FortiGate Firewall

FortiGate Essentials

By- Mohamed Marfadi

الفهرس

المقدمة 1

كلمة شكر وعرفان 2

مقدمة عن فورتي جيت 3

طريقة تنزيل وضبط اعدادات FortiGate vm 4

ضبط اعدادات كرت الشبكة على جهاز الكلاينت(Client)..... 12

طريقة عمل reset لعدد الأيام (14) للVM 18

مشكله ظهور بان الايسنز(License) قد انتهى 20

طريقة عمل باك اب للإعدادات التابعه للVM وكيفيه استعادتها 20

شرح مكونات وواجهات الفورتي جيت 23

طريقة تغيير باسورد الأدمن (admin)بواسطة CLI 24

إيقاف او اعاده التشغيل او تغيير الباسورد او للخروج من الفورتي ويب عبر GUI 24

شرح الDASHBOARD 25

شرح القوائم 29

شرح استخدامات ومعلومات الWidget 29

طريقة توصيل الانترنت لجهاز الفورتي جيت 39

متى احتاج الى عمل ترقيه –تحديث- للـ Firmware التابع لجهاز الفورتي 44

طرق ترقيه النظام Upgrade firmware 44

عمليه الـ downgrade 45

Administration types &profiles 45

طريقة انشاء يوزر جديد بواسطة CLI 47

لحذف يوزر بواسطة CLI 49

ما هو FortiGuard ؟ 52

SD-WAN=WAN Link Load Balancing SD-WAN 53

طريقة انشاء SD-WAN Rule جديده 61

جعل الـ https traffic يطلع عبر الـ wan 2 62

جعل الـ http traffic يطلع عبر الـ wan1 63

انشاء SLA باسم INTERNET حيث تقوم بفحص الخط الأفضل 64

طريقة اظهار ميزه جديده مثلا تريد اظهار الخاصية(features) 66

طريقة انشاء Rule policy جديده 67

شرح Schedule 70

طريقة انشاء schedule 70

تحديد أيام محدده ووقت محدد مره واحده فقط وينتهي 73

أنواع الـ actions في الـ policy 74

Traffic shapers 75

APPLICATION CONTROL 76

Web Filter 82

ما هو الـfortiguard 82

ماهي فكره الـ Fortiguard 82

طريقة انشاء web filter profile 83

طريقة اغلاق موقع معين بالإضافة الى sub domain بواسطة ال web filter 89

بعض التمارين والأمثلة حول الـweb filter واستخدام static URL filter 90

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 الفايرووول
116 ..... Bandwidth ,Throughput ,Concurrent Sessions
118 .....FortiGate Series
119 ..... موديلات فورتي جيت
119 .....Operating system OS key features 5 2
120 .....Home lab Design
121 .....FortiGate basics Registering FortiGate
121..... طريقة عمل Registration لجهاز الفورتي جيت
122 ..... ماهي الfeatures
126 ..... ما هو Revisions في الفورتي جيت
129 .....NTP server(Network time protocol)
131 ..... تصميم الشبكة
133 .....Advice administration

طريقة رفع مستوى الأمان عند الوصول الى جهاز الفورتي جيت 136

ما هو Trusted hosts 144

Interface ip address..... 147

Static route(default gateway)(static gateway)..... 153

Password recovery 156

طريقة عمل DISABLE لـMAINTAINER MODE..... 158

Password policy..... 159

كيف تفعيل DHCP server على الفورتي 162

بعض الأوامر(Cmd) التي يتم تطبيقها على اجهزه الكلاينت..... 165

طريقة تعديل الـ leased duration في الـdhcp server 168

DNS(domain name service)..... 172

FortiGuard Concept..... 173

Fortiguard distribution network (FDN)..... 175

FortiExplorer..... 178

Fortigate firewall policy..... 179

ماهي انواع الـ objects الأساسية (الضرورية)..... 180

طريقة انشاء البوليسي 182

Firewall objects..... 185

شرح بعض اعمده الـaddress list 193

ماهي أنواع الـservices ؟..... 201

ما هو الـ service group 206

Schedule 208

طريقة انشاء schedule جديد 208

طريقة انشاء schedule group 214

Policy order 219

Managing devices 224

كيف يقوم فورتي جيت بأداره الأجهزة ؟ 225

Access control list (ACL) 232

ما هو Mac reservation 233

FortiClient 243

طريقة تنزيل الفورتي كلاينت على الاجهزه 245

Authentication 246

ماهي طرق الـ authentication (التحقق من الهوية) في الفورتي جيت..... 247

Local authentication 248

Max invalid authentication 256

Authentication timeout 257

Restricting number of concurrent user logons 261

Managing guests 262

FSSO(fortinet single sign on) 273

الطريقة الأولى Poll Active Directory server 279

الطريقة الثانية لعمل الـ integeration بين الفورتي جيت والـAD 284

الطريقة الثانية(خيار اخر) لعمل integration عبر اختيار الـCollector Agent..... 302

Antivirus..... 303

كيف تفرق بين قواعد بيانات الفايروسات على جهاز الفورتي جيت ؟..... 304

كيف بيتم عمليه التحديث للAntivirus DB ؟..... 304

طريقة تفعيل الـ antivirus على الفورتي جيت وعمل حمايه للشبكة من أي تهديدات ... 309

طريقة انشاء بروفايل جديد لـantivirus 309

طريقة اختيار البروفايل مخصص في البوليسي 311

Antivirus Mode 312

متى يتم استخدام flow base ومتى يتم استخدام proxy base ؟..... 314

ماهي طريقة عمل مكافح الفايروسات في الفورتي..... 314

Antivirus Profile configuration..... 316

Web filtering..... 317

أسباب التحكم في Web filtering 317

Web filtering mode..... 318

ماهي الخيارات المتاحة على الفورتي جيت بخصوص الـweb filtering..... 319

ماهي علاقه فورتي جار بالفورتي جيت 320

كيفيه التعامل مع الـ fortiguard category في الـweb filter 321

أنواع الـ action 332

Web URL filtering..... 348

Web content filter..... 357

Application controller..... 362

Application control action 363

ما هو الـTraffic shape 363

طريقة التحكم في التطبيقات عبر الـApplication control 370

لمعرفة ماهي البرامج(signatures)التي بتكون مندرجه تحت الـ category 371

Application and Filter Overrides.....373

طريقة عمل حظر(ban)لجهاز معين 379

Email filter.....383

ماهي الطرق التي يستخدمها الفورتي جيت لكي يساعدك لاكتشاف الاسبام ايميل ؟.... 387

Logging and monitoring 393

VPN(Virtual private Network) 395

اشكال الاتصال الـVPN او يسمى (VPN Tunnel designs) 396

أنواع بروتوكولات الـ VPN 398

VPN Encryption 398

التطبيق العملي لـIPSec Client/server 400

IPSec SITE to SITE 413

vpn over SSL.....416

تمرين اخر حول VPN SITE TO SITE.....435

VPN SITE TO SITE DYNAMIC DNS(DDNS) 440

Network address 442

Traffic shaper 443

انوع الـtraffic shaper 445

طريقة انشاء Traffic shaping policy 445

Virtual IP 447

طريقة انشاء Virtual ip 448

Virtual group 450

طريقة انشاء virtual group بحيث أقوم بضم الـ4 virtual ip's بداخلها 451

IPV4 DOS policy configuration 454

DNS Filtering 457

الفرق بين الweb filter And dns filter 459

الخاتمة 460

المقدمـــــــة

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 وعرفان

رسالة شكروحبّ وعرفان 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 سارحبهم في الوجدان إلى من أمرني ربي بطاعتهم والإحسان لهم أبي وأمّي كلمات الحبّ عجزت عن وصف حبّي الكبيرلعظمتكم حروف العشق عجزت عن نظم أجمل القصائد والألحان فيكم أنتم قلبي، أنتم فرحي أنتم سرّ السّعادة في قلبي أبي وأمّي حفظكم الله وأبقاكم لناظري أمّي أبي أنتم قلبي النّابض حبكم يسري في شراييني كيف لا وأنتم أول من نظرتُ إليهما أول أصوات سمعتها أول اسمين نطقت بها شفتاي حبّكما في قلبي كملء الأرض بل يطاول عنان السّماء إلى شمعة دربي وبلسم جروحي إلى من سهروا اللّيالي من أجلي، من أجل راحتي ورسم البسمة على شفاتي إلى من إذا عشتُ الدّهركلّه لن أوفي حقّهما إلى من أوصاني ربّي بطاعتهما دون معصيته إلى سبب نجاحي وسعادتي في الدّنيا والآخرة إلى جنّتي شكراً أمّي الحنونة أبي الغالي حفظكم الله وعافاكم ..

شكرا لكل افراد اسرتي ...

واشكر كل أصدقائي وكل من وقفوا معي حتى بكلمه تشجيع ...
اسال الله ان يحفظ اليمن كافه والحديدة خاصه وان يعم الأمن والأمان في كل ارجاء اليمن .

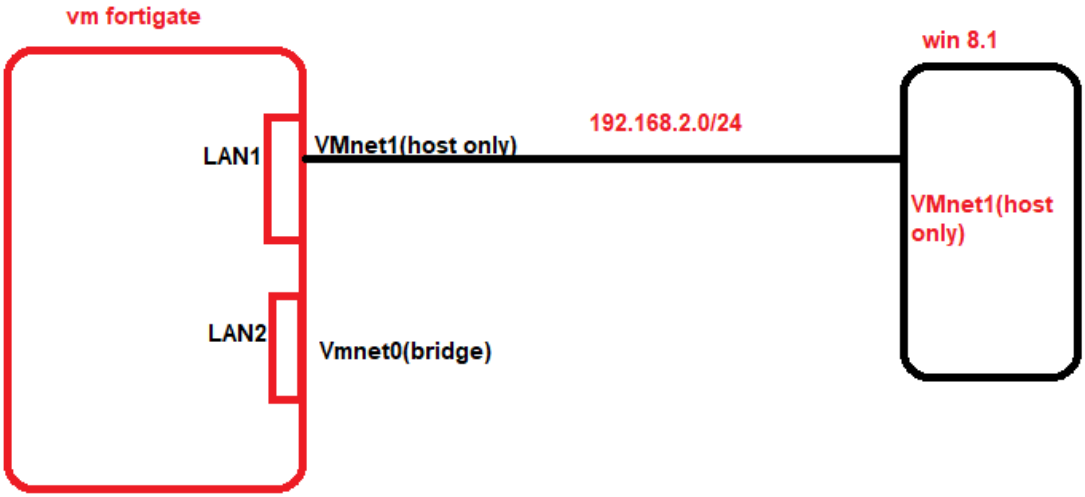
مقدمة عن فورتي جيت FortiGate

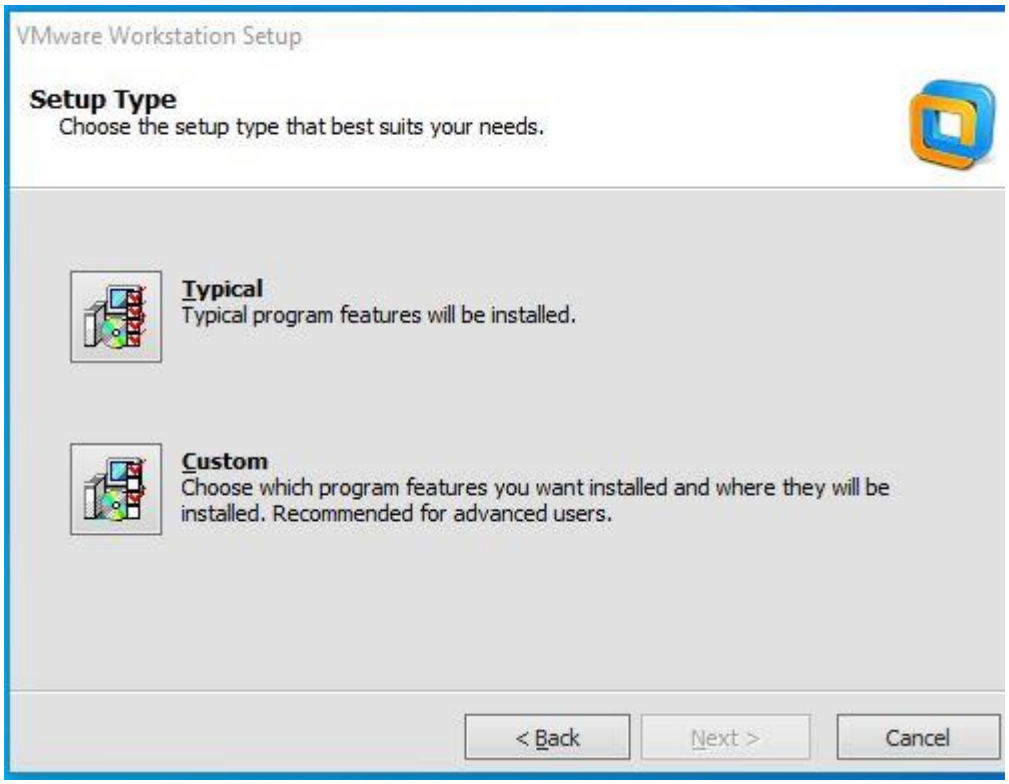
الفورتي جيت هو التطور الطبيعي للفايرول نظرا لانتشار الفيروسات والملفات الخبيثة فأصبحت الجدران النارية غيركافيه لتامين الشبكات ومن هنا ظهر مصطلح الـ UTM(Unified Threat Management)

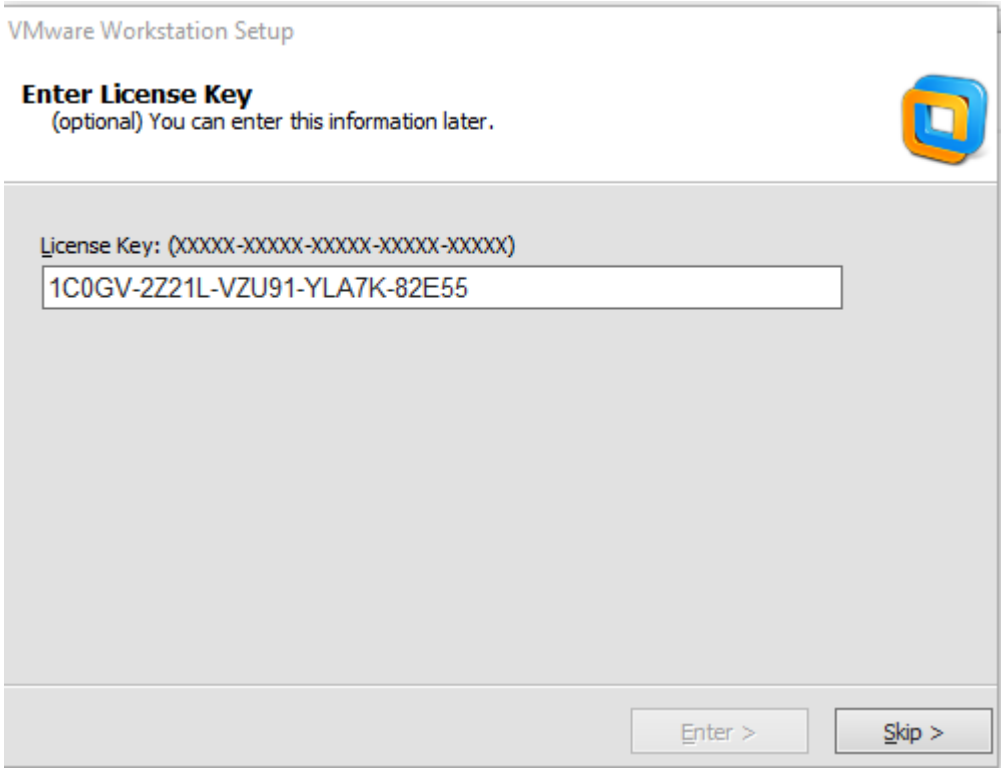
تعني إدارة التهديدات المجمعة او الموحدة بمعني توفير اكثر من حمايه للشبكة.

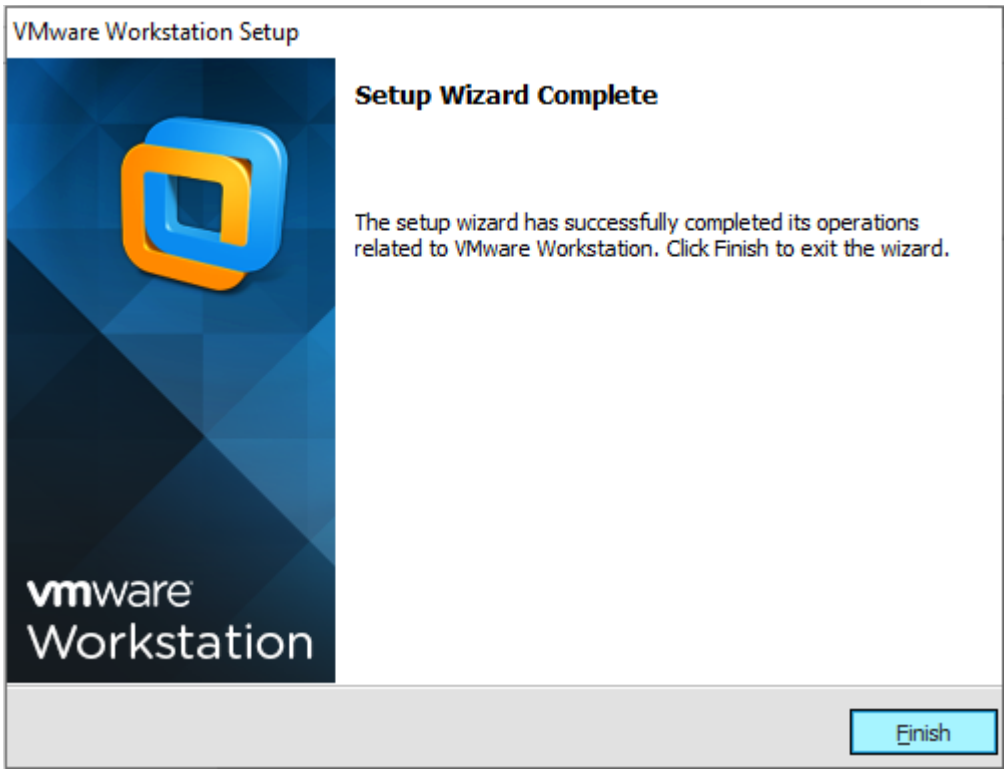
حيث يقدم مجموعه واسعه من الوظائف الامنية في جهازواحد يدعى FortiGate ويعمل هذا المنتج كأحد حلول UTM المعروفة وهي ان يعمل كـ , ips , vpn , firewall , WAN acceleration , Web filtering , antivirus , antispam , والعديد من الوظائف التي لا غنى عنها لبناء شبكة عملاقة مؤمنة ،،هناك العديد من الموديلات الصغيرة والكبيرة لتغطية جميع الاحتياجات.

❖ طريقة تنزيل وضبط اعدادات الـــVM FortiGate :

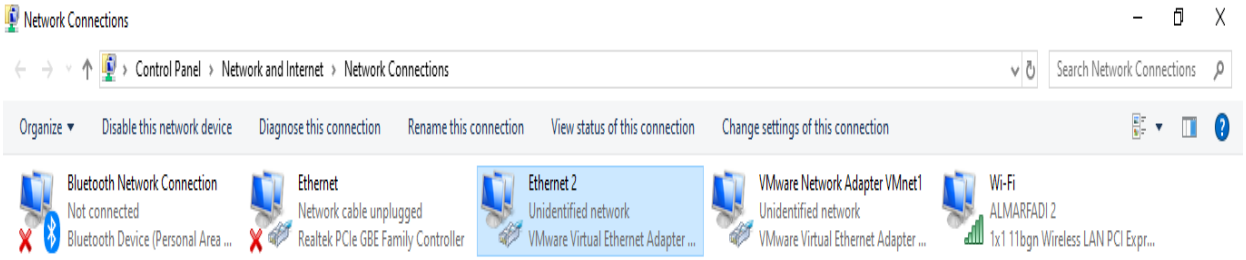


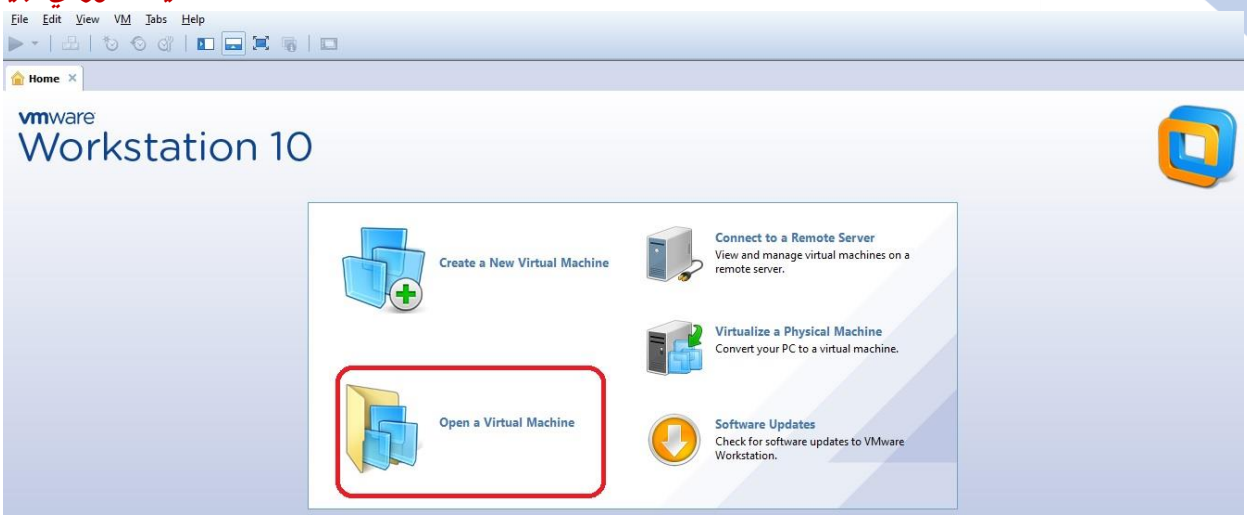

VMware Workstation Setup
Setup Type
Choose the setup type that best suits your needs.
Typical
Typical program features will be installed.
Custom
Choose which program features you want installed and where they will be installed. Recommended for advanced users.
< Back
Next >
Cancel


VMware Workstation Setup
Enter License Key
(optional) You can enter this information later.
License Key: (XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)
1C0GV-2Z21L-VZU91-YLA7K-82E55
Enter >
Skip >

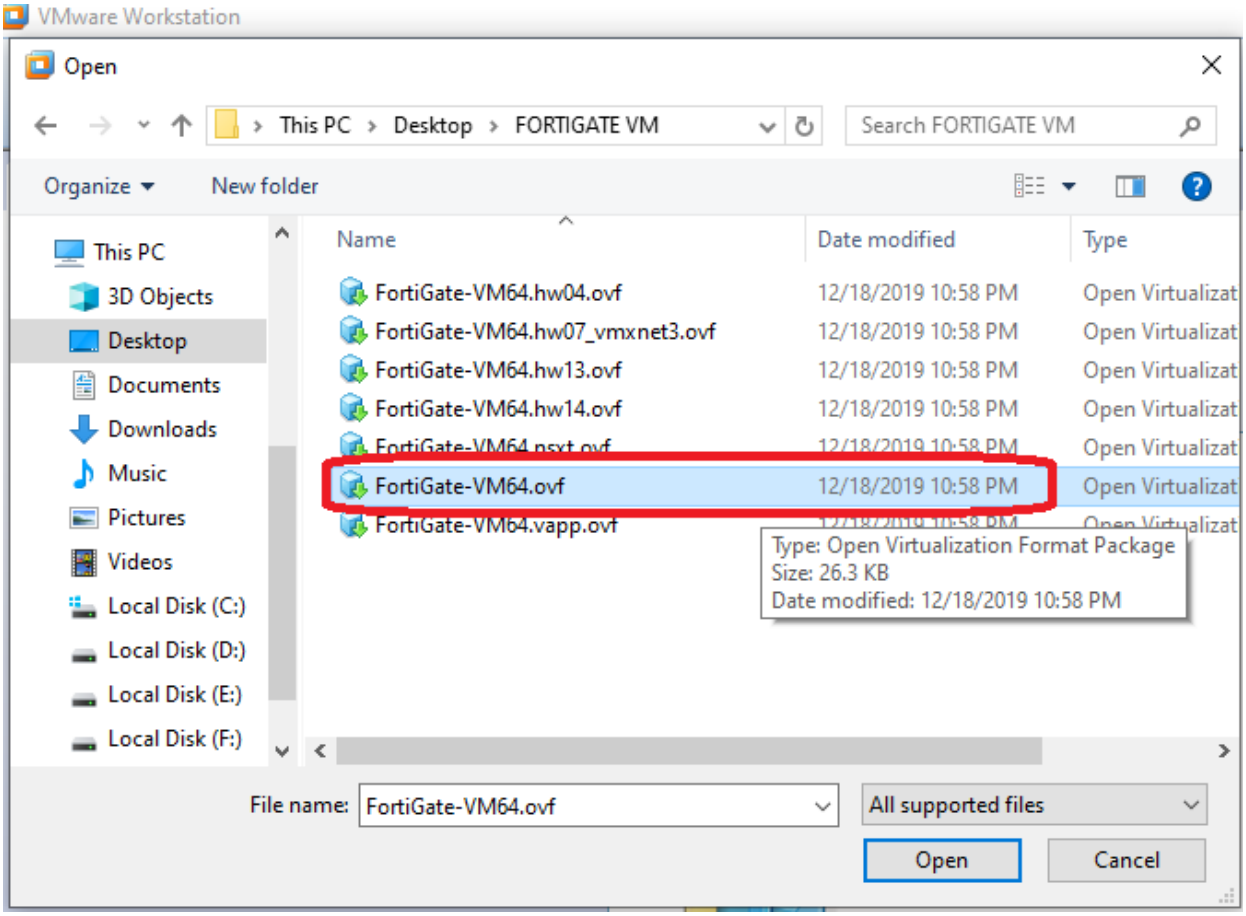


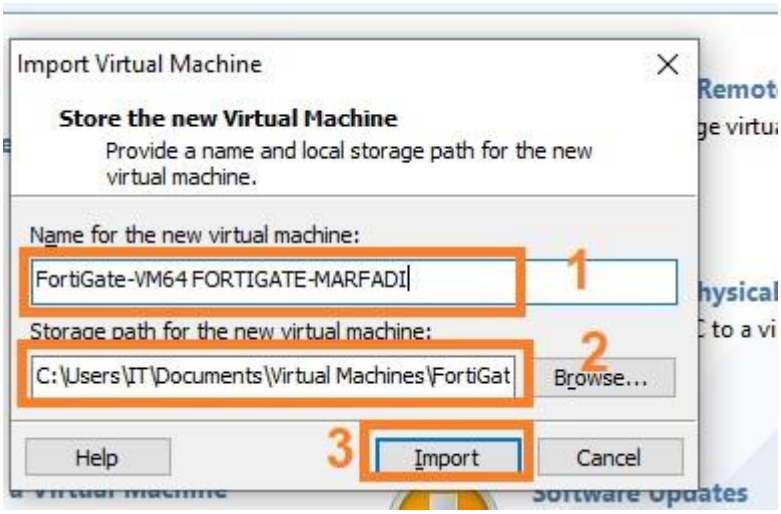
نلاحظ بالصورة ادناه بظهور كروت شبكة افتراضيه (وهميه)تابعه لvmware work station





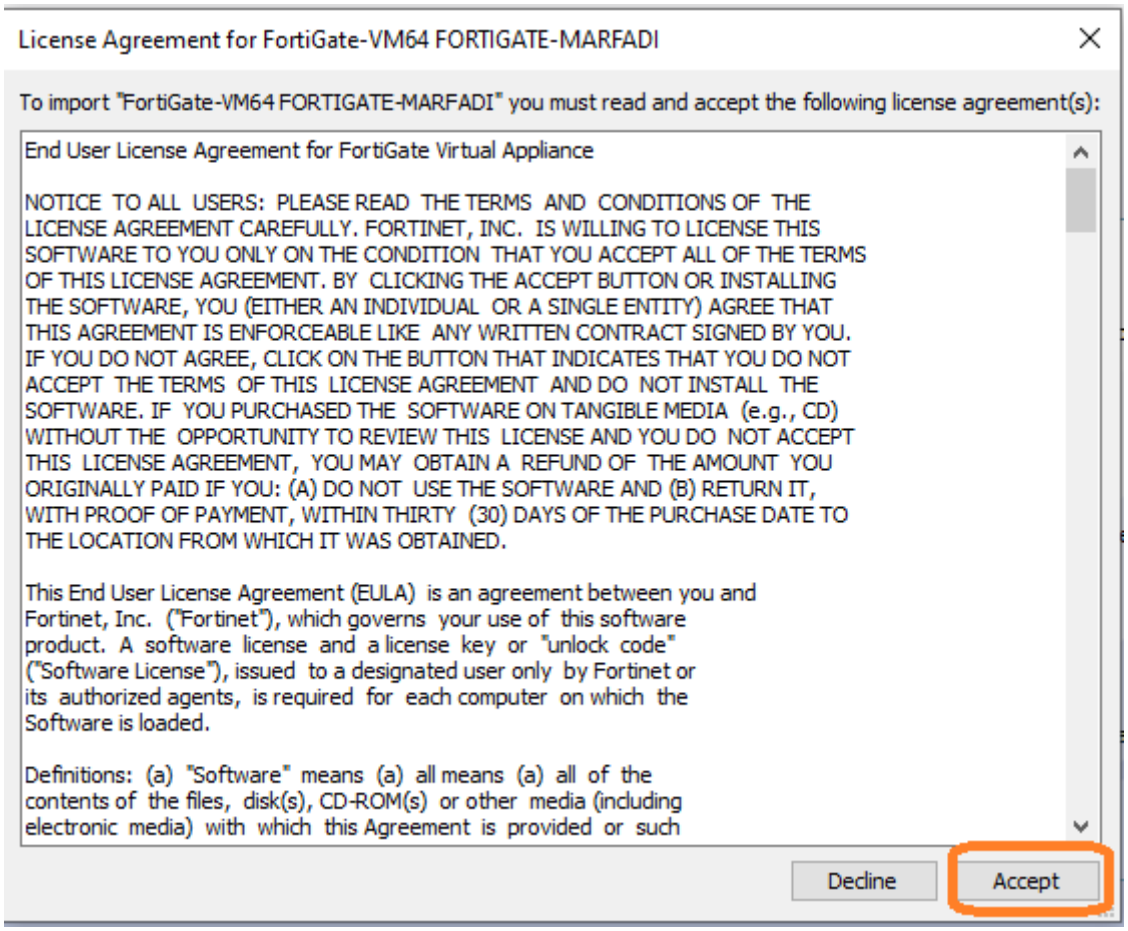
نقوم باختيار مكان fortigate vm والتي باسم FortiGate-VM64.ovf





نكتب اسم للـvm مثلا FortiGate-VM64 FORTIGATE-MARFADI

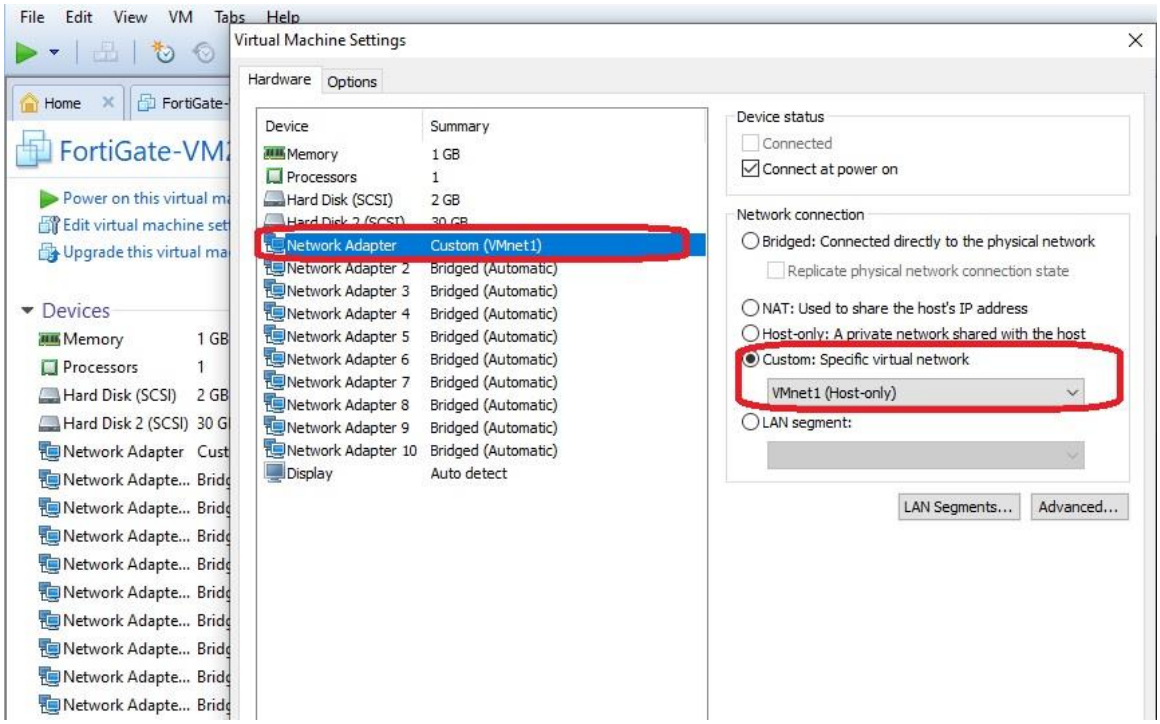
ونحدد مكان حفظ نسخه الـvm ثم نقوم بعمل استيراد ...



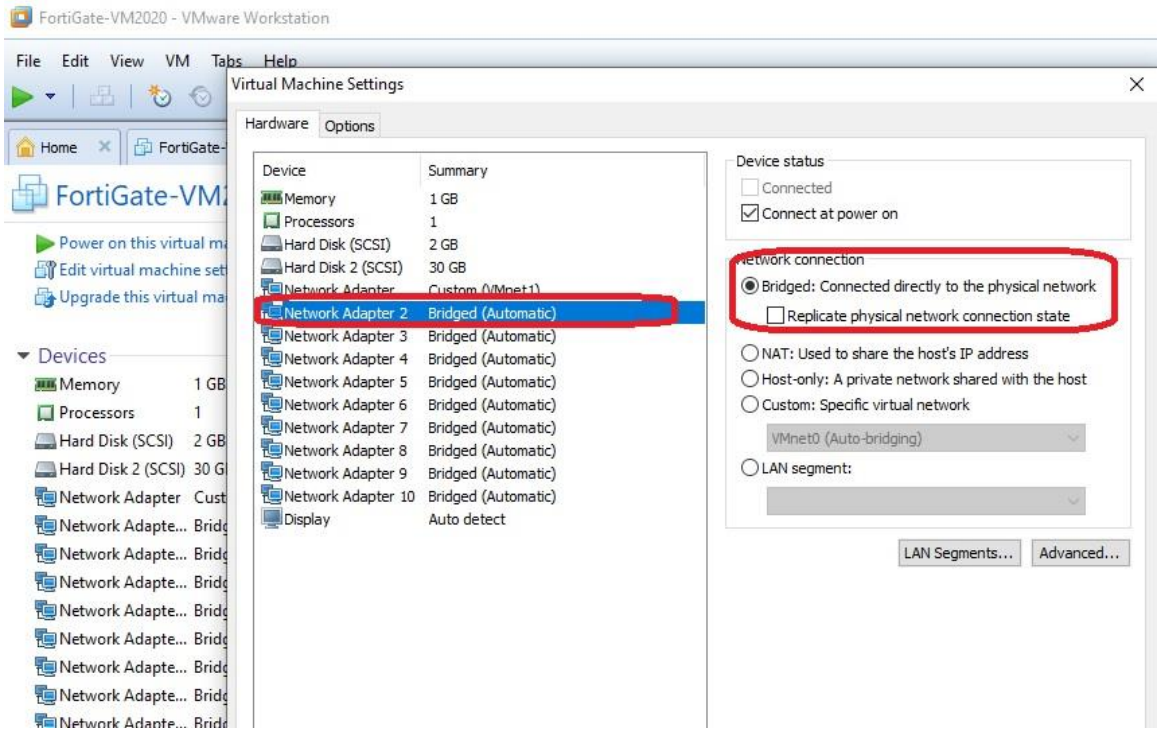
موافق...

