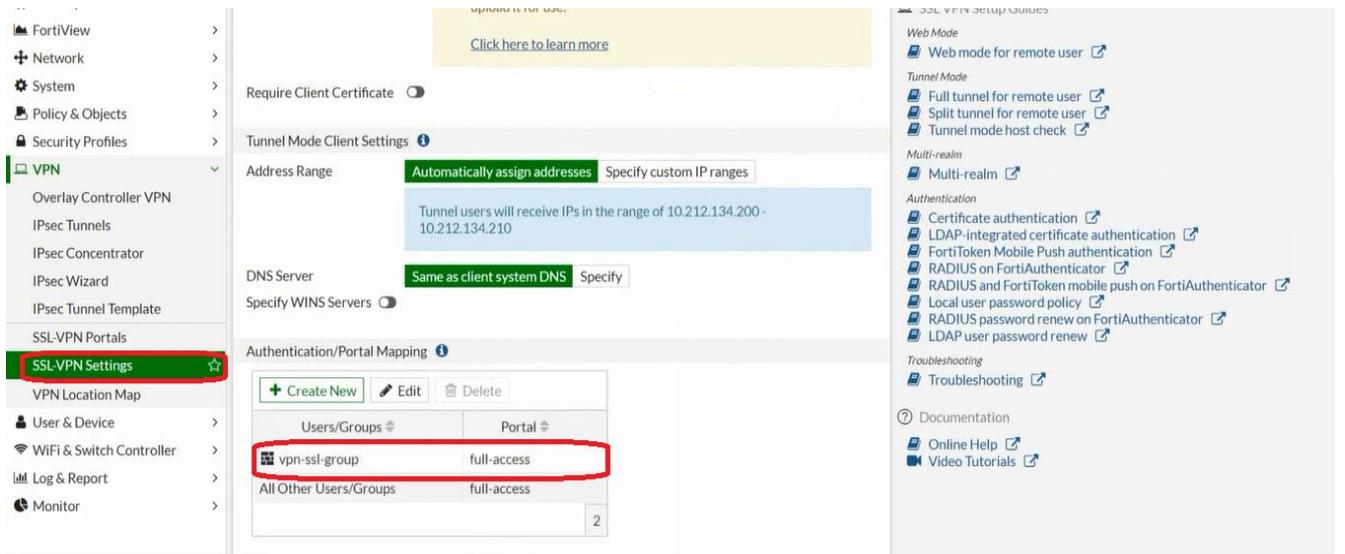
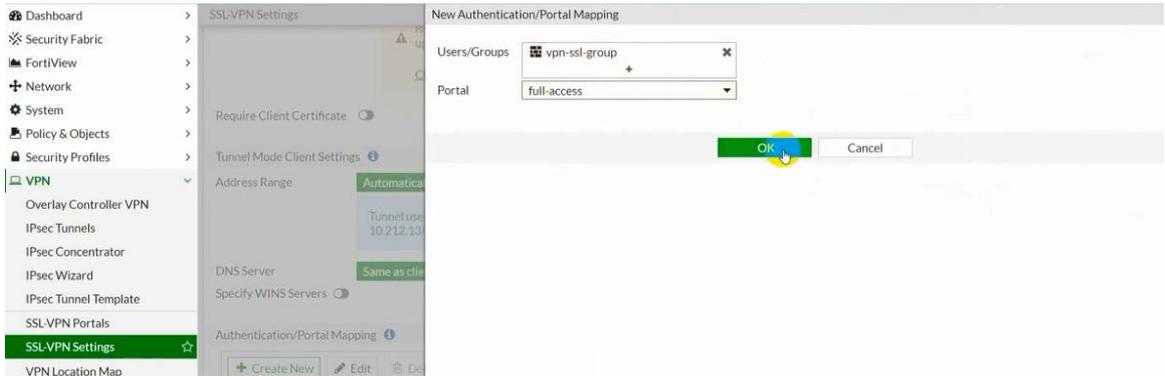
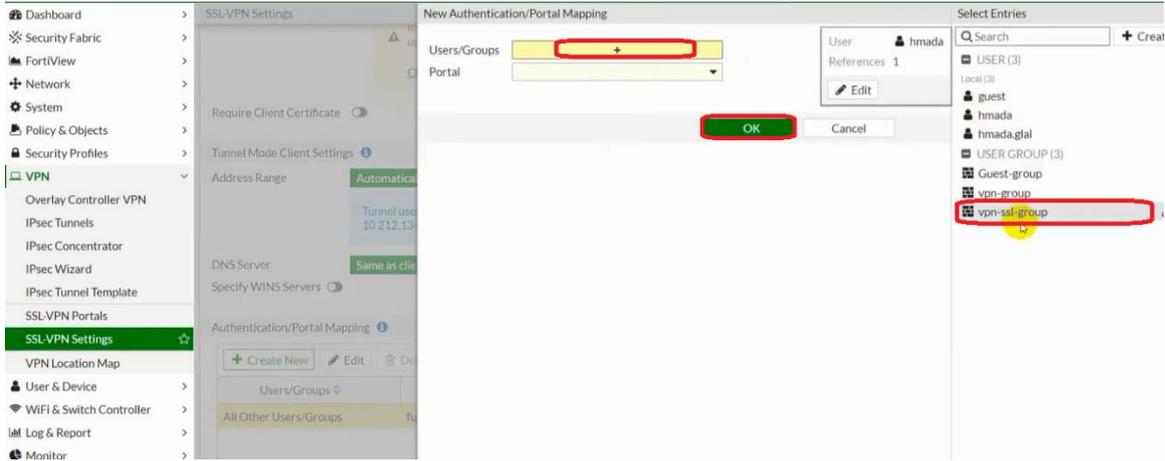
وكما نترك ال dns server هو نفسه التابع للفورتي جيت .

يتم تحديد اليوزرات التي لهم صلاحيات للوصول عبر الVPN للفورتني جيت .

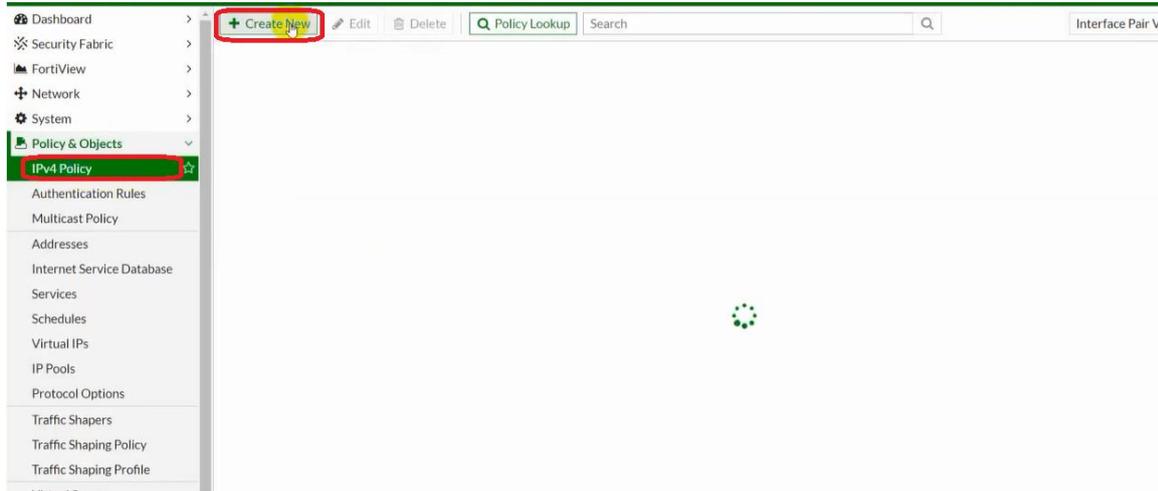
حيث بشكل افتراضي يكون All other users/groups لديها full-access

حيث أي local users بالفورتني جيت له حق الوصول ..

ويمكن تحديد فقط الجروب التي قمنا بإنشائها سابقا كما بالصورة التالية :



اخر الخطوات نقوم بعمل Rule تسمح بمرور الترافيك ما بين ال vpn و local network وبين ال VPN وبين الانترنت .



قمنا بتسميه ال rule باسم ssl-vpn-to-localnetwork

ونقوم بتحديد ال incoming interface ليكون (ssl.root) interface(ssl-vpn-tunnel

و outgoing interface سيكون lan أي كرت الشبكة الداخليه

حيث ال source هم الأشخاص (الجروب) التي تم أنشائها سابقا وهو vpn-ssl-group

وال destination سيكون all أي كل اجهزه الشبكة الداخليه ونقوم بتفعيل خيار ال nat

في خيارات ال security profiles حيث يمكنني تفعيل ال Antivirus وال web filter و

ال Application control و IPS على تلك ال Rules .

كما بالصور ادناه

أساسيات فورتني جيت

The screenshot shows the 'Edit Policy' configuration page for an IPv4 Policy. The left sidebar contains a navigation menu with 'Policy & Objects' expanded and 'IPv4 Policy' selected. The main configuration area includes the following fields:

- Name: ssl-vpn-to-localnetwork
- Incoming Interface: SSL-VPN tunnel interface (ssl.roo)
- Outgoing Interface: lan
- Source: all, vpn-group, vpn-ssl-group
- Destination: all
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY
- Inspection Mode: Flow-based (checked), Proxy-based
- Firewall / Network Options: NAT (checked)
- IP Pool Configuration: Use Outgoing Interface Address (checked), Use Dynamic IP Pool

On the right side, a summary panel displays:

- ID: 16
- Last used: 1 hour(s) ago
- First used: 27 day(s) ago
- Hit count: 4,191
- Active sessions: 0
- Total bytes: 475.40 MB
- Current bandwidth: 0 B/s

Documentation and Online Help links are visible at the bottom right.

This screenshot shows the 'Edit Policy' page with the 'Security Profiles' section expanded. The 'NAT' option is checked. The 'IP Pool Configuration' is set to 'Use Outgoing Interface Address' and 'Use Dynamic IP Pool'. The 'Security Profiles' section includes:

- AntiVirus:
- Web Filter:
- DNS Filter:
- Application Control:
- IPS:

The 'SSL Inspection' is set to 'no-inspection'. The 'Logging Options' section shows 'Log Allowed Traffic' checked, with 'Security Events' selected. A 'Comments' field is at the bottom with a character count of 0/1023.

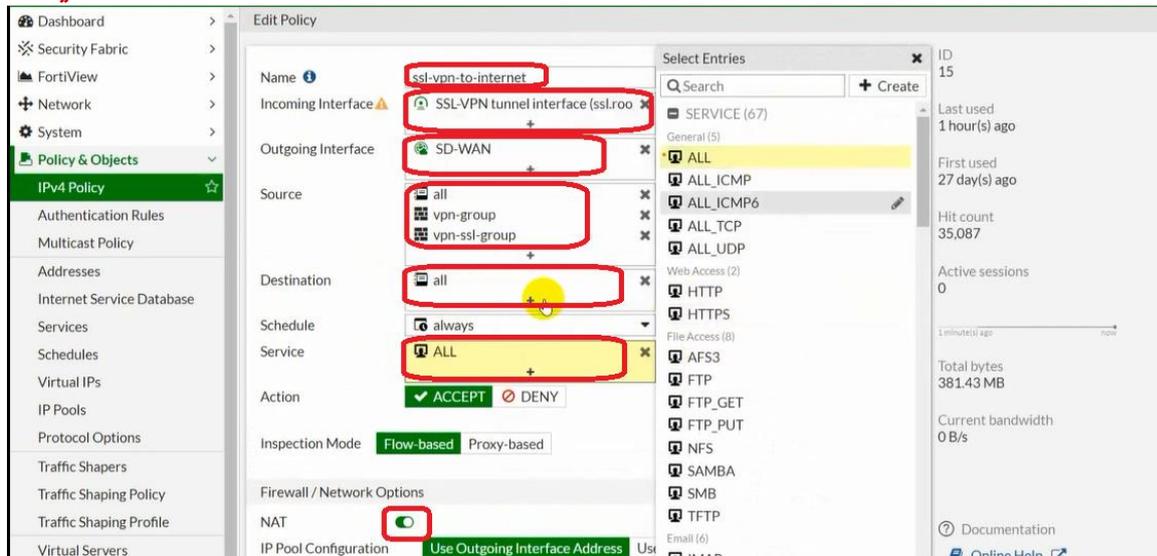
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
16	ssl-vpn-to-localnetwork	all	all	always	ALL	ACCEPT	Enabled	SSL no-inspection UTM	475.40 MB	

نلاحظ كما بالصورة أعلاه بأنه تم انشاء Rule تسمح بالوصول من خارج الشبكة (عبر VPN) الى الشبكة الداخلية لكن كل اليوزرات التي عبر الVPN لن تستطيع الوصول الى الانترنت ابدأ ويجب ان نقوم بإنشاء Rule تسمح للناس بعد ما يقوموا بعمل vpn ان يكون لديهم انترنت عبر HQ أي الشبكة الداخلية حيث سيتعامل معهم الفورتني جيت ك proxy server .