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

نقوم بتجهيزكروت الشبكة الوهمية التابعه لـvm fortigate



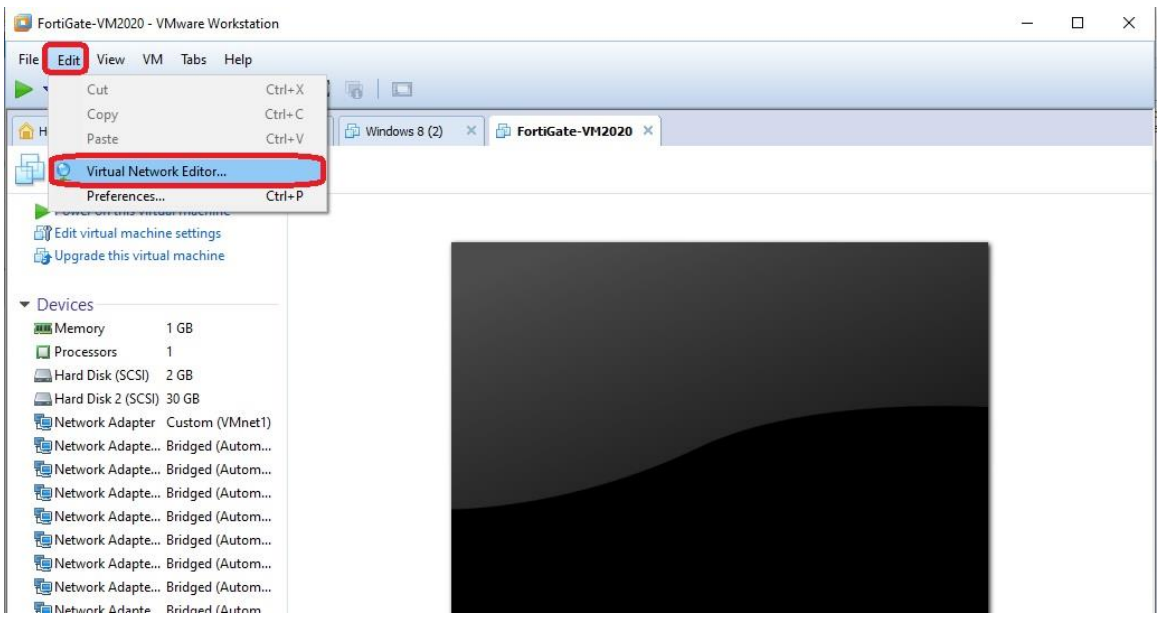
كما بالصورة أعلاه تم ضبط كرت الشبكة lan1 كـVmnet1(host only)

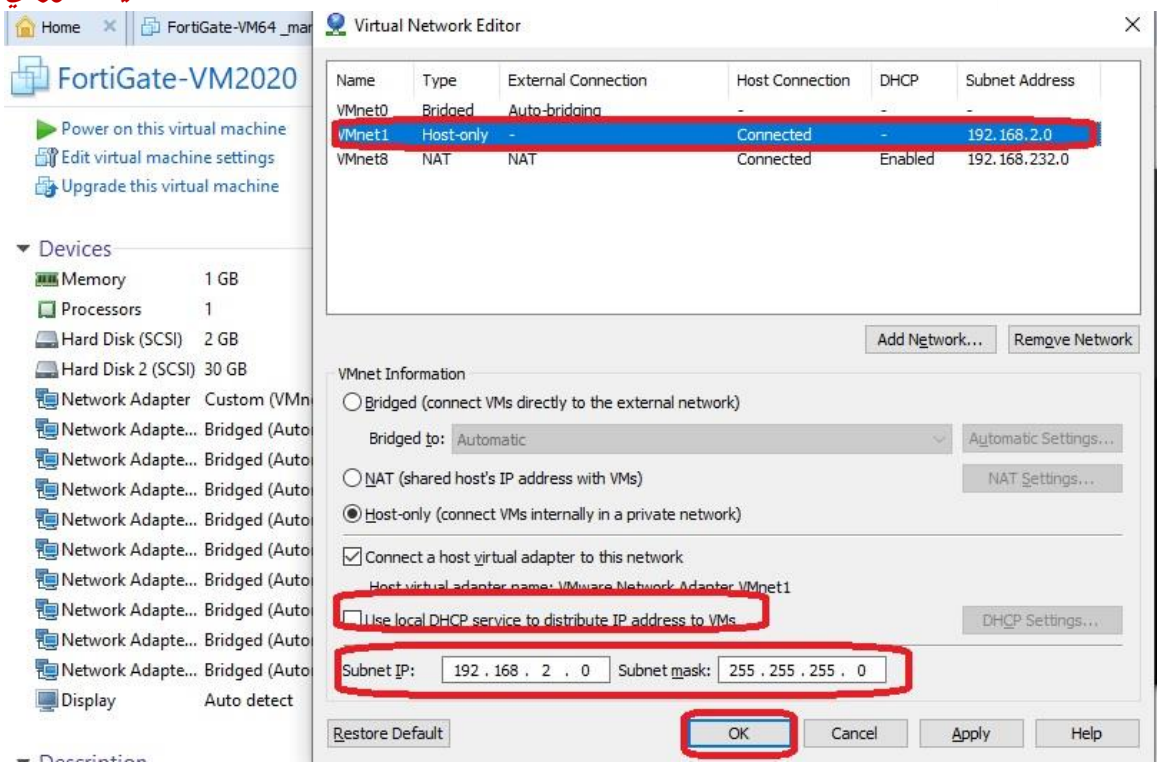


اما كرت الشبكة lan2 والذي وسوف يتم تغييره الى WAN سيتم ضبط إعداداته كما بالصورة أعلاه

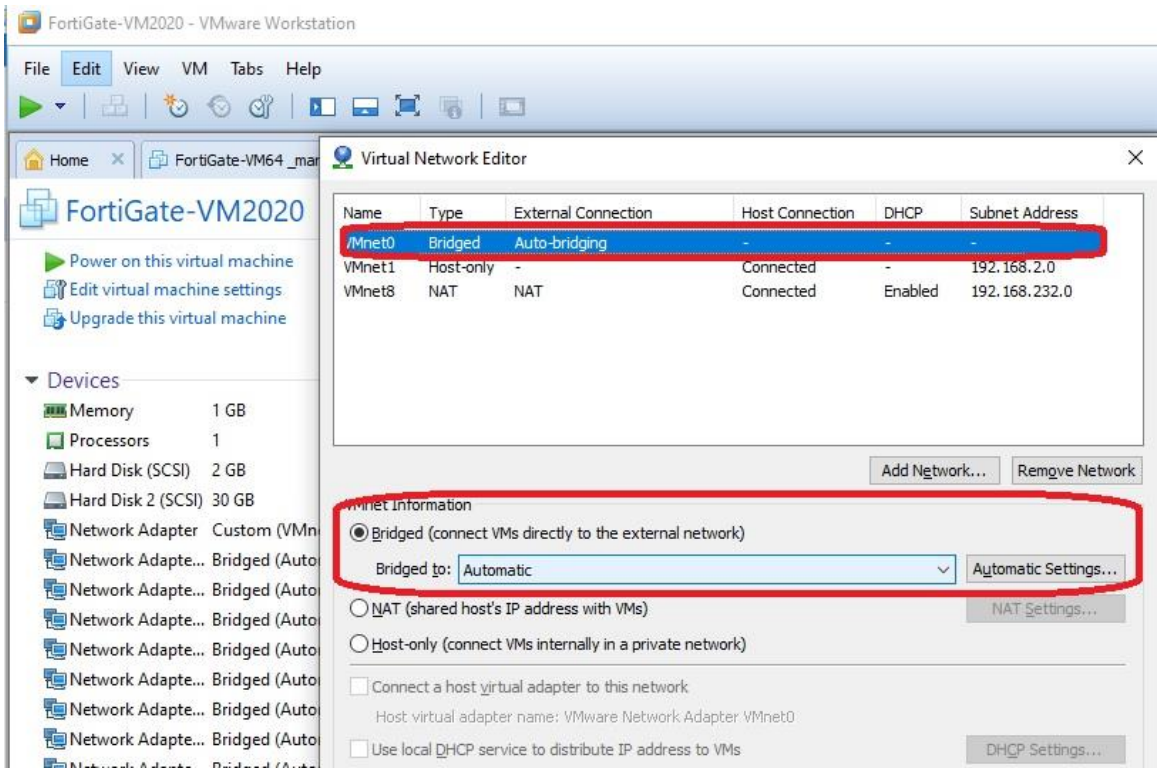
Bridge connected directory to the physical network

وذلك لكي يكون قادرعلى الوصول الى الروتر(المودم)لأنه سوف يكون موصل مع كرت الشبكة الوايرلس التابع للابتوب حيث سنقوم بجعل اعدادات كرت الشبكة الـWAN بالايبي 192.168.1.60 .. ثم سوف نقوم بضبط اعدادات كرت الشبكة الوهمي التابع لـVMWARE كما بالخطوات التالية :





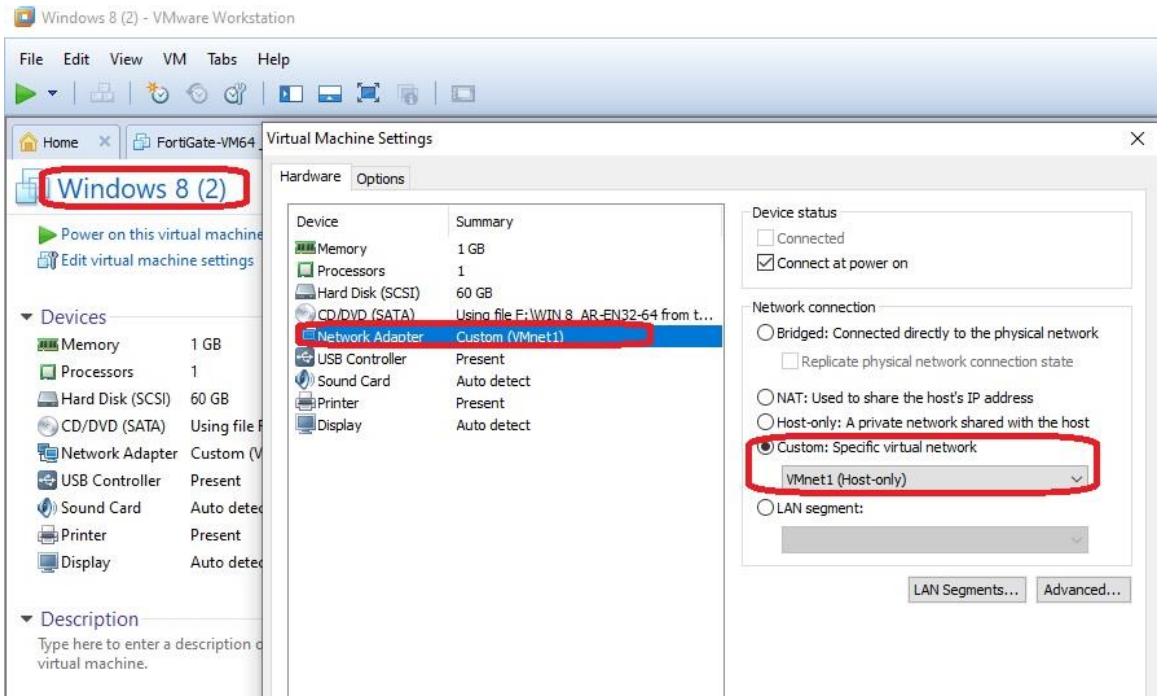
جعلنا كرت الشبكة الوهمي (Vnet1(host only من subnet 192.168.2.0 .



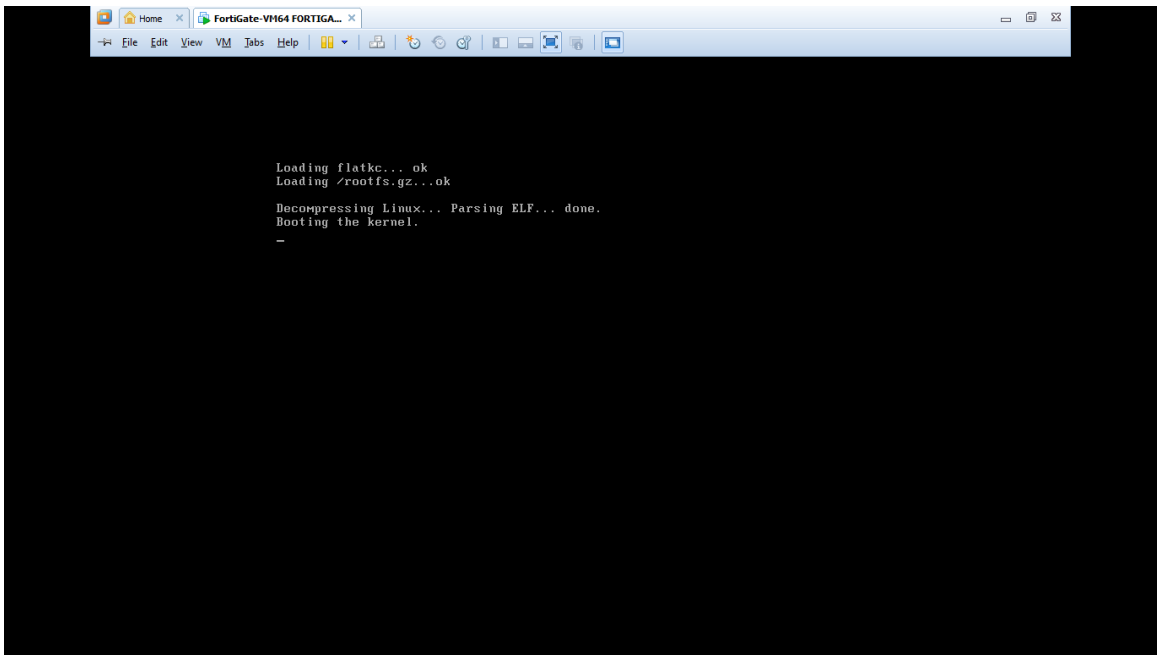
وأيضا ضبط الكرت vmnet0 بانه من نوع bridge

ضبط اعدادات كرت الشبكة على جهاز الكلاينت(Client):

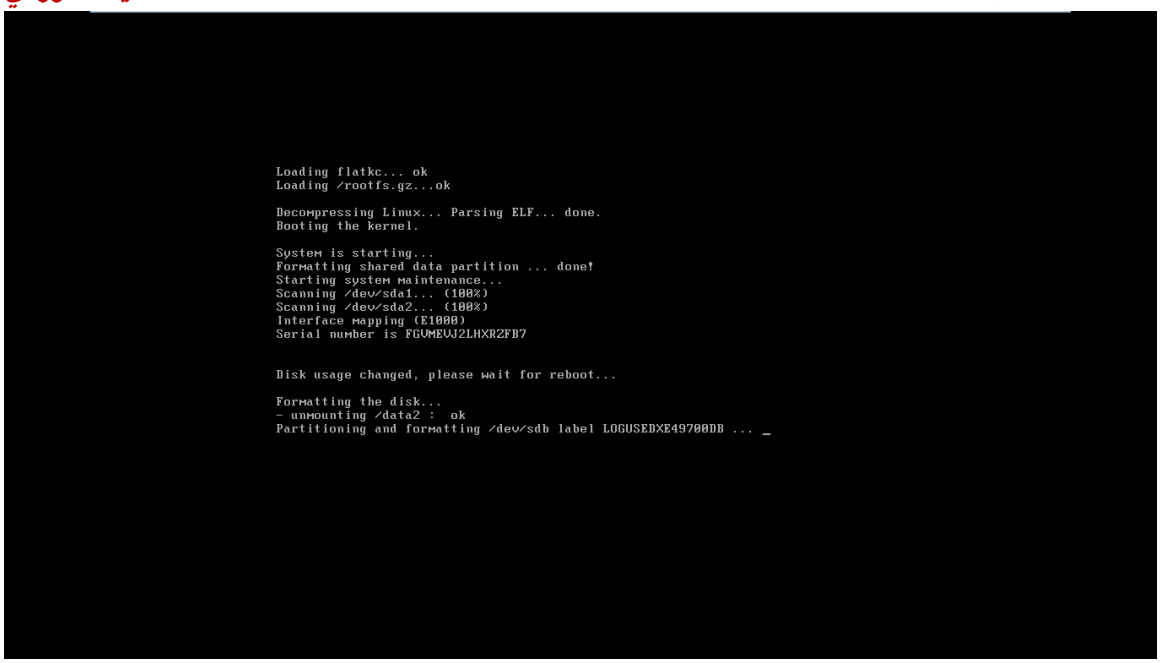
يجب ضبط اعدادات كرت الشبكة لـ اجهزه الكلاينت كما بالصورة التالية حيث يتم توصيله بنفس السويتش التابع لكرت الشبكة lan1 التابع VM FortiGate

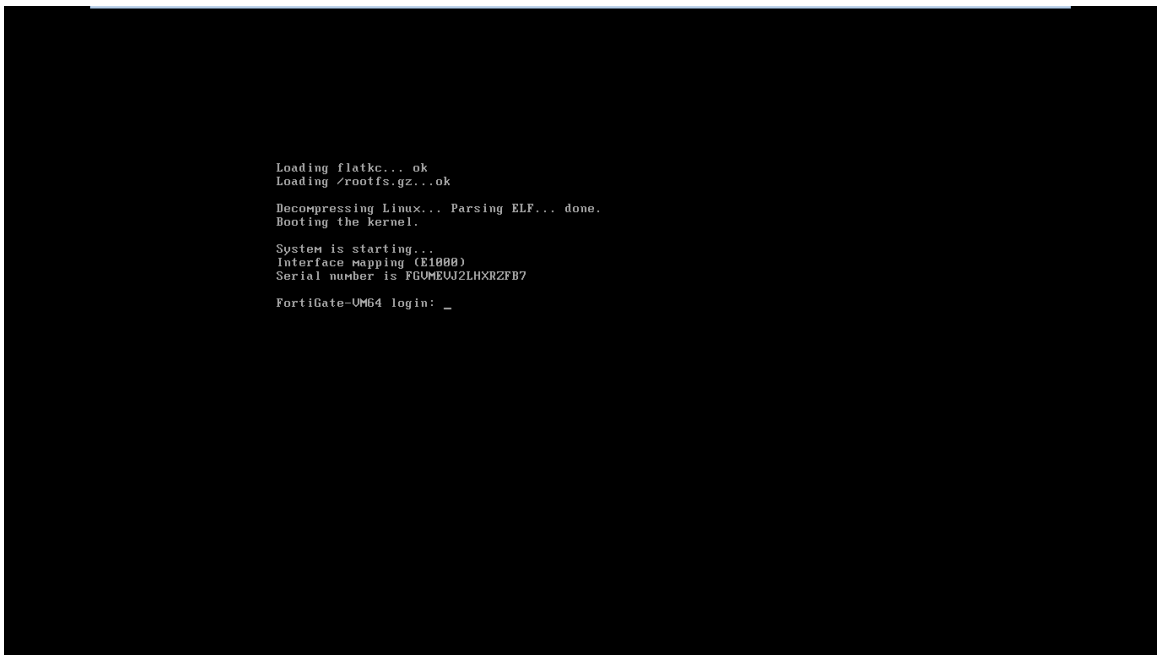


نقوم بتشغيل الـVM fortiGate

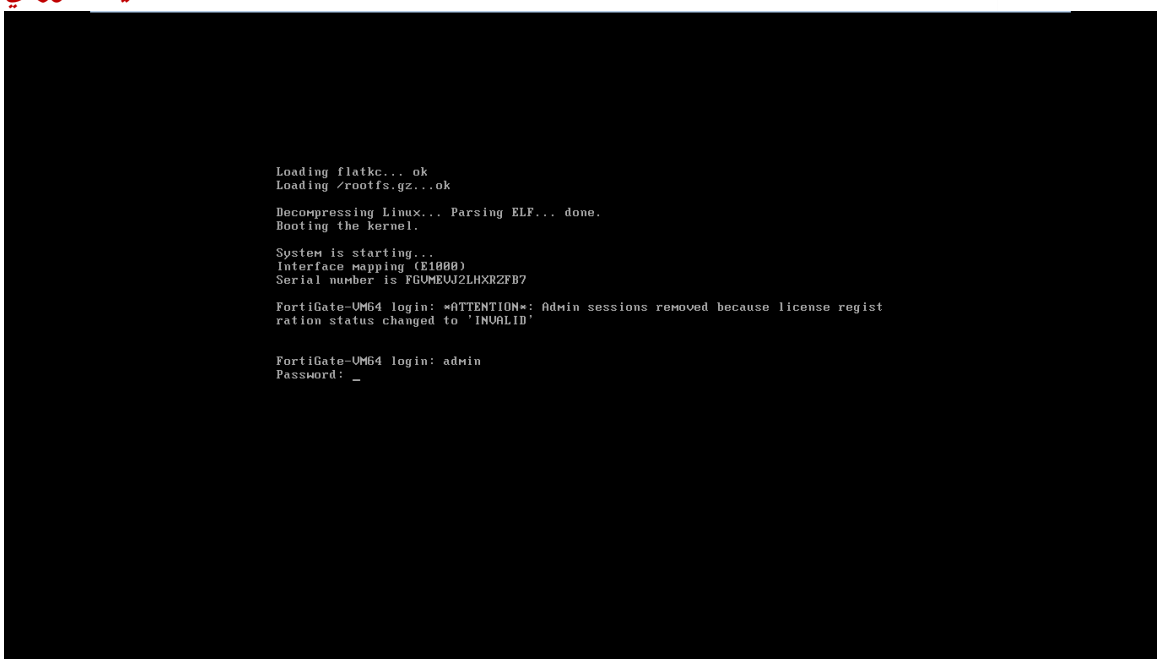


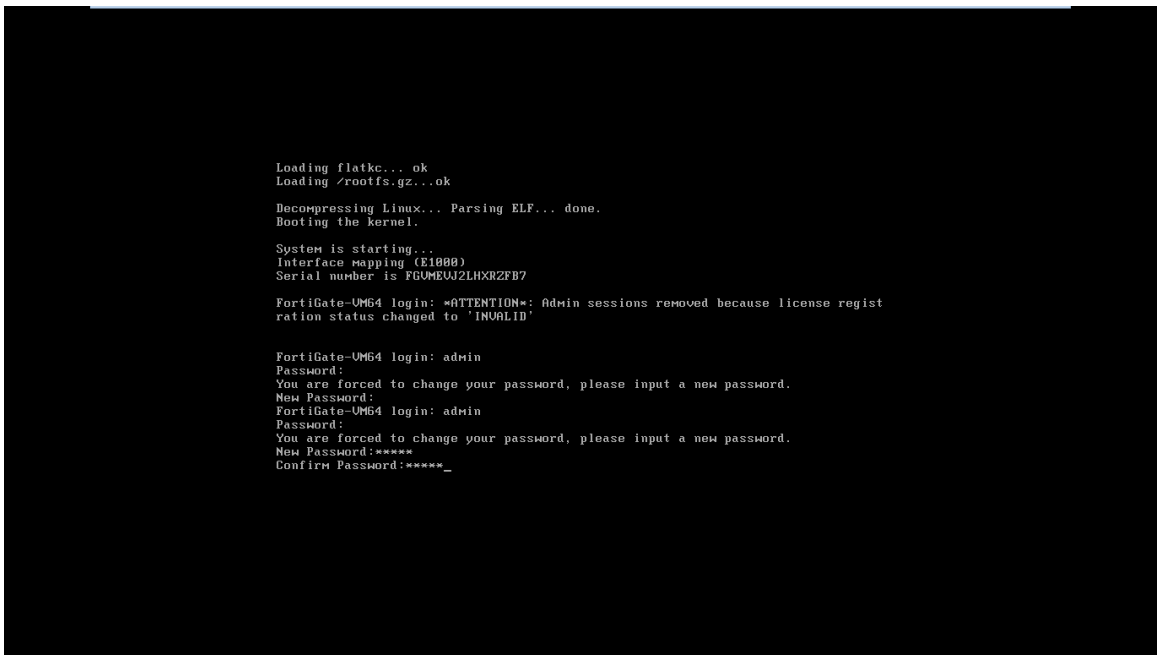
جاااري التشغيل ...





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





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

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

لذا سيتم الوصول الى الفورتي جيت من على الجهاز الوهمي لويندوز 8.1 (الكلاينت)والذي هو أصلا موصل على نفس السويتش مع كرت الشبكة lan1 لـvm fortigate ..

كرت الشبكة الـlan1 التابع للفورتي جيت موصل بنفس السويتش لجهاز الكلاينت عبر السويتش VMnet1 ونوعه Host only ..

لذا الان سوف نقوم بتجهيز كرت الشبكة الـport1 والتابع لـVM وذلك كما بالأوامر ادناه .

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

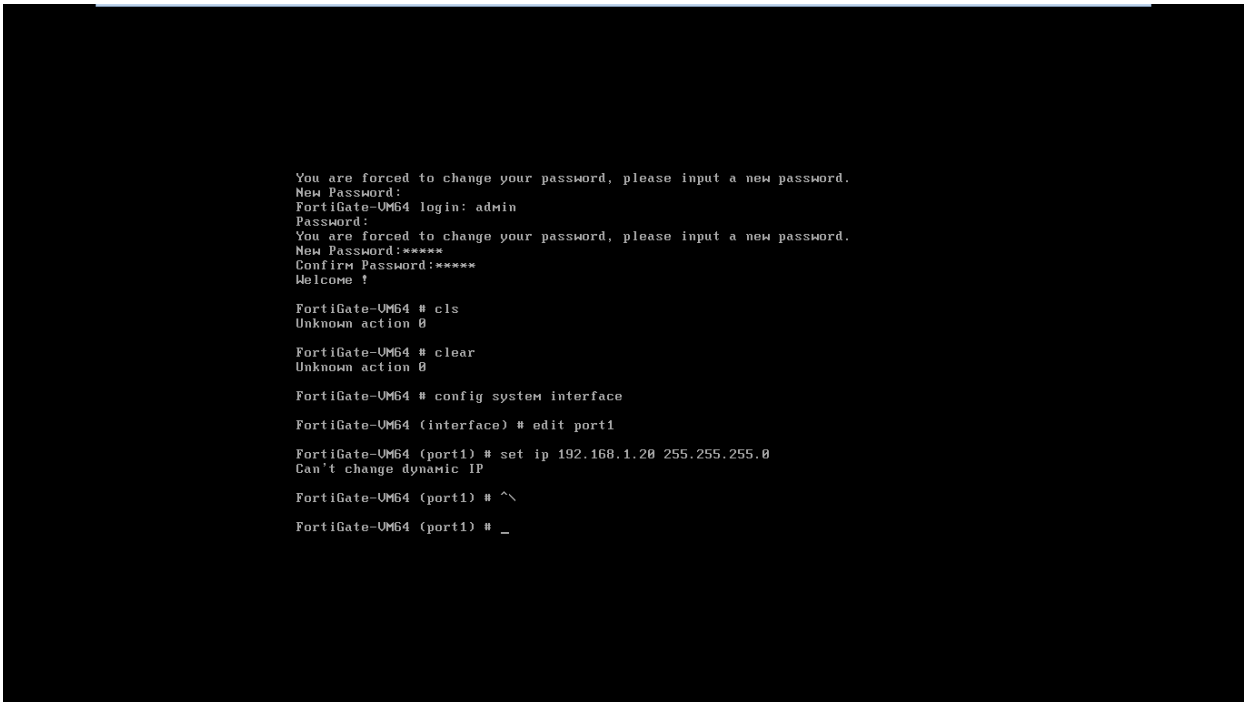
Config system interface

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"



وذلك لأن كرت الشبكة بيوزع ايبيهات 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

Set allowaccess https http ping ssh telnet

حيث قمنا بتحديد ايبي للكرت port1 وحولناه الى كرت ثابت ثم حددنا له الايبي

192.168.2.20 وسمحنا بالوصول اليه عن طريق https و http و ping و ssh و telnet ..

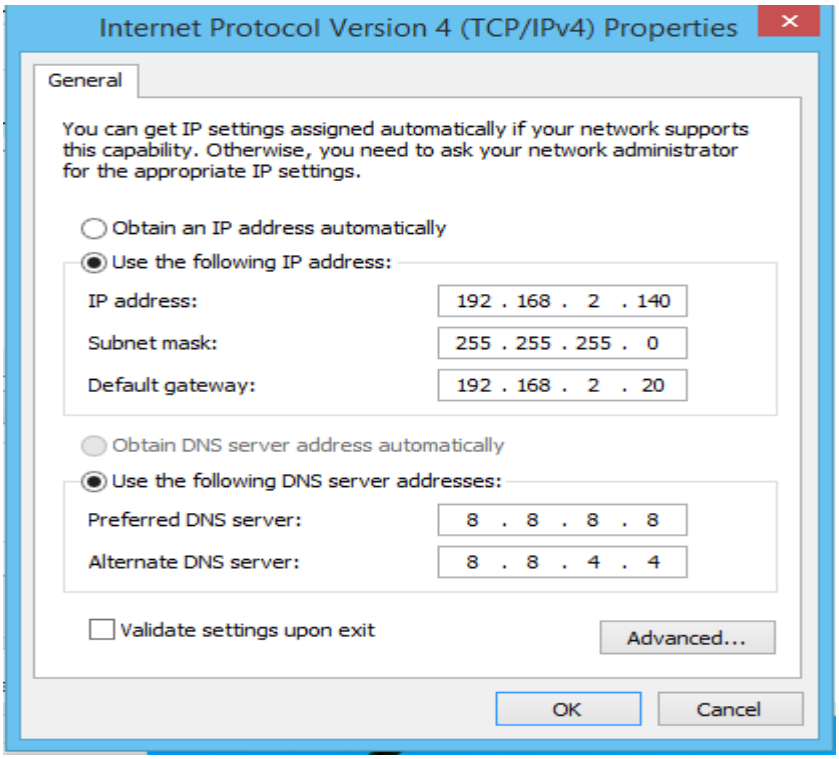
```
        set snmp-index 3
    next
    edit "port4"
        set vdom "root"
        set type physical
        set snmp-index 4
    next
    edit "port5"
FortiGate-VM64 (interface) # end

FortiGate-VM64 # config system interface

FortiGate-VM64 (interface) # edit port1

FortiGate-VM64 (port1) # set mode static

FortiGate-VM64 (port1) # set ip 192.168.2.20 255.255.255.0

FortiGate-VM64 (port1) # set allowaccess https http pin ssh telnet

FortiGate-VM64 (port1) # end
end

FortiGate-VM64 # _
```

عملية البينج غير شغاااااااال من الابتوب نفسه(Host) وذلك لأن كرت الشبكة lan1 على Vnet1(host only) أي غير موصول بسويتش واحد مع كرت الشبكة الخاص بالابتوب ...

حيث كرت الشبكة الوايرلس للابتوب هو 192.168.1.121 وكرت الشبكة lan1 لـ vm fortigate هو 192.192.168.2.20..

لذا سنقوم بتجهيز vm win 8.1 ونجعل كرت الشبكة موصل على السوتش الوهمي

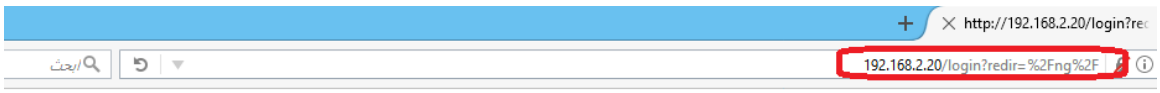
Vnet1(host only) لكي يكون موصل مع كرت الشبكة lan1 لـvm fortigate .

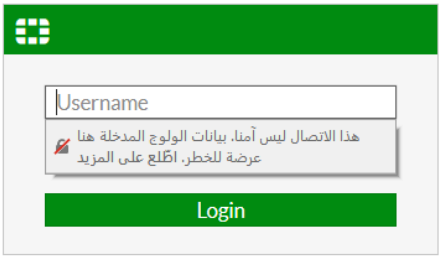


ثم سنفتح الفورتي من خلاص الويب (192.168.2.20)بواسطة متصفح من على جهاز الكلاينت (win 8.1)

ملاحظة: lan1:192.168.2.20

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



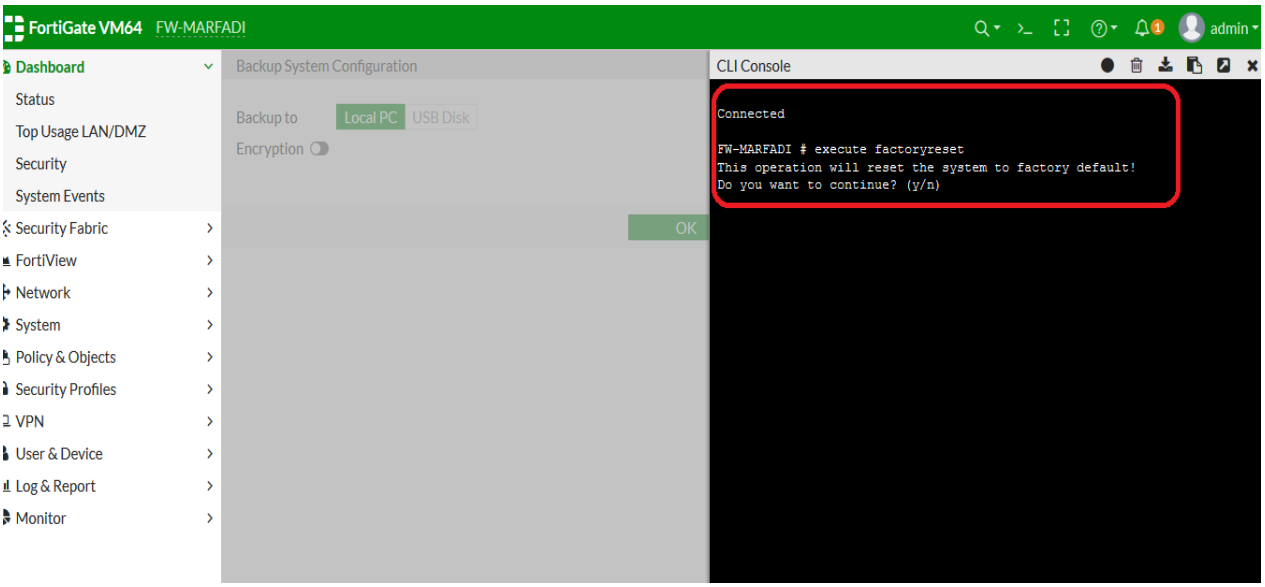


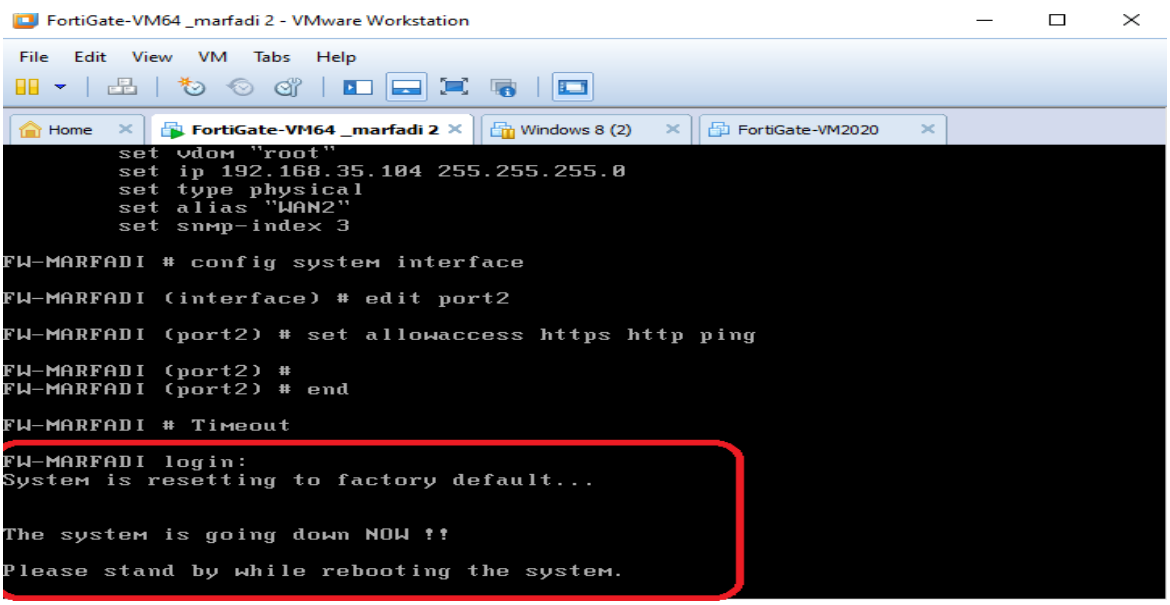
❖ طريقة عمل reset لعدد الأيام (14) للـــVM :

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

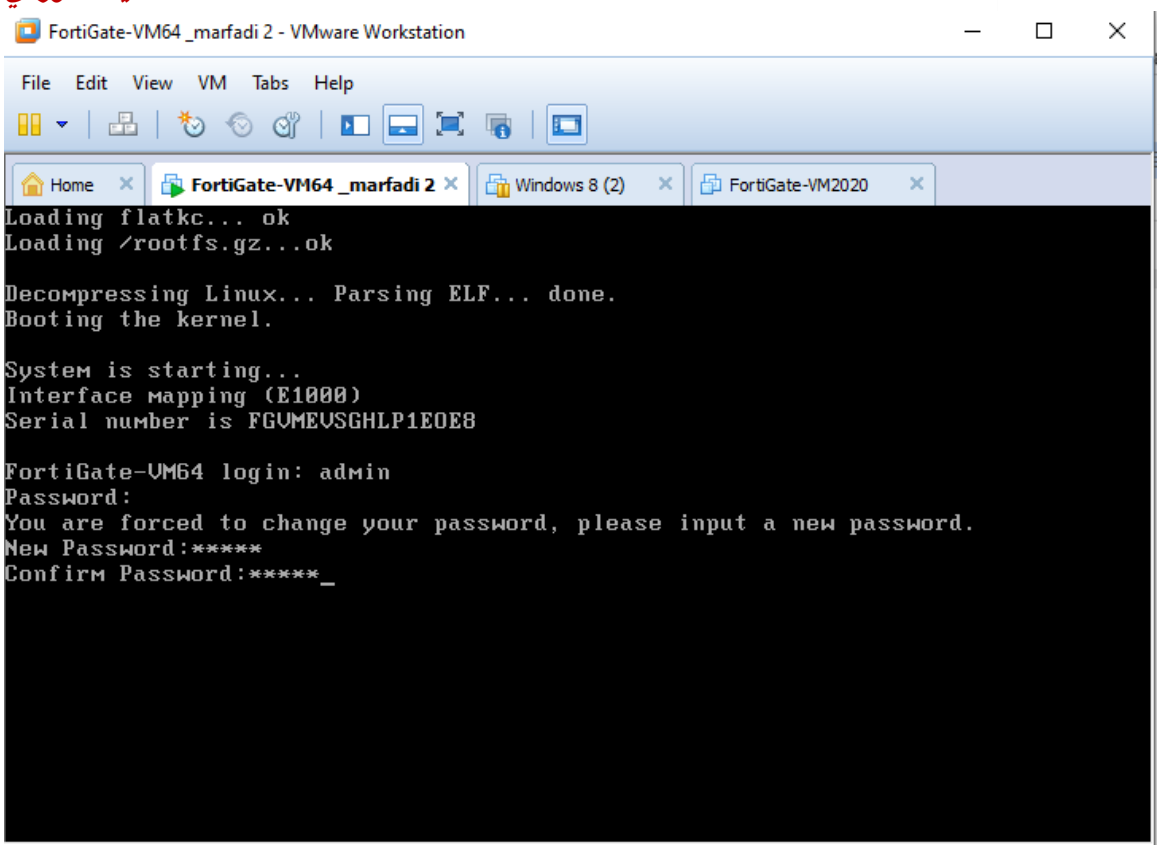
1- اخذ نسخه باك اب من الاعدادات (سيتم شرحة لاحقا)

2-عمل reset للـــvm بكتابه الامر كما بالصورة ادناه





يتم حاليا عمل استعاده اعدادات المصنع (Reset)



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

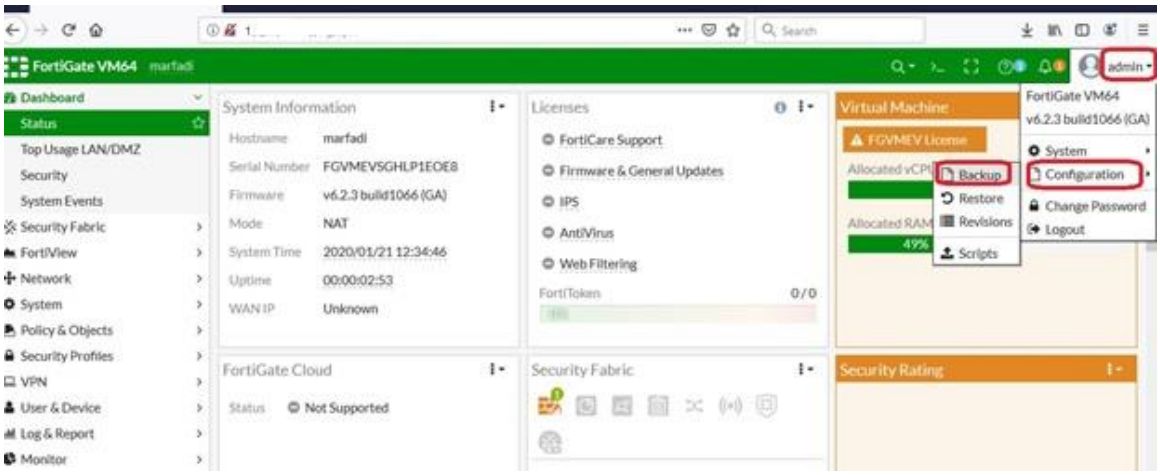
WIN 8.1=192.168.2.140

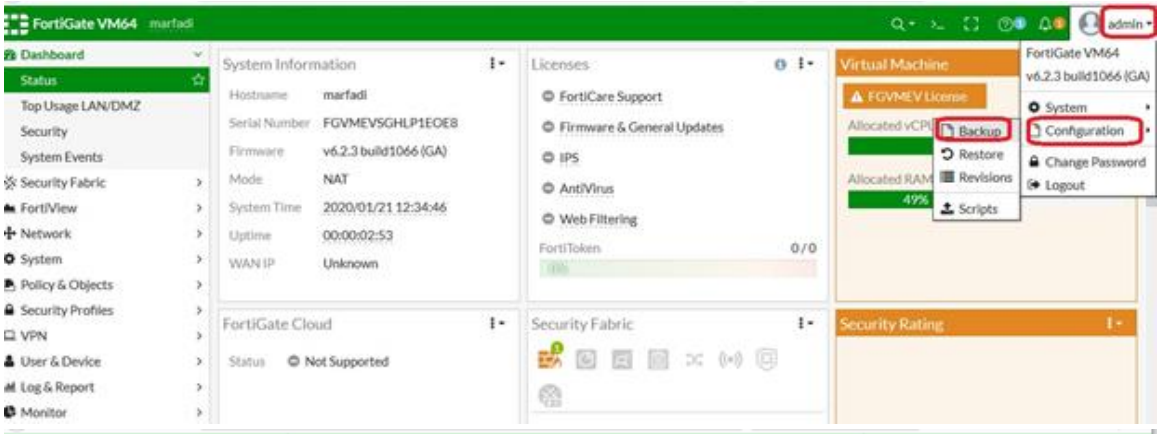
❖ **مشكله ظهور بان الايسنز(License) قد انتهى كما بالصورة ادناه بالرغم اني لم استخدمه الا لساعه فقط ..**

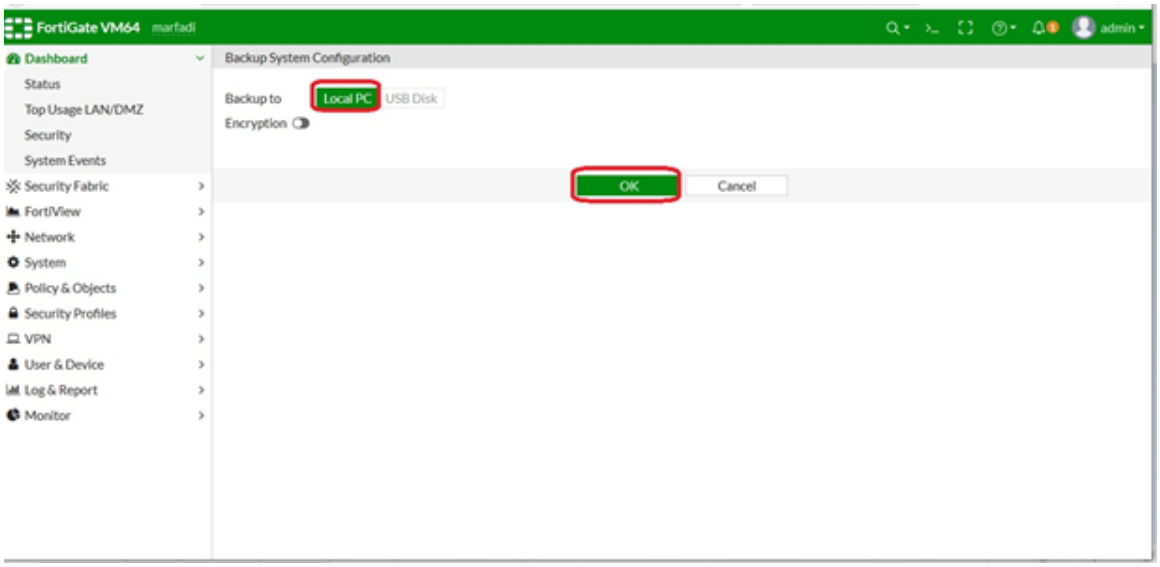
E

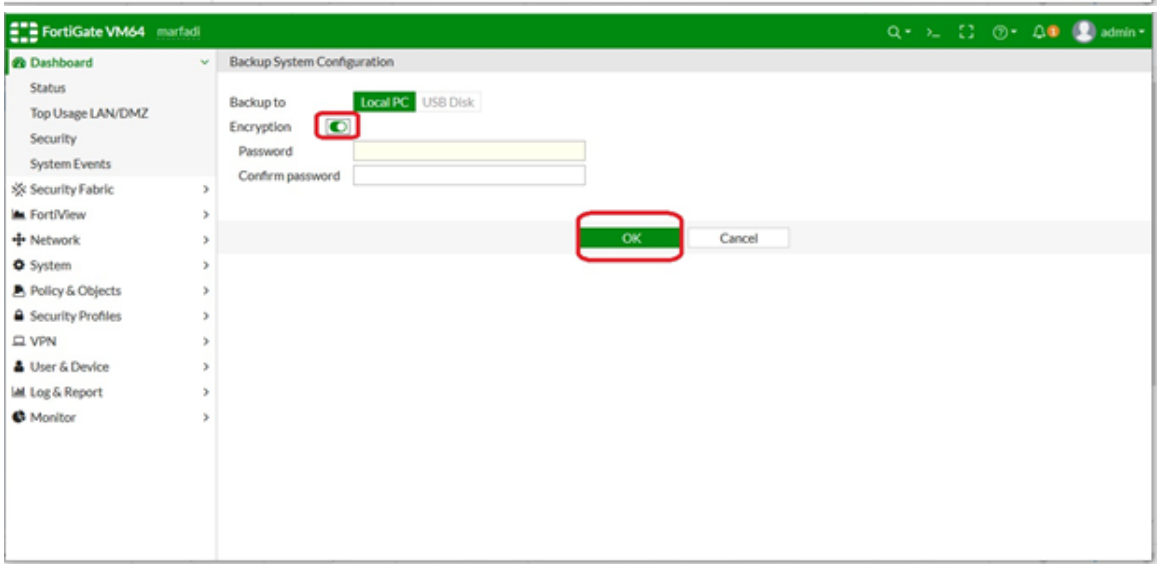
فقمت بتنزيل الـVM واعدادها مره أخرى ....واشتغلت واعطت لي 14 يوم تجريبي..

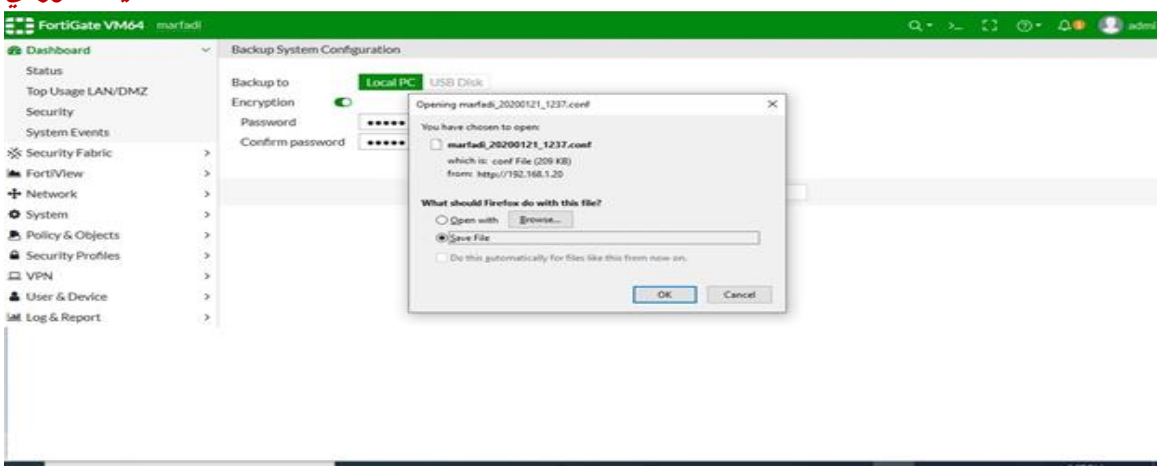
❖ **طريقة عمل باك اب للإعدادات التابعه للـــVM وكيفيه استعادتها :**



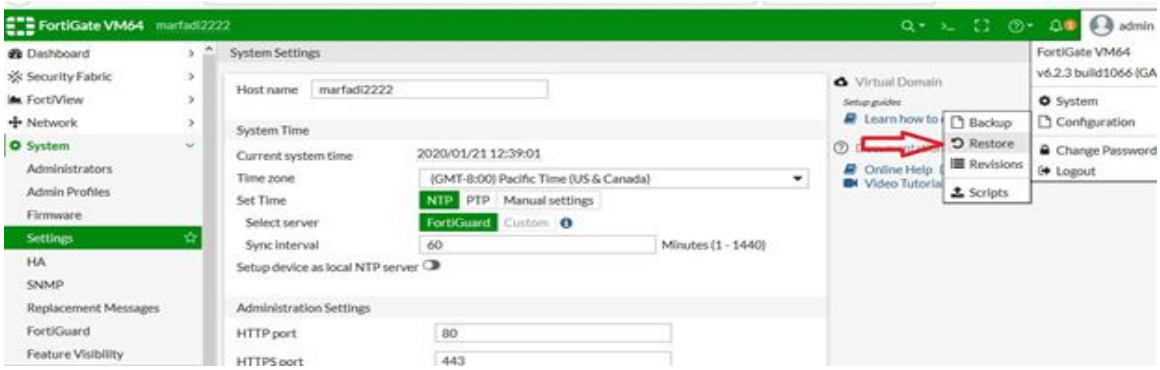

FortiGate VM64 marfadi
admin
Dashboard
Status
Top Usage LAN/DMZ
Security
System Events
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
System Information
Hostname marfadi
Serial Number FGVMEVSGHLP1E0E8
Firmware v6.2.3 build1066 (GA)
Mode NAT
System Time 2020/01/21 12:34:46
Uptime 00:00:02:53
WAN IP Unknown
Licenses
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken 0 / 0
Virtual Machine
FGVMEV License
Allocated vCPU
Allocated RAM
49%
FortiGate VM64
v6.2.3 build1066 (GA)
System
Configuration
Change Password
Logout
Backup
Restore
Revisions
Scripts
FortiGate Cloud
Status Not Supported
Security Fabric
Security Rating

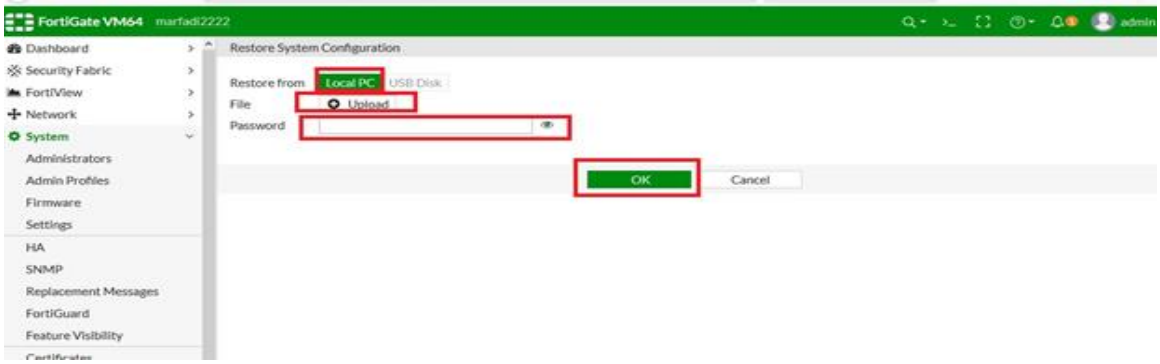

FortiGate VM64 marfadi
admin
Dashboard
Status
Top Usage LAN/DMZ
Security
System Events
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
Backup System Configuration
Backup to
Local PC
USB Disk
Encryption
OK
Cancel

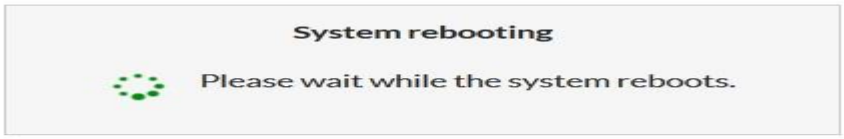

FortiGate VM64 marfadi
admin
Dashboard
Status
Top Usage LAN/DMZ
Security
System Events
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
Backup System Configuration
Backup to
Local PC
USB Disk
Encryption
Password
Confirm password
OK
Cancel


FortiGate VM64 marfadi
Backup System Configuration
Backup to
Local PC
USB Disk
Encryption
Password
Confirm password
Opening marfadi_20200121_1237.conf
You have chosen to open:
marfadi_20200121_1237.conf
which is: conf File (209 KB)
from: http://192.168.1.20
What should Firefox do with this file?
Open with
Browse...
Save File
Do this automatically for files like this from now on.
OK
Cancel
Dashboard
Status
Top Usage LAN/DMZ
Security
System Events
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report

للاستعادة ...


FortiGate VM64 marfadi2222
admin
System Settings
Host name
marfadi2222
System Time
Current system time
2020/01/21 12:39:01
Time zone
(GMT-8:00) Pacific Time (US & Canada)
Set Time
NTP
PTP
Manual settings
Select server
FortiGuard
Custom
Sync interval
60
Minutes (1 - 1440)
Setup device as local NTP server
Administration Settings
HTTP port
80
HTTPS port
443
Virtual Domain
Learn how to
Online Help
Video Tutorials
Backup
Restore
Revisions
Scripts
System
Configuration
Change Password
Logout
FortiGate VM64
v6.2.3 build1066 (GA
Dashboard
Security Fabric
FortiView
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility

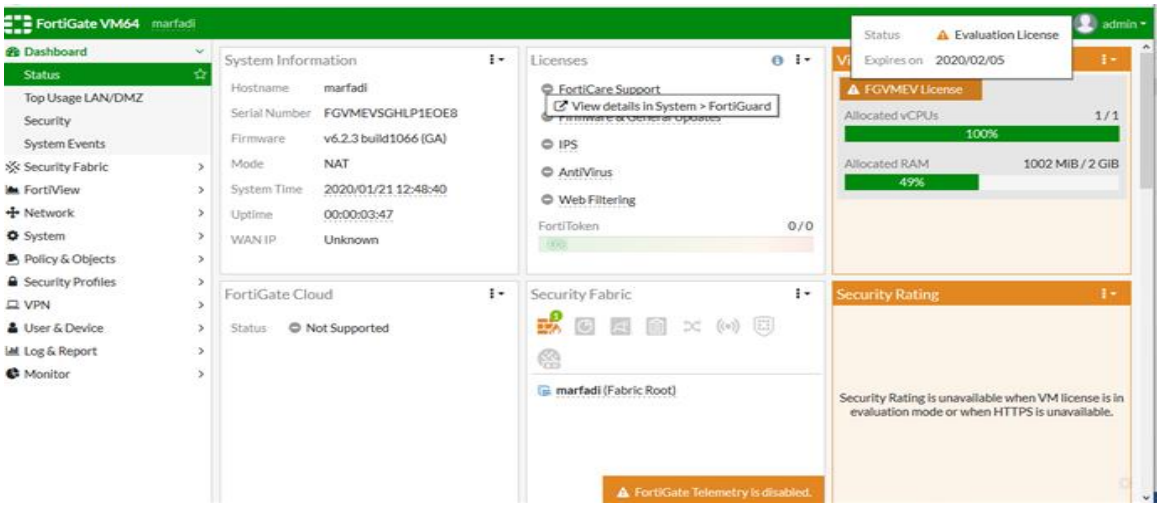

FortiGate VM64 marfadi2222
admin
Restore System Configuration
Restore from
Local PC
USB Disk
File
Upload
Password
OK
Cancel
Dashboard
Security Fabric
FortiView
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility


System rebooting
Please wait while the system reboots.

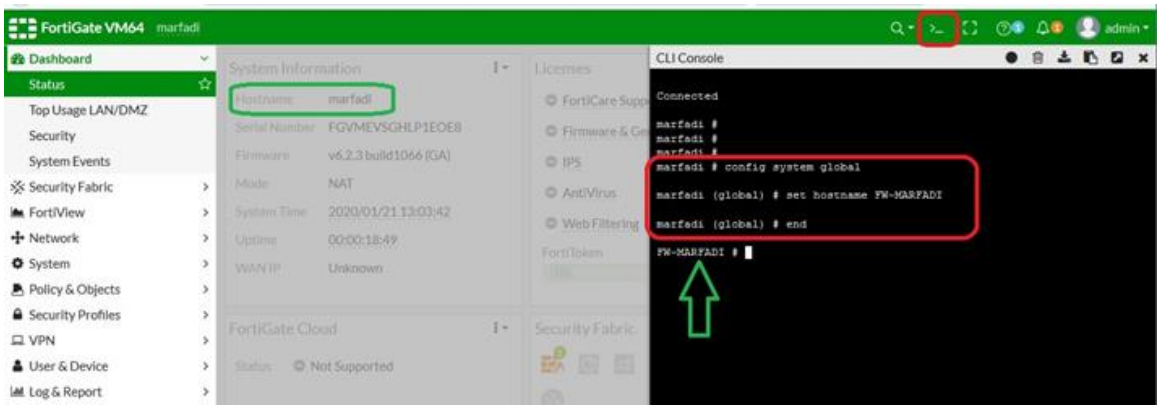
❖ شرح مكونات وواجهات الفورتي جيت :

ال Dashboard توضح لنا معلومات حول النظام مثل اسم الجهاز والسيريال وإصدار

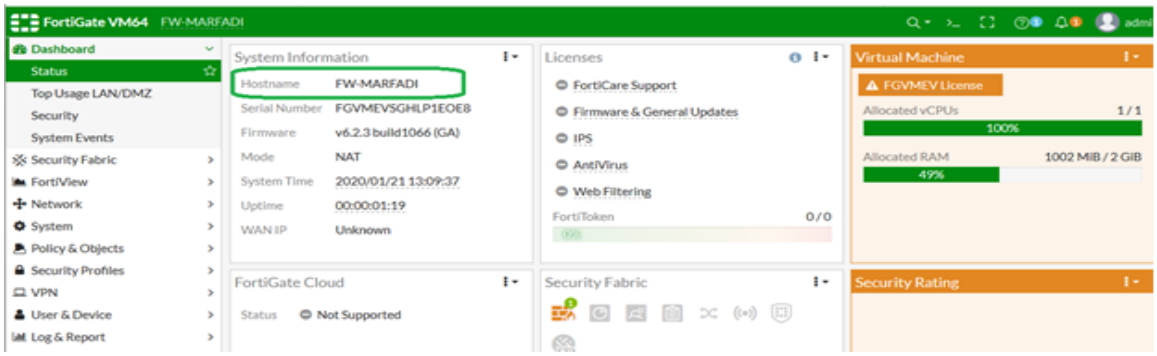
الفريم ويروالتاريخ والوقت للجهازالفايروول ومتى تاريخ انتهاء الايسزنزلكل خدمه.



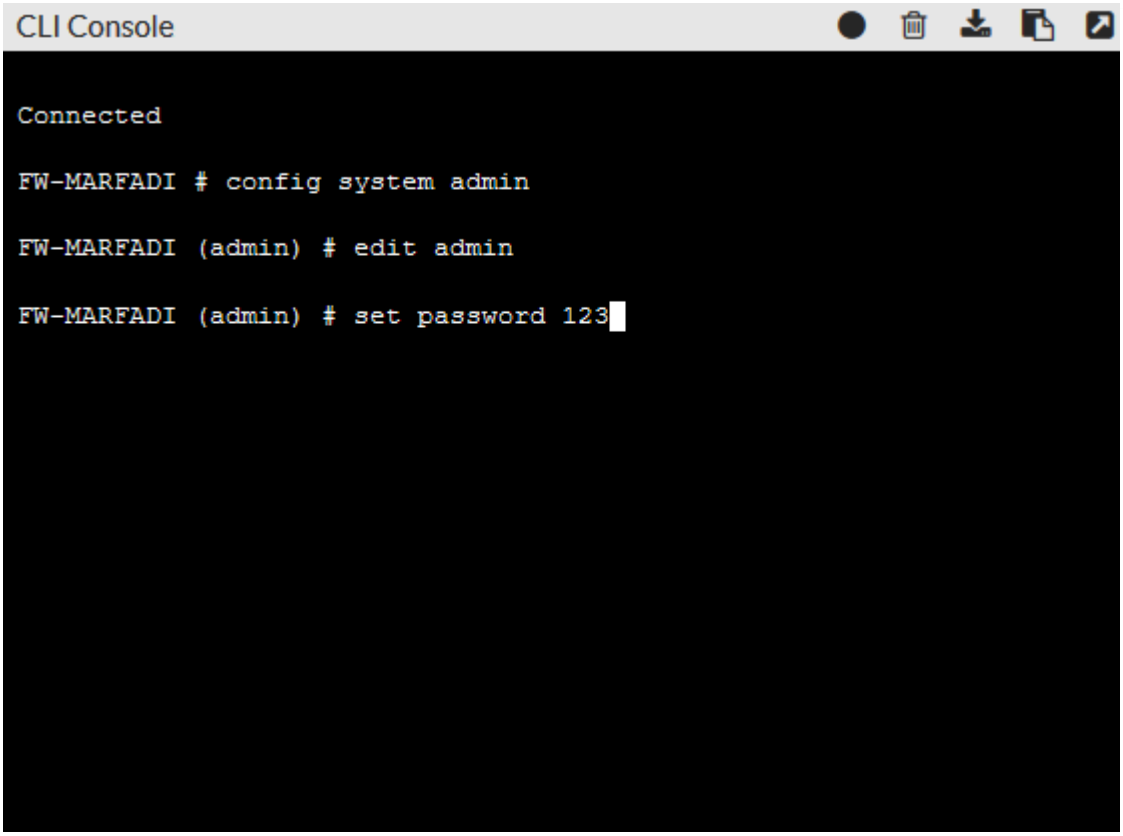
طريقة تغيير اسم الجهازبواسطة الأوامر:



بعد تعديل اسم الجهازواعاده التشغيل



❖ طريقة تغيير باسورد الأدمن (admin) بواسطة CLI

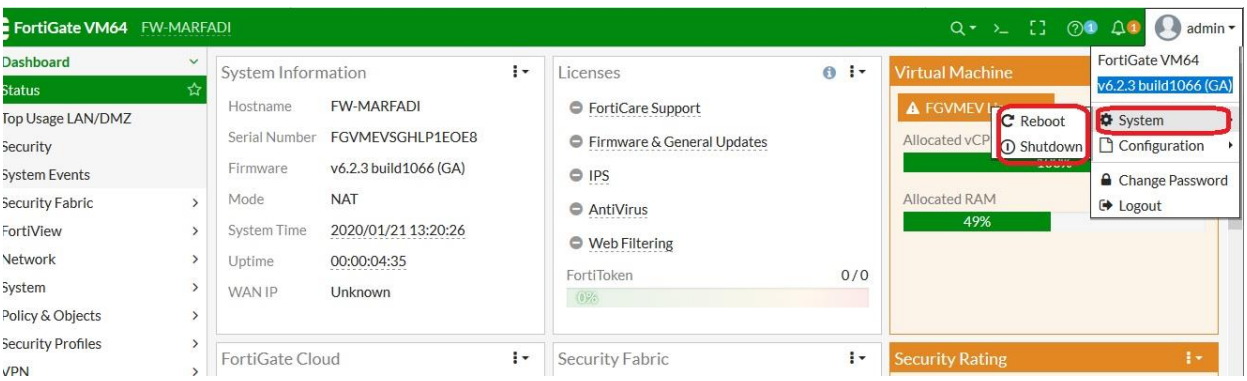


حيث يجب ان تقوم بكتابه الامر **end** بعد الأوامر أعلاه لكي يتمكن من حفظ التغيرات..

حيث اصبح الباسورد لليوزر **admin** هو **123** .

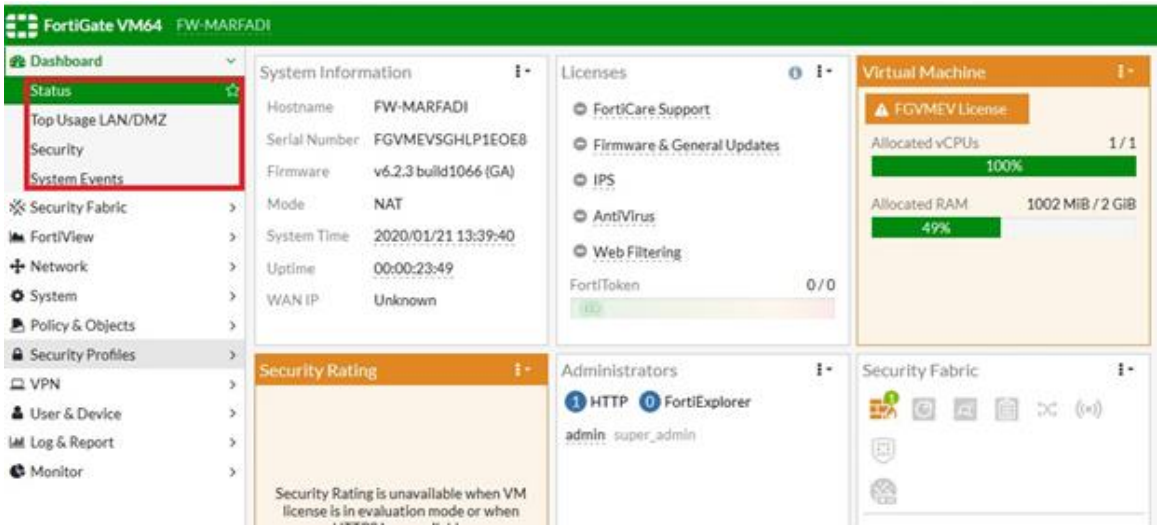
****

إيقاف او اعاده التشغيل او تغيير الباسورد او للخروج من الفورتي ويب ، عبر GUI كما بالصورة ادناه ..

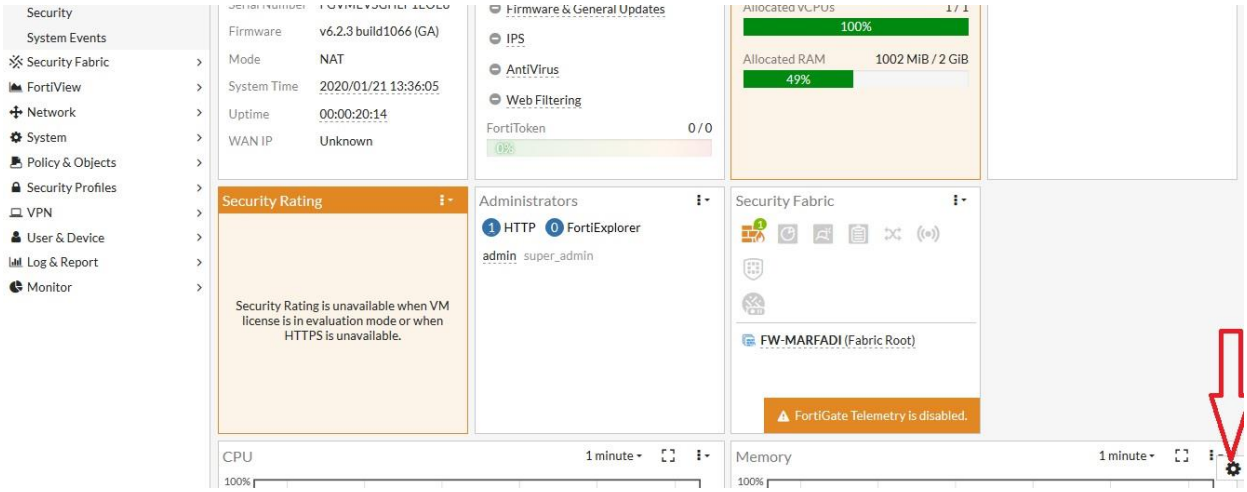


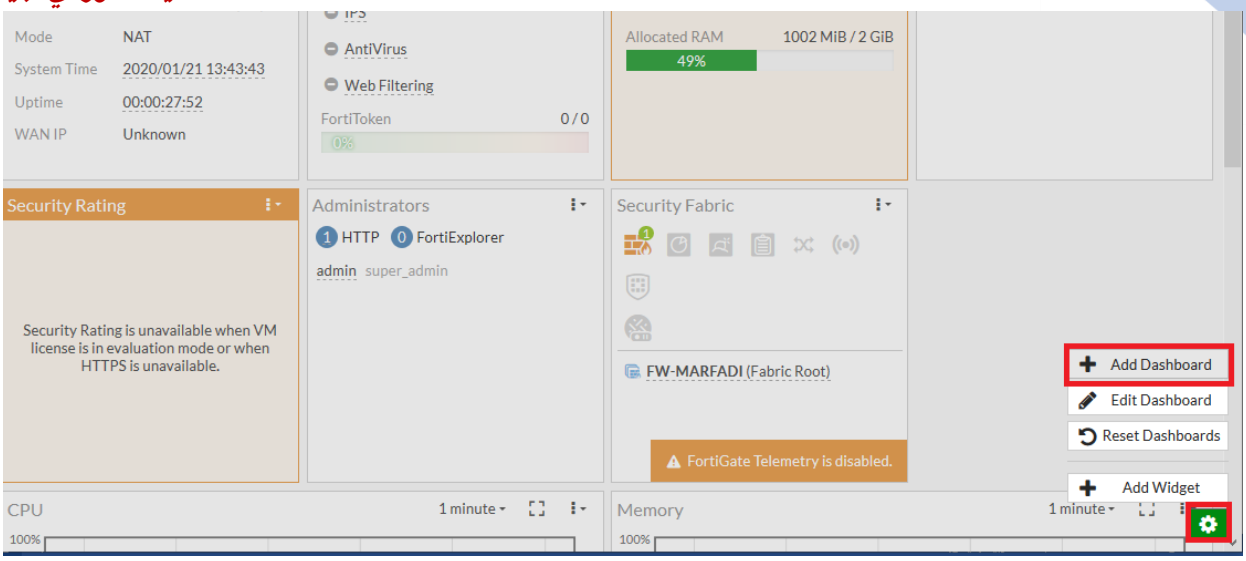
شرح ال DASHBOARD :

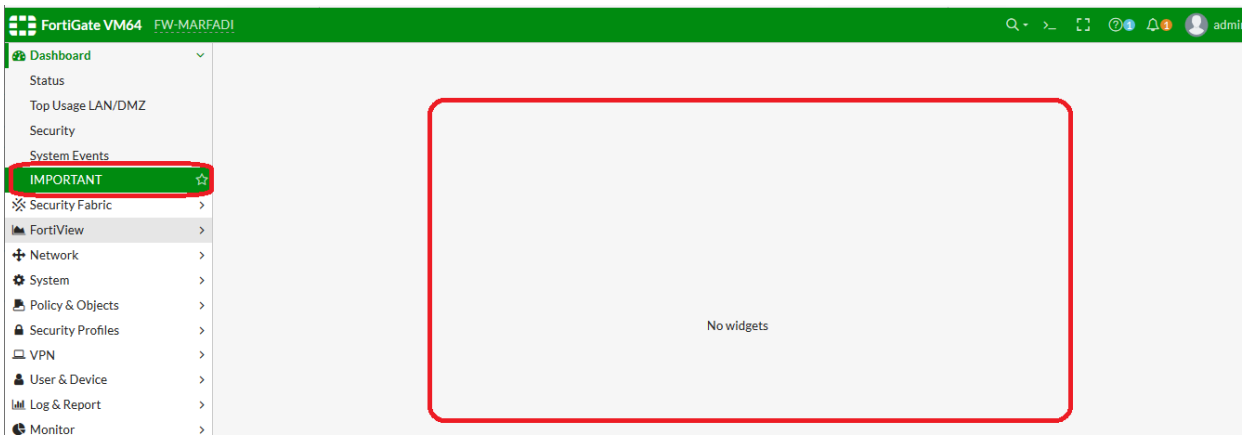
هي القوائم الموجودة على يسار الشاشة والمشار اليها بالمربع الأحمر حيث ممكن أضافه أي قائمة وتسميها حسب ما تريد وتضيف اليها نوافذ(Widget)..



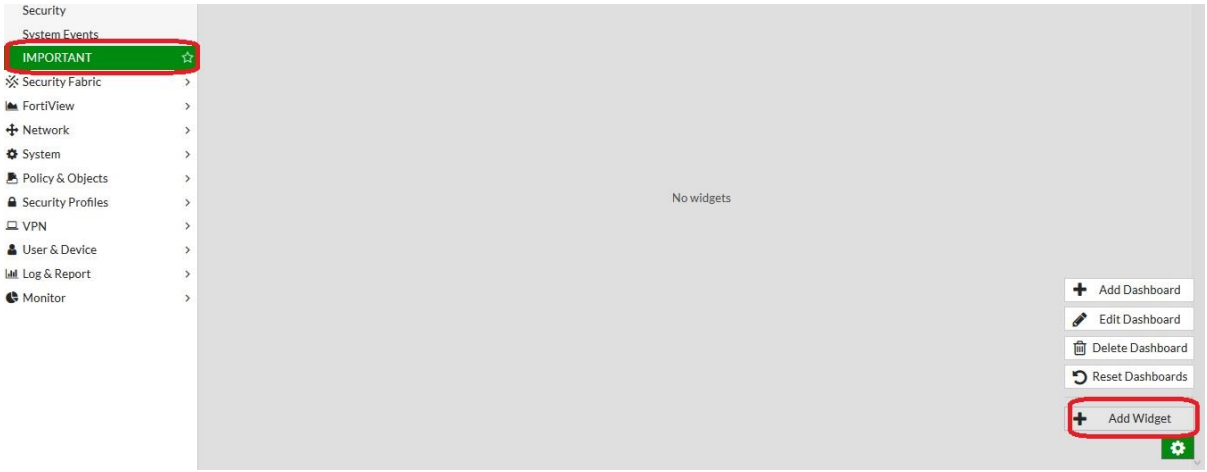
مثلا سوف نقوم بأضافه Dashboard باسم IMPORTANT وسوف نظيف اليها نوافذ محدده