الآن سنقوم بعملية انشاء تلك الRule باسم ssl-vpn-to-internet:

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
12	lan -> sd-wan									
13	sd-wan -> lan									
14	SSL-VPN tunnel interface (ssl.root) -> lan									
15	SSL-VPN tunnel interface (ssl.root) -> sd-wan									
1	Implicit									

أساسيات فورتيجيت



حيث نلاحظ بأن الـ Outgoing interface = SD-Wan حيث جهاز الفورتيجيت معمول دمج لأكثر من خط ولذا اليوزرات التابعة لـ vpn والتي تم تحديدها بـ source سوف تحصل على الانترنت عبر SD-Wan لجهاز الفورتيجيت .

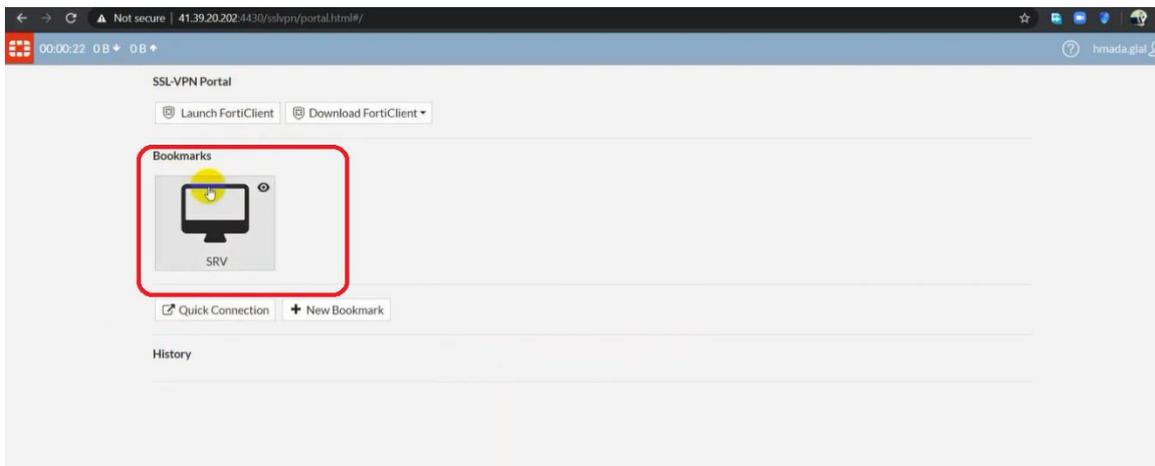
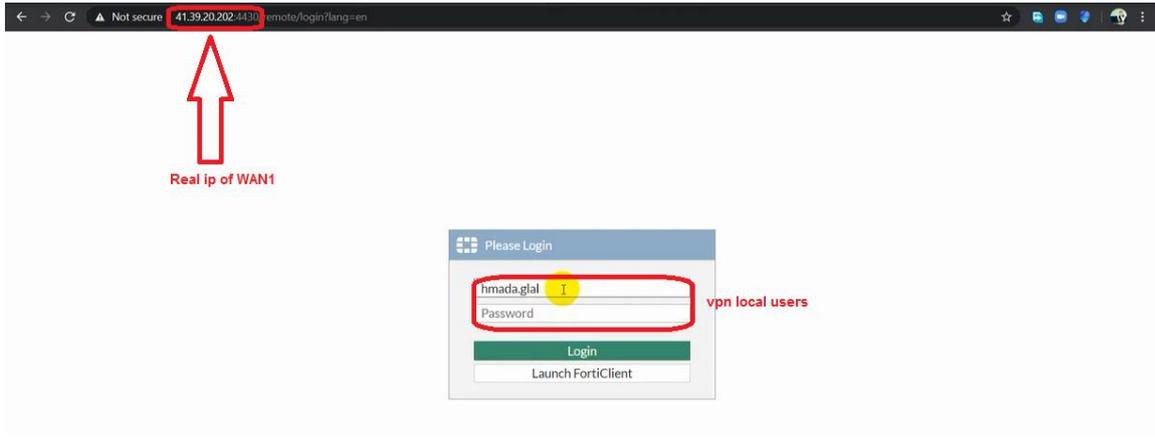
ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
16	ssl-vpn-to-localnetwork	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	475.40 MB
15	ssl-vpn-to-internet	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	381.43 MB

الآن لدي Rule 2 التي تسمح بالترافيك بين VPN و LOCAL NETWORK

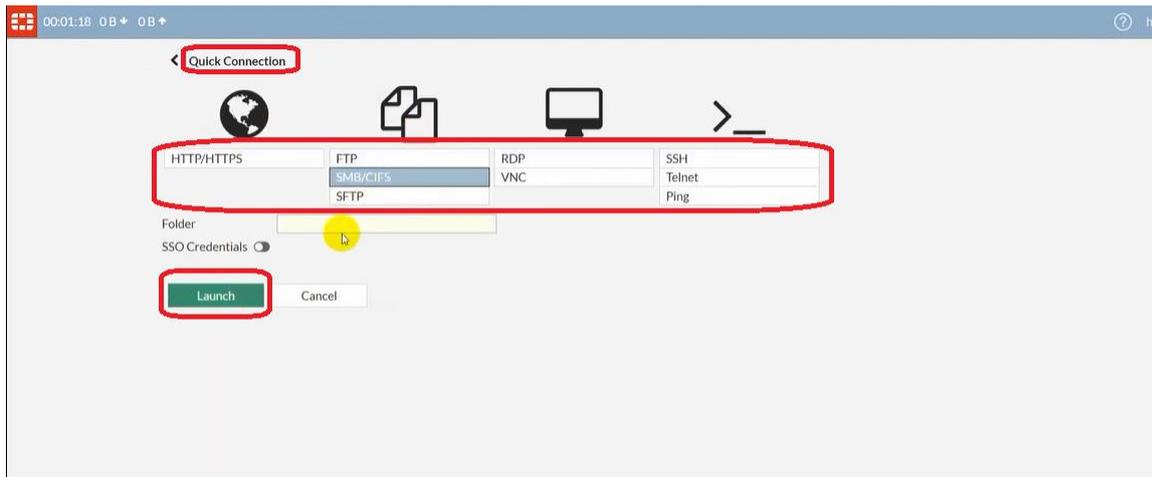
حيث الرابط (URL) التي بواسطته يمكنك الوصول الى الشبكة الداخليه عبر الـ VPN Web mode هو ip wan of fortigate+4430 والذي تم اعداده سابقا

كما بالصورة التالية :

أساسيات فورتى جيت



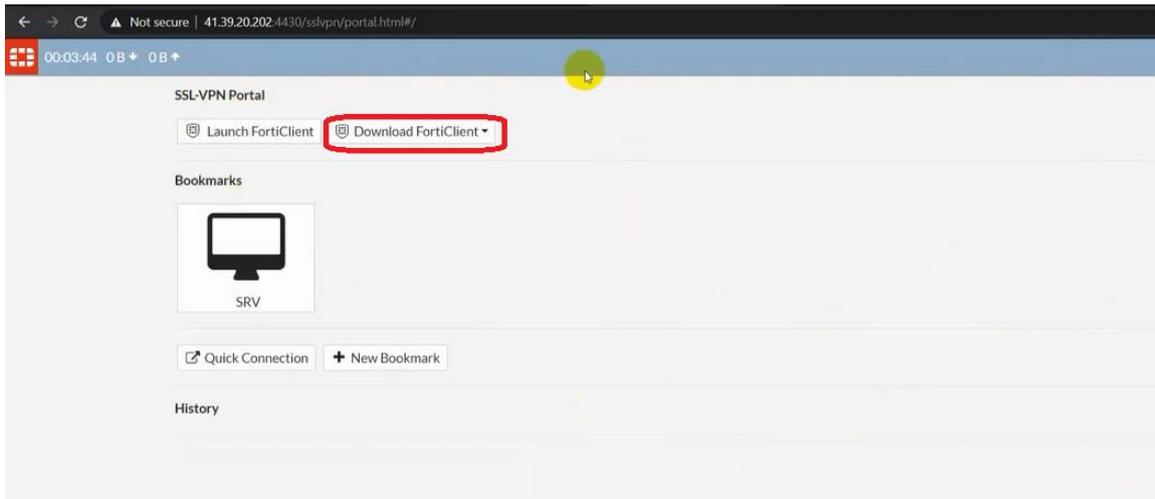
كما بالصورة أعلاه فإن ال bookmark التي قمنا بإنشائها سابقا باسم SRV موجودة وهو Remote Desktop للسيفر 192.168.10.100 وبمجرد النقر مرتين عليه يفتح لنا السيرفر...



او يمكنك عبر ال Quick Connections ان تصل الى أي Service تريدها سواء HTTP/HTTPS RDP SSH Ping الخ..

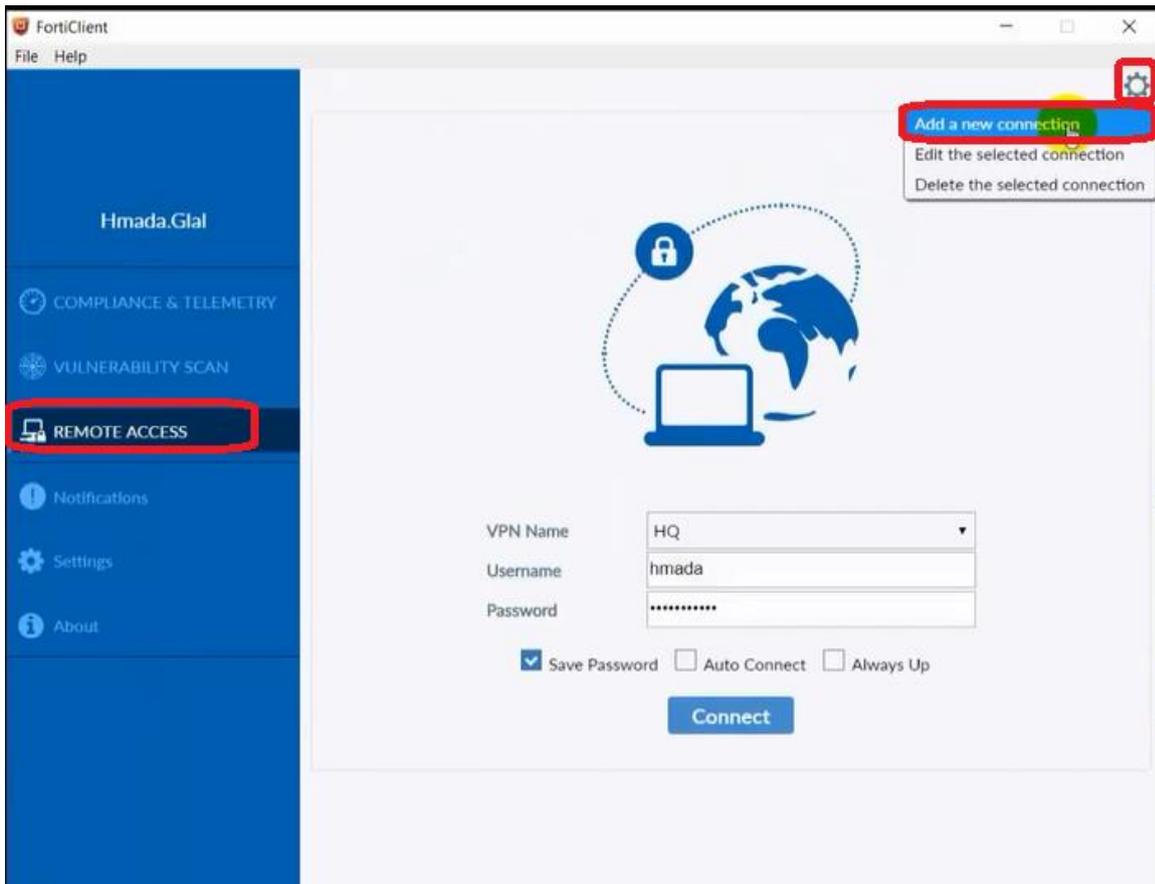
وهذه الطريقة الأولى vpn/ssl عبر web mode

والطريقة الأخرى عبر الفورتى كلاينت كما بالصورة التالية :



حيث يمكنك تنزيل برنامج الفورتى كلاينت عبر موقع الفورتى جيت نفسه او من الصفحة التابعة ل web access كما بالصورة أعلاه ...

ثم نقوم بعمل install للتطبيق

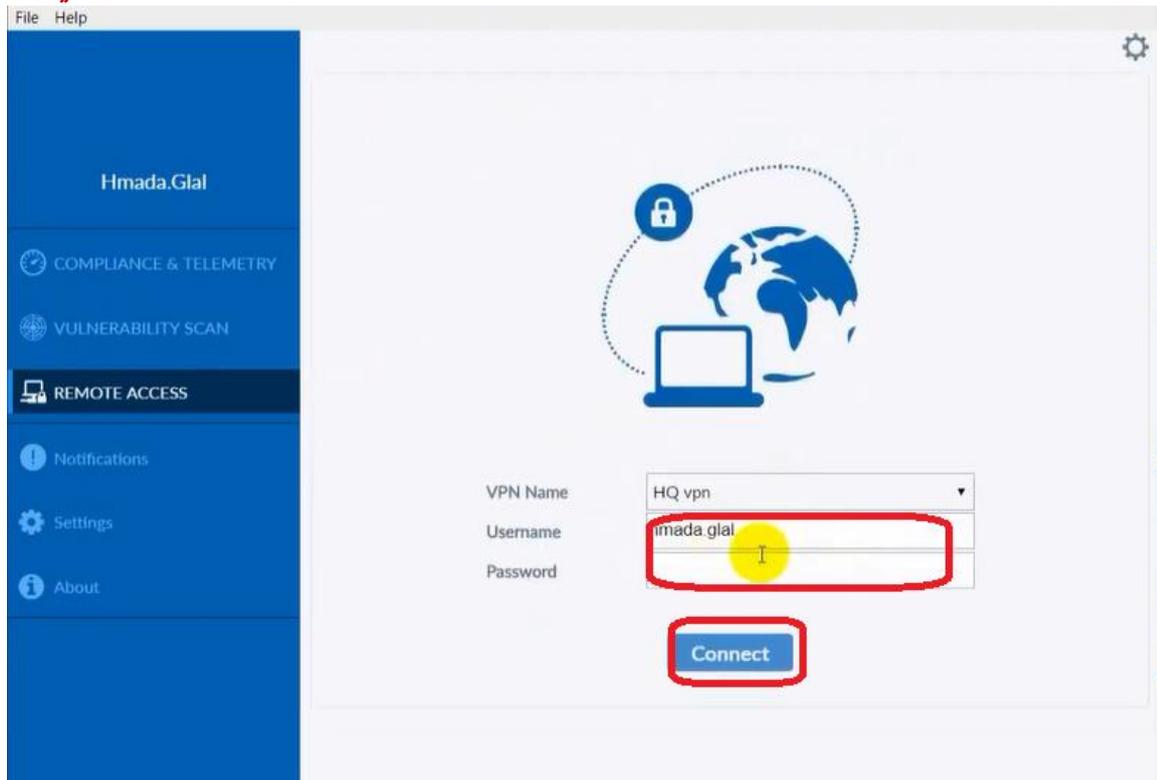


أساسيات فورتني جيت

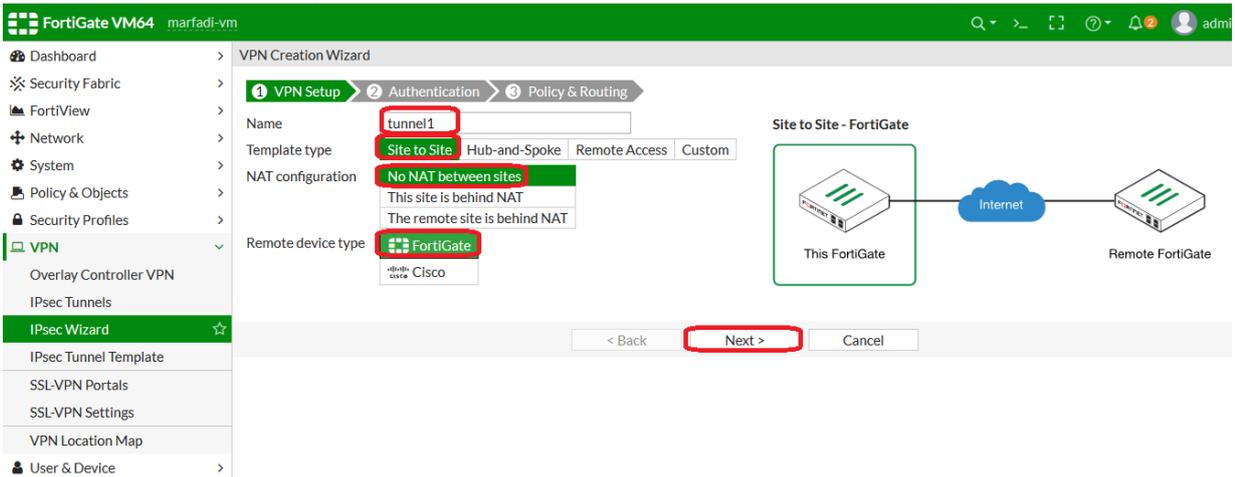
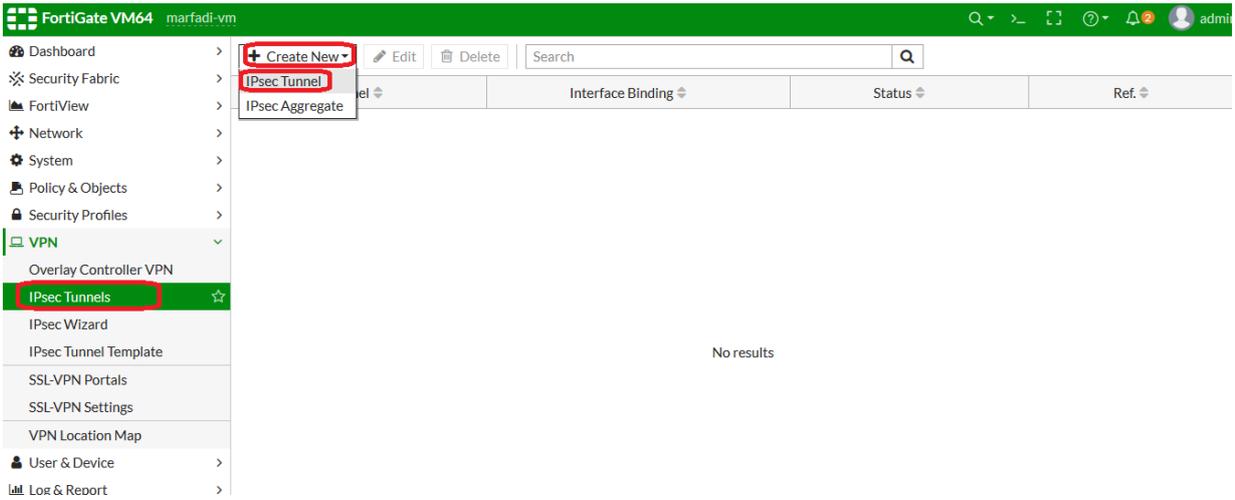
حيث نوع الاتصال هو SSL-VPN واسمه مثلا HQ-VPN ونضع الايبي لـ WAN في Remote Gateway ونحدد البورت 4430 ثم نختار Save logging لو تريد الفورتني كلاينت لا يطلب اليوزرنيم كل مره عند تشغيله

اما انت تريده ان يطالب المستخدم بكتابه اليوزرنيم والباسورد في كل مره فنختار الخيار prompt on login

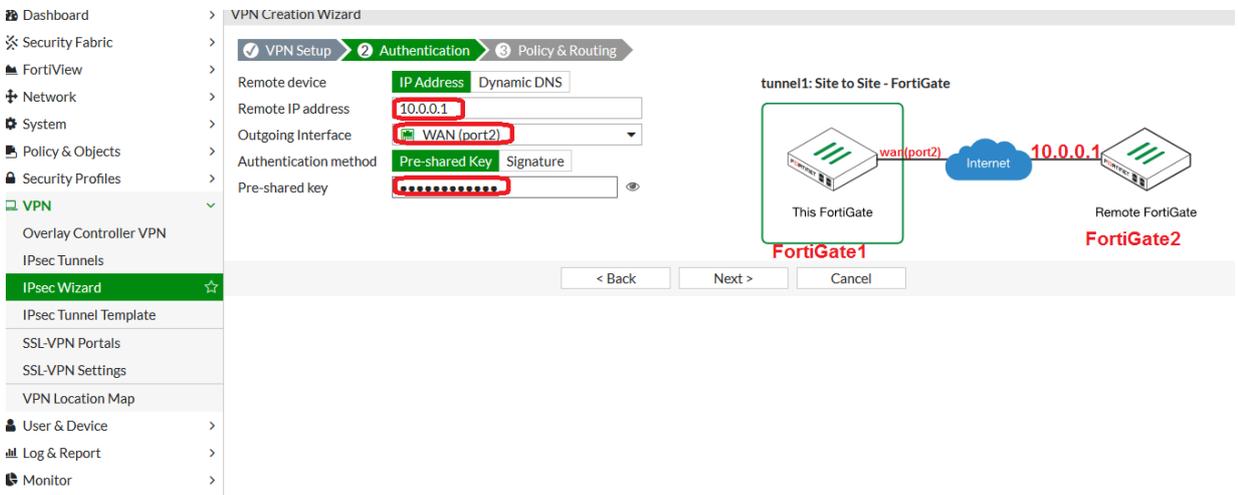
The screenshot shows the 'New VPN Connection' dialog in FortiClient. The 'VPN' type is set to 'SSL-VPN'. The 'Connection Name' is 'HQ vpn'. The 'Remote Gateway' is '41.39.20.202'. The 'Add Remote Gateway' checkbox is checked. The 'Customize port' checkbox is checked, and the port is set to '4430'. The 'Client Certificate' is set to 'None'. The 'Authentication' options are 'Prompt on login' and 'Save login', with 'Save login' selected. The 'Username' is 'hmada.glal'. The 'Do not Warn Invalid Server Certificate' checkbox is checked. The 'Save' button is highlighted with a yellow circle.



فمجرد ادخال اليوزرنيم والباسورد وعمل connect فانه سوف يتصل ويمكنك بعد ذلك الوصول الى HQ ومنها الى السيرفرات ...



كما بالصورة أعلاه توضح بأن اسم ال tunnel هو tunnel1 ونوعيه الربط هو site to site حيث تم اختيار الجهاز الموجود بالفرع البعيد هو فورتى جيت 2..

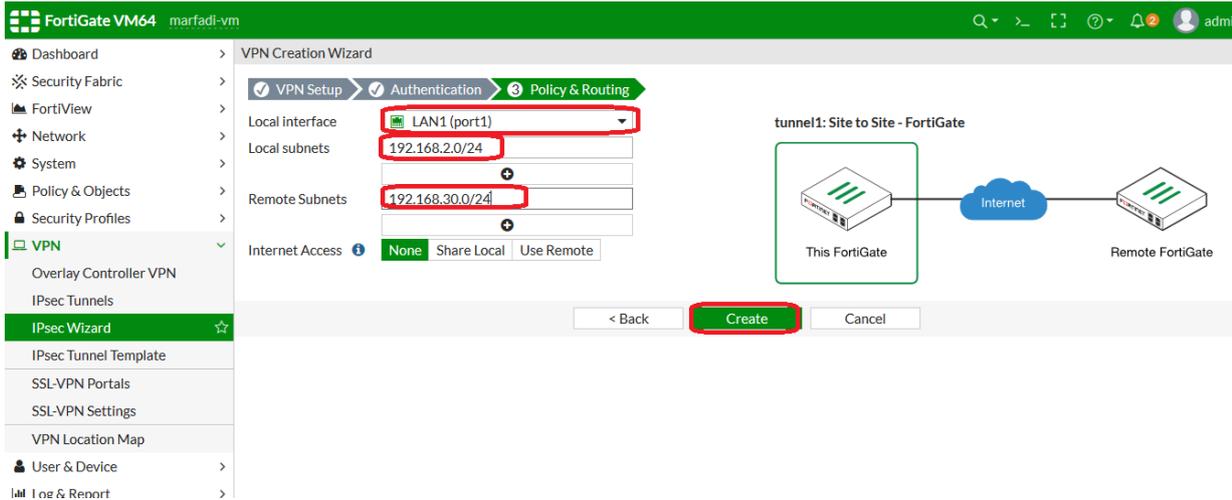


أساسيات فورتى جيت

كما بالصورة أعلاه تبين بأن الايبي لجهاز الفورتى جيت 2 الموجود في الـ site البعيد هو 10.0.0.1 وهو الـ real Ip ..

وتختار الـ wan interface للفورتى جيت 1 للـ site الذي سوف يخرج منه الى 10.0.0.1 .

ونكتب كلمه السر (pre-shared Key) ..