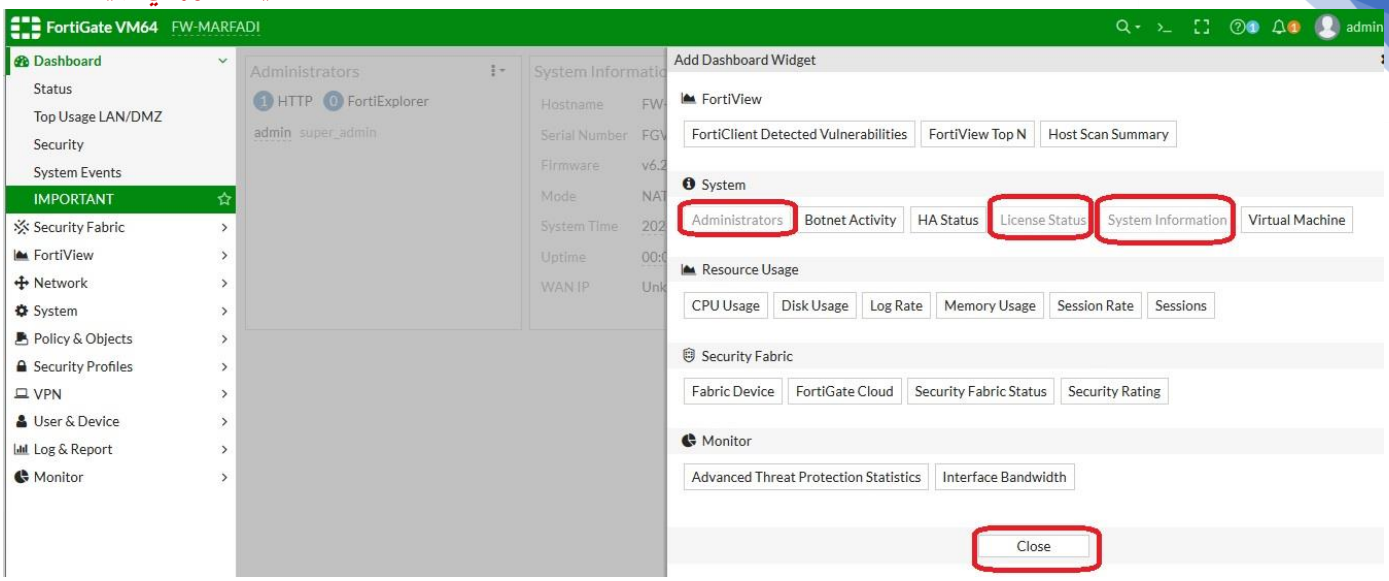


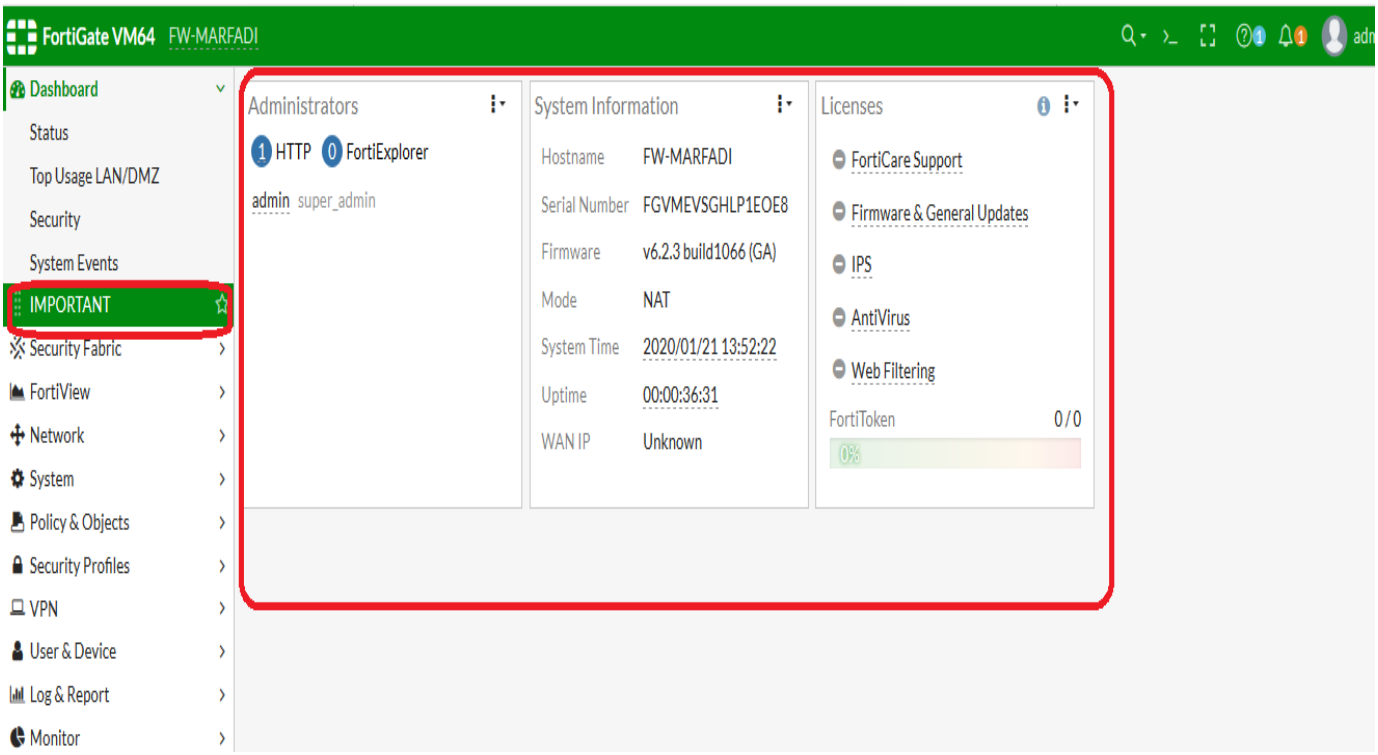


الآن سوف نقوم بإضافة نافذه جديده للDASHBOARD المسماة IMPORTANT

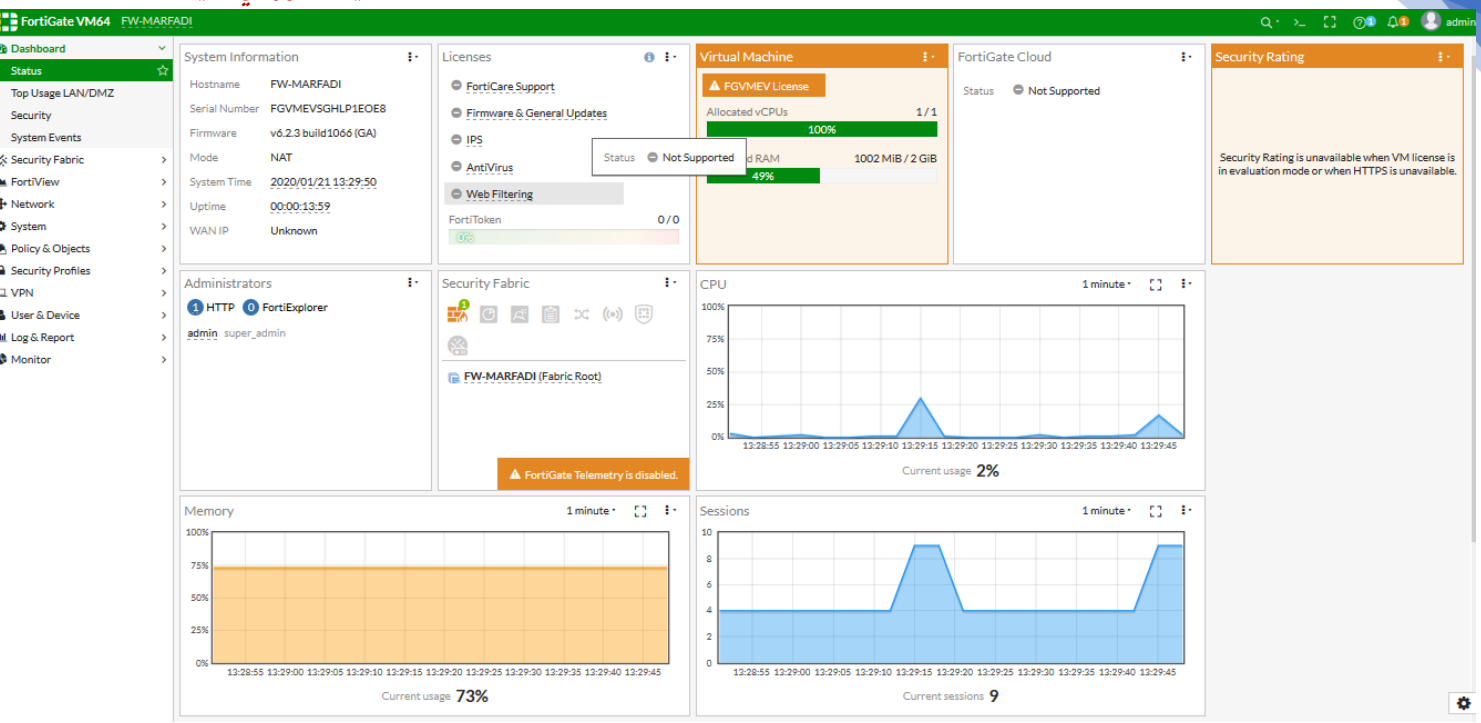


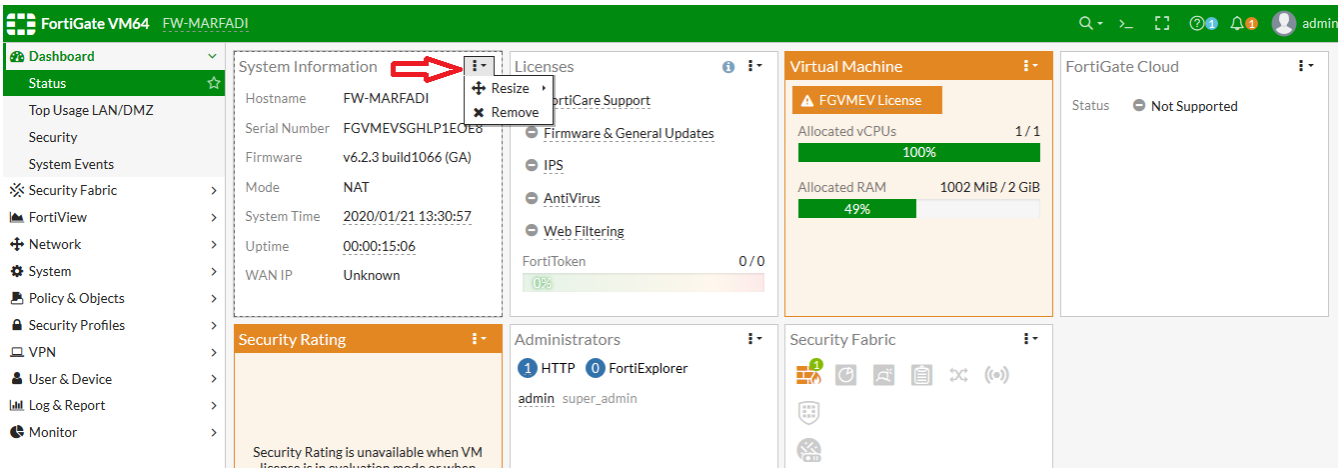
حيث سنضيف نوافذ كما بالصورة ادناه

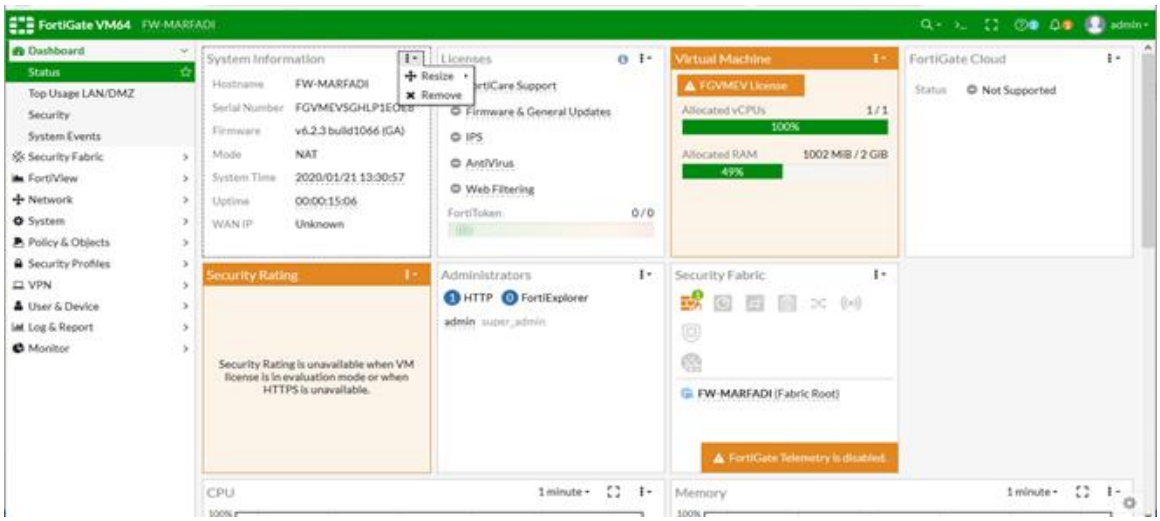




وللتحكم من حيث حذف او تصغير او تكبير حجم النافذه على الـ DASHBOAARD نتبع الخطوات كما بالصور ادناه ...



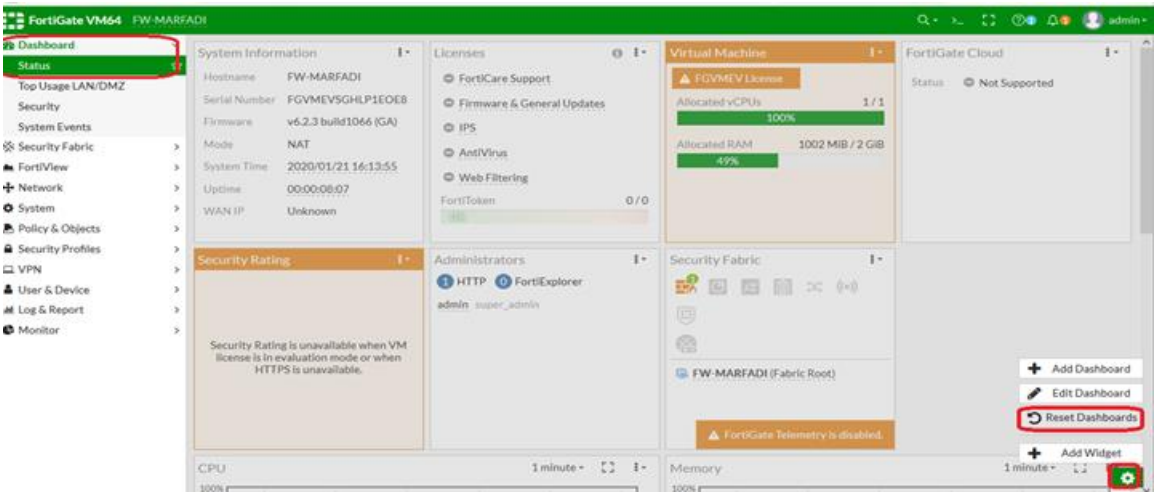




حيث يمكنك تعديل حجم او حذف أي نافذة (Widget)من الDashboard .

ملاحظات :

- ممكن نقل النوافذ(Widget) من مكان الى اخر بواسطة السحب والافلات .
- لا يمكن حذف الـMain Dashboard .
- في حالة قمت بتعديلات على ال Dashboard وتريد استعادتها كما كانت افتراضيا فأننا ننقر على الرمز العجله 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 مختلفة عن الأخرى مثل

System information ,license ,forti cloud,adinistrators,security fabric,current usage ,

ويمكن أضافه dashboard او widget كما تم شرحه سابقا ...

شرح استخدامات ومعلومات الـWidget :

A- System information :

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

B- License :

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

C- Forticloud :

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

D- Administrators Widget :

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

٢- Security fabric :

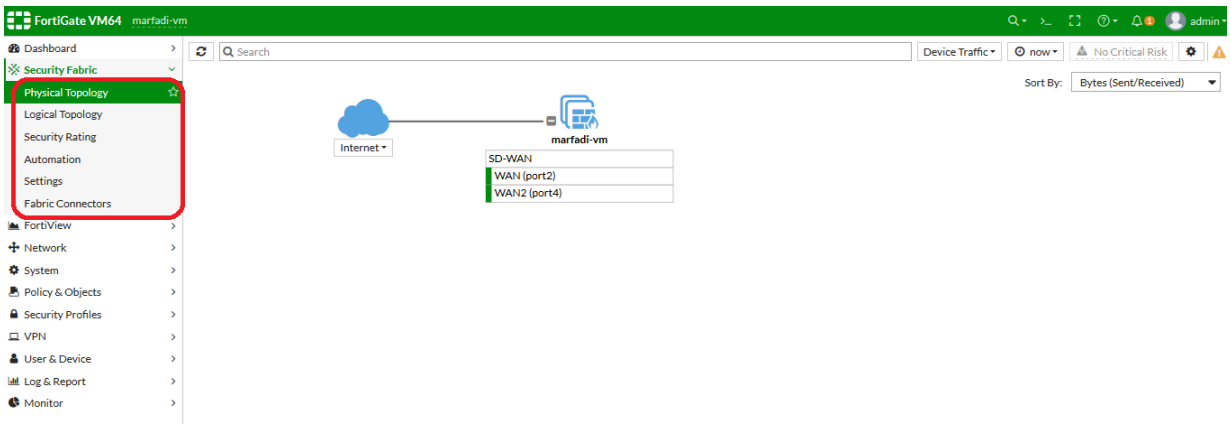
هي عباره عن خاصية عرض فقط (View) لكل الاجهزه التابعه لشركه فورتي من معلومات حول الشبكة وعرض تفاصيل عن الشبكة ومتابعة الlogs والترافيك ...الخ

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

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

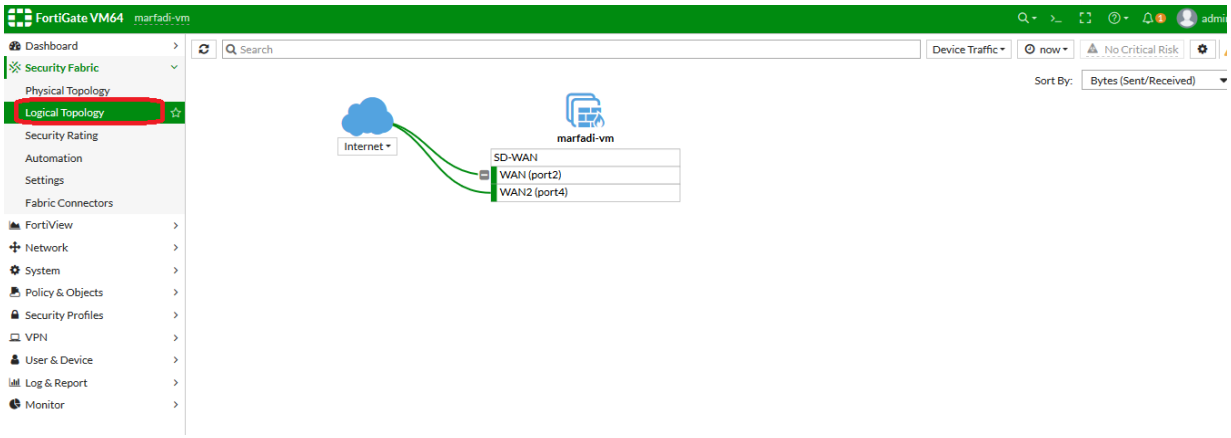
توجد طريقتين للعرض :

١- Physical topology

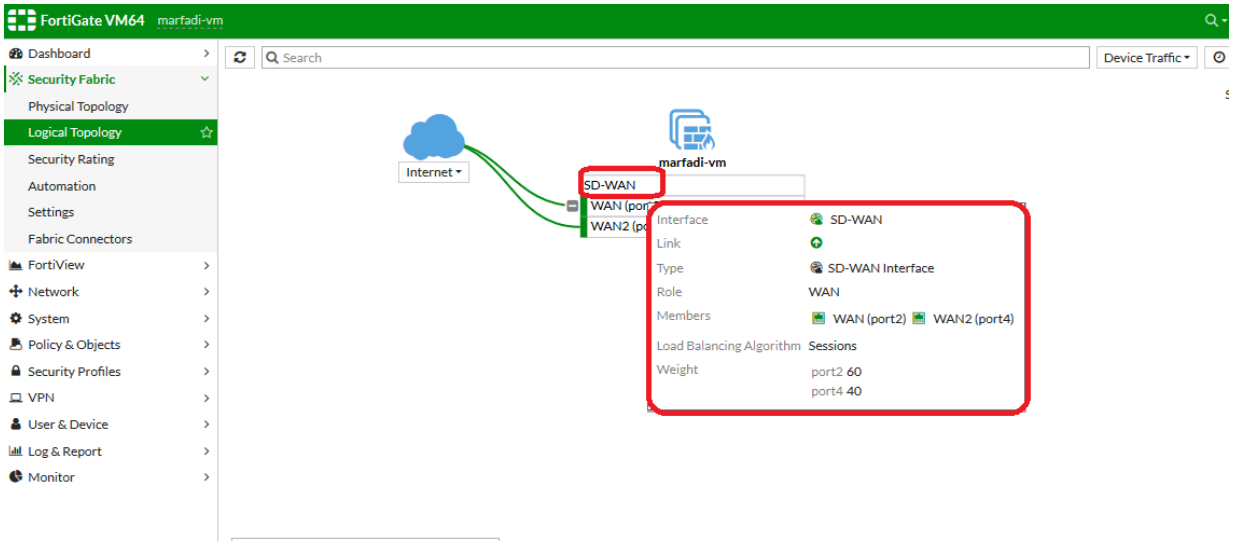


يمكنك بواسطته ان تظهر Topology للفورتي جيت كما بالصورة أعلاه ...

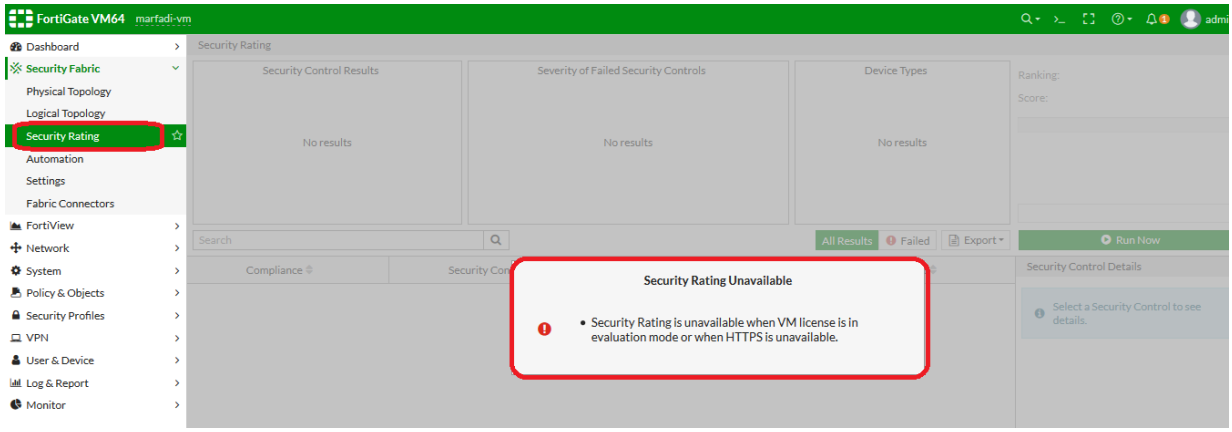
Logical topology -٢



حيث بمجرد تمرير مؤشر الماوس على العناصر بيوضح لك مثلا الايبهات والـinterface ...الخ



Security Rating -3 :



غير متاح في VM ولكن فعليا يتم استخدامه كآليه فحص للأجهزة التابعه لفورتي نت مثلا FortiAnalyzer و غيرها ...

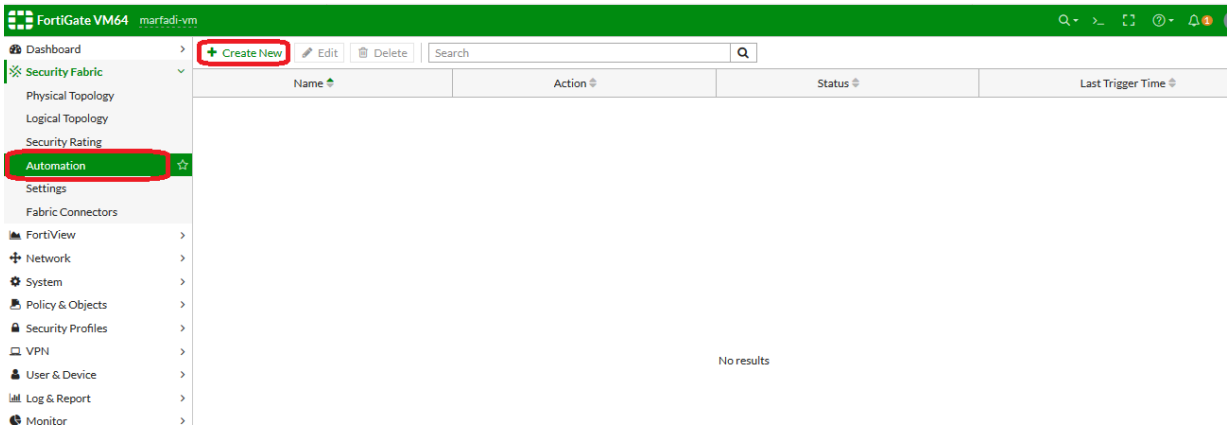
Automation -4 :

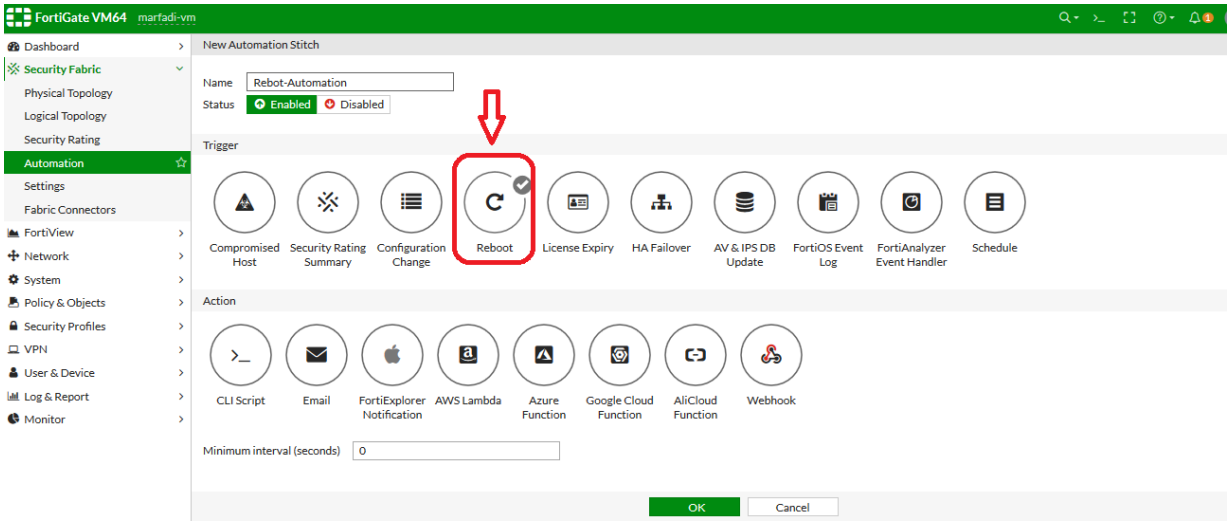
فكره الـAutomation قائمه على Trigger(حدث)فأما يحدث(true) واما لا يحدث

(False) فلوا كان true قم بعمل action معين .

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

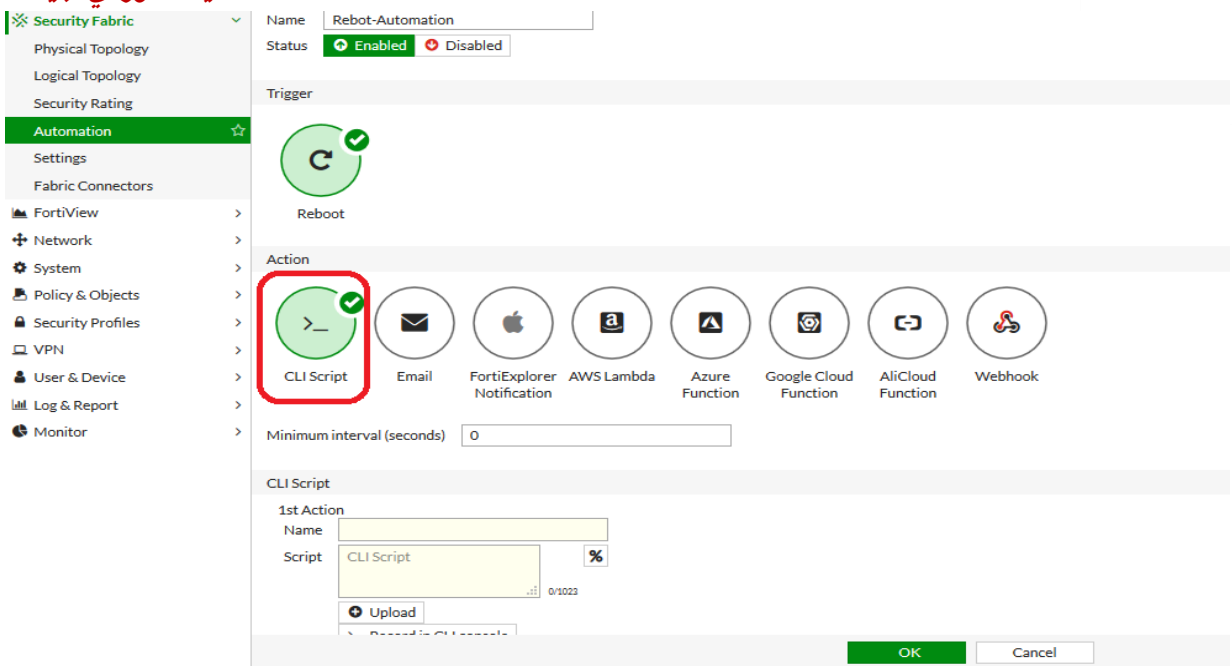
مثال لو قمت بعمل اعاده تشغيل لجهاز الفورتي جيت فقم بإرسال أوامر عبر cli

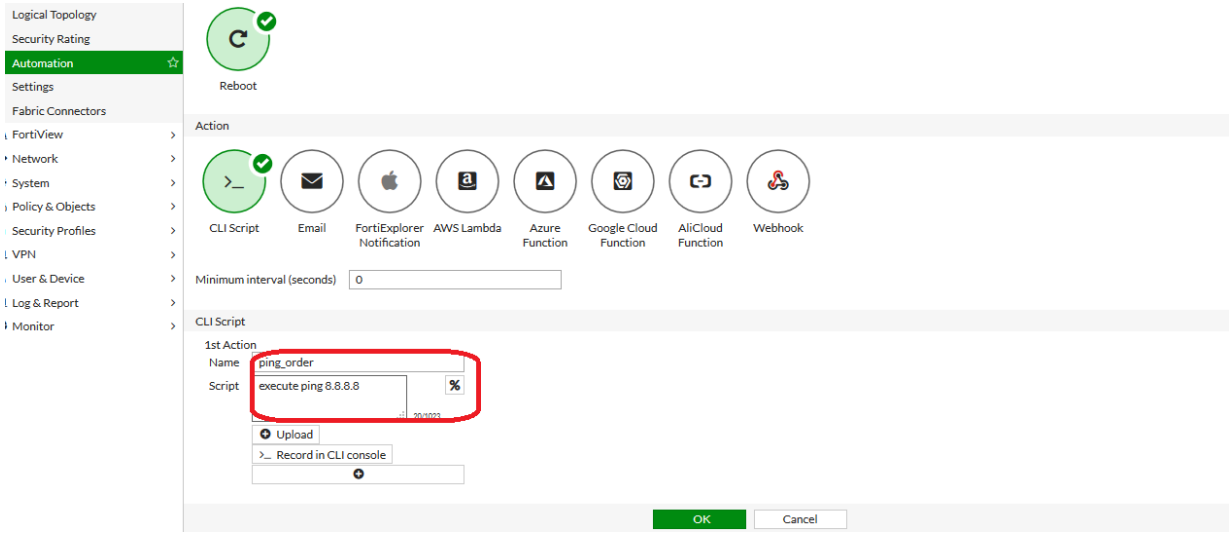




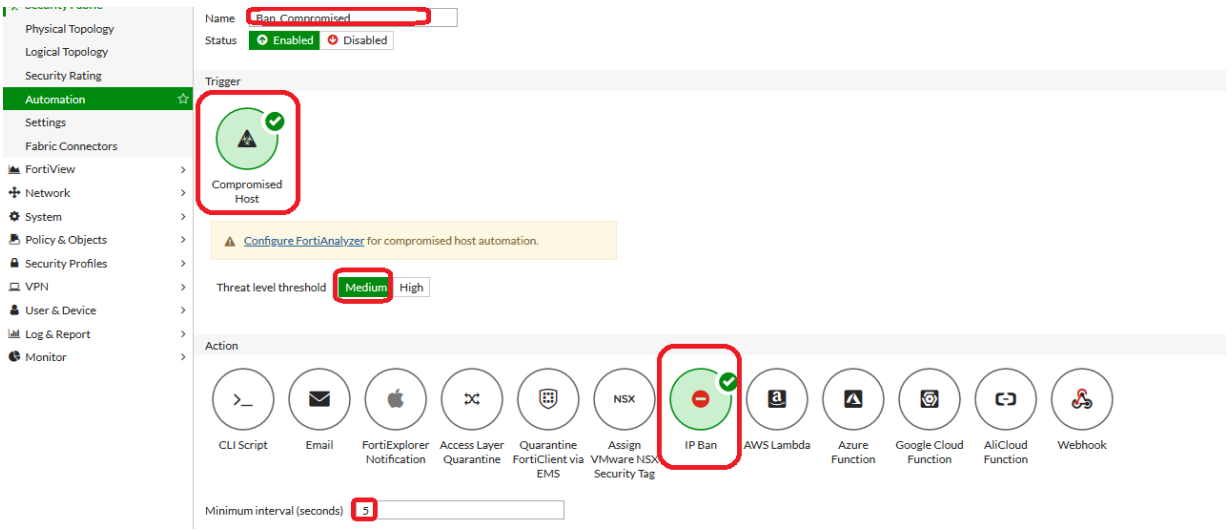
كما بالصورة أعلاه قمنا بالنقر على الحدث Reboot

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





مثلا اريد اعمل Ban او حضر لجهاز بمجرد حصل له Hacked



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

٣- FortiView :

هو نظام مراقبة للشبكة الخاصة بك مثل الLOGS و عمل 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 وحقيقيه عن تفاصيل مثل من اخد dhcp او اي حالة ال VPN وهكذا تختلف عن ال fortiview اللي يعرض لك احداث مسجله مش شرط تكونreal time .

٤- Networks :

يقوم بعرض معلومات عن كروت الشبكة و تندرج تحت هذه القائمة :

١- Interfaces:

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

٢- DNS :

يوضح الDNS المستخدم هل هو التابع لفورتي 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 حفضها 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 ايبيهات

Port(s):443 مراقبه الترافيك التابعhttps

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 الـ 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 ايبي الروتر..

٥- System :

١- Administrator : يظهرلك يوزرباسم admin وهو الافتراضي حيث له الحق بالوصول الى الفورتي 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 الفورتي جيت حيث بشكل افتراضي super_admin و prof_admin ويمكنك ان تقوم بتخصيص بروفايل وتحدد نوع صلاحيه الوصول بحسب ما تريد.

٣- Firmware : يعرض لك الإصدار الحالي لـOS الخاص بجهاز الفورتي وممكن تعمل Upload للـFirmware وأيضا يعرض لك الإصدارات المتاحة ويمكن عمل ترقيه (upgrade)او انزال (downgrade) من هنا.

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

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

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

٥- HA : في حالة وجود جهاز فورتي جيت وحيد بالشركة فأن النمط هو Mode=standalone اما في حالة وجود اكثر من جهاز فورتي 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 الفورتي فأن الاخر يعمل بشكل تلقائي بدون توقف للشبكة .

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

٧- Replacement Messages : هي عباره عن الرسائل التي تظهر لك كأدمن للفورتي او كيوزر في حالات مختلفة مثل فتح مواقع محجوبه او خطأ في الولوج الى الفورتي جيت ...الخ

ويمكنك تعديل الرسائل كما تريد ..

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

٩- Certificate : لو قمت 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 البوليسي على منفذ الـWAN لأن الهجوم لا يأتي الا عبر

Incoming interface :wan

٣- Address :لإنشاء عناوين للأجهزة .

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

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

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

٧- Security profiles :تستخدم لحمايه الشبكة من الهجمات .

١- Antivirus :عمل سكان للترافيك الداخل 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 لحمايه 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 الـWeb filter فان الفورتي جيت يواجه مشكله وهي ان لو اليوزر فتح موقع الفيسبوك بجلسه مشفره أي عبر https فأن الفورتي 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 نواعا 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 الأجهزه 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 بالفورتي الذي تم انشاءه مسبقا من قائمه User definition للوصول الى الانترنت .

٩- **WiFI &switch controller**: في حالة وجود fortiAP بالشبكة وتريد عمل له اداره وتحكم كامل بواسطة الفورتي ...حيث fotiAP هو عباره عن اكسس بوينت ولكن خاص بشركه فورتي نت .

١٠- **Log & Reports :**

١١- **Monitor :**

❖ طريقة توصيل الانترنت لجهاز الفورتي جيت :

يجب ان يكون جهاز الفورتي 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

و ايضا لأنه سيكون هو الجيتواي(Gateway) للأجهزة الموجودة بالشبكة

و ايضا لو اردت عمل update لـ firmware الخاص بك .

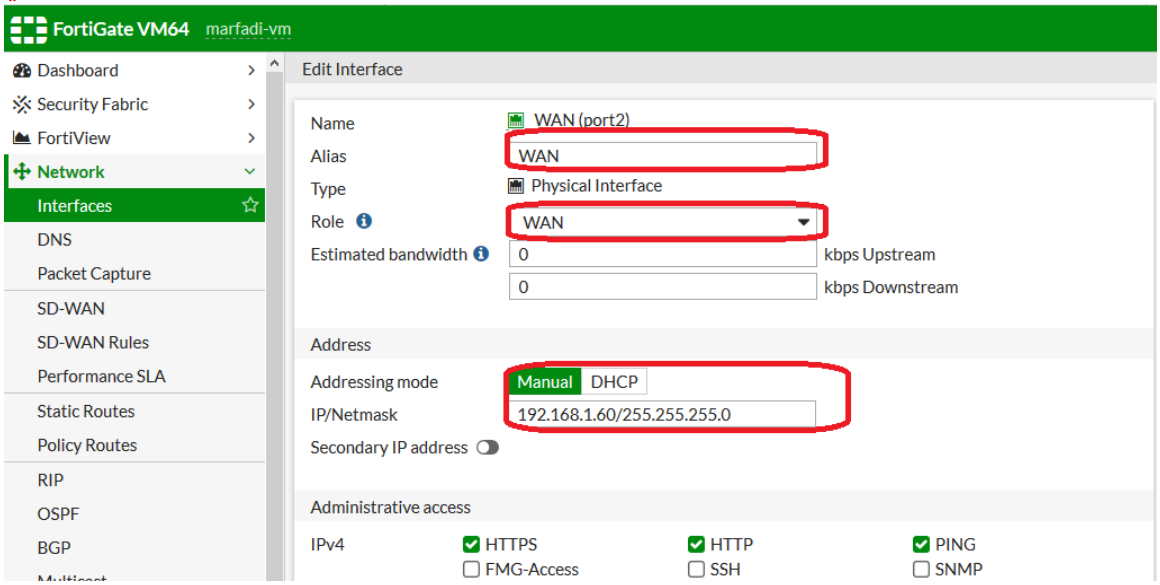
وللقيام بذلك يجب ان تقوم بالخطوات التالية :

١- اظافه ايبي لـWAN 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

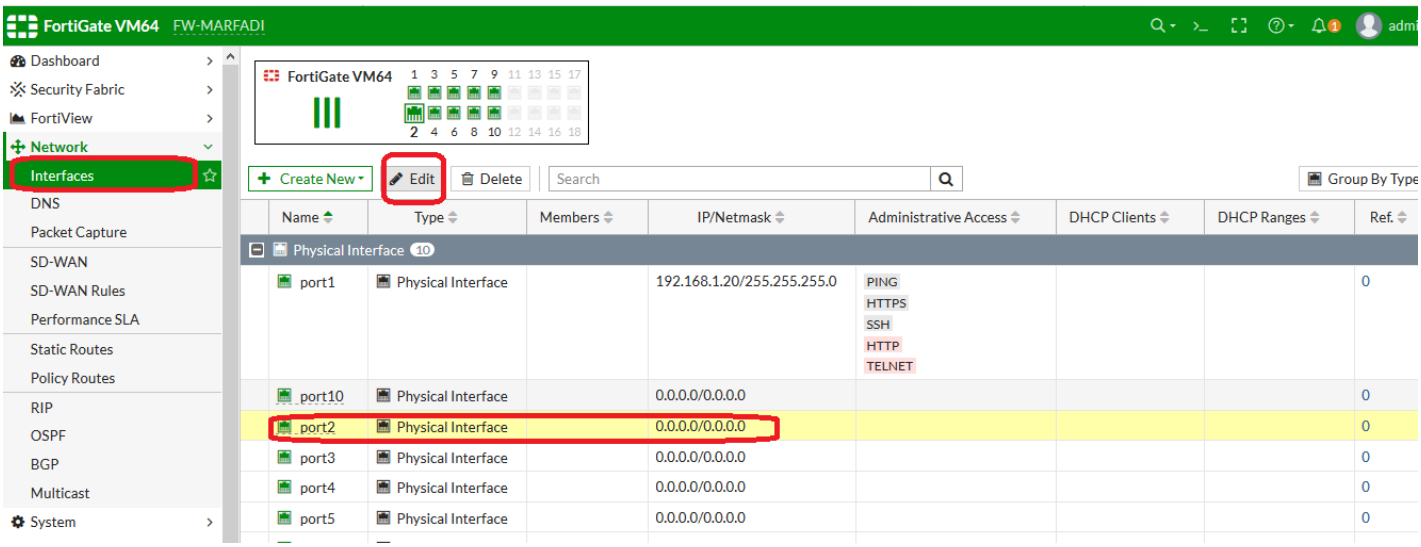
ولو اخترت DHCP فأنه سوف يأخذ بشكل اوتو من الروتر..

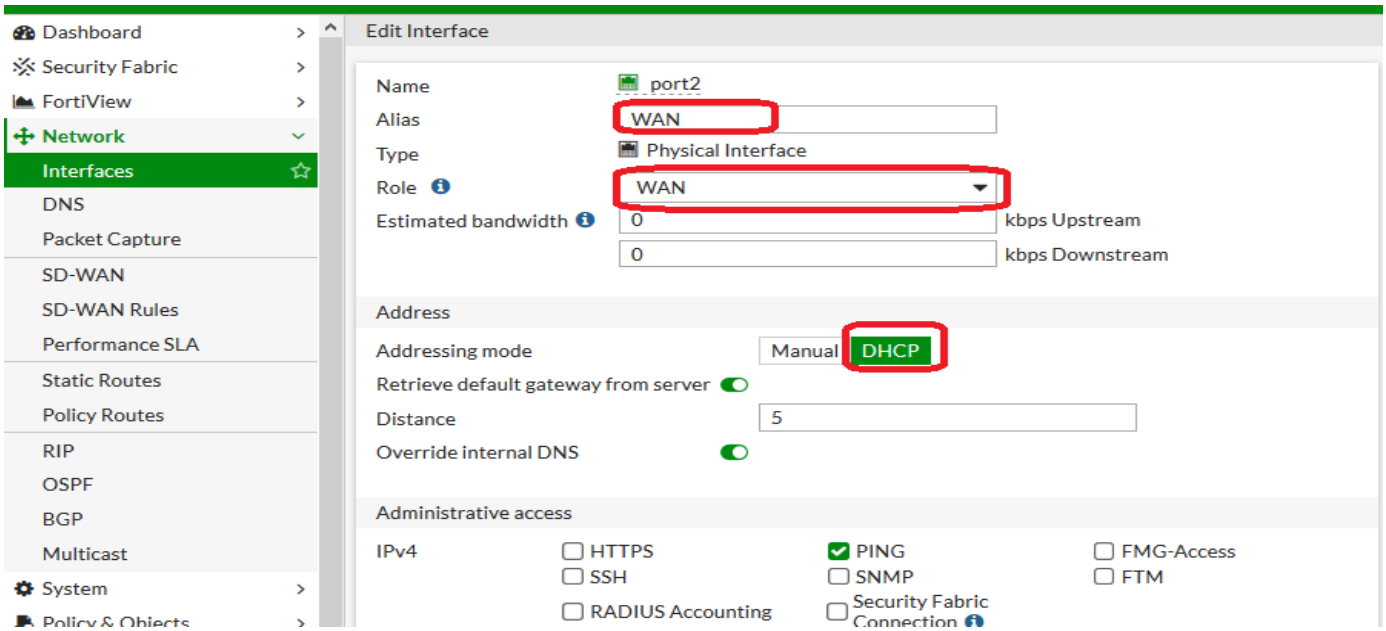
حيث من الممكن تحديد طريقة الوصول الى المنفذ الWAN بأكثر من طريقة مثل HTTPS و HTTP ووالخ

ولكن كنوع من السيكيورتي يتم فقط السماح بالوصول الى البورت عبر الPING .

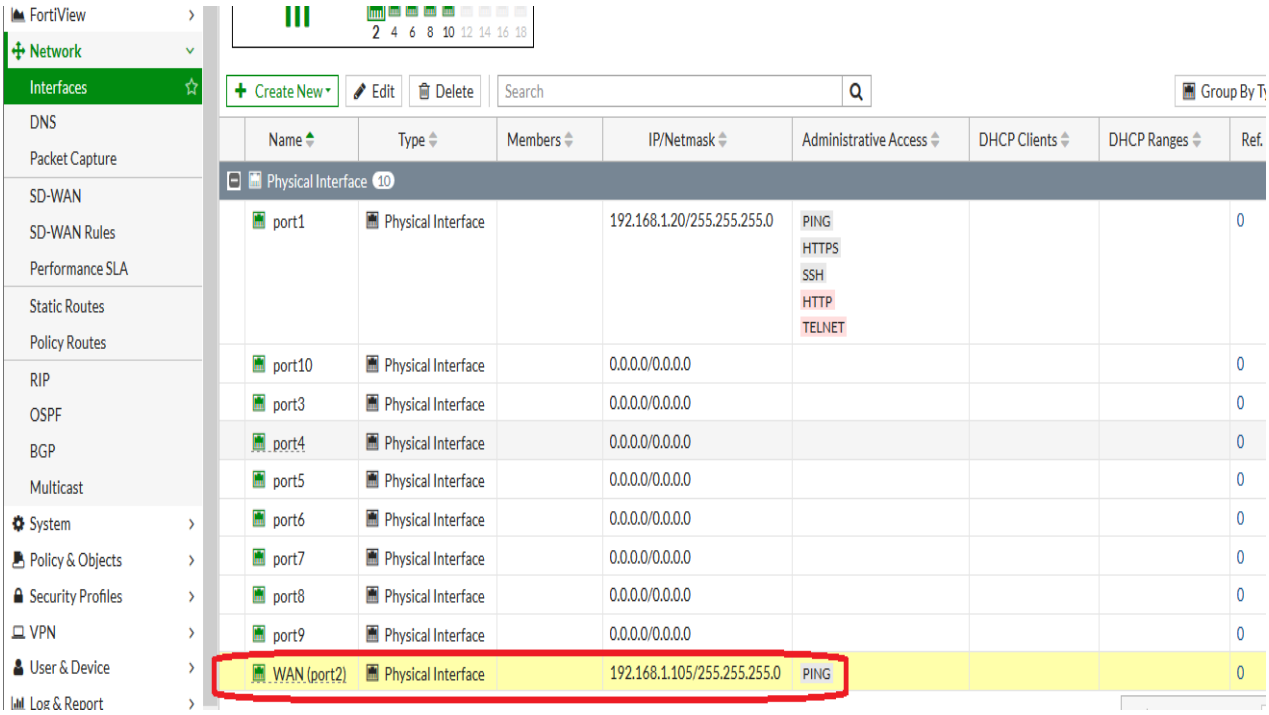
حيث بعد ذلك يمكن من الابتوب الشخصي(Host) ان تعمل

Ping 192.168.1.60 وهو ايبي بورت الWAN





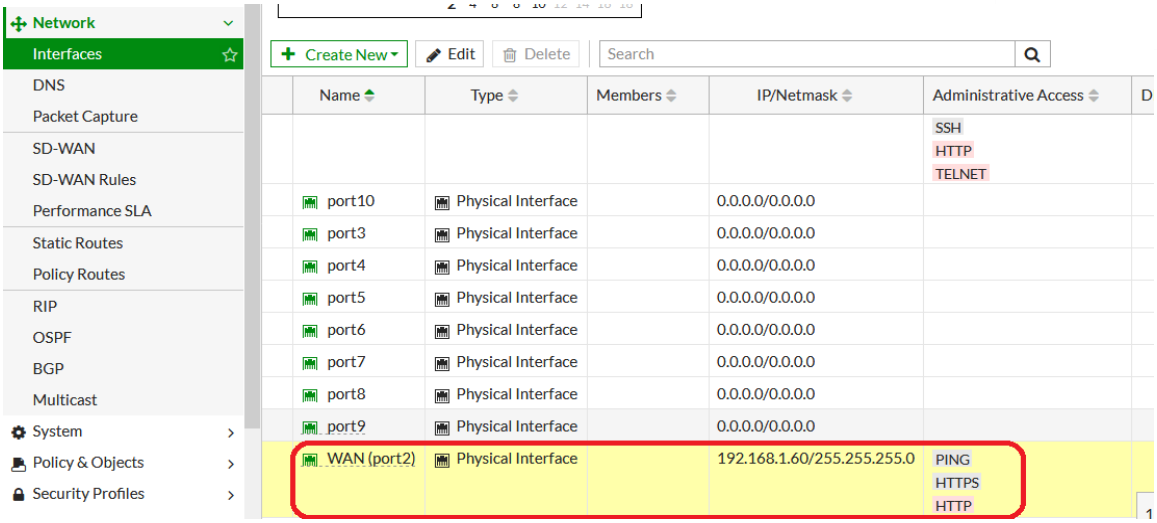
ثم OK .



تلاحظ بان المنفذ WAN حصل على ايبي 192.168.1.105 وكما هو ظاهر بان الping مفتوح ...

نحن سوف نجعل كرت lan2=wan ايبي static

192.168.1.60 كما بالصورة أدناه



حيث يمكنك بعد ذلك ان تدخل الى اعدادات الفورتي جيت عبر الويب من نفس الابتوب (Host)وذلك بكتابه ايبي wan وهو 192.168.1.60 في متصفح الانترنت وبهذا يكون قد قللت استهلاك الresources للابتوب عند العمل والتطبيق والتعلم ،

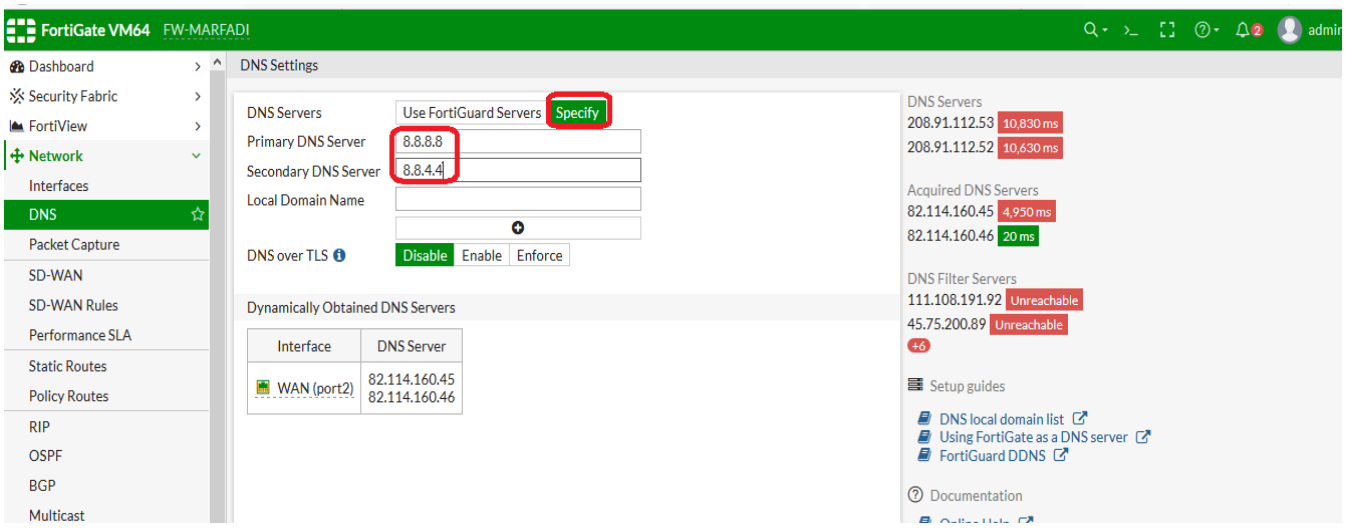
حيث ليس هناك داعي الدخول الى اعدادات الفورتي جيت عبر جهاز الكلاينت ..

الخطوة الثانية :

ضبط اعدادت الDNS لجهاز الفورتي جيت كما بالخطوات التالية :

Network >DNS>Specify>:8.8.8.8 8.8.4.4

>apply



الخطوة الثالثة :

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

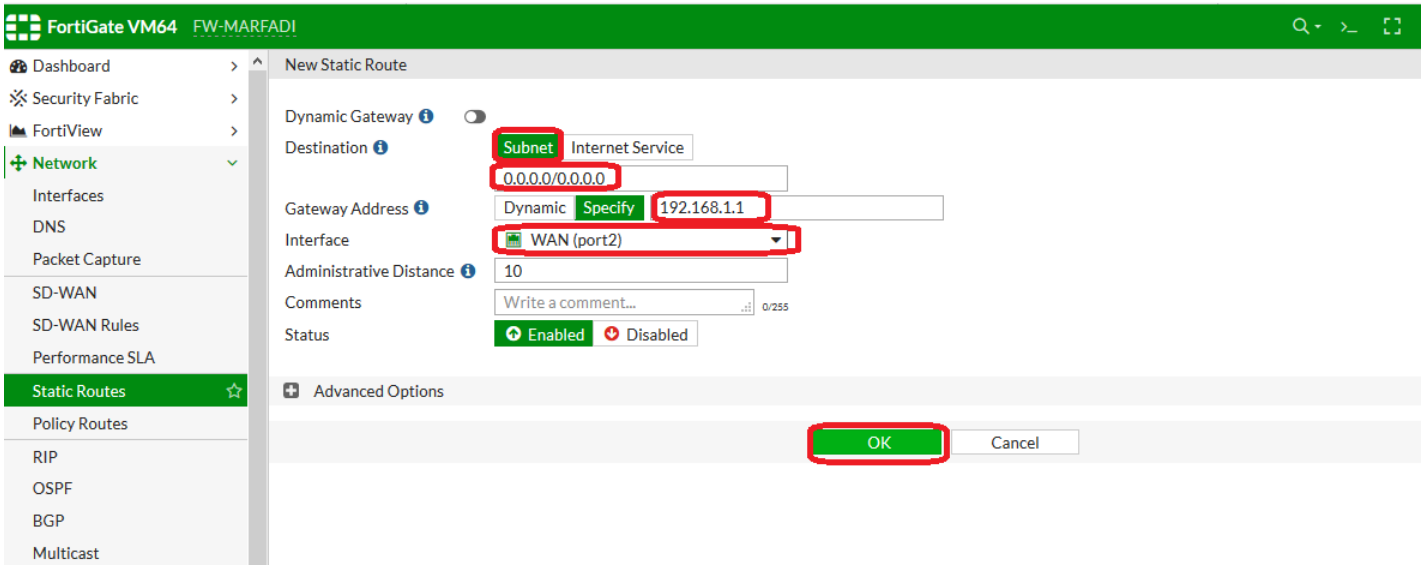
Interface :port2(WAN)

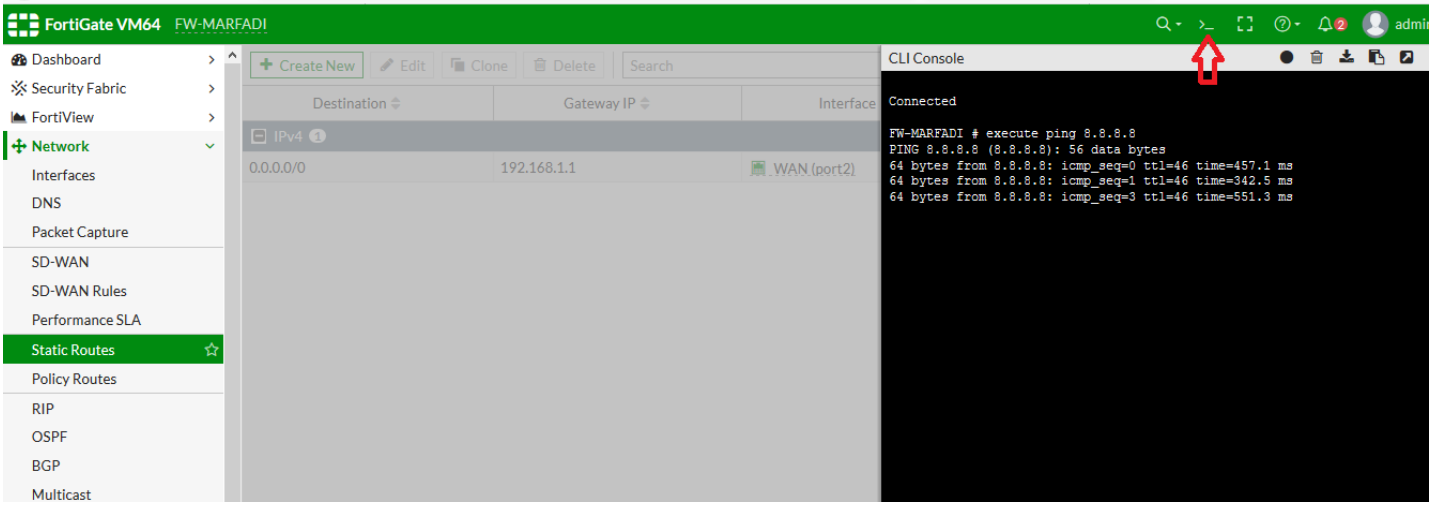
OK

ثم نقوم بالدخول الى CLI عبرGUI ثم نكتب الامر

Execute ping 8.8.8.8

فتلاحظ بان الانترنت اصبح متاح لجهاز الفورتي جيت الآن ..





❖ متى احتاج الى عمل ترقيه –تحديث- للـ Firmware التابع لجهاز الفورتي:

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 الـ Upgrade(ترقيه) يجب ان تقوم بالتالي :

١- يجب ان يكون لديك باك اب للـCurrent 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 استعاده لـ configuration التي قمت بها في الخطوة رقم 1

٣- يجب ان يكون لديك Upgrade path لأنه لا يمكن ان تقوم بعمل ترقيه من اصدار 5.0 الى 6.00 مباشره بل يجب ان تقوم بالترقية بالتدريج بحسب upgrade path مثلا من 5.0 الى 5.6 والخ الى ان تصل الى الإصدار المطلوب 6.0

❖ طرق ترقيه النظام Upgrade firmware :

١- بواسطة الـfortiGuard أي ان نقوم بتنزيل الإصدار الحديث من الانترنت مباشره بواسطة شركة فورتي جيت

٢- بواسطة local device (أي ان تكون نسخه ال OS في جهازك

ثم نقوم بالخطوات التالية

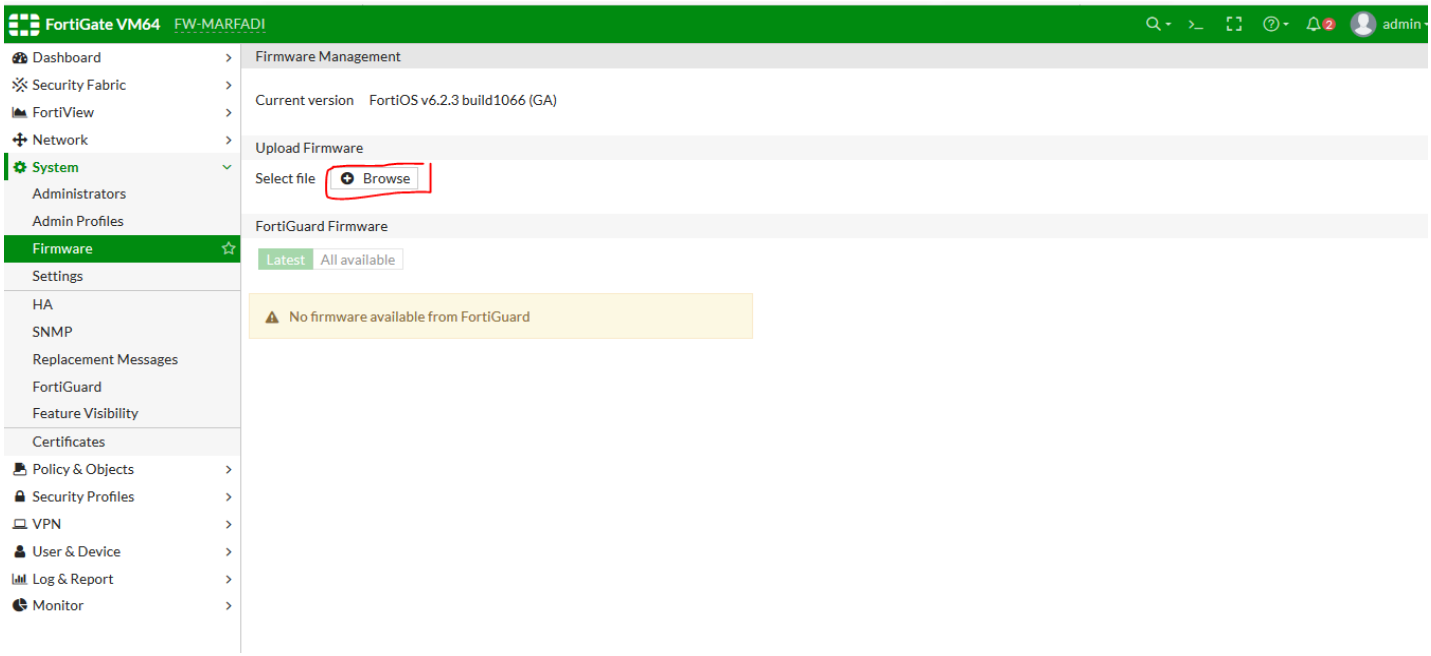
System >upload firmware >select file>choose the file of OS>Backup config and upgrade >

ثم سيتم اعاده التشغيل مرتين ...

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

Main>firmware >

❖ عمليه الـــ downgrade هي نفس خطوات الـــ Upgrade ...

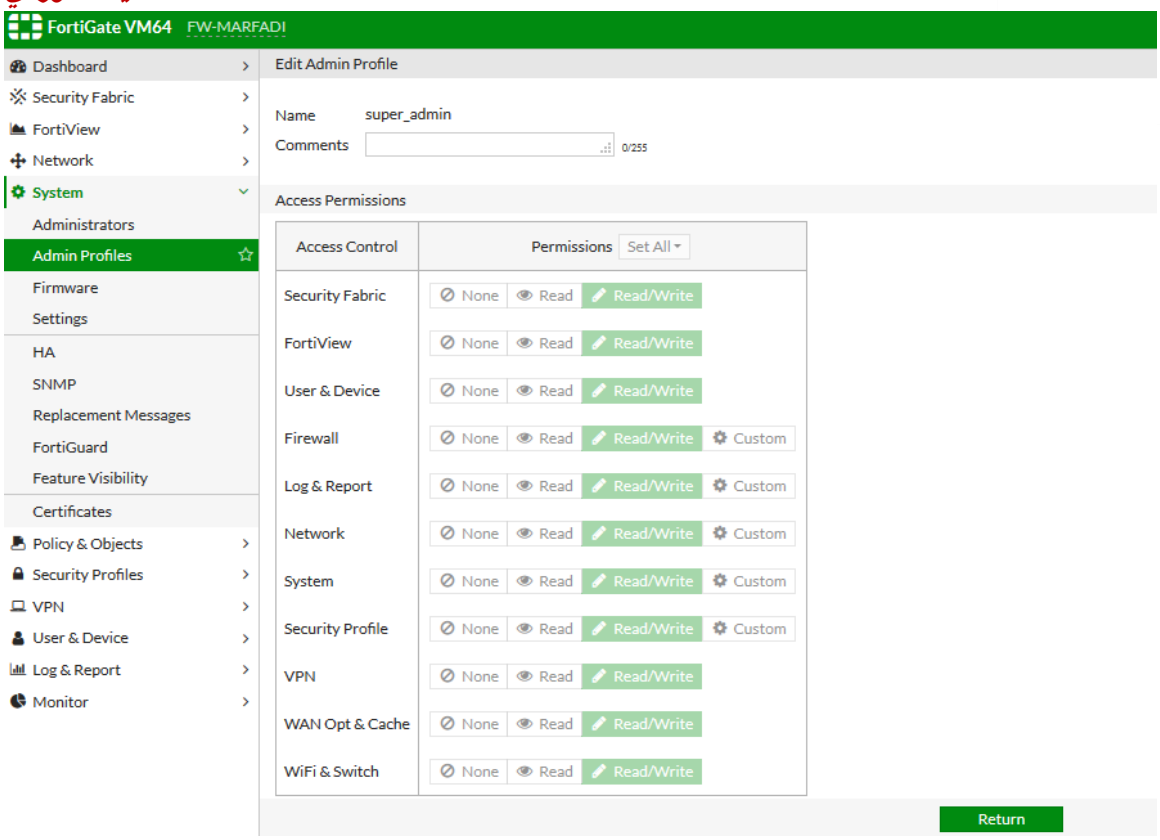


Administration types &profiles :

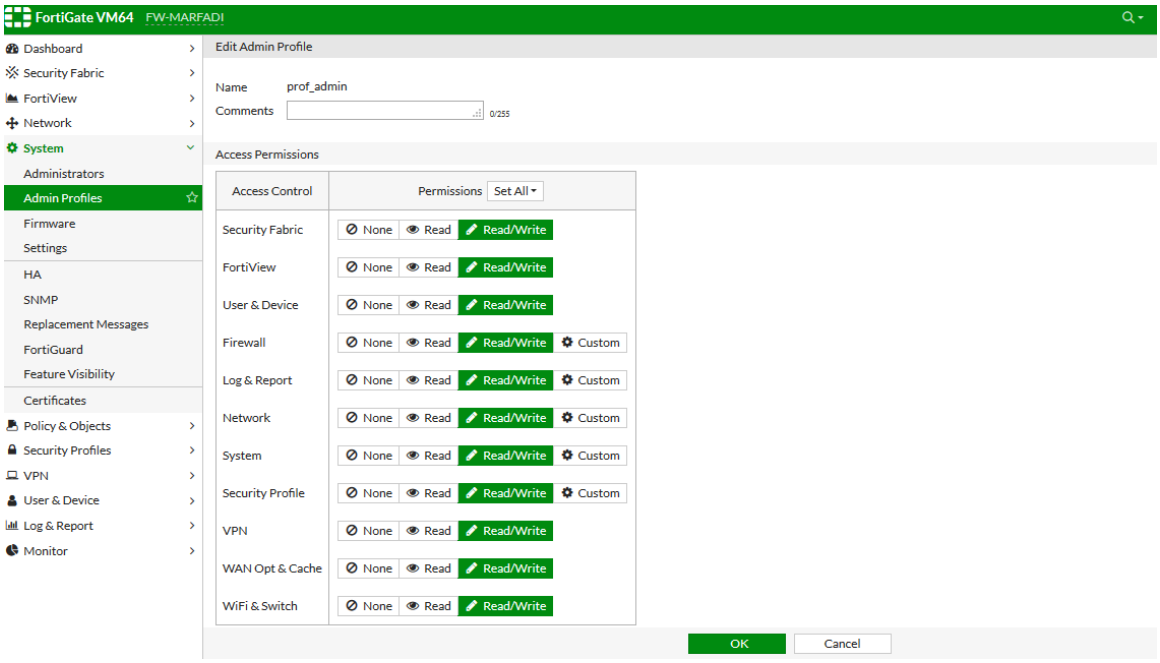
Admin profiles: من خلاله تحدد اليوزر الذي سوف يعمل login على الفورتي جيت يعمل ماذا!

ويشوف ماذا !!! ويتحكم بماذا ...

البروفايلات الافتراضية هما super admin و prof admin



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



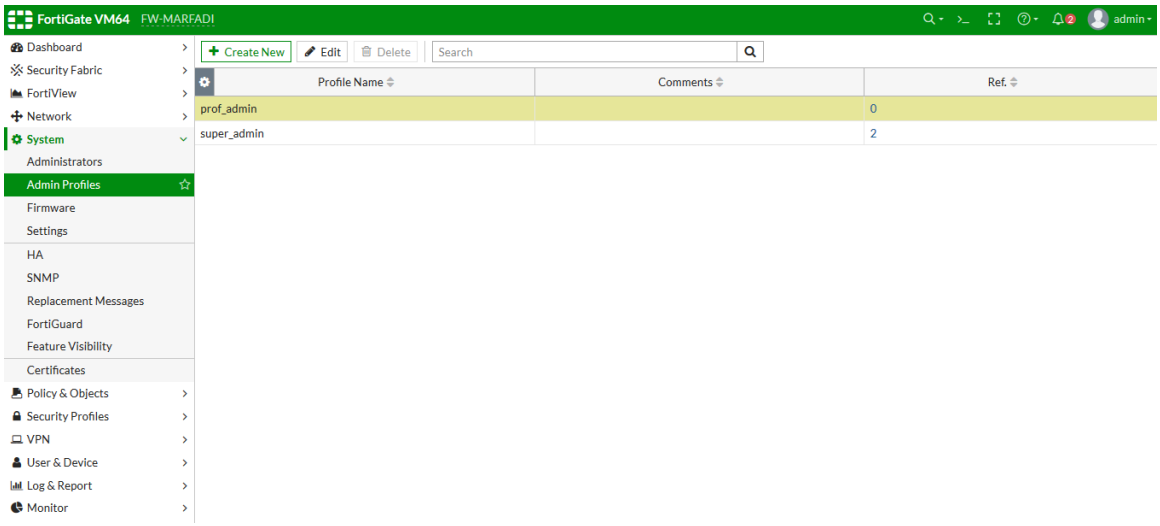
نلاحظ من الصوره أعلاه بأن البروفايل prof_admin قابل للتعديل ..

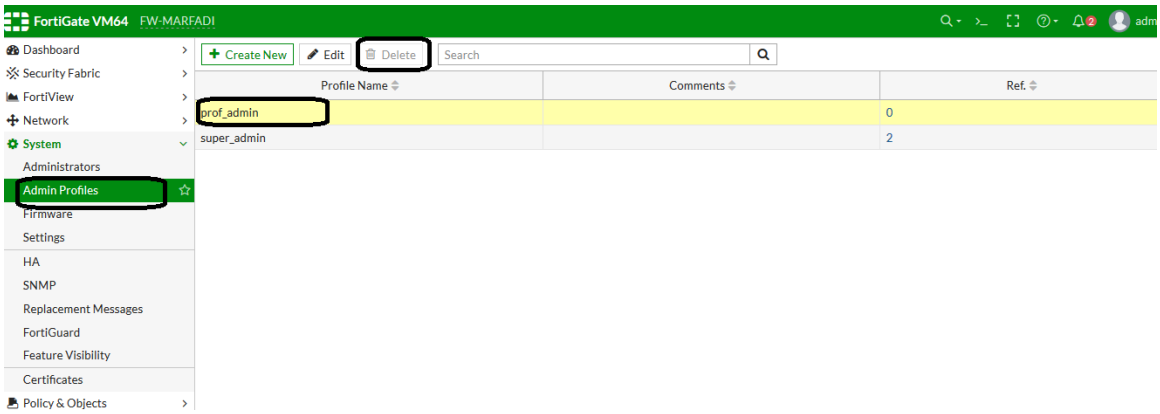
Super admin : له full access عل كل مكونات الفورتي جيت مثل delete او create لـ other

administrator ويعمل باك اب واستعاده وأيضا ترقيه او تنزيل لنسخه ال firmware ..

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

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

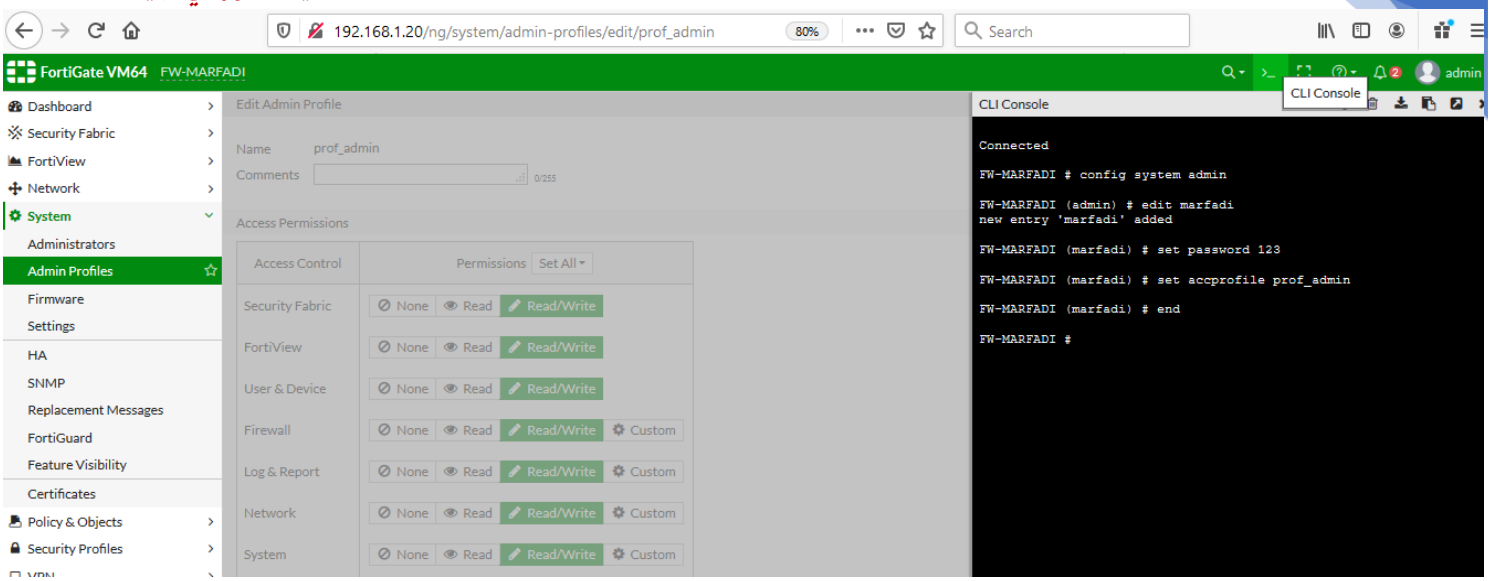




كما تلاحظ بالصورة أعلاه فانه لا يمكن حذف البروفايل ولكنك يمكن تعديله ...

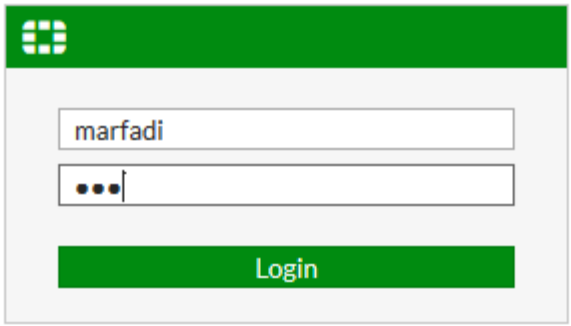
❖ **طريقة انشاء يوزر جديد بواسطة CLI :**

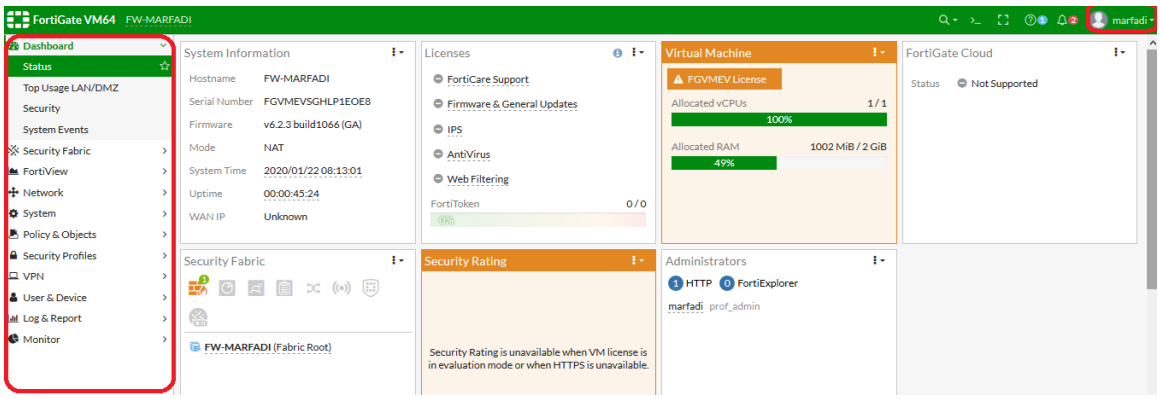
```
#config system admin

#edit marfadi

#set password 123

#set accprofile prof_admin   or  super_admin

#end
```



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

ثم حفظ الاعدادات ...



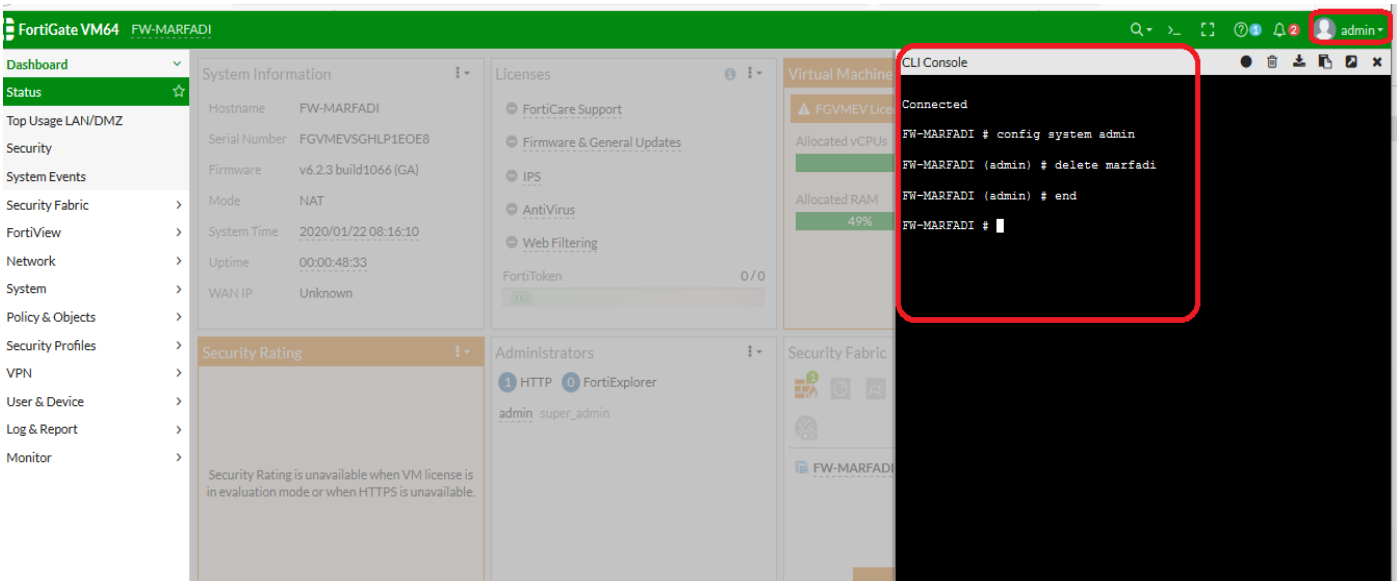


❖ لحذف يوزر بواسطة CLI :

#config system admin

#delete marfadi

End



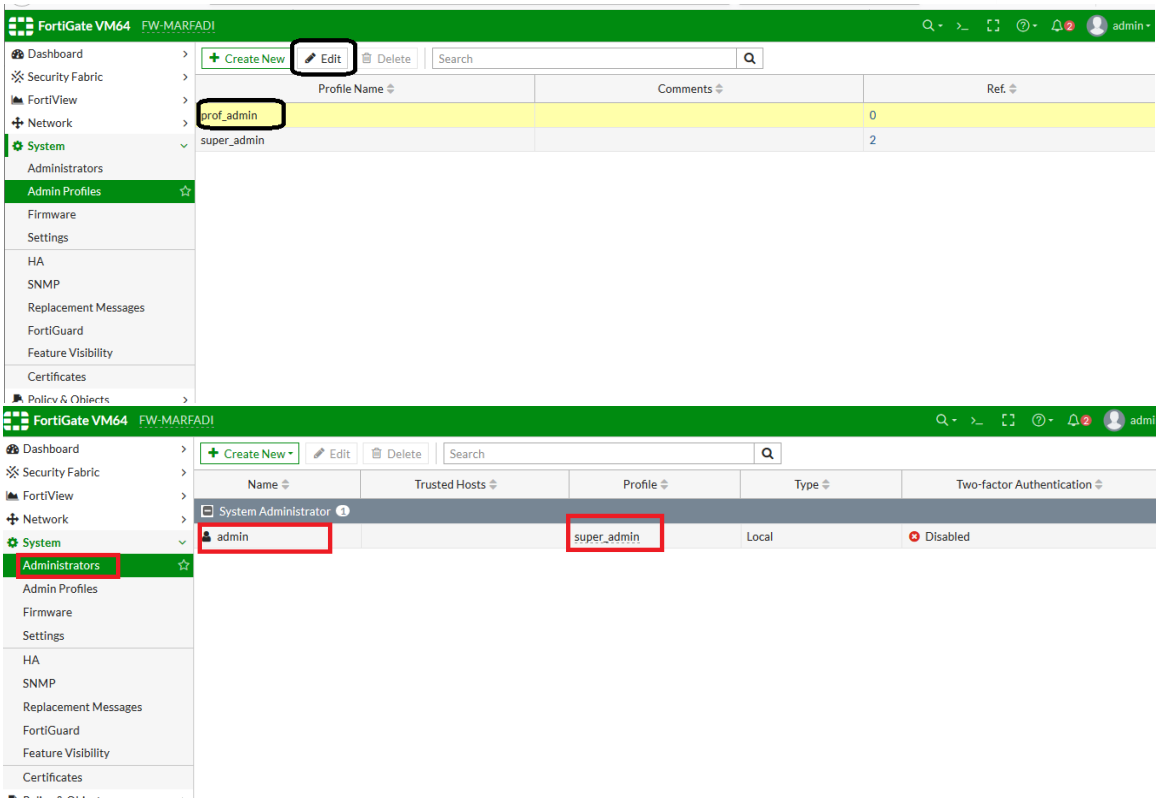
كما بالصورة أعلاه اليوزر admin له الحق ان يحذف اليوزر marfadi ..

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 .