حيث سنحدد الـ local interface للساييت 1 FortiGate وهو الـ LAN1

وبشكل تلقائي سوف يتعرف على الشبكة كما بالصورة أعلاه 24/192.168.2.0

وهي الشبكة التي نريد ربطها مع الفرع البعيد (site 2)

ثم نكتب الـ remote subnet وهي للشبكة البعيده والموجودة على site 2 وهو 24/192.168.30.0

ملاحظة: سيقوم الفورتى جيت بإنشاء Network object لـ 24/192.168.2.0 .

وأیضا للـ 192.168.30.0/24 وهي لـ remote subnet كما بالصورة ادناه .

The screenshot shows the FortiGate VPN Creation Wizard interface. The left sidebar is expanded to 'Policy & Objects' > 'IPv4 Policy' > 'Addresses'. The main content area shows the 'Summary of Created Objects' section, which lists the following objects:

- Phase 1 Interface: tunnel1
- Local Address Group: tunnel1_local (Edit)
- Remote Address Group: tunnel1_remote (Edit)
- Phase 2 Interface: tunnel1
- Static Route: 2 (Edit)
- Blackhole Route: 3 (Edit)
- Local to Remote Policy: vpn_tunnel1_local (3) (Edit)
- Remote to Local Policy: vpn_tunnel1_remote (4) (Edit)

Below this, the 'Addresses' table is visible, showing the configuration for the subnets:

Name	Type	Subnet	Visible
tunnel1_local_subnet_1	Subnet	192.168.2.0/24	Visible
tunnel1_remote_subnet_1	Subnet	192.168.30.0/24	Visible

At the bottom, the 'Address Group' section shows the configuration for the tunnel1_local and tunnel1_remote address groups, both pointing to their respective subnets.

نلاحظ بانه تم انشاء عناوين ومجموعات بشكل تلقائيه كما بالصوه أعلاه ..

وأیضا سيتم انشاء سياستين (two policies) بشكل تلقائي كما بالصورة ادناه

The screenshot shows the FortiGate Policy & Objects section, specifically the 'IPv4 Policy' configuration. The table below shows the configuration for the two policies:

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
3	vpn_tunnel1_local	tunnel1_local	tunnel1_remote	always	ALL	ACCEPT	Disabled	SSL, no-inspection	UTM
4	vpn_tunnel1_remote	tunnel1_remote	tunnel1_local	always	ALL	ACCEPT	Disabled	SSL, no-inspection	UTM

تم انشاء 2 policy كما بالصورة أعلاه ...

1-تسمح للترافيك من الـ local site الى الـ remote site

أساسيات فورتني جيت

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > IPv4 Policy

Edit Policy

Name: vpn_tunnel1_local

Incoming Interface: port1

Outgoing Interface: tunnel1

Source: tunnel1_local

Destination: tunnel1_remote

Schedule: always

Service: ALL

Action: ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT:

2-تسمح للترافيك من الremote site الى الlocal site .

Dashboard > Security Fabric > FortiView > Network > System > Policy & Objects > IPv4 Policy

Edit Policy

Name: vpn_tunnel1_remote

Incoming Interface: tunnel1

Outgoing Interface: port1

Source: tunnel1_remote

Destination: tunnel1_local

Schedule: always

Service: ALL

Action: ACCEPT

Inspection Mode: Flow-based

Firewall / Network Options

NAT:

Protocol Options: PRX default

*ملاحظة: لا يتم تفعيل الNAT ..

أيضا سيتم انشاء static route بشكل تلقائي كما بالصورة ادناه

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.1.1	WAN (port2)	Enabled	
tunnel1_remote		tunnel1	Enabled	VPN: tunnel1 (Created by VPN wizard)
tunnel1_remote		Blackhole	Enabled	VPN: tunnel1 (Created by VPN wizard)

Destination: Subnet | **Named Address** | Internet Service

Interface: tunnel1_remote

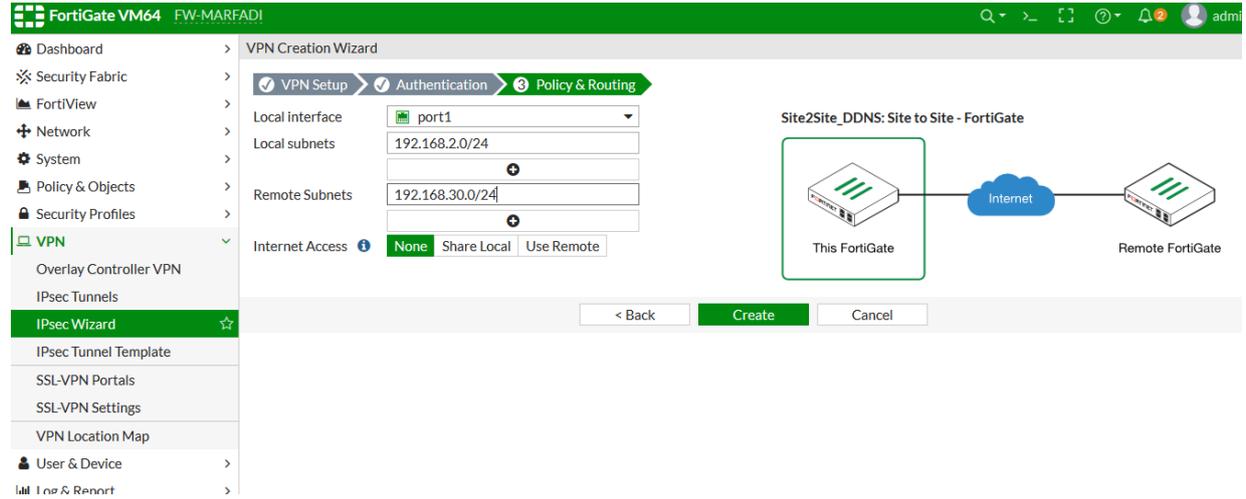
Interface: tunnel1

Administrative Distance: 10

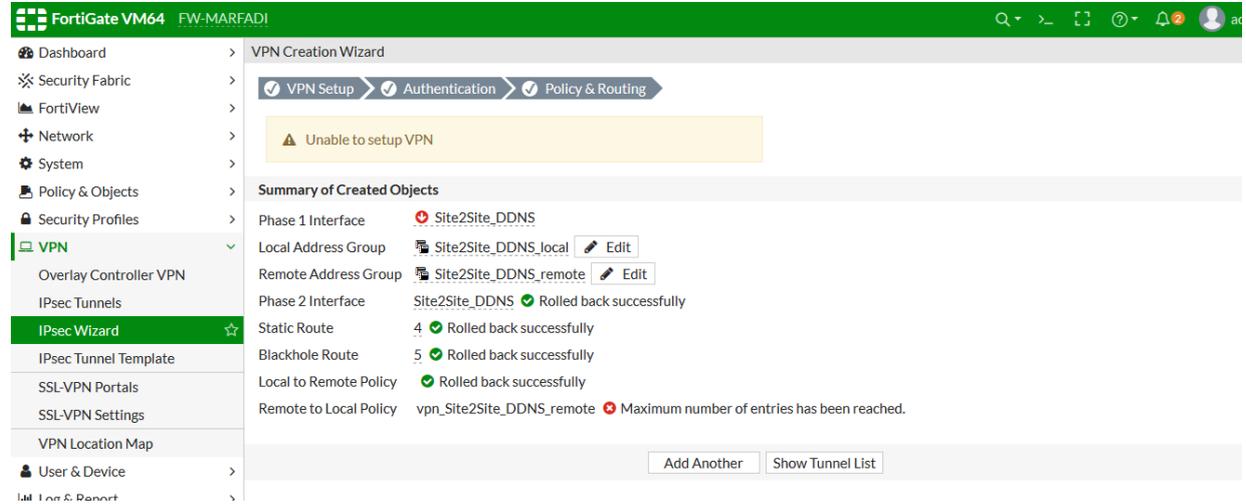
Comments: VPN: tunnel1 (Created by VPN wizard)

Status: **Enabled** | Disabled

سوف نقوم بتكرار نفس العملية ولكن على الـ Site 2 أي على الفورتى جيت 2...



كما بالصورة أعلاه . كم تم بالإعدادات الـ site to site سابقا



تمت العملية على الـ site1 وسوف نكرر نفس العملية على الـ site 2
لكن في حال الـ site1 لديه static ip فاني سوف أقوم باستخدامه ...

طريقة انشاء عناوين بالفورتى جيت

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1

New Address

Name: marfadi_pc

Color: Change

Type: Subnet

IP/Netmask: 192.168.2.121/32

Interface: any

Show in address list:

Static route configuration:

Comments: Ip of Marfadi computer

OK Cancel

Name	Type	Details	Interface	Visibility	Ref.
FABRIC_DEVICE	Subnet	0.0.0.0/0		Visible	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet	0.0.0.0/0		Hidden	0
PC-Client-MAC	Device (MAC Address)	00:0c:29:ff:72:33	LAN1 (port1)	Visible	1
Range_ip_servers	IP Range	192.168.2.1 - 192.168.2.30	LAN1 (port1)	Visible	0
SSLVPN_TUNNEL_ADDR1	IP Range	10.212.134.200 - 10.212.134.210	SSL-VPN tunnel interface (ssl.root)	Visible	1
Subnet1	Subnet	192.168.2.0/24	LAN1 (port1)	Visible	2
VLAN1 address	Interface Subnet	192.168.3.0/24	virtual interface 1 (VLAN1)	Visible	0
YEMEN	Geography	United States		Visible	1
all	Subnet	0.0.0.0/0		Visible	15
gmail.com	FQDN	gmail.com		Visible	1
login.microsoft.com	FQDN	login.microsoft.com		Visible	1
login.microsoftonline.com	FQDN	login.microsoftonline.com		Visible	1
login.windows.net	FQDN	login.windows.net		Visible	1
marfadi_pc	Subnet	192.168.2.121/32		Visible	0
none	Subnet	0.0.0.0/32		Visible	0
pc1	Subnet	192.168.2.144/32	LAN1 (port1)	Visible	1
server1	Subnet	192.168.2.122/32	LAN1 (port1)	Visible	1
wildcard.dropbox.com	FQDN	*dropbox.com		Visible	0
wildcard.google.com	FQDN	*google.com		Visible	1

تم انشاء عنوان باسم marfadi_pc وتم تخصيص ايبي له 192.168.2.121

هي عملية تخصيص سرعه معينه سواء ل download traffic او upload traffic

Guaranteed B.W	Maximum B.W
200 KBps	400 KBps

بحسب الجدول أعلاه يوضح Shaper بأن

Guarantees Bandwidth : فأن اقل سرعه بيعطيها الفورتى جيت هي 200 كيلو بايت بالثانية سواء لعملية ال download او ال Upload .

Maximum Bandwidth : اقصى سرعه هي 400 كيلو بايت بالثانية سواء لعملية ال download او ال Upload .