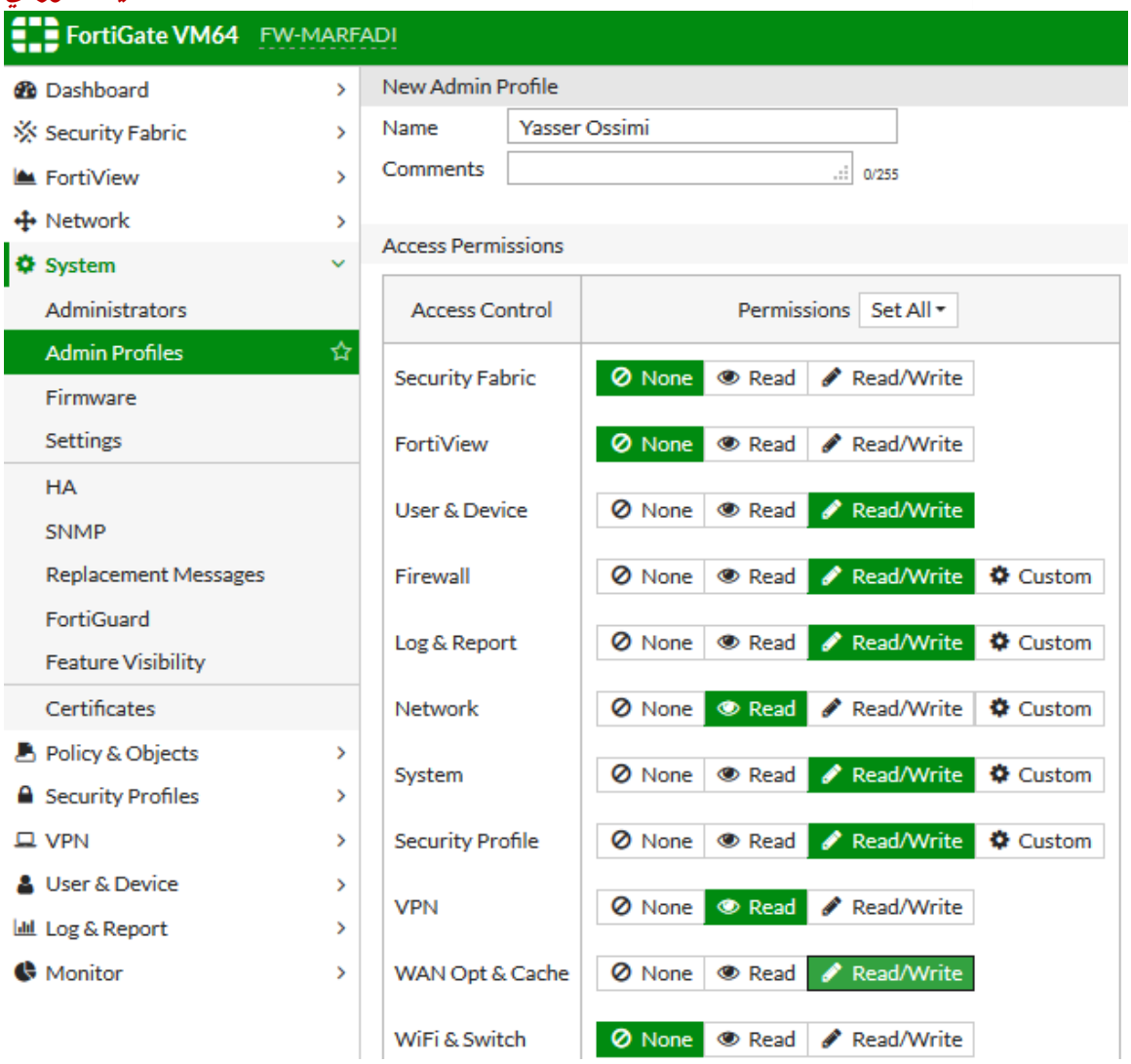
تلاحظ بالصورة أعلاه بأن اليوزر المسمى admin من نوع super_admin profile

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

مثل سوف انشى بروفايل باسم Yasser Ossimi

System >admin profile>create New>

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

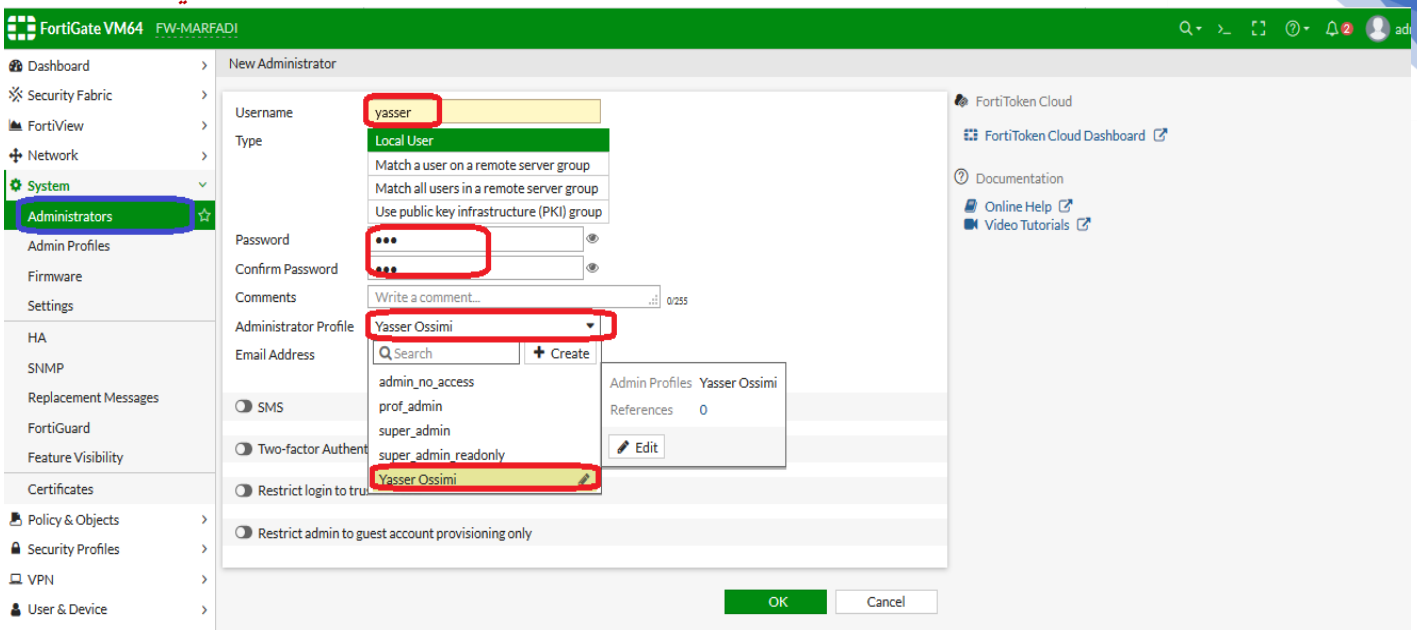


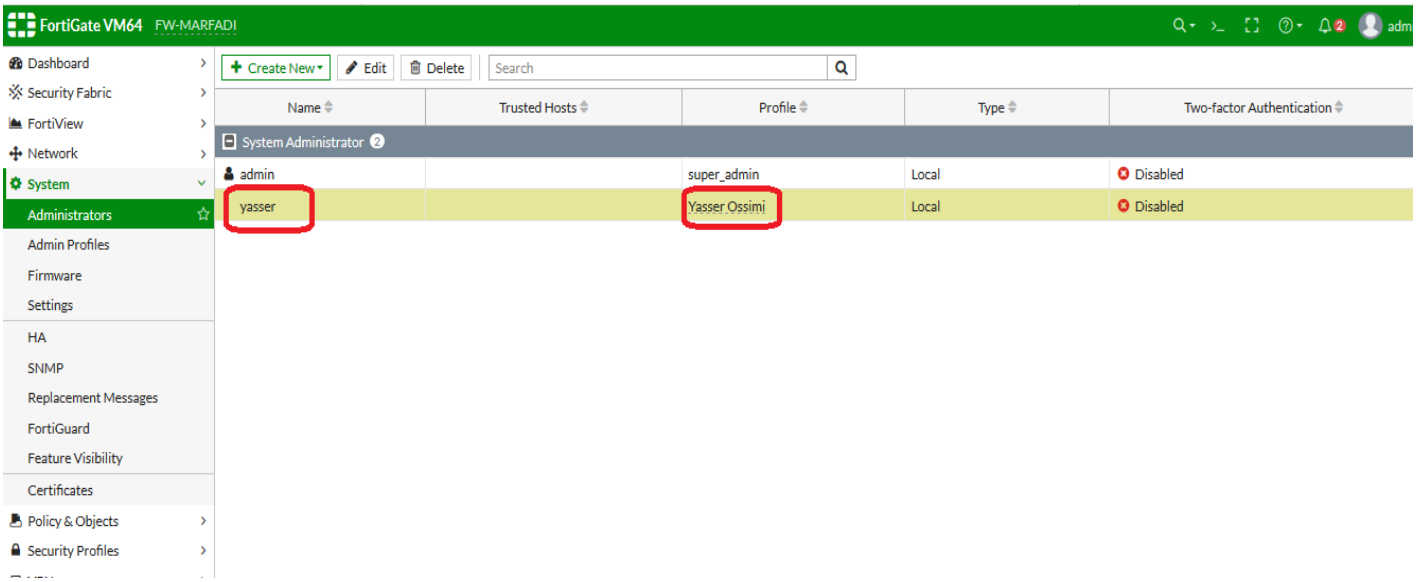
ثم OK ...

الان سوف نقوم بإنشاء يوزرباسم Yasser وسوف يكون نوع البروفايل الخاص به هو Yasser ossimi

حيث هذه المره سيتم انشاء اليوزرعن طريق الGUI كما بالصورة ادناه

System>administrators>Create New>administrator>





نلاحظ بأنه تم انشاء يوزرباسم Yasser تابع للبروفايل الذي تم تخصيصه سابقا باسم Yasser Ossimi

❖ ما هو FortiGuard ؟

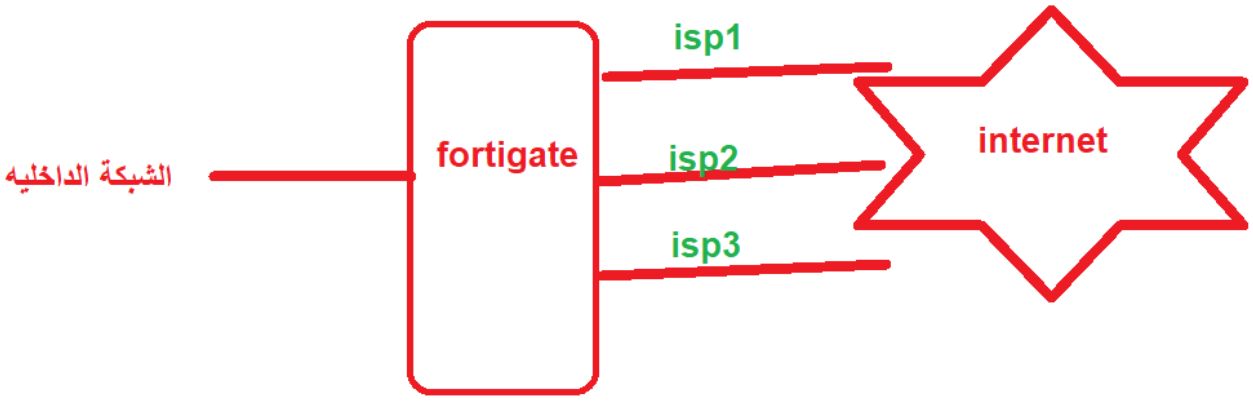
هو خدمه في الكلاود يتم الوصول اليه عن طريق الانترنت ،

يتم تحديث كل من Antivirus،antispam،IPs، Web filter ، Application control..الخ الموجود في جهاز الفورتي جيت عبر Fortiguard ..

حيث أي فايروس جديد يتم عمل update وتنزيله الى جهاز الفورتي جيت وأيضا أي هجمات جديده يتم تنزيل update جديد لها وهكذا ..

لذا يجب ان تكون مشترك (license)مع Fortiguard

SD-WAN=WAN Link Load Balancing



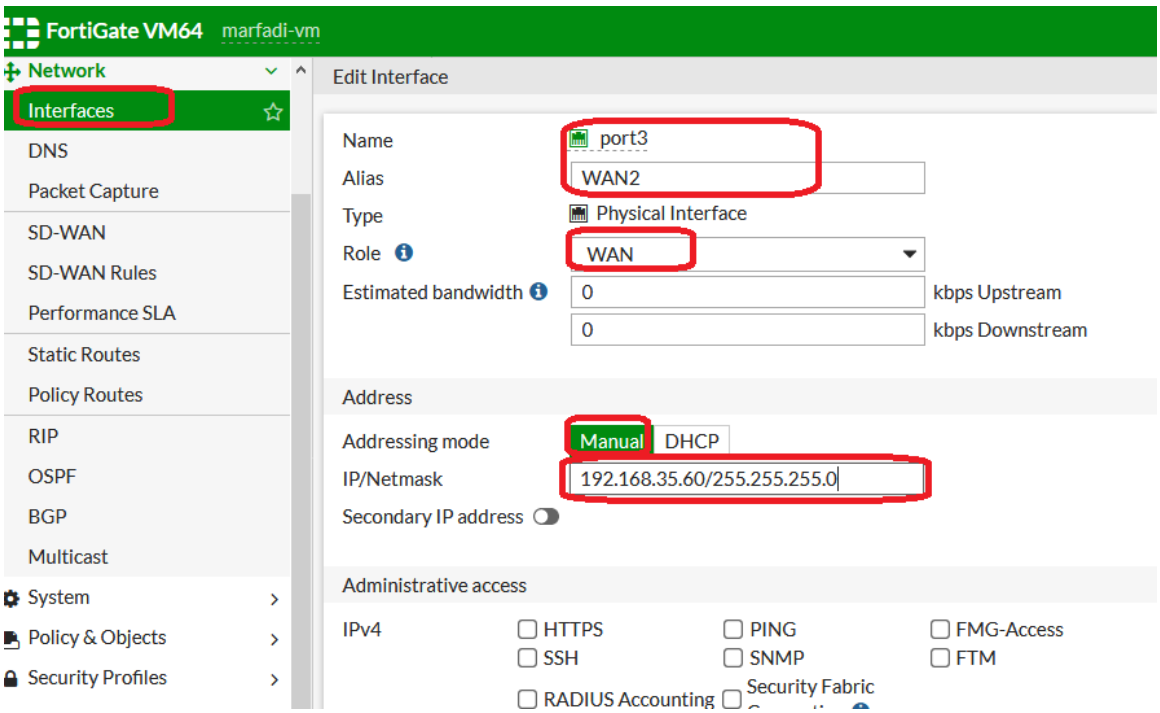
تحويل اكثر من physical interfaces الى logical interface واحد فقط ...

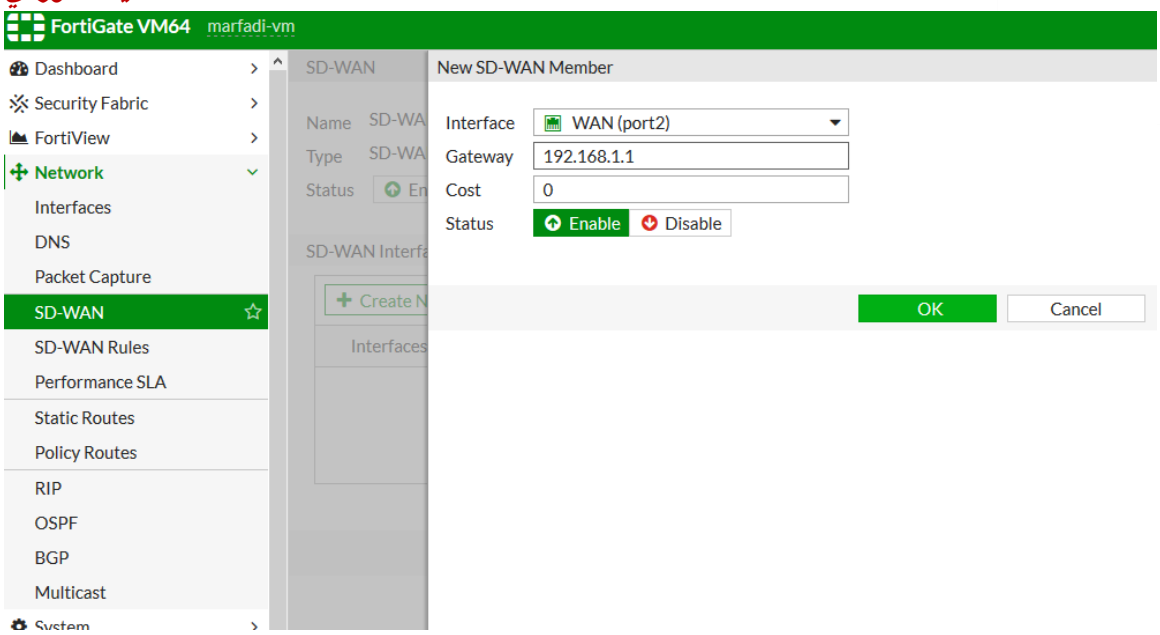
Network>SD-WAN>status:enable>create New>interfaces:

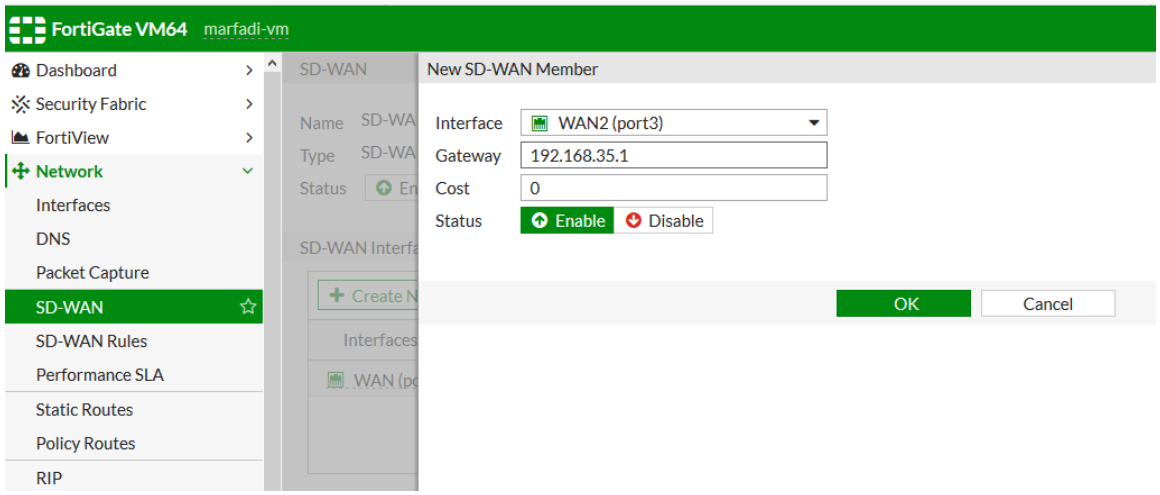
ثم نقوم بتحديد كروت الشبكة المراد دمجها (load balance)

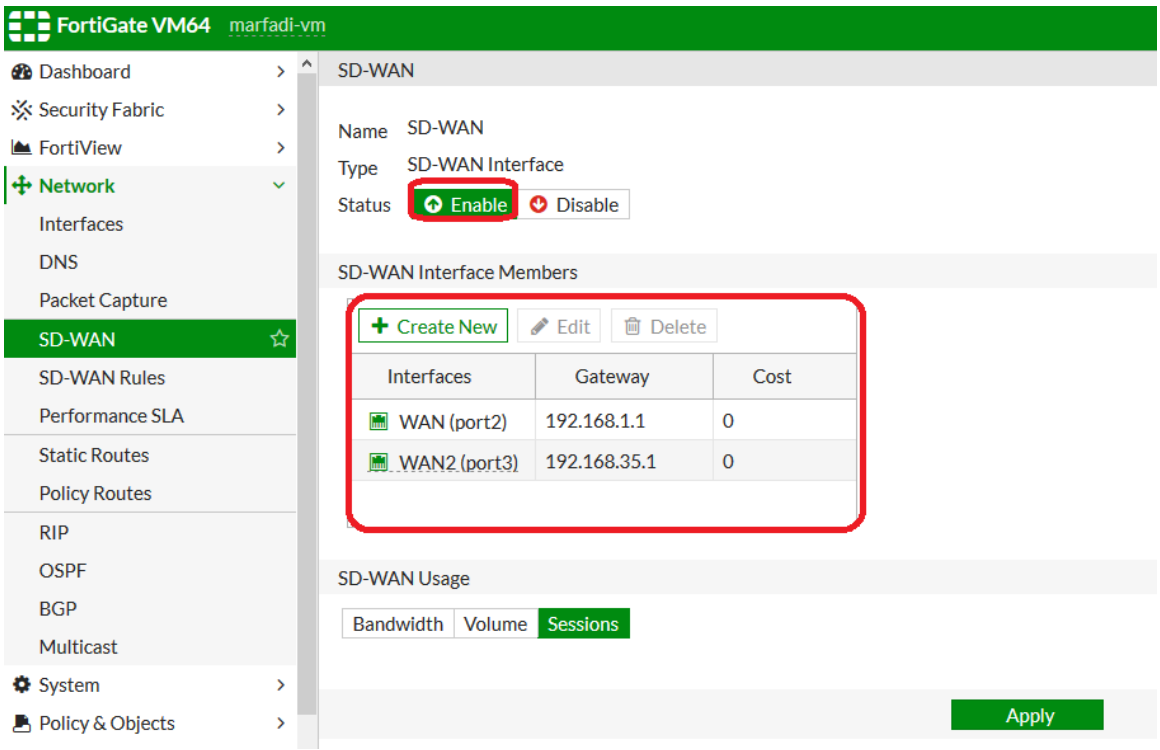
لنفترض بان لدينا 2 خطوط انترنت موصله على كروت الشبكة WANو WAN2 ثم نحدد خوارزميه لتوزيع الانترنت للمستخدمين.

أولا نقوم بضبط اعداد كرت الـwan2 كما بالصورة ادناه

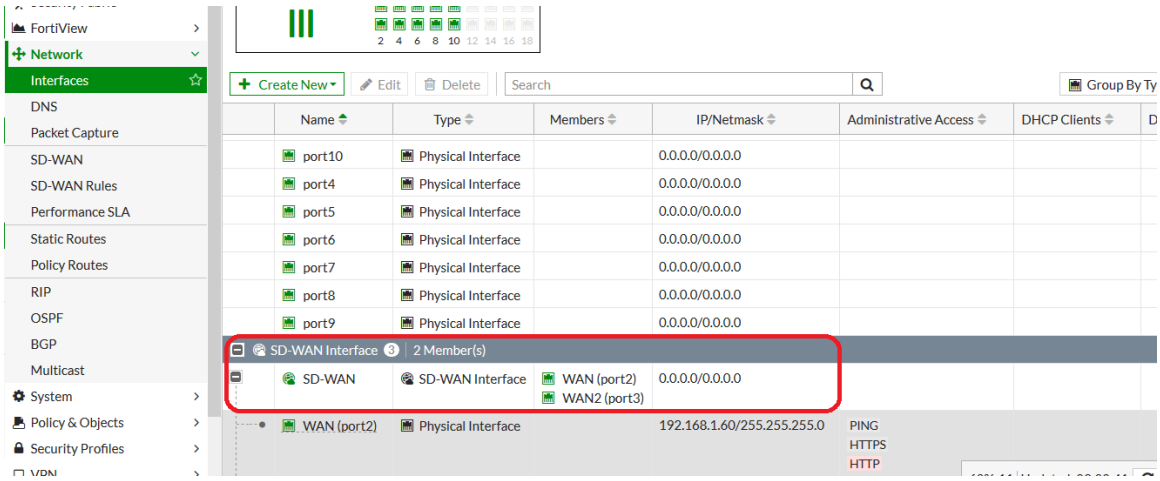


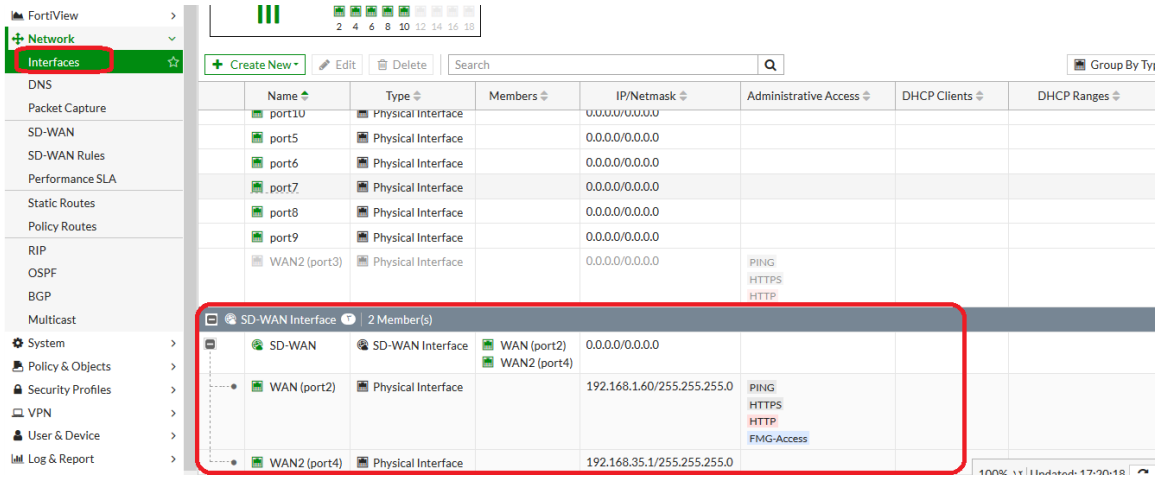

FortiGate VM64
marfadi-vm
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
OSPF
BGP
Multicast
System
SD-WAN
New SD-WAN Member
Interface
WAN (port2)
Gateway
192.168.1.1
Cost
0
Status
Enable
Disable
OK
Cancel

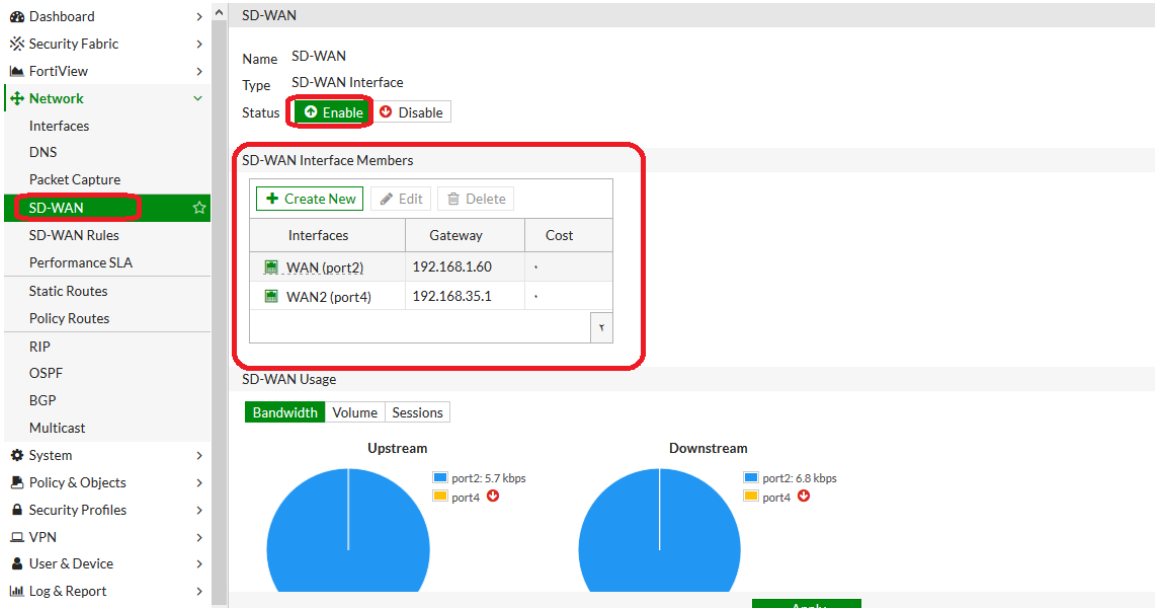

FortiGate VM64
marfadi-vm
Dashboard
Security Fabric
FortiView
Network
Interfaces
DNS
Packet Capture
SD-WAN
SD-WAN Rules
Performance SLA
Static Routes
Policy Routes
RIP
SD-WAN
New SD-WAN Member
Interface
WAN2 (port3)
Gateway
192.168.35.1
Cost
0
Status
Enable
Disable
OK
Cancel


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
SD-WAN
Name SD-WAN
Type SD-WAN Interface
Status Enable Disable
SD-WAN Interface Members
Create New
Edit
Delete
Interfaces
Gateway
Cost
WAN (port2)
192.168.1.1
0
WAN2 (port3)
192.168.35.1
0
SD-WAN Usage
Bandwidth
Volume
Sessions
Apply

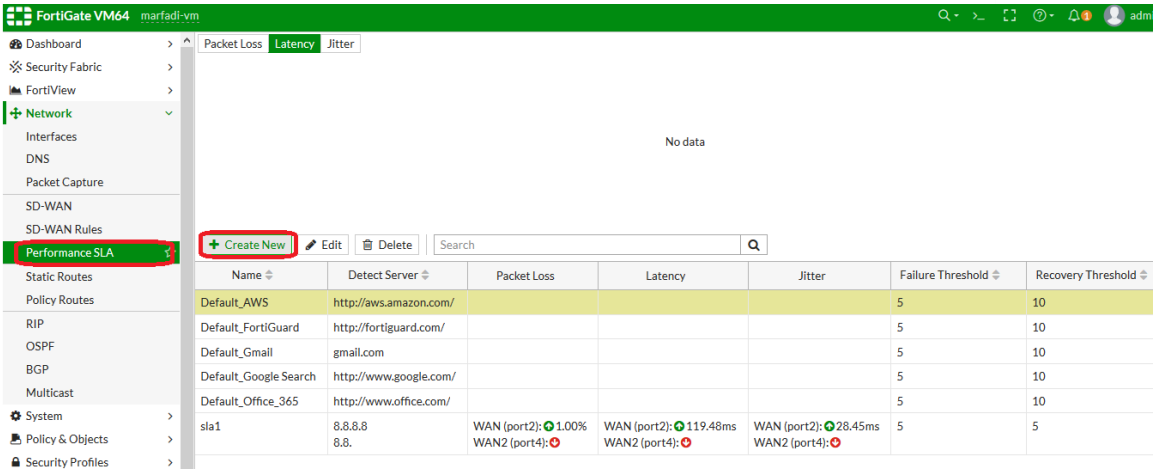
ثم نلاحظ بانه تم انشاء logical interface باسم SD-WAN كما بالصورة ادناه ...







تفعيل خاصيه الـsdwan بعد أضافه 2 كروت الـwan



Performance SLA : يتم من خلاله انشاء monitoring profile مثلا SLA1

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

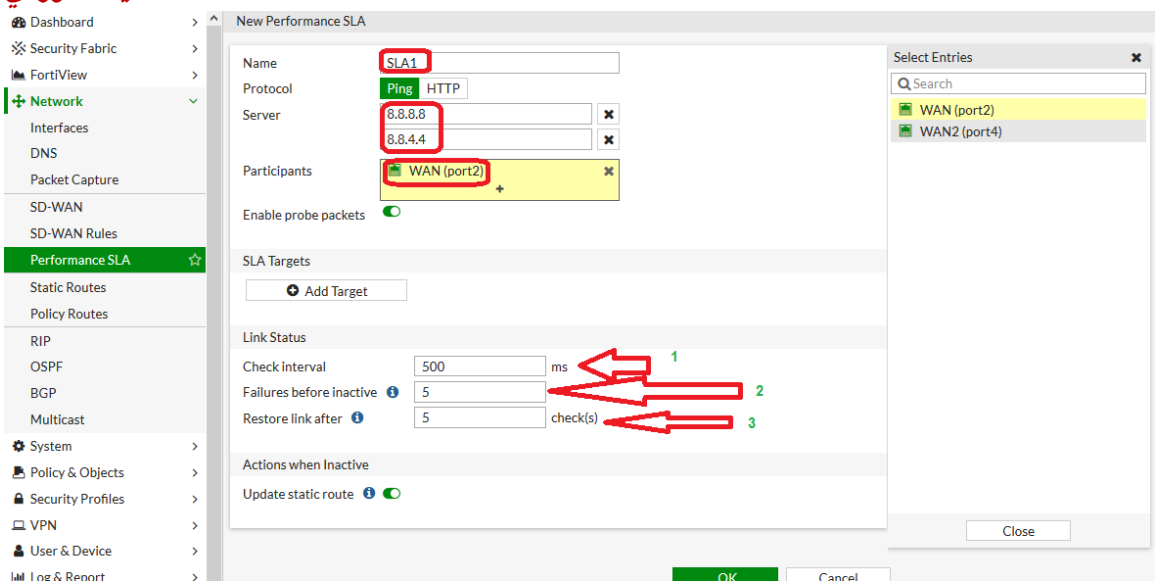
حيث عبر الخيار Participants تقوم بتحديد من اين سيقوم بعمليه الـ ping هل من خلال الخط wan1 مثلا او عبر wan2 او عن طريق الاثنين .

مثلا سوف أقوم بعمليه الping 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 عمليه 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 -

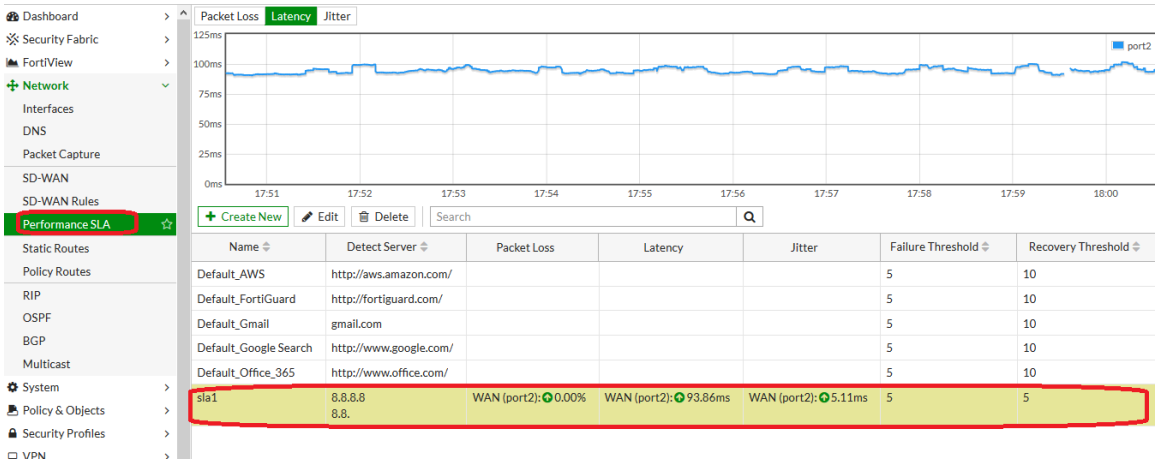


١- حيث سيتم عمليه ارسال الفحص (ping) الى 8.8.8.8 و8.8.4.4 كل 500 ملي ثانية -أي كل نصف ثانية قم بعمل ارسال echo request -

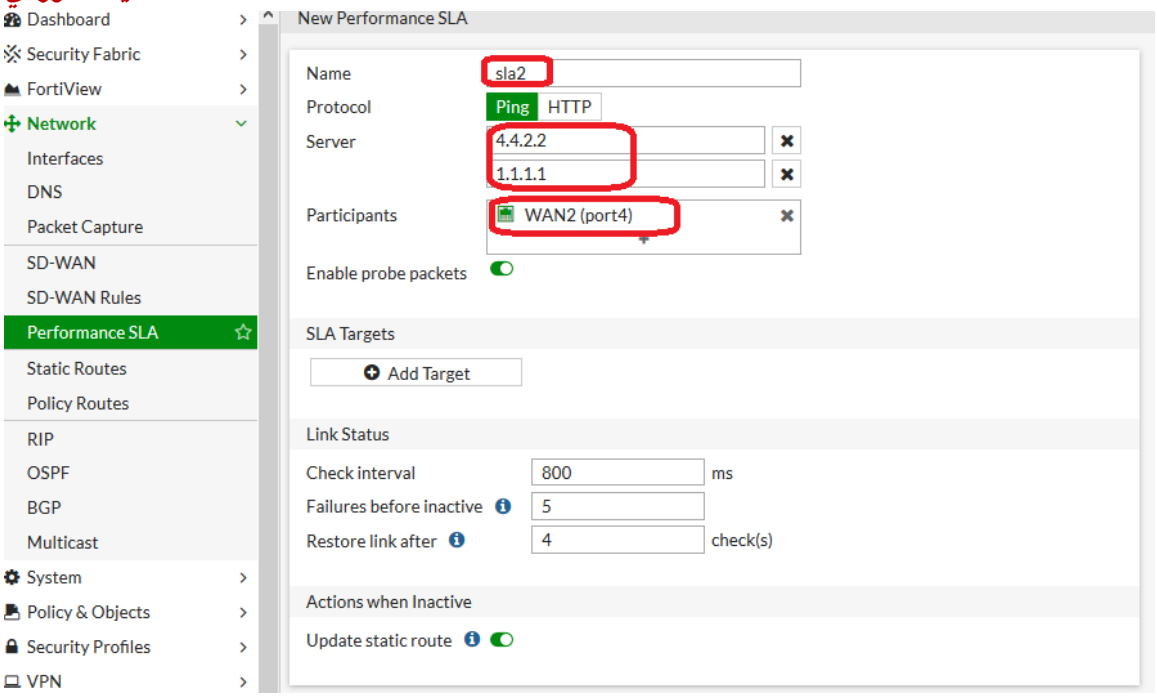
٢- فلو تم ارسال 5 echo request الى 8.8.4.4 , 8.8.8.8 ولم تستلم أي رد (echo reply)

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

٣- بعد ان اصبح الخط wan1=down فبأي وقت لو حصل echo reply لعدد 5 مرات فاجعل الـwan1=up

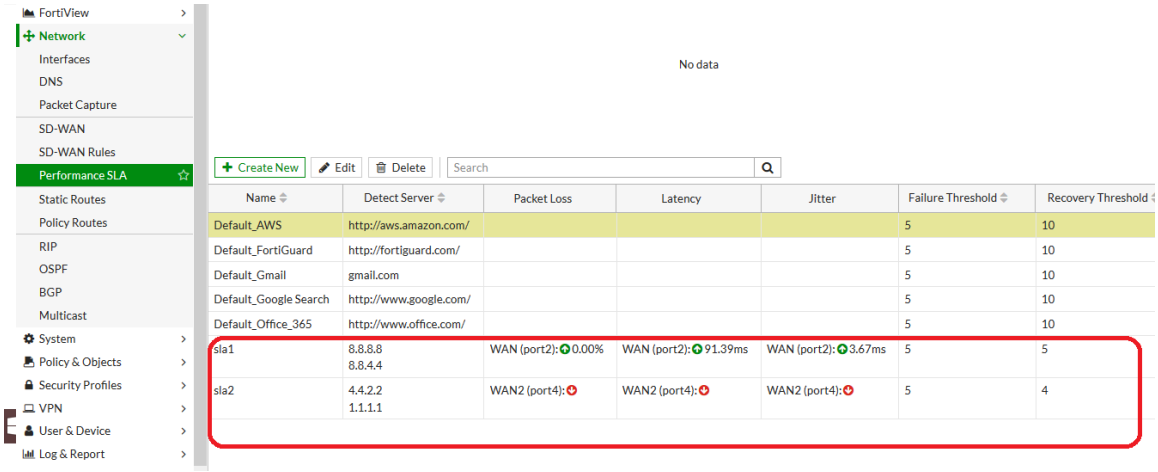


انشاء monitoring profile للخط wan2 عبر البروفايل sal2

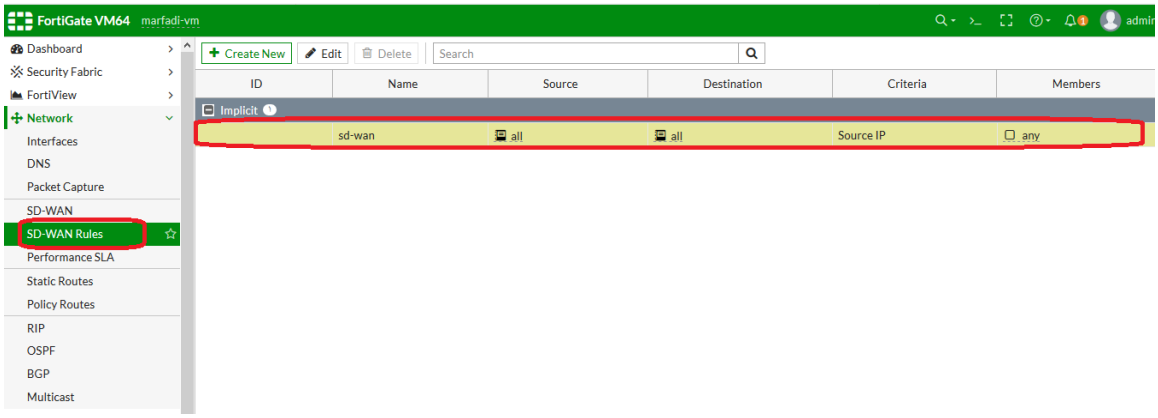


ملاحظة :لا يمكن فحص نفس السيرفر مثلا ان تجعل عمليه الـ ping لـsla1 و sla2

على نفس ايبي 8.8.8.8 و8.8.4.4 لذا تم تغييرهم ..

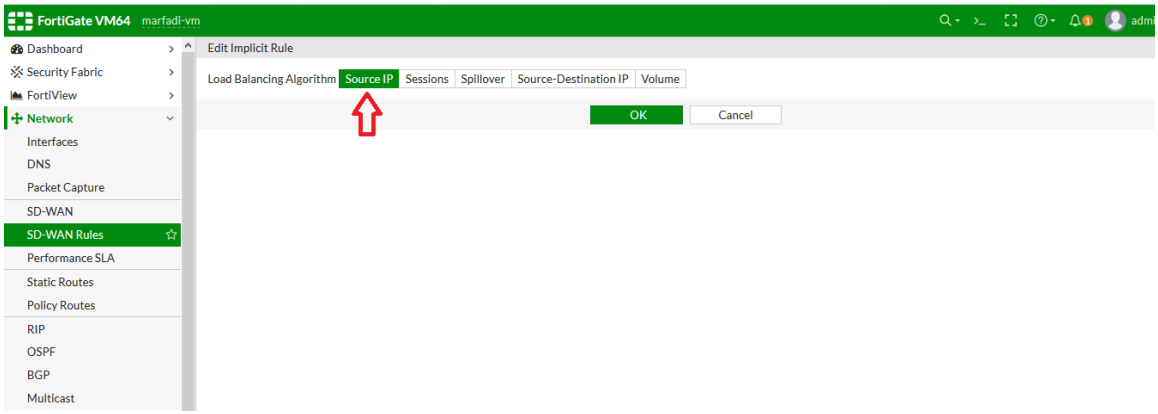


عمليه الـ sd-wan سيتم تطبيقها عبر SD-Wan rules بحيث لو تركتها بشكل افتراضي كما بالصورة ادناه

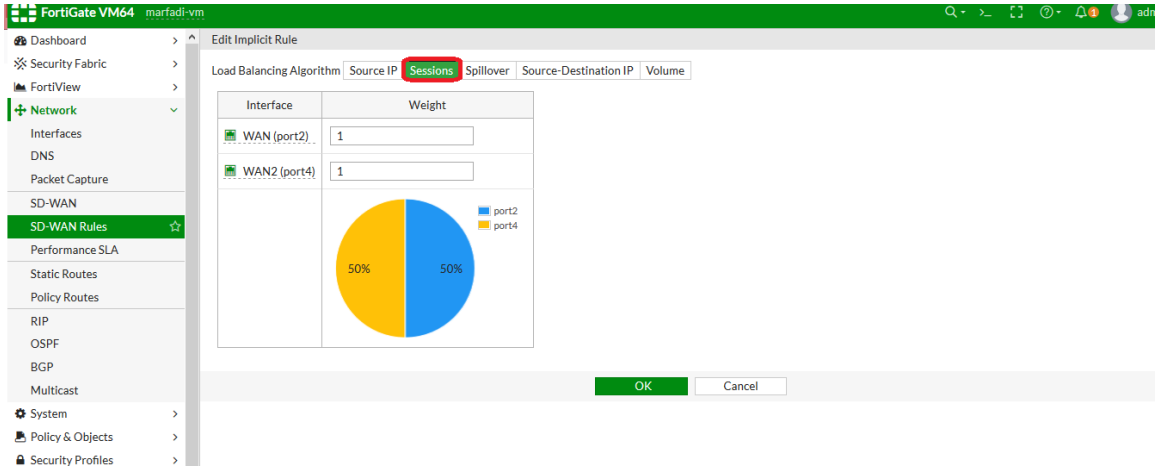


أي انني لم أقوم بإنشاء Rule فأن الرول الافتراضية هي حيث عند النقر عليها مرتين

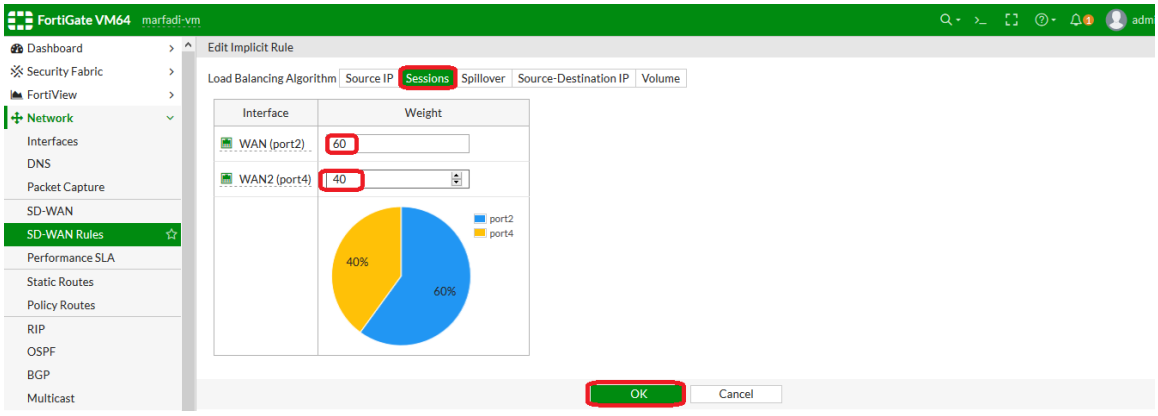
تظهر لك الـcriteria المطبقة هي Source IP حيث يمكنك تغييرها ..



مثلا يمكنك تغيرها الى Sessions :



حيث يمكنني تغيير النسبة مثلا 60% لـWAN1 و 40% لـWAN2



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

****

اما النوع الاخر المسمى Source-Destination IP :

لو الـ source ip والـdestination ip يكونوا ثابتين على نفس الـinterface يتم إخراجه عبر نفس الـinterface

اما لو الـ source رايح على destination مختلف فأنه يتم اخارجه 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

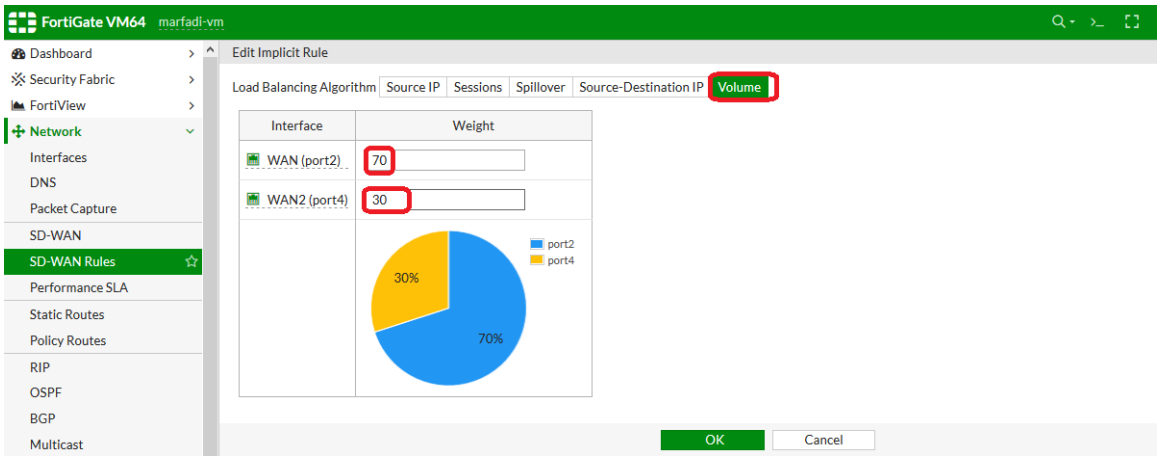
From 192.168.1.60 to 8.8.8.8 >>>WAN2

وهكذا....

From 192.168.1.20 to 4.2.2.2 >>>WAN2

****

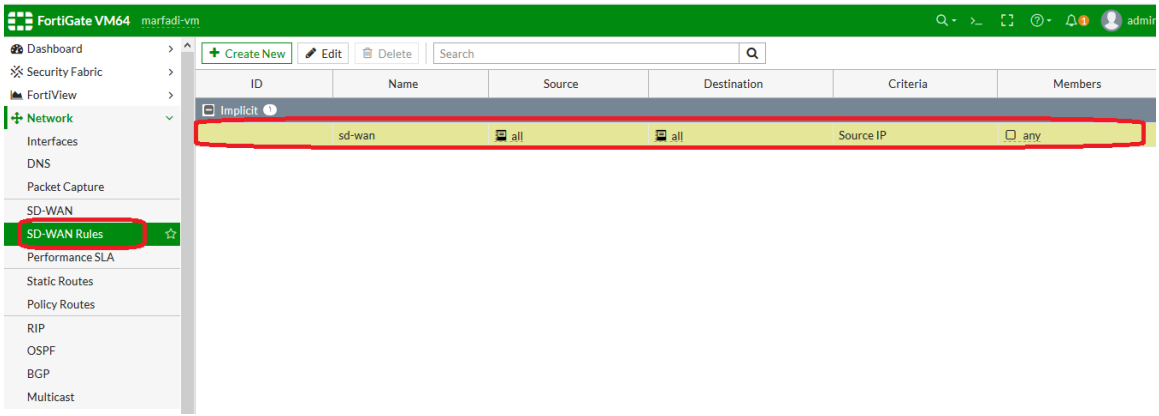
النوع الثالث Volume :



هذا النوع من الخوارزميات تعتمد على كميه الـbytes

فلوا كانت لدينا packets بحجم مثلا 1000 بايت فأن 70% منها سوف تكون عبر WAN1 و 30% البقيه ستكون عبر الـWAN2

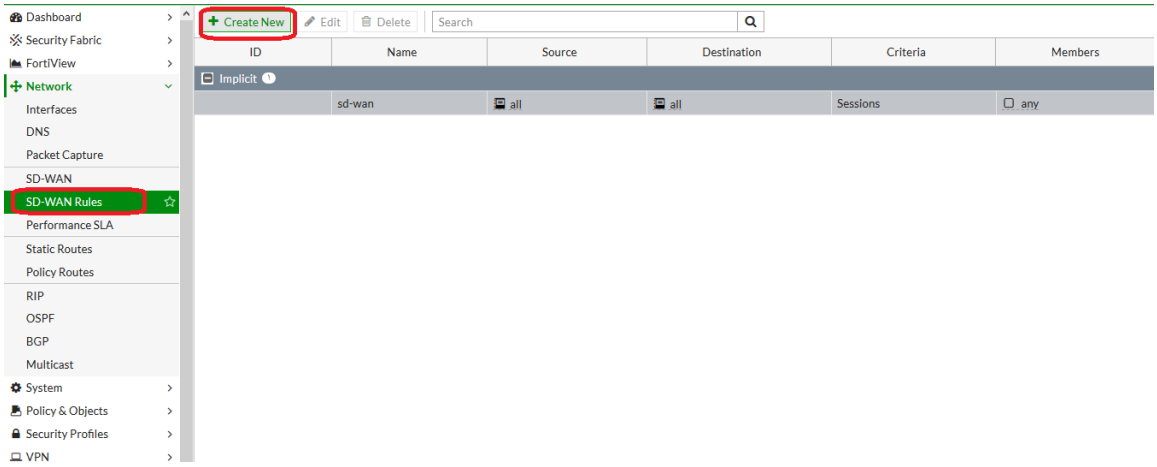
فلوا لم نقم بإنشاء أي SD-WAN Rule وتركناها افتراضي فان أي ترافيك سوف يتم تطبيق الـ rule الافتراضية كما بالصورة أدناه وسيتم تطبيق الـcriteria بحسب ما تم اختياره ..

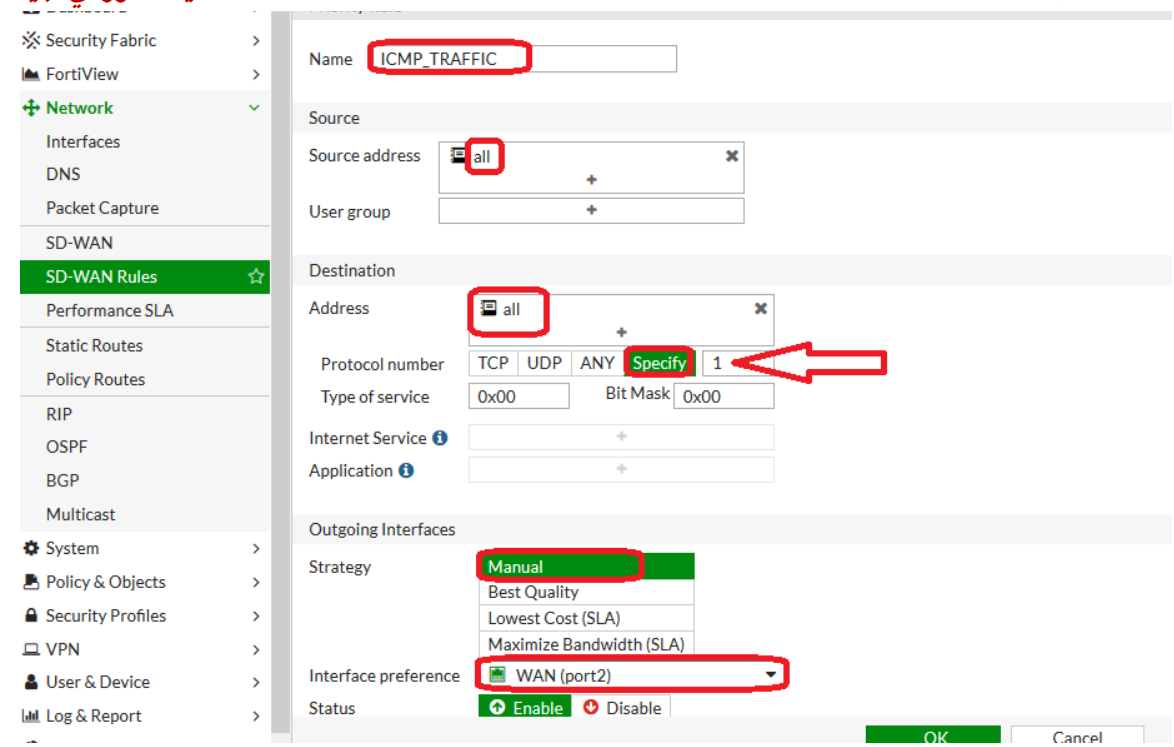


❖ طريقة انشاء SD-WAN Rule جديده كما بالتالي :

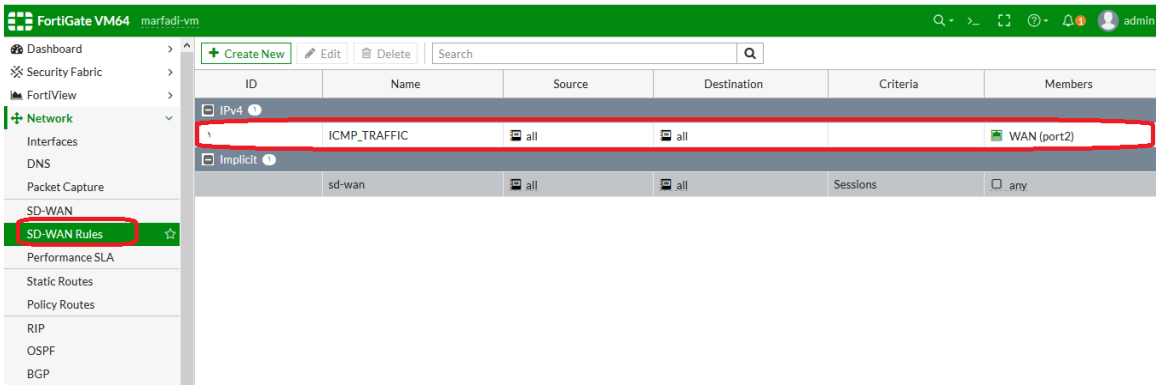
✓ جعل الICMP traffic يطلع عبر الWAN1 :

أي ان أي عمليه ping اريدها تطلع عبر الwan1 بالتحديد .

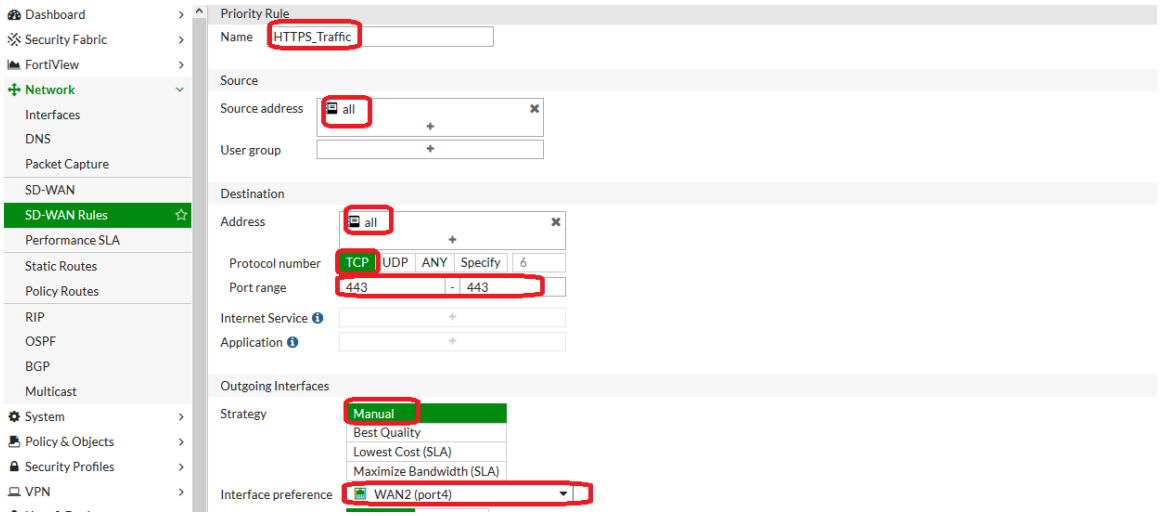




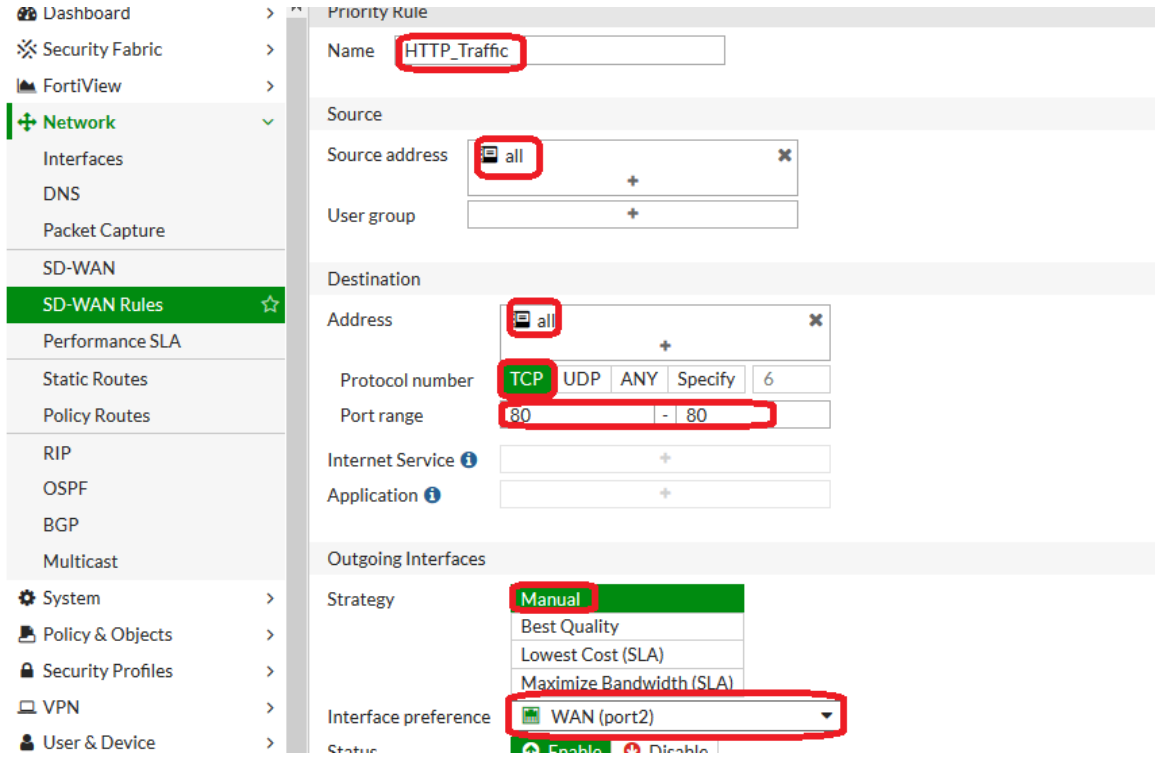
ملاحظة: protocol number لـICMP هو 1 حيث يمكنك البحث في جوجل عن ارقام protocol numbers .

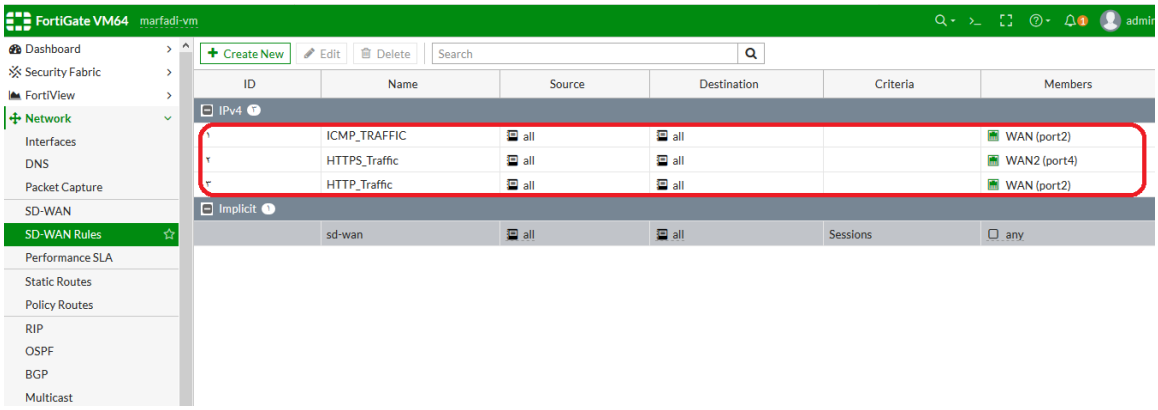


❖ جعل الـ https traffic يطلع عبر الـ wan 2 :

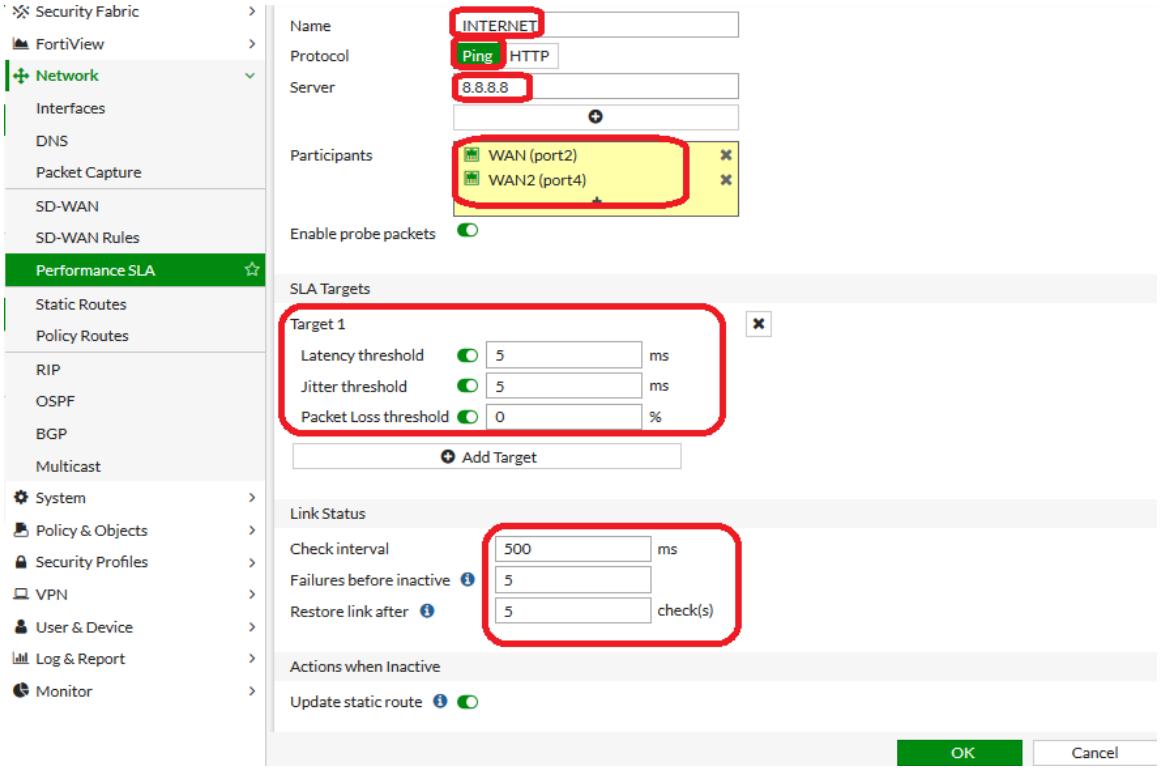


❖ جعل الـ http traffic يطلع عبر الـ wan 1 :