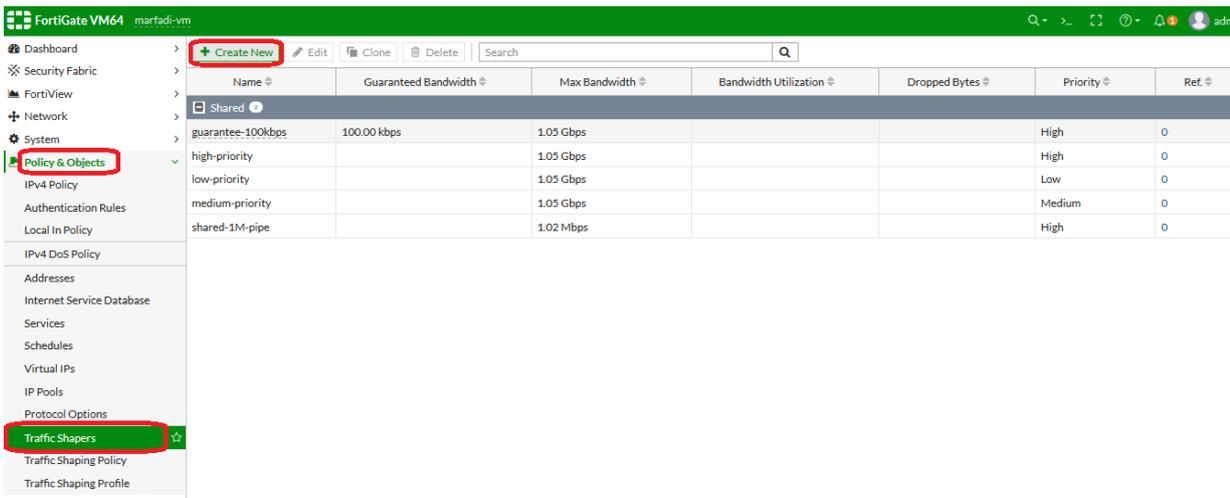
ملاحظة:

KBps : كيلو بايت بالثانية

Kbps : كيلوبت بالثانية

KBPS=8 Kbps

حيث سوف نقوم بإنشاء Traffic shaper كما بالخطوات التالية:



FortiGate VM64 marfadi-vm

New Traffic Shaper

Type: **Shared** Per IP Shaper

Name: IT-shaper-Download

Quality of Service

Traffic priority: High

Bandwidth unit: kbps

Maximum bandwidth: 3200 kbps

Guaranteed bandwidth: 1600 kbps

DSCP:

OK Cancel

Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref.
IT-shaper-Download	1.60 Mbps	3.20 Mbps			High	0
guarantee-100kbps	100.00 kbps	1.05 Gbps			High	0
high-priority		1.05 Gbps			High	0
low-priority		1.05 Gbps			Low	0
medium-priority		1.05 Gbps			Medium	0
shared-1M-pipe		1.02 Mbps			High	0

الآن سوف نقوم بإنشاء traffic shaper for upload للـ IT مثلاً

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

IPv4 Policy

Authentication Rules

Local In Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shapers

Traffic Shaping Policy

Traffic Shaping Profile

Edit Traffic Shaper

Type: **Shared** Per IP Shaper

Name: IT-shaper-Upload

Quality of Service

Traffic priority: High

Bandwidth unit: kbps

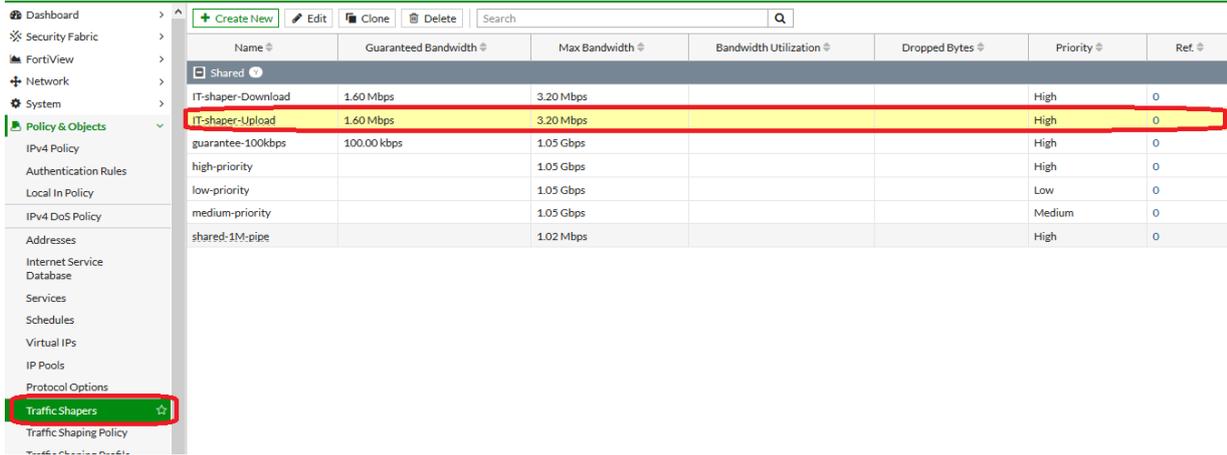
Maximum bandwidth: 3200 kbps

Guaranteed bandwidth: 1600 kbps

DSCP:

OK Cancel

أساسيات فورتني جيت



Name	Guaranteed Bandwidth	Max Bandwidth	Bandwidth Utilization	Dropped Bytes	Priority	Ref
IT-shaper-Download	1.60 Mbps	3.20 Mbps			High	0
IT-shaper-Upload	1.60 Mbps	3.20 Mbps			High	0
guarantee-100kbps	100.00 kbps	1.05 Gbps			High	0
high-priority		1.05 Gbps			High	0
low-priority		1.05 Gbps			Low	0
medium-priority		1.05 Gbps			Medium	0
shared-1M-pipe		1.02 Mbps			High	0

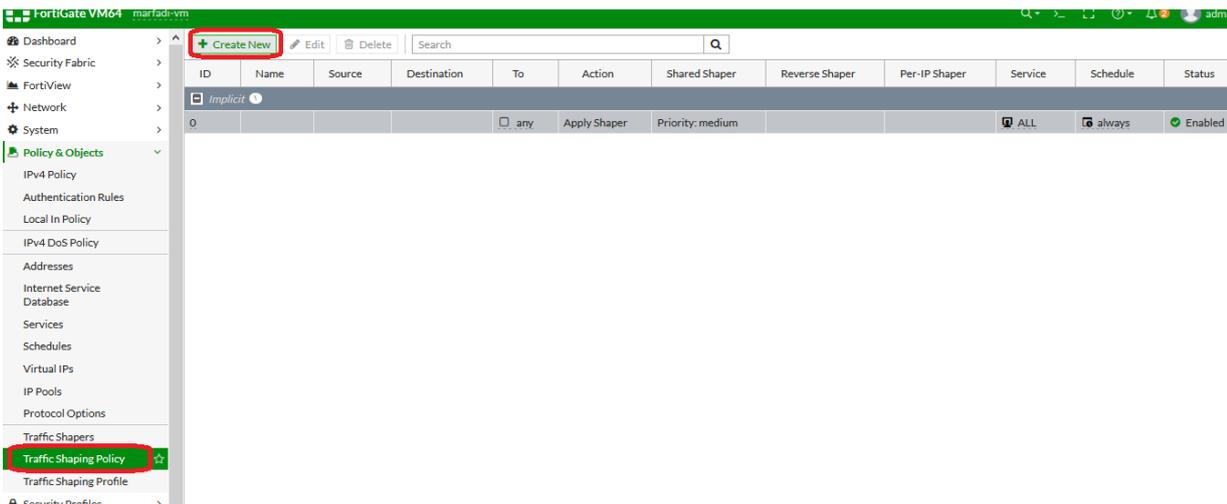
Traffic priority : وظيفتها إعطاء اولويه من يأخذ سرعات حيث الذي لديه priority اعلى هو من يكون له الأولوية في السرعات .

انواع ال traffic shaper :

Shared : يتم تقاسم ال traffic shaper حيث 400 كيلو سوف تقسم على عدد الأشخاص .

Per ip : يتم تخصيص traffic shaper لكل ابي اي سيتم تخصيص 400 كيلو لكل شخص .

طريقة انشاء Traffic shaping policy :



ID	Name	Source	Destination	To	Action	Shared Shaper	Reverse Shaper	Per-IP Shaper	Service	Schedule	Status
0				<input type="checkbox"/> any	Apply Shaper	Priority: medium			ALL	always	Enabled

أساسيات فورتني جيت

New Traffic Shaping Policy

Name: IT-traffic-shaping-policy

Status: Enabled

Comments: Write a comment... 0/255

If Traffic Matches:

Source: all, FSSO-GROUP-IT

Destination: all

Schedule: [Off]

Service: ALL

Application: [None]

URL Category: [None]

Then:

Action: Apply Shaper, Assign Shaping Class ID

Outgoing interface: SD-WAN

Shared shaper: IT-shaper-Upload

Reverse shaper: IT-shaper-Download

Per-IP shaper: [Off]

تم انشاء بولييسي لموظفي الايتي(FSSo-Group-IT)حيث

Upload Shared shaper يقصد بها ال

Reverse shaper يقصد بها ال download حيث تم تحديد ال traffic shaper الذي قمنا بإنشائها

سابقا باسم IT-shaper-Upload و IT-shaper-Download

وبهذا أي يوزر ضمن الجروب FSSO-GROUP-IT سوف يطبق عليها سياسه traffic shaping

كما بالصورة ادناه ...

ID	Name	Source	Destination	To	Action	Shared Shaper	Reverse Shaper	Per-IP Shaper	Service	Schedule	Status
1	IT_traffic_shaping_policy	all	all	SD-WAN	Apply Shaper	IT-shaper-Upload	IT-shaper-Download		ALL		Enabled
0	Implicit			any	Apply Shaper	Priority: medium			ALL	always	Enabled

ملاحظة هامه :

أي بولييسي موجودة في قائمه ال IPv4 Policy فانه سوف يتم المرور على ال traffic shaping policy كما بالصورة أعلاه سيتم المرور على البولييسي المسماة IT_traffic_shaping_policy فان لم تطابق السياسة فإنه يمر على البولييسي المسماة Implicit والذي معناه لا تطبق traffic shaping على هذا البولييسي ...

أساسيات فورتى جيت

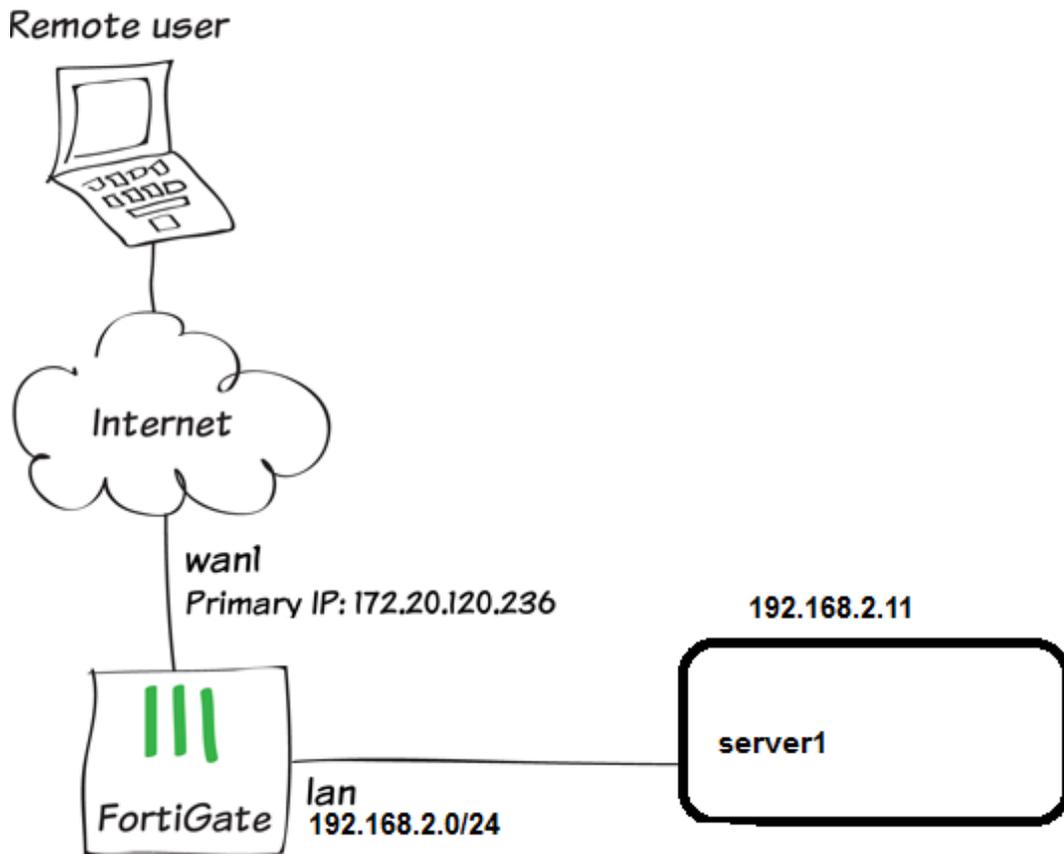
أي لو كانت ال rule لا تطبق عليها احدى traffic shaping policy فأنها تمر على السياسة المسماة Implicit وهي موجودة بشكل افتراضي .. والتي تعني لا تطبق على هذه السياسة أي traffic ... shaping policy

Virtual IP : عمليه الوصول من برع الشبكة الى جهاز معين في الشبكة الداخلية.

مثلا: الوصول الي سيرفر موجود بالشبكة الداخليه عم طريق ال remote desktop protocol او ما يسمى (RDP) ويسمى بعملية ال publishing .

او تريد مثلا عمل publish ل web server الموجود بالشركة وتريد الوصول اليه من خارج الشركة..

حيث أقول للفورتى جيت لو وصل لك اتصال عبر بورت معين قم بإدخاله الى السيرفر الفلاني ..



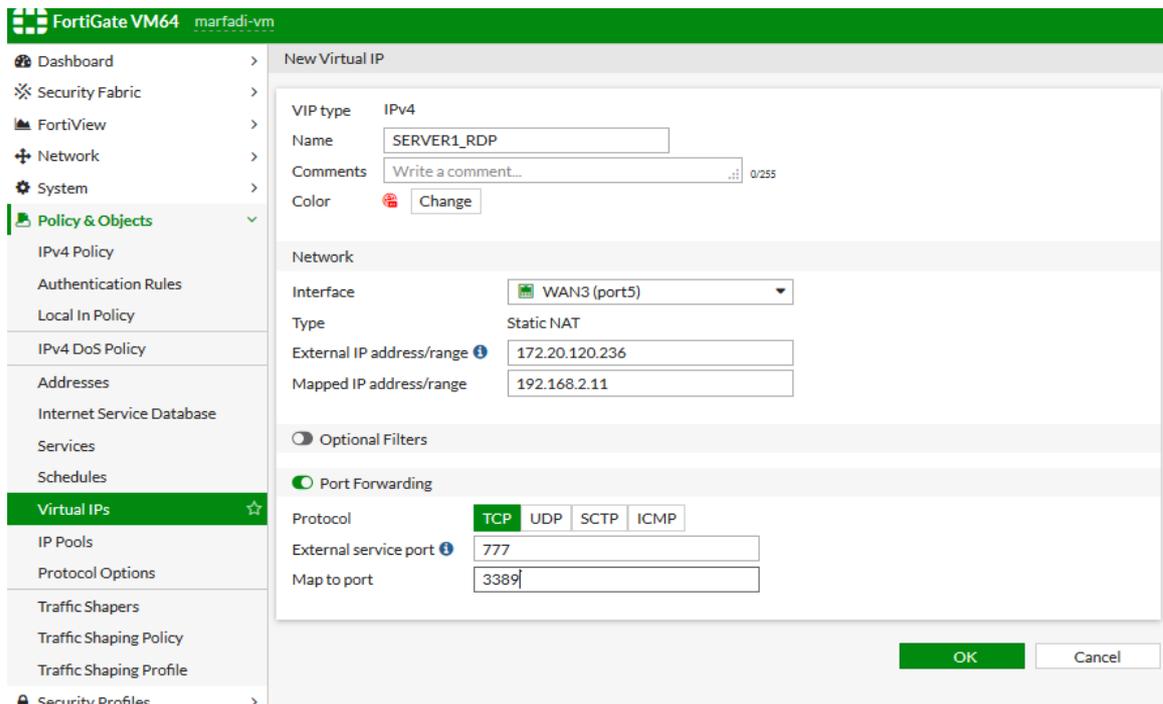
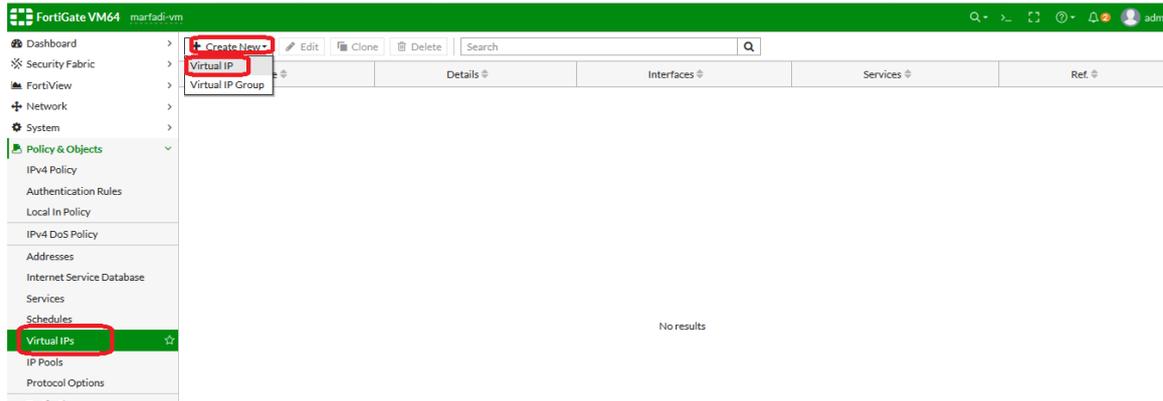
حيث wan1=172.20.120.236 هو public ip ..

أساسيات فورتى جيت

فلووصل لك أي اتصال الى المنفذ wan1 عبرالport مثلا 777 فقم بتحويله الى الايبي التابع للسيرفر 192.168.2.11 عبرالport 3389 وهو البورت الافتراضي لـ RDP .
حيث قمنا بتغيير البورت الافتراضي لـ rdp الى 777 كنوع من الأمان وتجنبنا من فايروس التشفير(الفيديه)

....

طريقة انشاء Virtual ip :



حيث interface: wan3 وهو البورت الي موصل عليه الـ static ip وهو 172.20.120.236

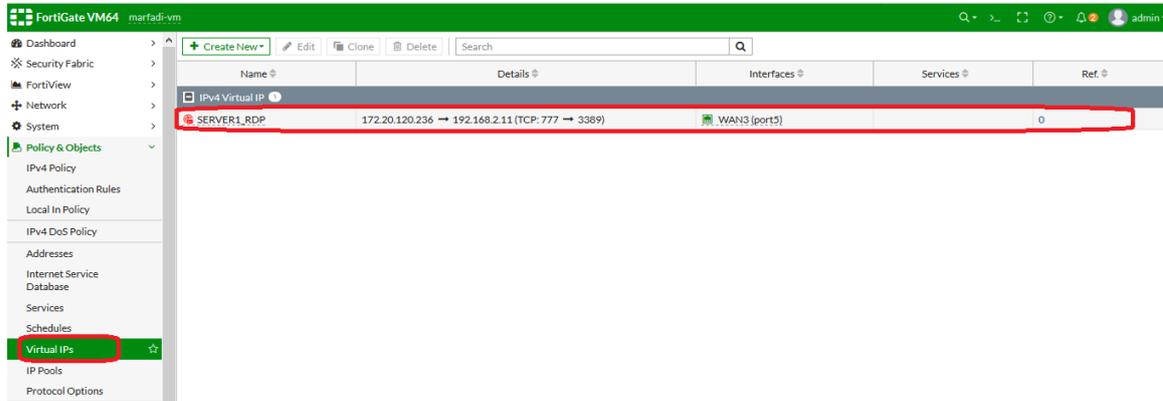
External IP address : هو الايبي الـ static الذي سيستقبل الـ connection

Mapped IP address : هو الايبي الـ private وهو ايبي السيرفر server1 وهو 192.168.2.11 .

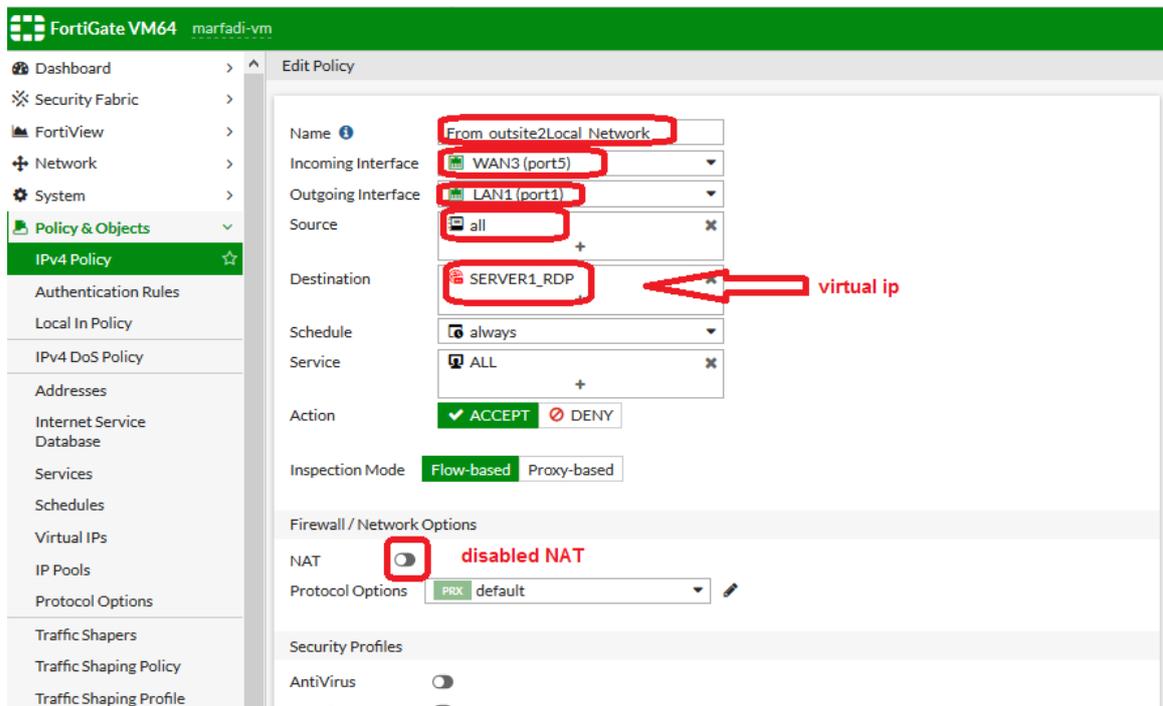
حيث سنقوم بتمكين الخيار port forwarding

ونضع البورت 777=external والmap to port=3389

حيث اللي واصل لك عبر البورت 777 قم بتحويله الى البورت 3389 .



فبعد ذلك يجب ان أنشئ بوليسي تسمح بالاتصال من خارج الشبكة الى داخل الشبكة (local network الى internet).



ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	public	Subnet1	all	always	ALL	DENY			Disabled	3.17 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_all	all	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
4	From_outside2Local_Network	all	SERVER1_RDP	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

تم انشاء البوليسي

الآن سنقوم بتجربة الوصول الى السيرفر server1 وذلك كالتالي



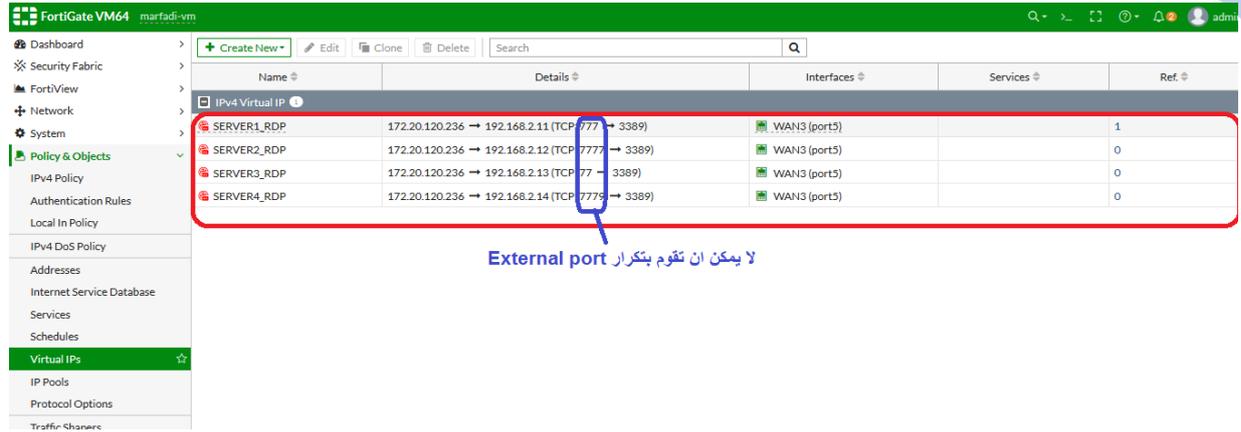
حيث بمجرد الدخول الى 172.20.120.236:777 سوف يتم تحويلك الى السيرفر 192.168.2.11 مباشرة.

: Virtual group

نفترض لدينا 4 سيرفرات معمول لهم 4 virtual ip

مثلا server1_RDP ، server2_RDP ، server3_RDP ، server4_RDP كما بالصورة ادناه ..

أساسيات فورتى جيت

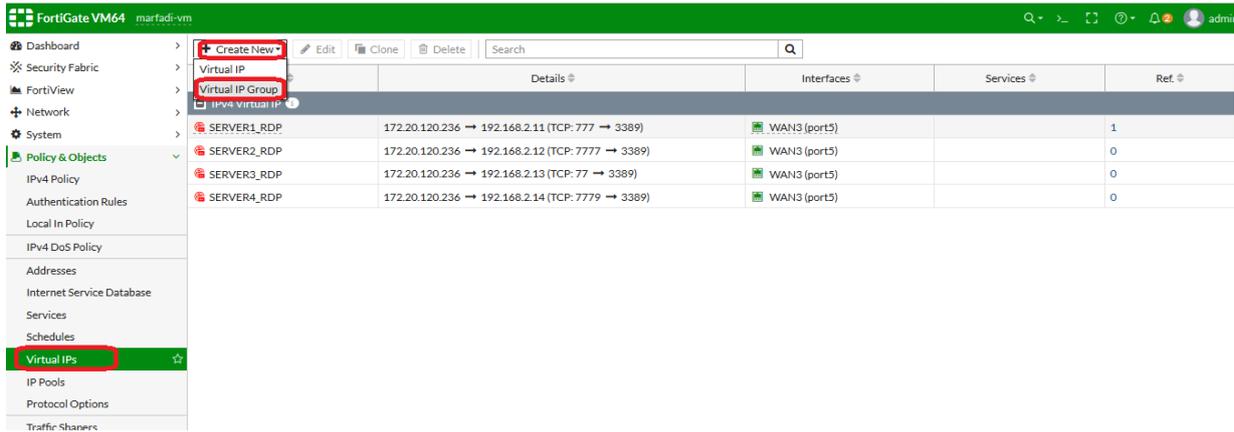


Name	Details	Interfaces	Services	Ref.
SERVER1_RDP	172.20.120.236 → 192.168.2.11 (TCP: 777 → 3389)	WAN3 (port5)		1
SERVER2_RDP	172.20.120.236 → 192.168.2.12 (TCP: 7777 → 3389)	WAN3 (port5)		0
SERVER3_RDP	172.20.120.236 → 192.168.2.13 (TCP: 77 → 3389)	WAN3 (port5)		0
SERVER4_RDP	172.20.120.236 → 192.168.2.14 (TCP: 7779 → 3389)	WAN3 (port5)		0

لا يمكن ان تقوم بتكرار External port

يجب External port يختلف من virtual ip لآخر...

طريقة انشاء virtual group بحيث أقوم بضم الـ 4 virtual ip's بداخلها ..



Name	Details	Interfaces	Services	Ref.
Virtual IP				
Virtual IP Group				
SERVER1_RDP	172.20.120.236 → 192.168.2.11 (TCP: 777 → 3389)	WAN3 (port5)		1
SERVER2_RDP	172.20.120.236 → 192.168.2.12 (TCP: 7777 → 3389)	WAN3 (port5)		0
SERVER3_RDP	172.20.120.236 → 192.168.2.13 (TCP: 77 → 3389)	WAN3 (port5)		0
SERVER4_RDP	172.20.120.236 → 192.168.2.14 (TCP: 7779 → 3389)	WAN3 (port5)		0

The screenshot shows the 'New VIP Group' configuration page in FortiGate VM64. The 'Type' is set to 'IPv4'. The 'Name' is 'Servers_RDP_Group'. The 'Interface' is 'WAN3 (port5)'. The 'Members' list includes 'SERVER1_RDP', 'SERVER2_RDP', 'SERVER3_RDP', and 'SERVER4_RDP'. The 'Virtual IPs' menu item in the left sidebar is highlighted with a red box.

The screenshot shows the 'Virtual IPs' configuration page in FortiGate VM64. The table below lists the configured Virtual IP objects and their associated interfaces.

Name	Details	Interfaces	Services	Ref
IPv4 Virtual IP				
SERVER1_RDP	172.20.120.236 → 192.168.2.11 (TCP: 777 → 3389)	WAN3 (port5)		2
SERVER2_RDP	172.20.120.236 → 192.168.2.12 (TCP: 7777 → 3389)	WAN3 (port5)		1
SERVER3_RDP	172.20.120.236 → 192.168.2.13 (TCP: 77 → 3389)	WAN3 (port5)		1
SERVER4_RDP	172.20.120.236 → 192.168.2.14 (TCP: 7779 → 3389)	WAN3 (port5)		1
IPv4 Virtual IP Group				
Servers_RDP_Group	SERVER1_RDP SERVER2_RDP SERVER3_RDP SERVER4_RDP	WAN3 (port5)		0

سنقوم بإعداد البوليسي التي تسمح بالاتصال من خارج الشبكة الى الشبكة الداخليه

أساسيات فورتى جيت

The screenshot shows the FortiGate configuration interface. On the left, the 'Policy & Objects' menu is expanded to 'IPv4 Policy'. The main configuration area shows a policy named 'From_outside2Local_Network' with the following settings:

- Name: From_outside2Local_Network
- Incoming Interface: WAN3 (port5)
- Outgoing Interface: LAN1 (port1)
- Source: all
- Destination: (highlighted in yellow)
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (unchecked)
- Inspection Mode: Flow-based (selected), Proxy-based (unselected)

A dropdown menu for the Destination field is open, showing a list of virtual IP groups. The 'Servers_RDP_Group' is selected and highlighted in red. The list includes:

- none
- pc1
- pc2
- Range_ip_servers
- server1
- servers
- Subnet1
- VLAN1 address
- wildcard.dropbox.com
- wildcard.google.com
- YEMEN
- ADDRESS GROUP (1)
- G Suite
- Microsoft Office 365
- VIRTUAL IP/SERVER (4)
- SERVER1_RDP
- SERVER2_RDP
- SERVER3_RDP
- SERVER4_RDP
- VIP GROUP (1)
- Servers_RDP_Group** (highlighted in red)

كما بالصورة أعلاه تم تحديد الـ destination = Servers_RDP_Group
 فبدلاً من إضافته الـ 4 virtual ip's فقط نقوم باختيار virtual group.

The screenshot shows the 'Edit Policy' page for the 'From_outside2Local_Network' policy. The Destination field is now populated with 'Servers_RDP_Group' and highlighted in red. The configuration is as follows:

- Name: From_outside2Local_Network
- Incoming Interface: WAN3 (port5)
- Outgoing Interface: LAN1 (port1)
- Source: all
- Destination: Servers_RDP_Group (highlighted in red)
- Schedule: always
- Service: ALL
- Action: ACCEPT (checked), DENY (unchecked)
- Inspection Mode: Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:
 - NAT: (unchecked)
 - Protocol Options: PRX default
- Security Profiles:
 - AntiVirus: (unchecked)
 - Web Filter: (unchecked)
 - DNS Filter: (unchecked)

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
3	public	Subnet1	all	always	ALL	DENY			Disabled	3.17 kB
2	allow_internet_for_servers	server1	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
1	allow_all	all	all	work_time	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
5	3	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
4	From_outside2Local_Network	all	Servers_RDP_Group	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B
0	Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

: IPV4 DOS policy configuration ➤

الـ TCP Connection عموماً سيتم إرسال SYN من قبل المرسل ويتم الرد عليك من قبل المستلم بـ SYN, ACK بأن الـ port مفتوح وجاهز للاستلام ومن بعد ذلك تبدأ عملية الإرسال وتبدأ الجلسة بينهما ...

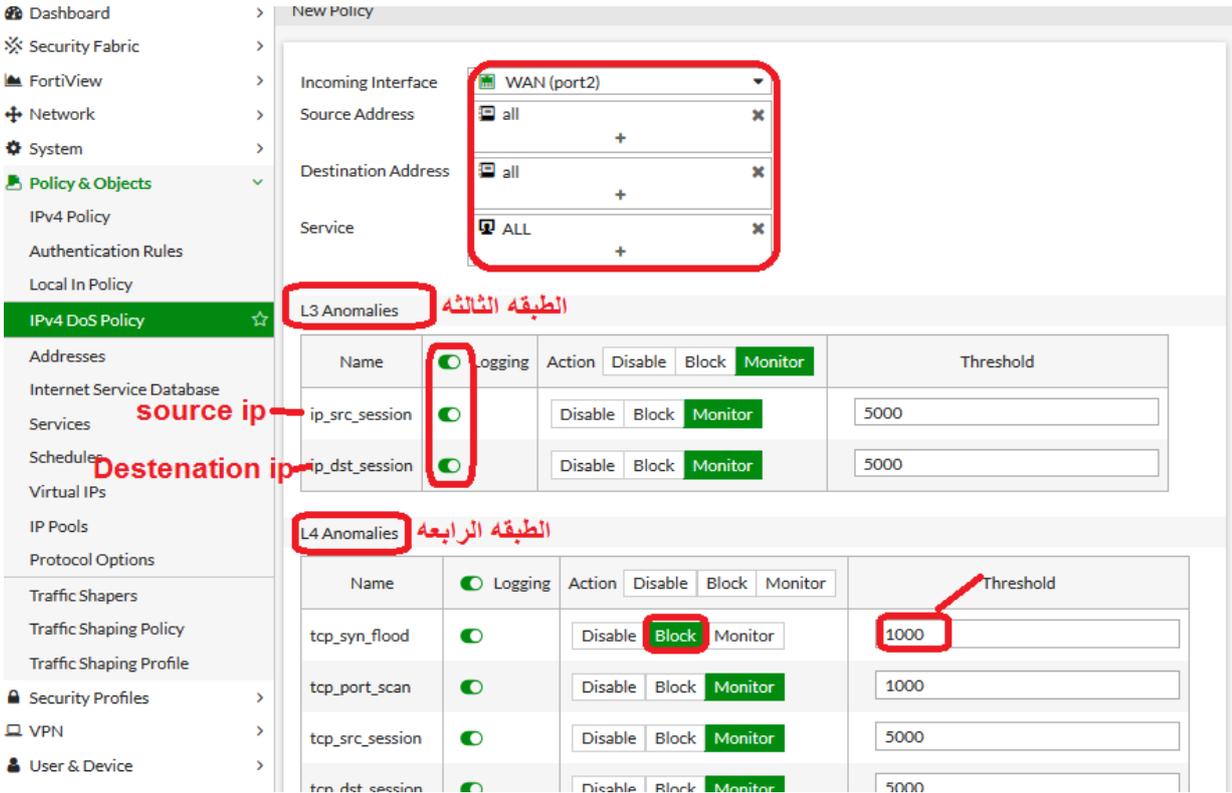
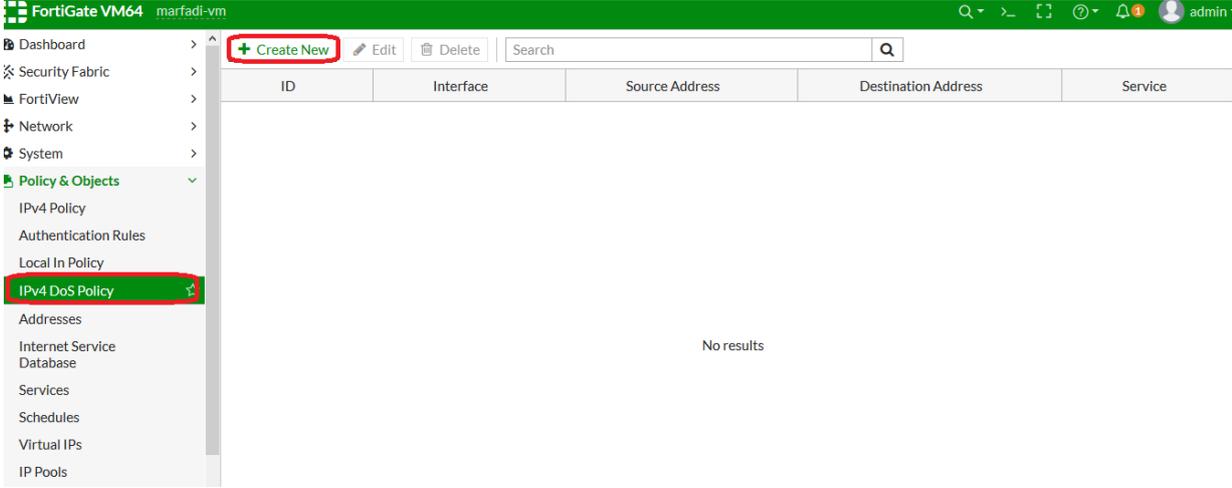
فأحياناً تحصل هجمات تسمى DOS حيث يتم إرسال كميات كثيرة جداً على خدمته معيّن من أجل إيقافها ...

مثلاً سيرفر عليه remote desktop connection يستلم الاتصال عبر البورت 3389 ، حيث ممكن استغلال هذا البورت المفتوح بحيث أقوم أنا كما هكر بإرسال SYN والسيرفر سوف يرد بـ SYN, ACK وتكرر العملية بيني وبين السيرفر إلى أن تتم عملية إيقاف الخدمة (RDP) لأن هناك أدوات وبرامج تقوم بعملية إرسال ملايين من SYN في توزيعه كإلى لينكس .. وهذا يسبب بأن الخدمة التابعة لـ RDP الموجودة في السيرفر تصبح Down وتسمى هذه العملية TCP syn flooding attack وتعتبر نوع من أنواع الـ DOS attack .

يوجد أيضاً هجمات أخرى مثل الـ ICMP syn flooding attack و UDP flooding وغيرها وكلها تندرج تحت الـ DOS attack .

فالفورتني جيت عنده خاصية جميلة اسمها IPV4 Dos policy حيث تستخدم هذه الميزة من أجل منع والتحكم بهذا النوع من الهجمات ..

الآن سنقوم بإنشاء policy تمنع هذه النوعيه من الهجمات من برع الشبكة (من الانترنت)



أساسيات فورتى جيت

Policy & Objects	Control	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	1000
tcp_port_scan	<input checked="" type="checkbox"/>	Disable Block Monitor	1000
tcp_src_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000
tcp_dst_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000
udp_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
udp_scan	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
udp_src_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000
udp_dst_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000
icmp_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	250
icmp_sweep	<input checked="" type="checkbox"/>	Disable Block Monitor	100
icmp_src_session	<input checked="" type="checkbox"/>	Disable Block Monitor	300
icmp_dst_session	<input checked="" type="checkbox"/>	Disable Block Monitor	1000
sctp_flood	<input checked="" type="checkbox"/>	Disable Block Monitor	2000
sctp_scan	<input checked="" type="checkbox"/>	Disable Block Monitor	1000
sctp_src_session	<input checked="" type="checkbox"/>	Disable Block Monitor	5000

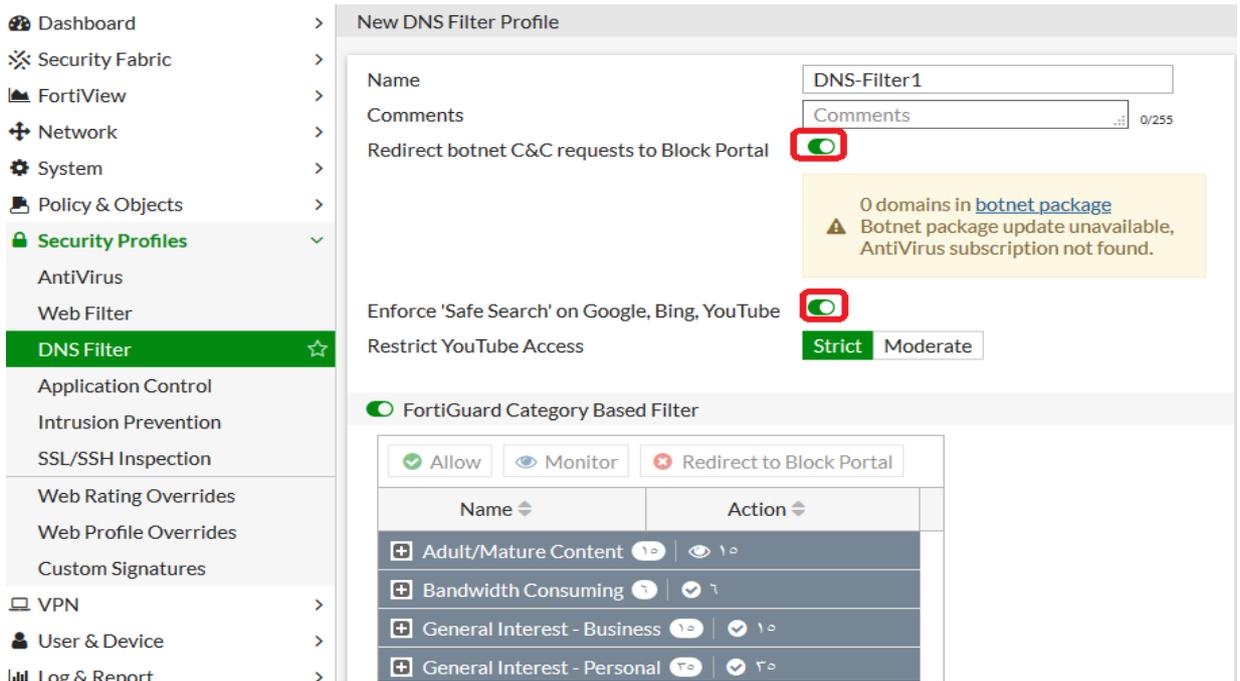
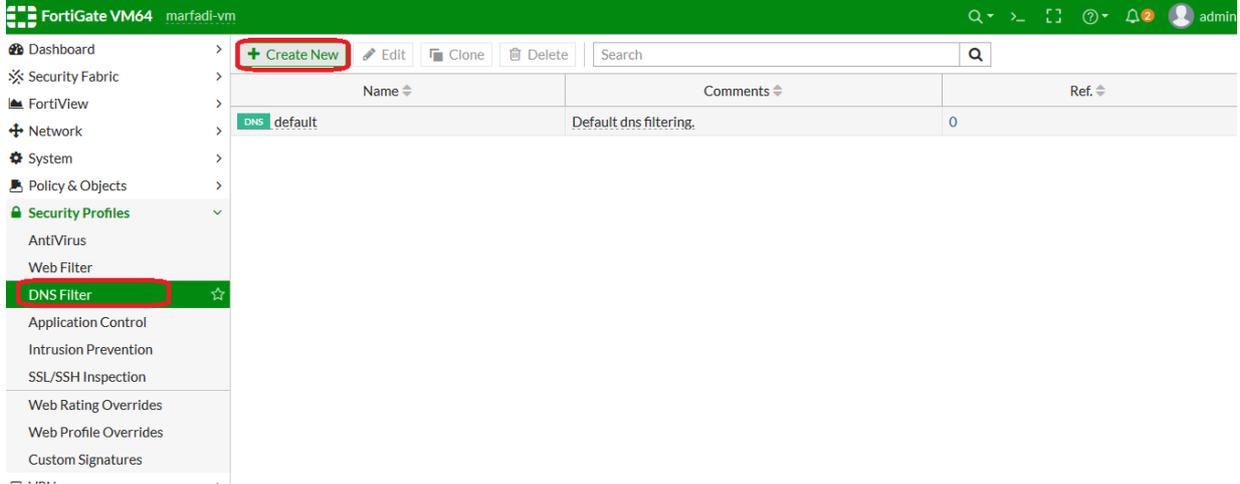
الصور أعلاه توضح بان عمليه الفحص والتحكم بال connection القادم الى ال wan interface حيث سيتم عمل log للاتصال القادم من او الى source ip و Destination ip وتعدى ال 5000 . أيضا يتم عمل Block ل tcp_syn_flood لو وصل عدد الجلسات عن 1000 لبورت معين ..وهكذا

ID	Interface	Source Address	Destination Address	Service
1	WAN (port2)	all	all	ALL

بهذا انا قمت بتأمين الترافيك الذي يأتي عبر ال wan interface سواء على شكل tcp او udp من هجمات ال DOS .

: DNS Filtering ➤

عبارة عن خاصية بالفورتى جيت تستطيع ان تعمل بها web filtering بواسطة الـ DNS



: Redirect botnet C&C requests to Block Portal

الفورتى جيت سوف يقوم بإغلاق الوصول لأي Domains خاص بالـ Botnet ..

: Enforce 'Safe Search' on Google, Bing, YouTube

أساسيات فورتى جيت

عند تفعيل هذه الخاصية فإن عملية البحث ستكون آمنة ويتم استخدام هذا الخيار خصوصا في المدارس ،حيث سيمنع الوصول أو البحث عن أي موقع محظور أو غير مناسب فلو قام اليوزر بالبحث مثلا عن مواقع اباحيه او مواقع تجاره الأسلحة ..الخ سيتم منعه وعمل له .

كما يمكننا اغلاق المواقع عبر FortiGuard Category Based Filter كما بالصورة ادناه

Comments | Comments 0/255

Redirect botnet C&C requests to Block Portal

0 domains in botnet package
Botnet package update unavailable, AntiVirus subscription not found.

Enforce 'Safe Search' on Google, Bing, YouTube

Restrict YouTube Access **Strict** Moderate

FortiGuard Category Based Filter

Allow Monitor Redirect to Block Portal

Name	Action
Adult/Mature Content 15 10	
Bandwidth Consuming 6 6	
General Interest - Business 15 10	
General Interest - Personal 35 30	

OK Cancel

استخدام Static Domain Filter لأغلاق المواقع :

Dashboard | Security Fabric | FortiView | Network | System | Policy & Objects | Security Profiles | AntiVirus | Web Filter | DNS Filter | Application Control | Intrusion Prevention | SSL/SSH Inspection | Web Rating Overrides | Web Profile Overrides | Custom Signatures | VPN | User & Device

New DNS Filter Profile

Potentially Liable 6 10 8
Security Risk 6 6
Unrated 1 1

Static Domain Filter

Domain Filter

Edit Delete Search

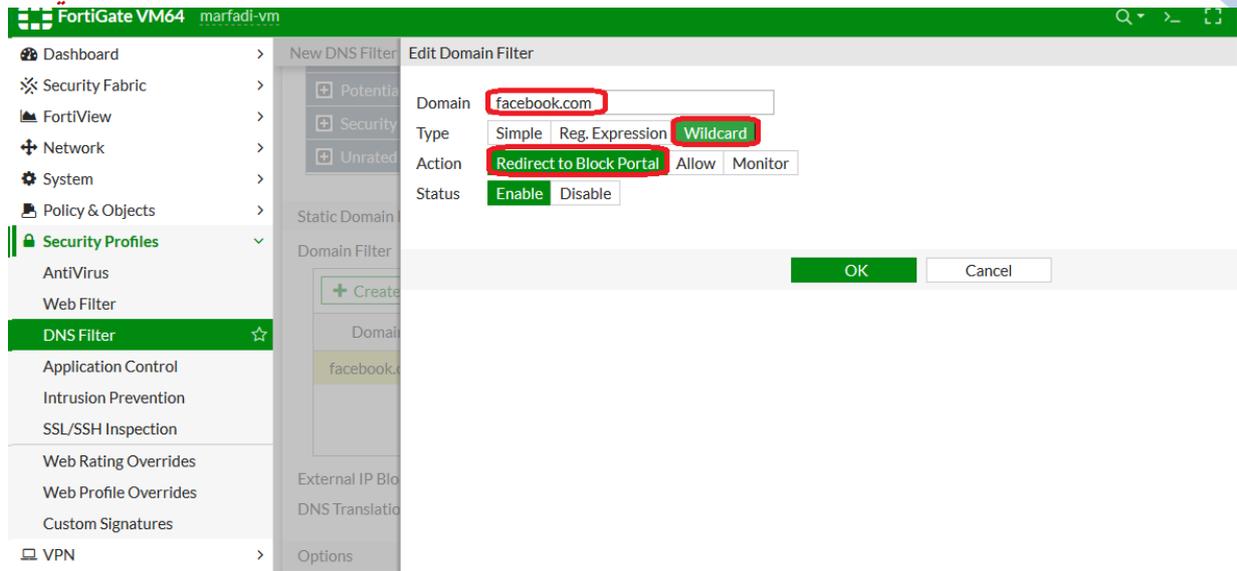
Domain	Type	Action	Status
No results			

External IP Block Lists

DNS Translation

Options

Redirect Portal IP **Use FortiGuard Default** Specify



عمل Block لموقع الفيسبوك ...

➤ الفرق بين ال web filter And dns filter :

الويب فلتر يعمل Block للموقع عبر الURL

يعني ممكن تقفل ال www.marfadi.com/test و بنفس الوقت تكون سامح ان المستخدمين يفتحوا

Www.Marfadi.com/users

لكن ال dns filter بيقتل عبر ال DNS Queries من البداية أصلا ..

يعني لا يعمل resolve ل www.marfadi.com أصلا ..

الحمد لله تعالى الذي وفقنا في تقديم هذا الكتاب، وها هي القطرات الأخيرة في مشوار هذا الكتاب، وقد كان الكتاب يتكلم عن فورتى جيت فايروول ، وقد بذلنا كل الجهد والبذل لكي يخرج هذا الكتاب بهذا الشكل. ونرجو من الله أن تكون رحلة ممتعة وشيقة لكل مبتدأ في هذا الموضوع، وكذلك نرجو أن تكون قد ارتقت بدرجات العقل الفكر، حيث لم يكن هذا الجهد بالجهد اليسير حيث استغرق تقريباً 8 اشهر من الاستماع لفيدويوهات مختلفة والبحث في الفورتى جيت من مصادر مختلفة، ونحن لا ندعى الكمال فإن الكمال لله عزوجل فقط وأنا أصلاً شخص مبتدأ في الفورتى جيت وهذا اجتهاد بسيط مني ولا ادعي الاحتراف فيه ، ونحن قدمنا كل الجهد لهذا الكتاب، فإن وفقنا فمن الله عزوجل وإن أخفقنا فمن أنفسنا، وكفانا نحن شرف المحاولة، وأخيراً نرجو أن يكون هذا الكتاب قد نال إعجابكم. وصل اللهم وسلم وبارك تسليماً كثيراً على معلمنا الأول وحبیبنا سيدنا محمد عليه أفضل الصلاة والسلام ..

من لديه أي ملاحظات او انتقاد فنرجو التواصل عبر الواتس اب 00967772898598

او عبر صفحتي بالفيسبوك <https://www.facebook.com/profile.php?id=100014064451982>