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



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

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

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

حيث الـ latency هي الوقت الذي يقطعه الباكت(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
```

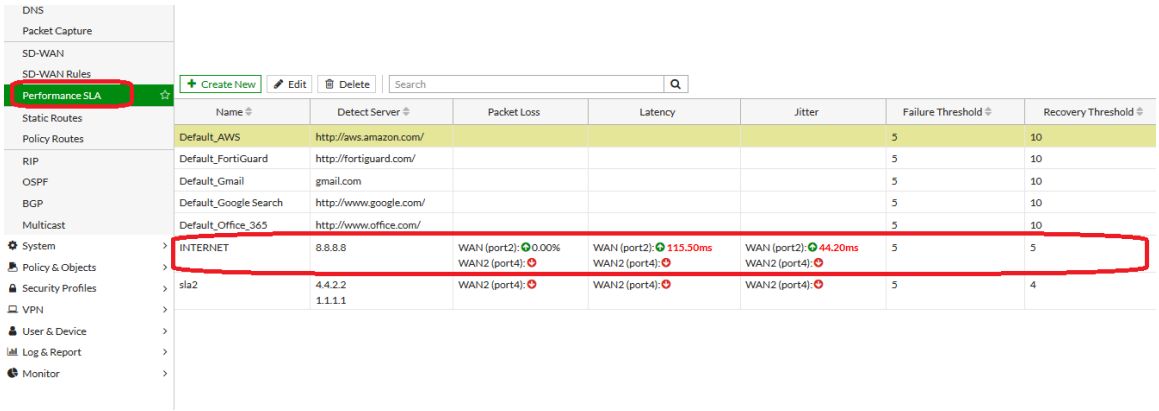
أي 88 نفسها ..

الـjitters : يحسب الفرق في الوقت بين الباكت الأول والثاني والاقل فارق بيتم اختياره كأفضل خط .

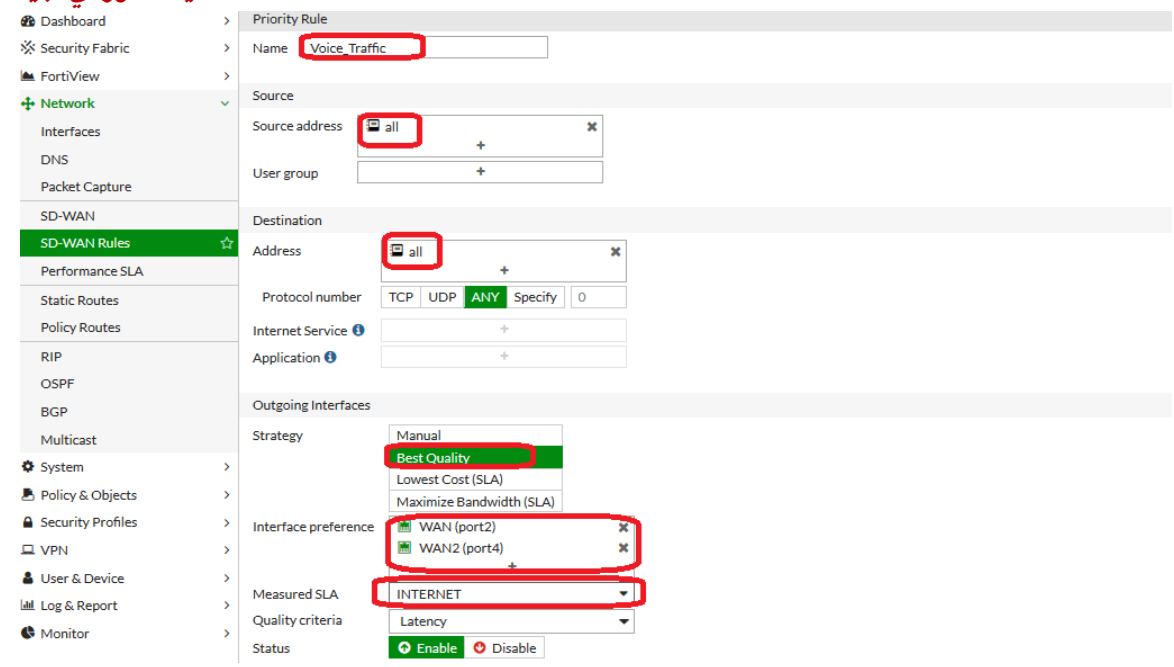
```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=88ms TTL=117
Reply from 8.8.8.8: bytes=32 time=89ms TTL=117
```

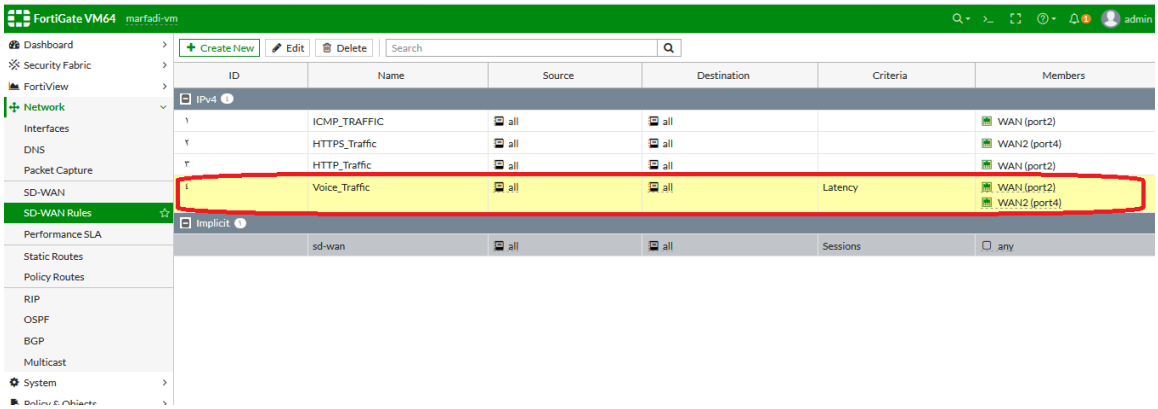
Jitters=89-88=1

الـpacket loss: هذا يقصد به الفقد في البيانات حيث ممكن يكون احدى الخطوط بيفقد 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.



الآن سنقوم بعمل Rule لتحديد الـ interface الأفضل للخروج منه بحسب SLA=INTERNET التي قمنا بإنشائها سابقا

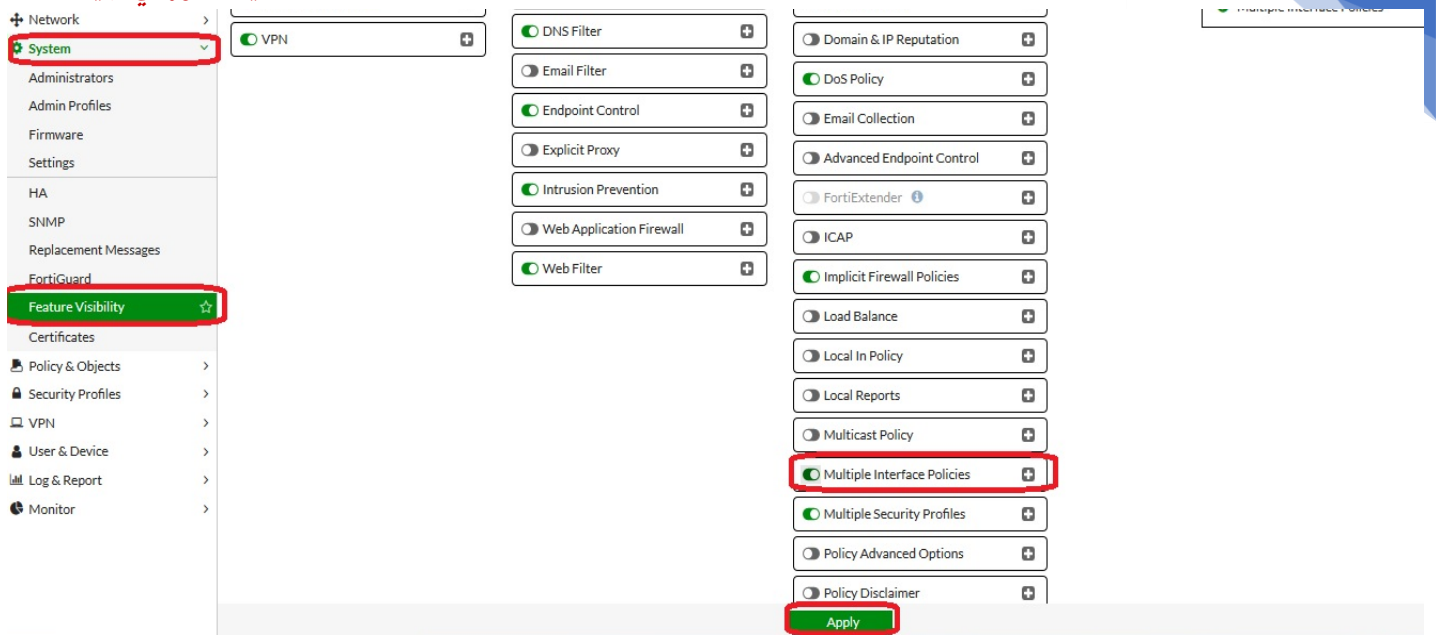




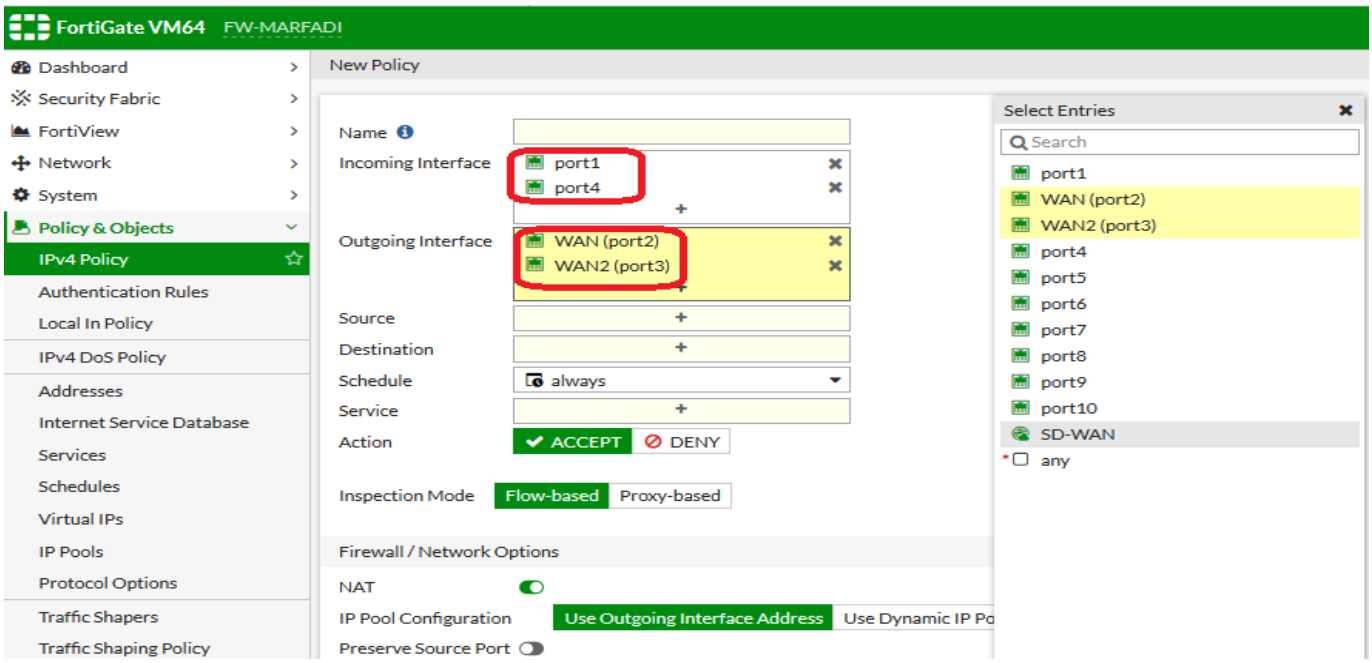
❖ طريقة اظهار ميزه جديده مثلا تريد اظهار الخاصية(features)

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 .



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



❖ طريقة انشاء Rule policy جديده :

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

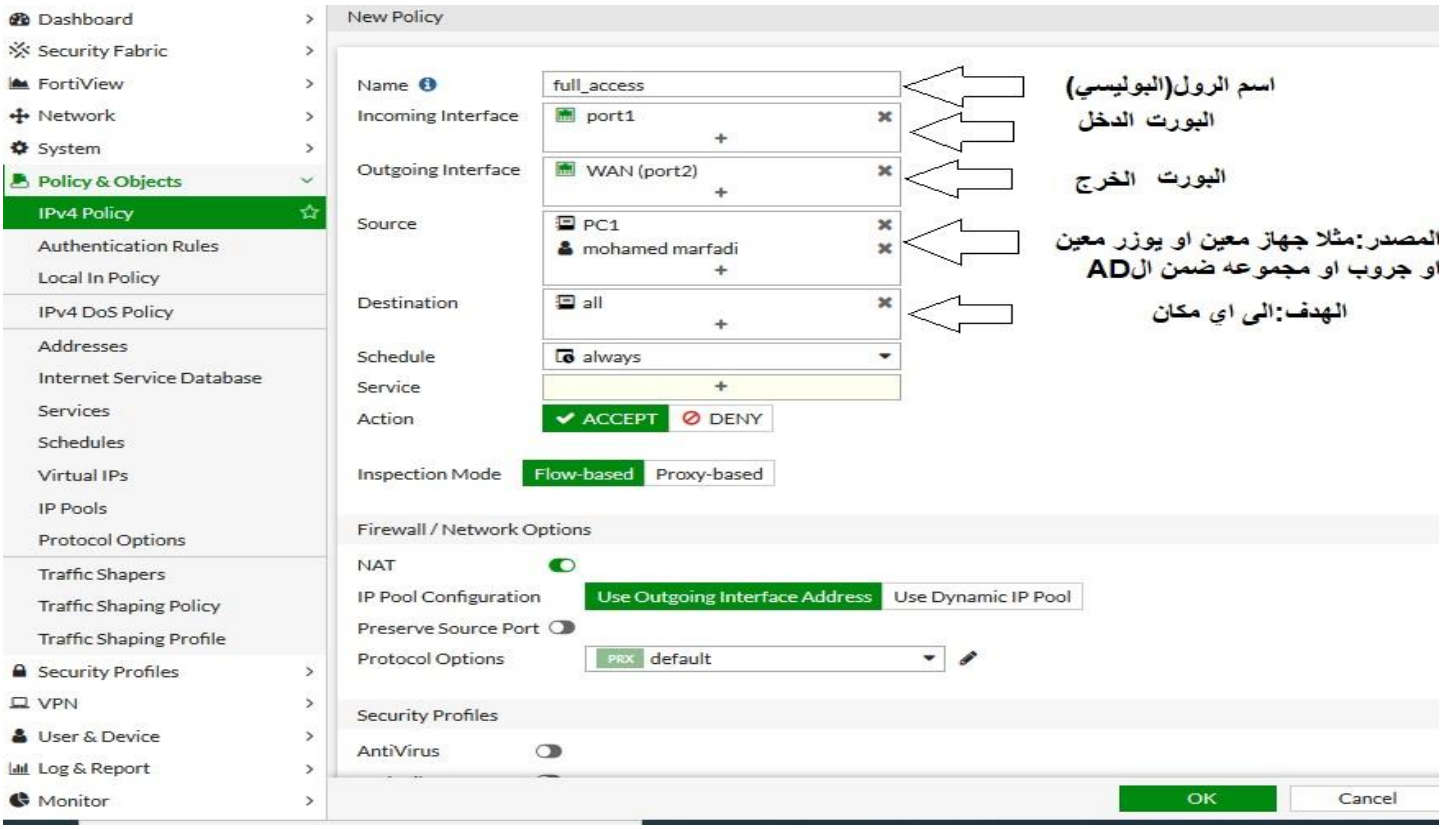
المصدر:

Address : ip،subnet،

User : ممكن يكون يوزرعادي على الفورتي جيت او يوزرعلى الدومين(AD)

Device :ربط جهازبواسطة الماك ادرس

الى أي مكان Destination :all



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

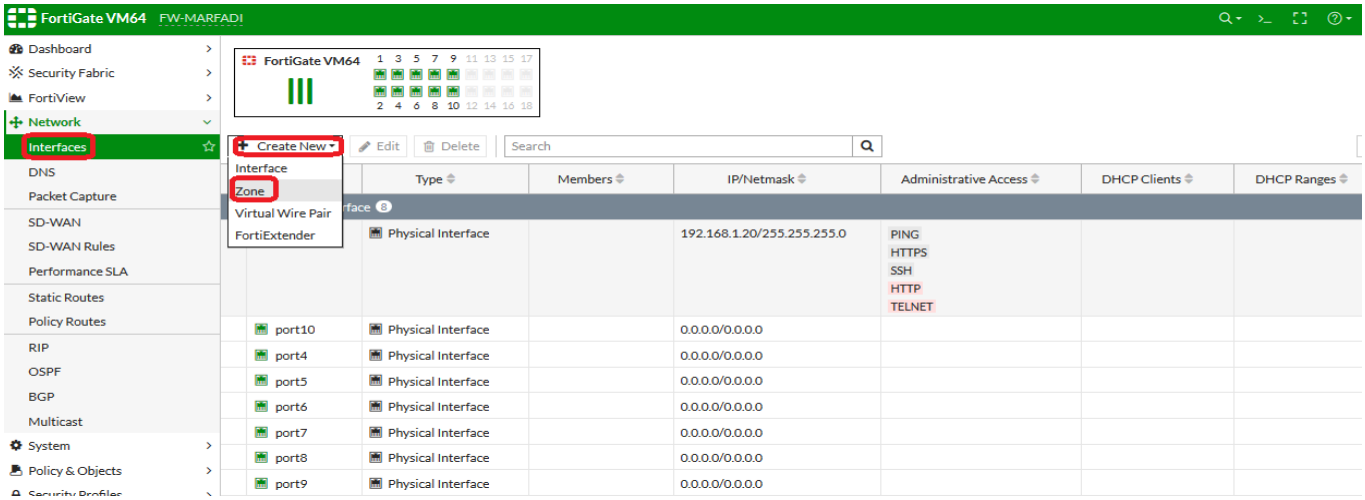
Port1 والخارج عبر wan(port2) ويطبق فقط على جهاز الكمبيوتر المسمى pc1 وهذا تم انشاءه مسبقا

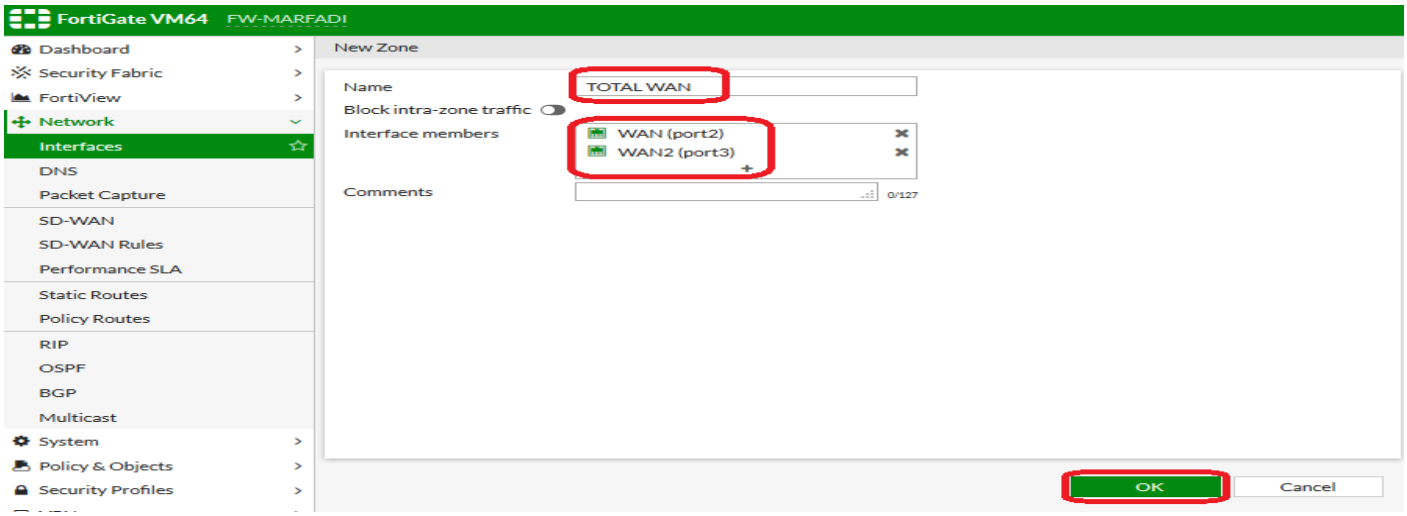
،والى أي مكان (all) ..

طريقة جمع (دمج)اكثرمن منفذ (interface) لكي يصبحوا logical interface واحد وذلك بواسطة الـ zone :

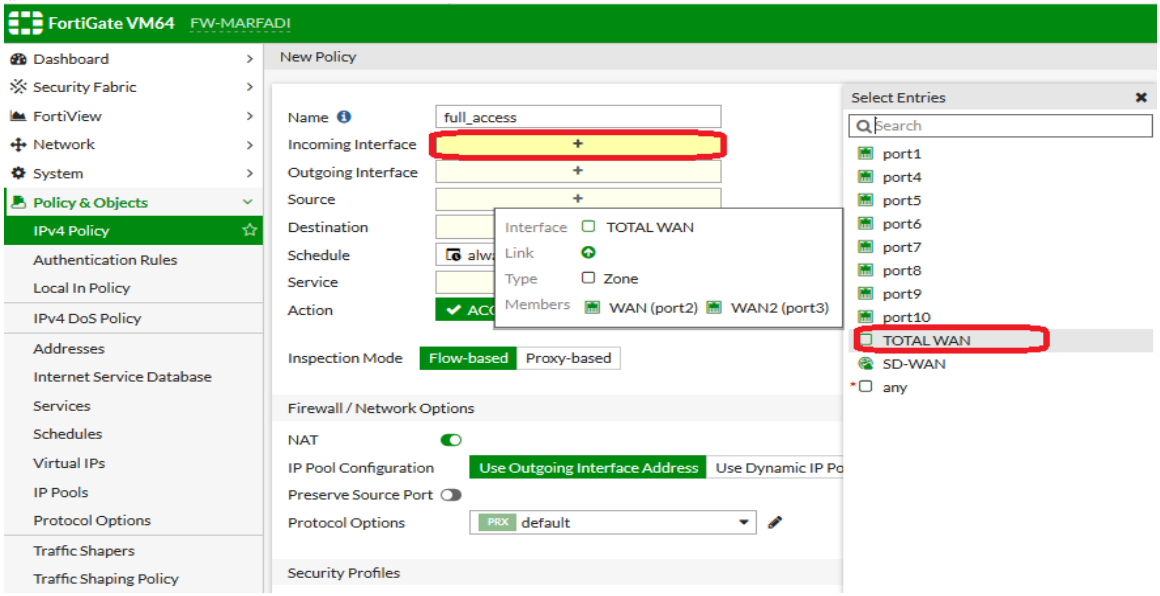
Network>interface>Create New>Zone>Name:أي اسم تريد

OK> نختار المنافذ المراد دمجها : Interface member>





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



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

شرح Schedule:

أنواع الـ schedule:

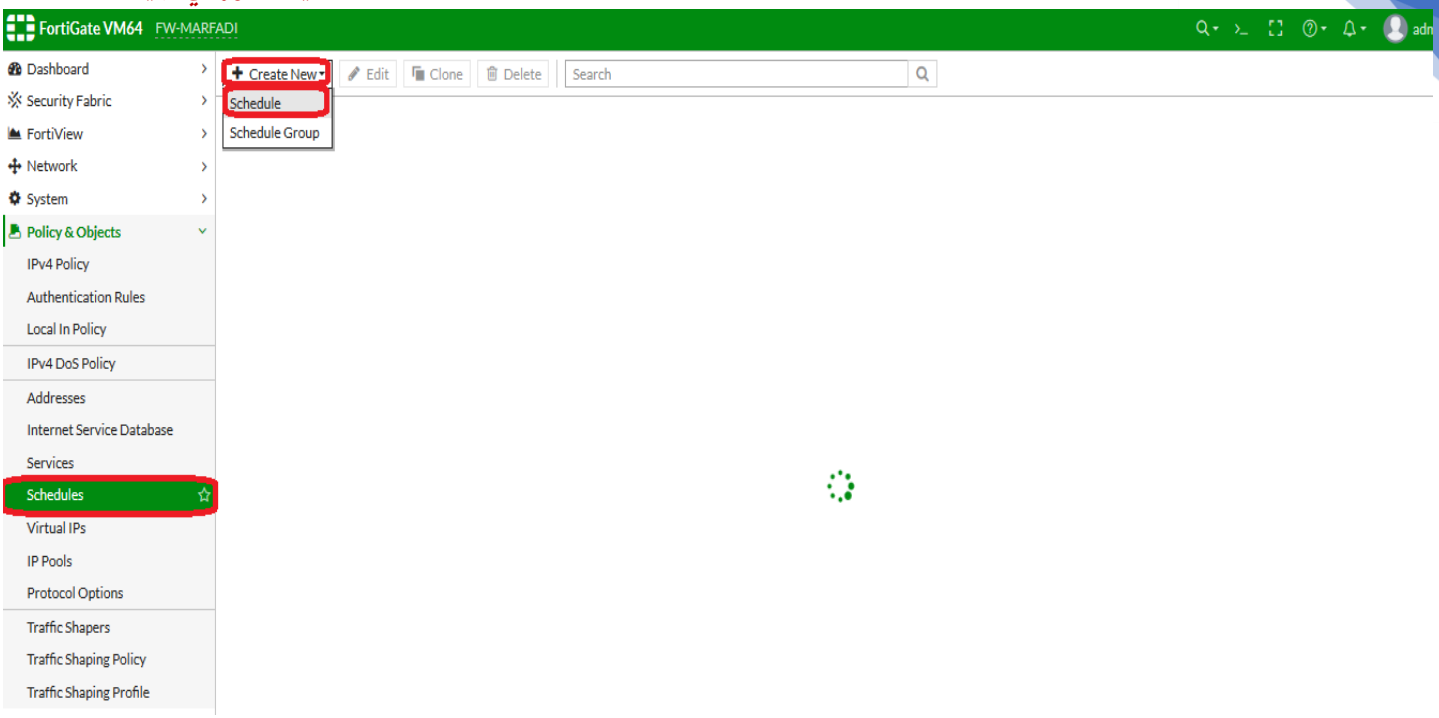
١- Onetime schedule : يتم تنفيذها مره واحده فقط ثم تلتغي .

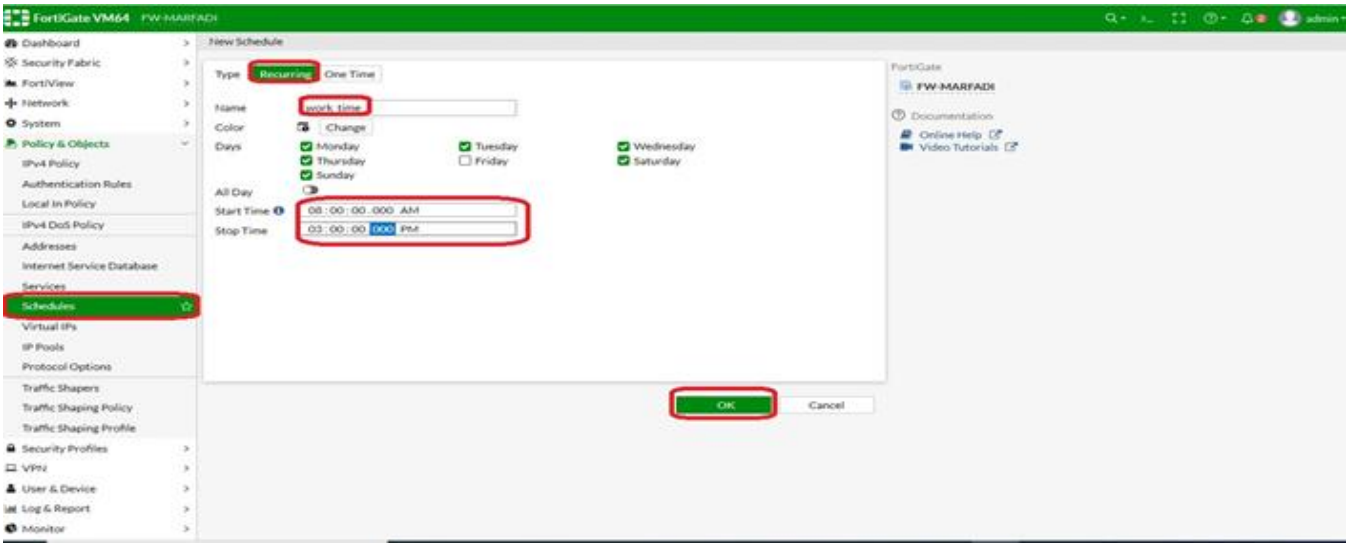
٢- Recurring schedule :يتم تنفيذها بشكل مستمر

❖ طريقة انشاء schedule :

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

>Name:أي اسم تريده >Days:تختار الأيام المطلوبة

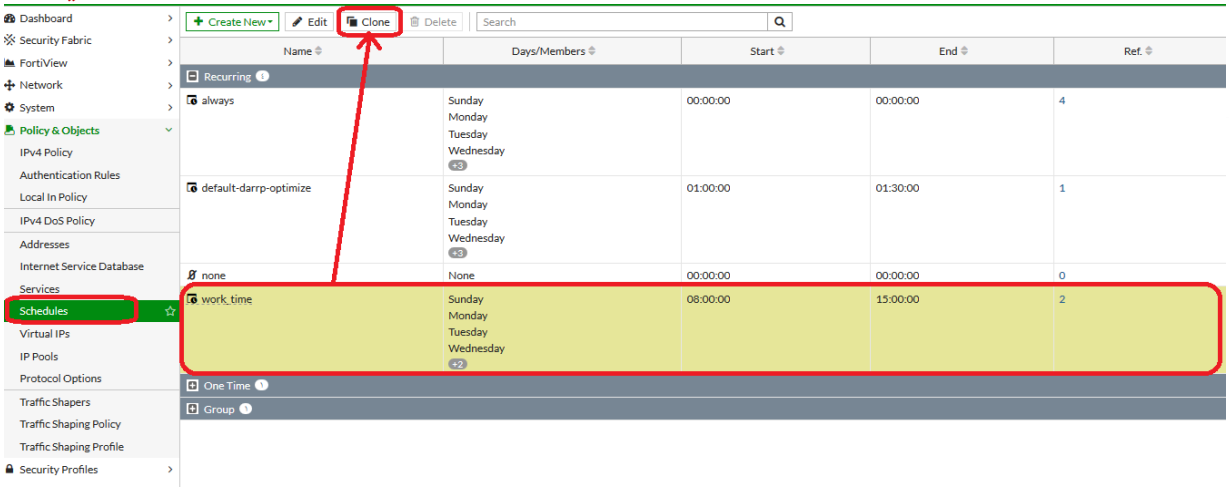




نحدد START TIME و Stop Time ...

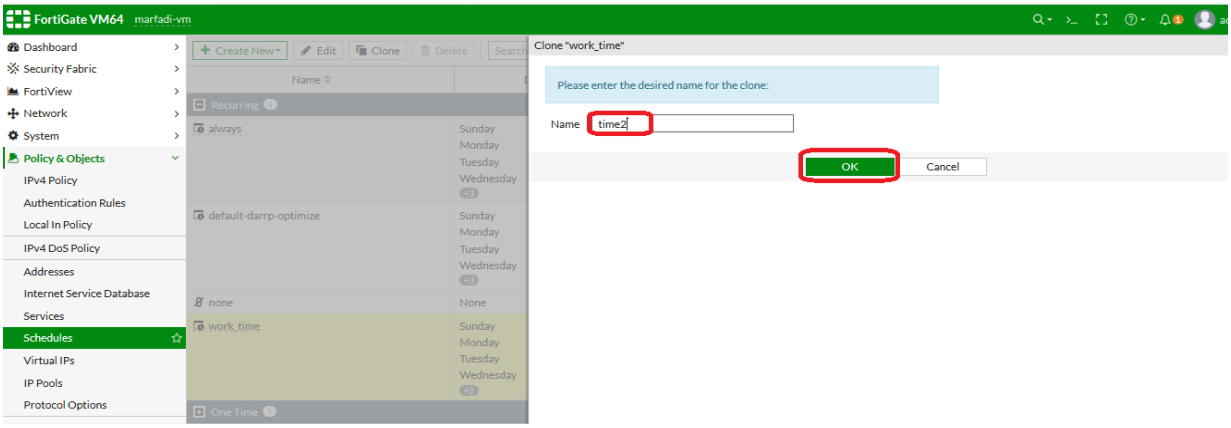
تم تحديد اسم لـ schedule باسم Work_time وتم تحديد أيام العمل والوقت .

- عمليه تكرار schedule معين :

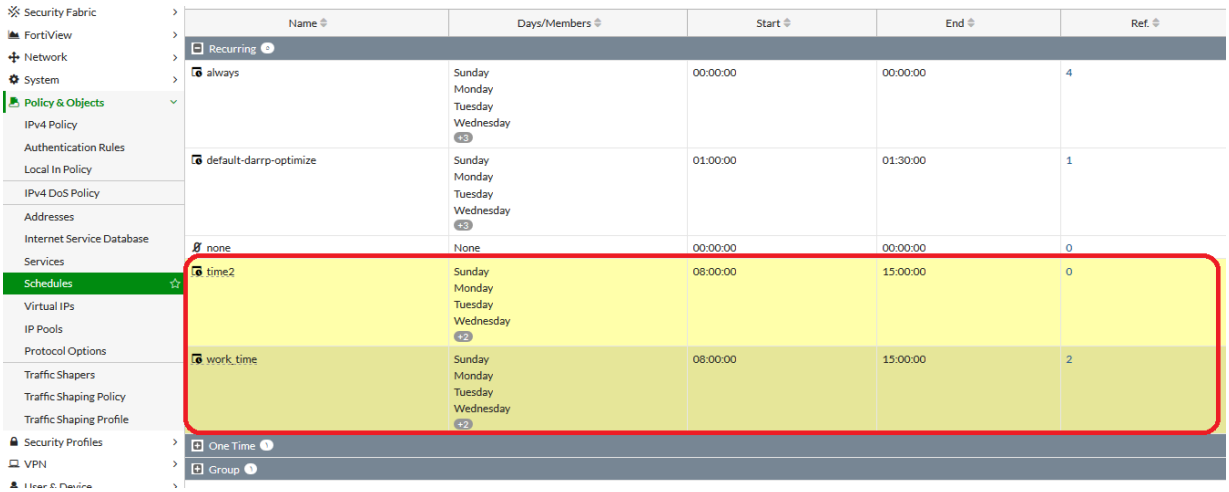


مثلا اريد انسخ نفس الاعدادات والاوقات لـwork_time وانشائها في schedule جديده مثلا باسم time2 مثلا

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



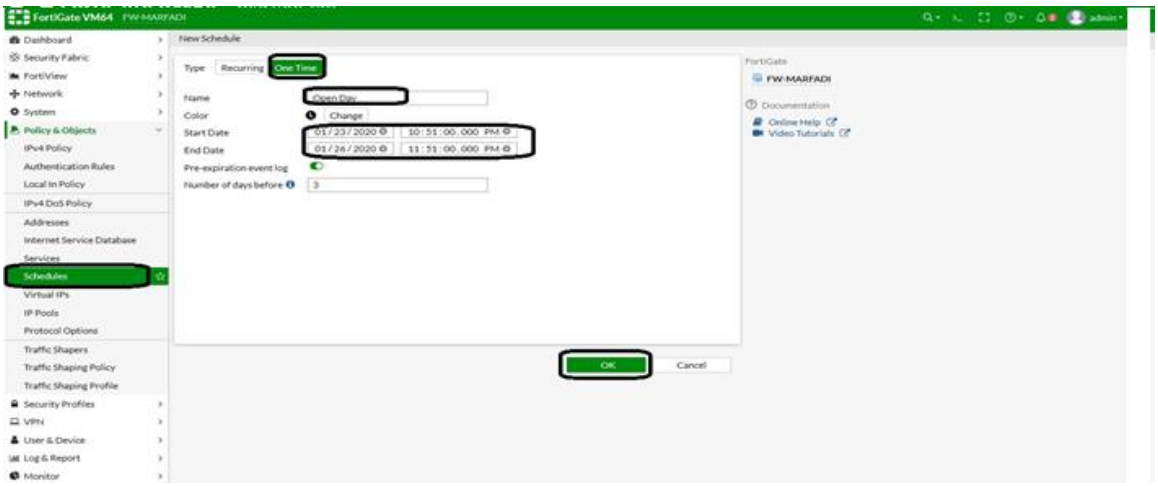
فقط قمنا بكتابه اسم الـschedule الجديد باسم time2 ونلاحظ بان الأوقات والأيام كما في الـwork_time كما بالصورة ادناه

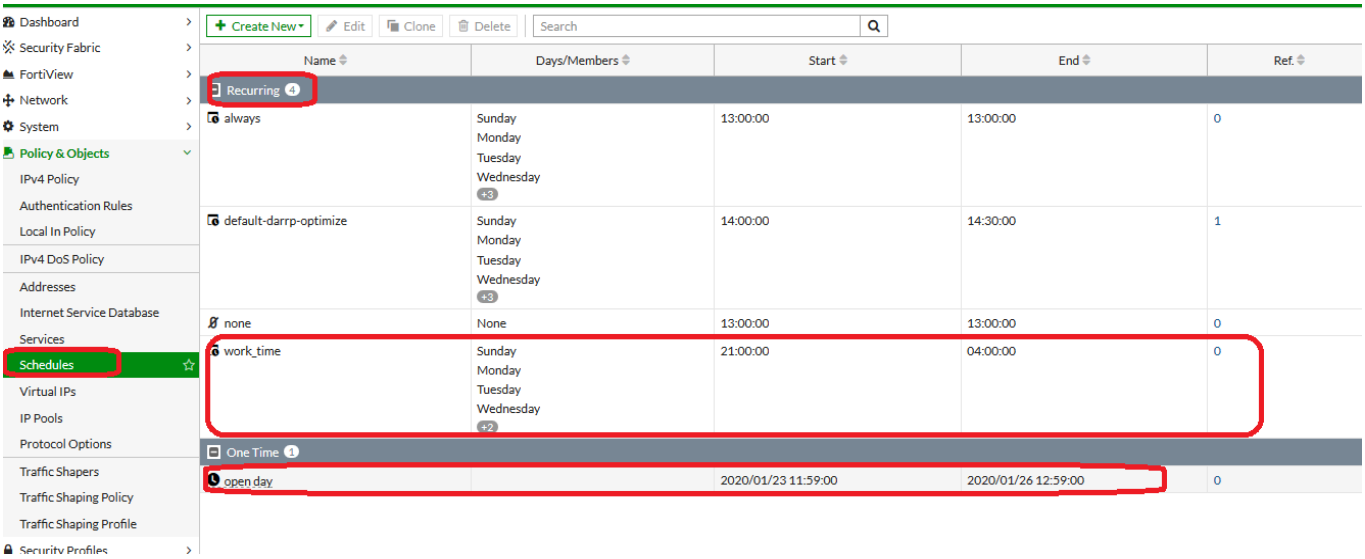


*** **** *** **

❖ تحديد أيام محدده ووقت محدد مره واحده فقط وينتهي ...

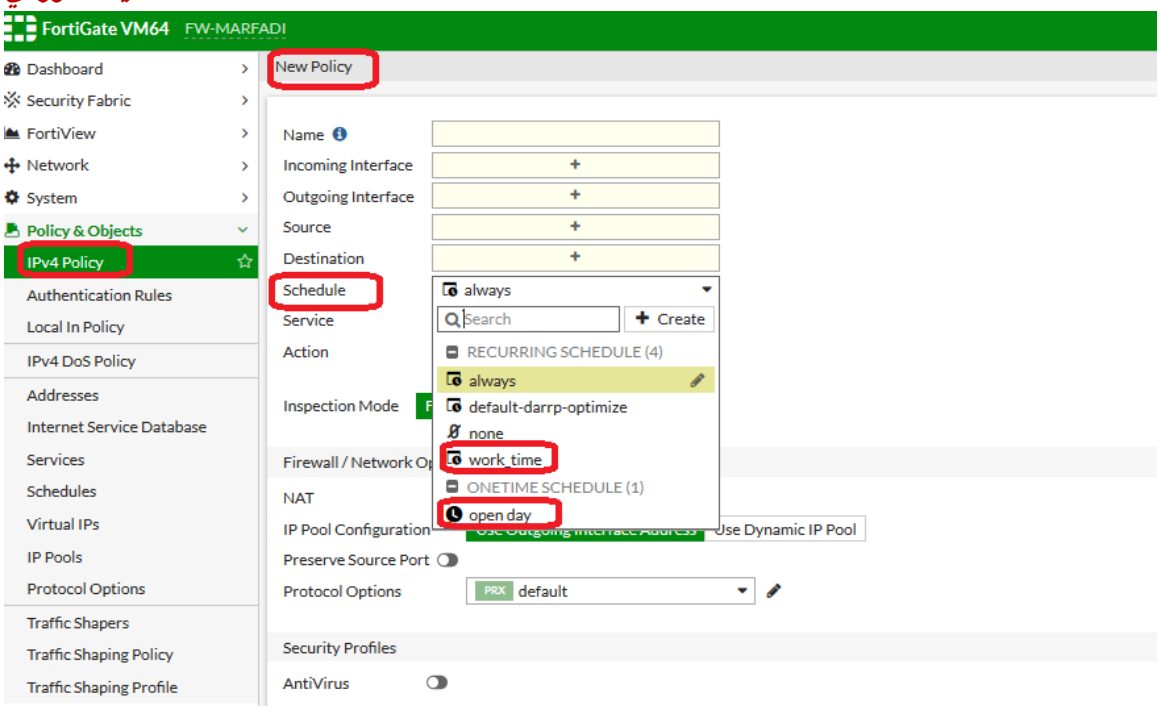
- ❖ Policy&objects>schedules>Create New>schedule >type: Onetime>
- ❖ بداية الوقت:start time: بداية التاريخ : start date> أي اسم تريده:Name>
- ❖ نهاية الوقت: stop time> نهاية التاريخ> stop date>





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

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



❖ أنواع الـــ actions في الـــ policy :

١- Accept : الموافقة وتمرير الباكت (الترافيك)

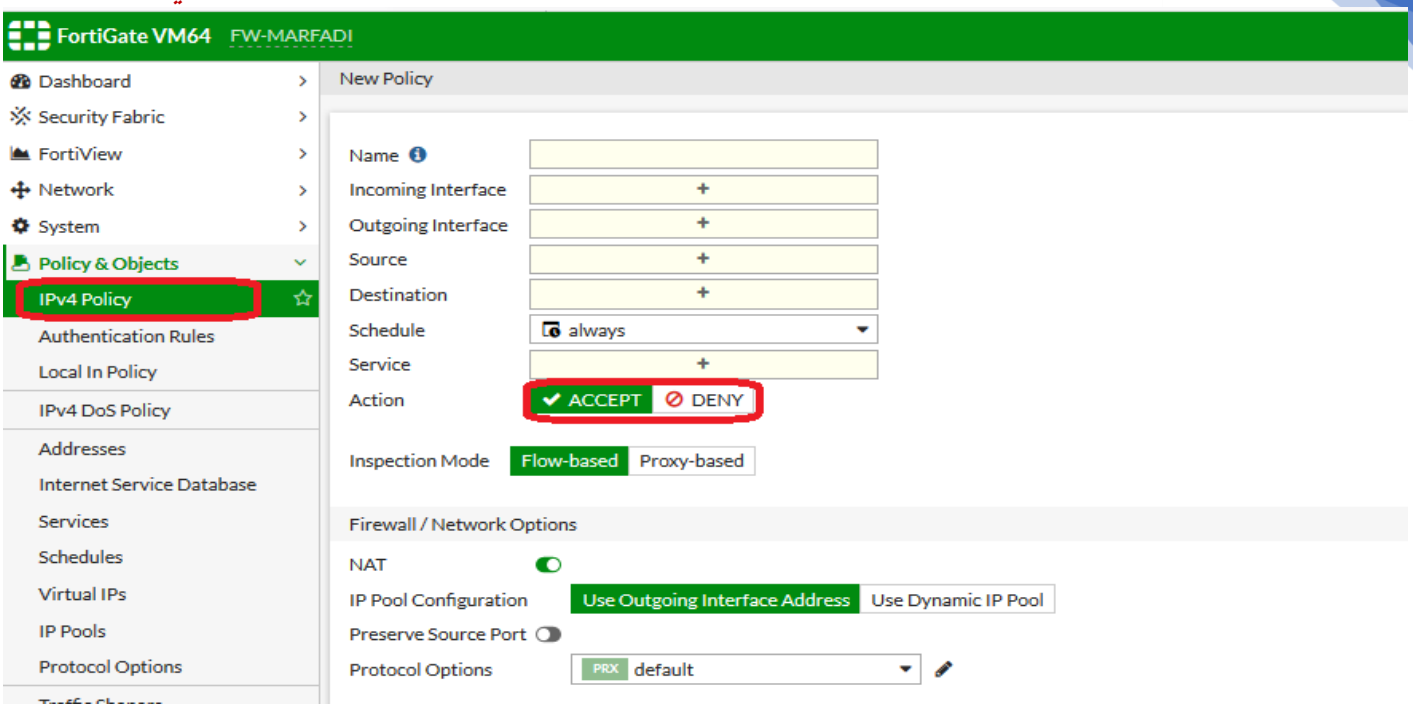
٢- Deny : منع مرور الباكت drop

حيث في الإصدارات القديمة يوجد نوع ثالث وهو learn

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

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

Log&reports>learning report>



❖ Traffic shapers :

هو عباره عن عمليه تحديد الـ Bandwidth .

أنواع ال traffic shapers :

١- Per-ip traffic shaper

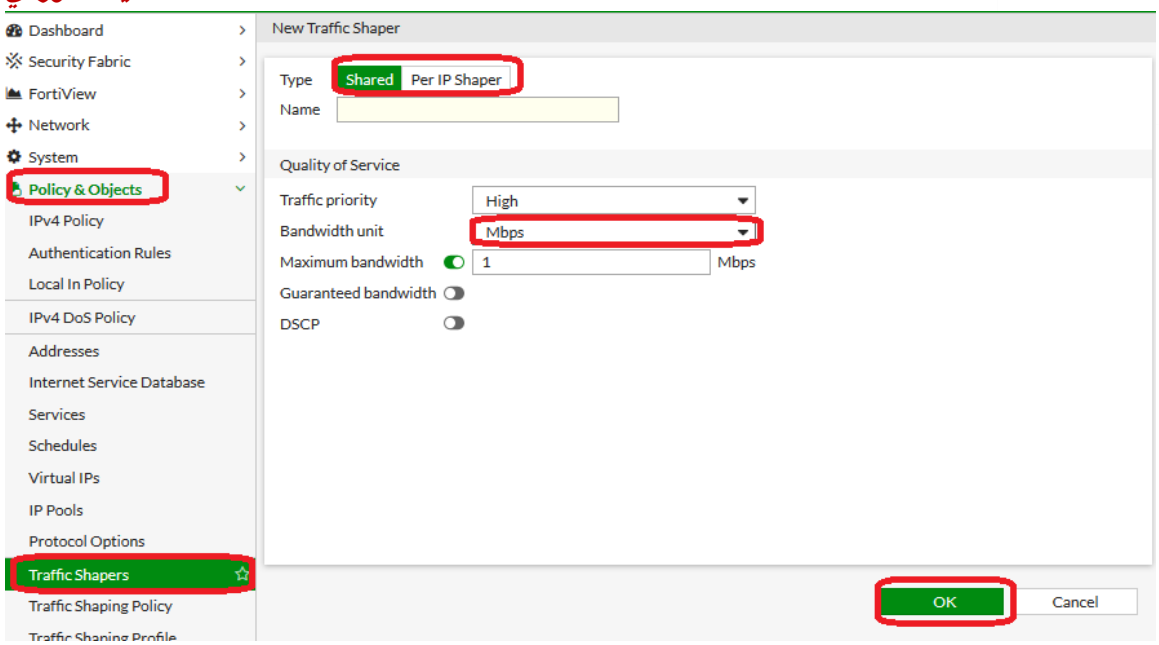
تحديد مثلا 5 ميجا لكل جهاز او ايبي حيث يكون سرعه هذا الجهاز هو 5 ميجا .

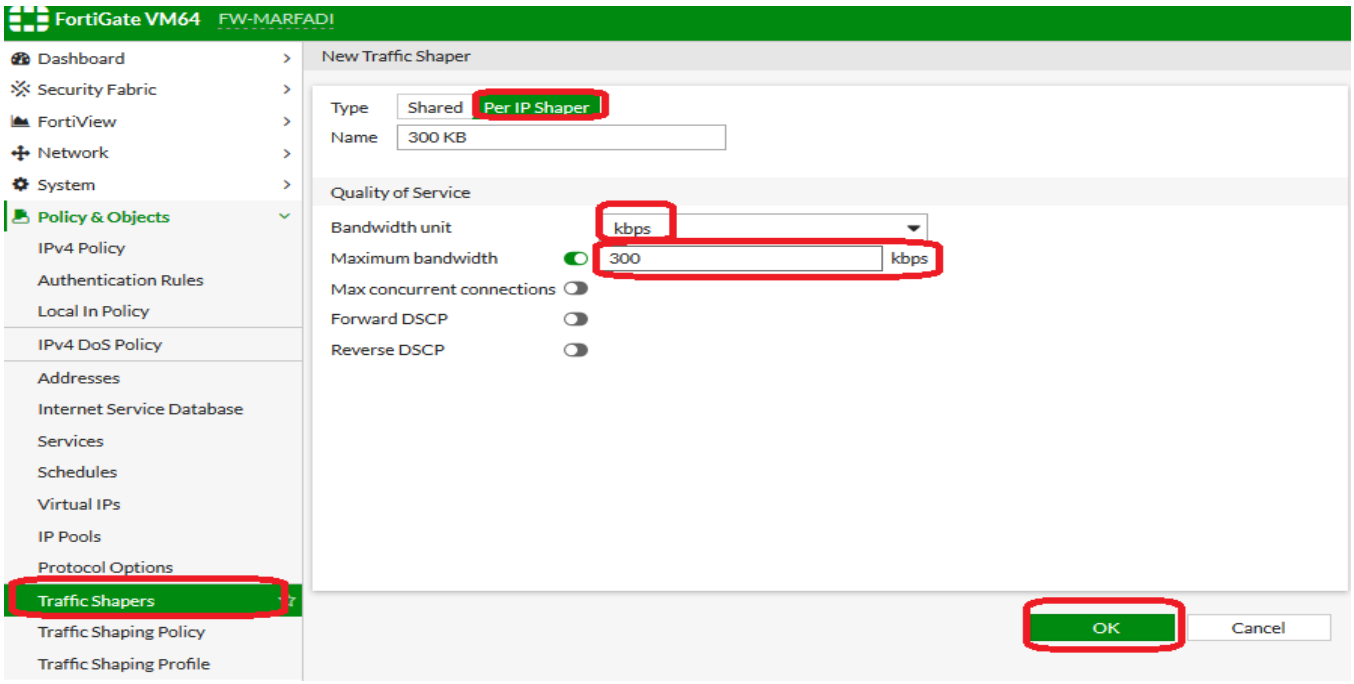
٢- Shared traffic shaper :

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

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

>





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

❖ APPLICATION CONTROL

هو عباره عن عمليه تحكم ومراقبه لكل التطبيقات التي سيتم تشغيلها على الشقrبكه

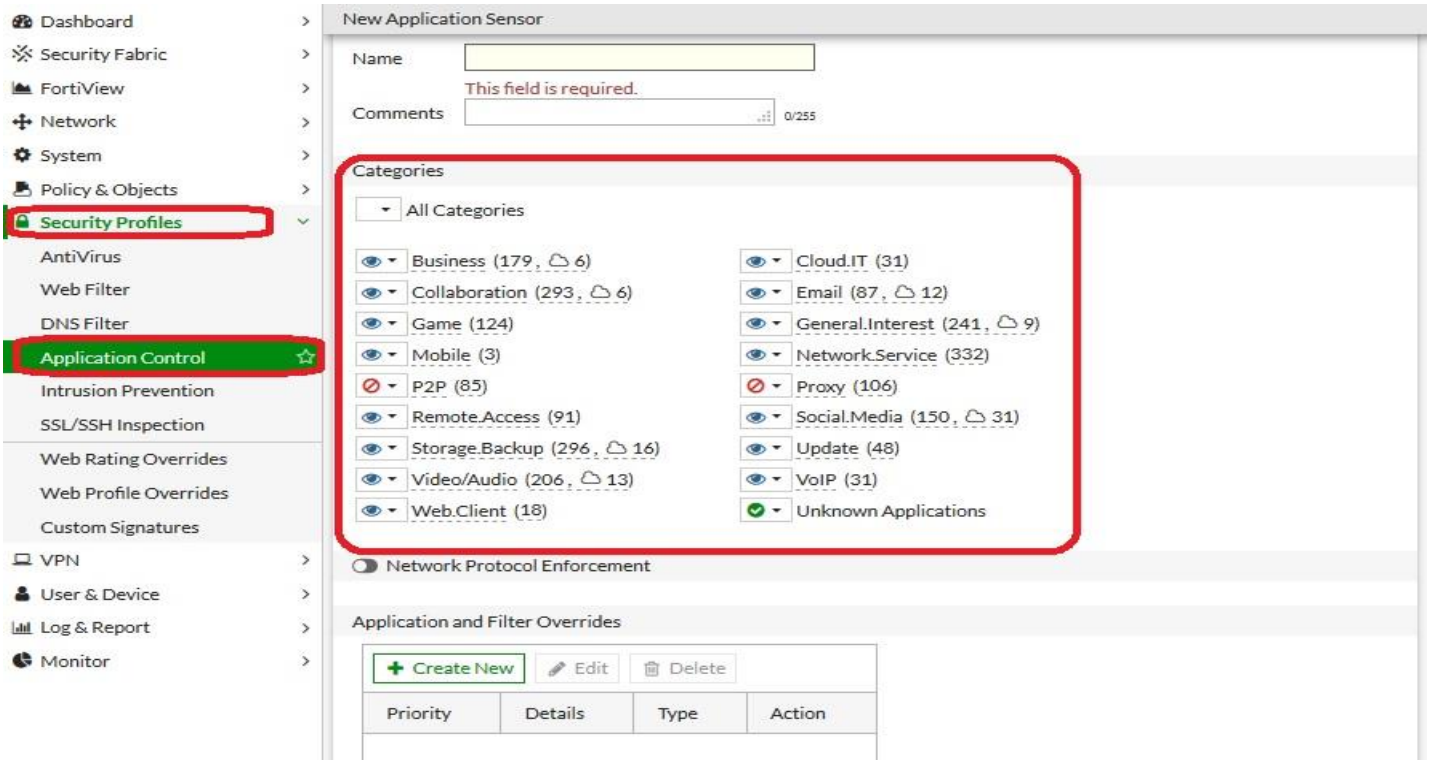
مثلا(فيسوك،يوتيوب،جوجل ...)حيث عن طريق APP CONTROL ممكن اقلل من استهلاك الانترنت او من الثغرات المتواجدة في تلك التطبيقات .

Application control مقسم الى ثلاث اقسام :

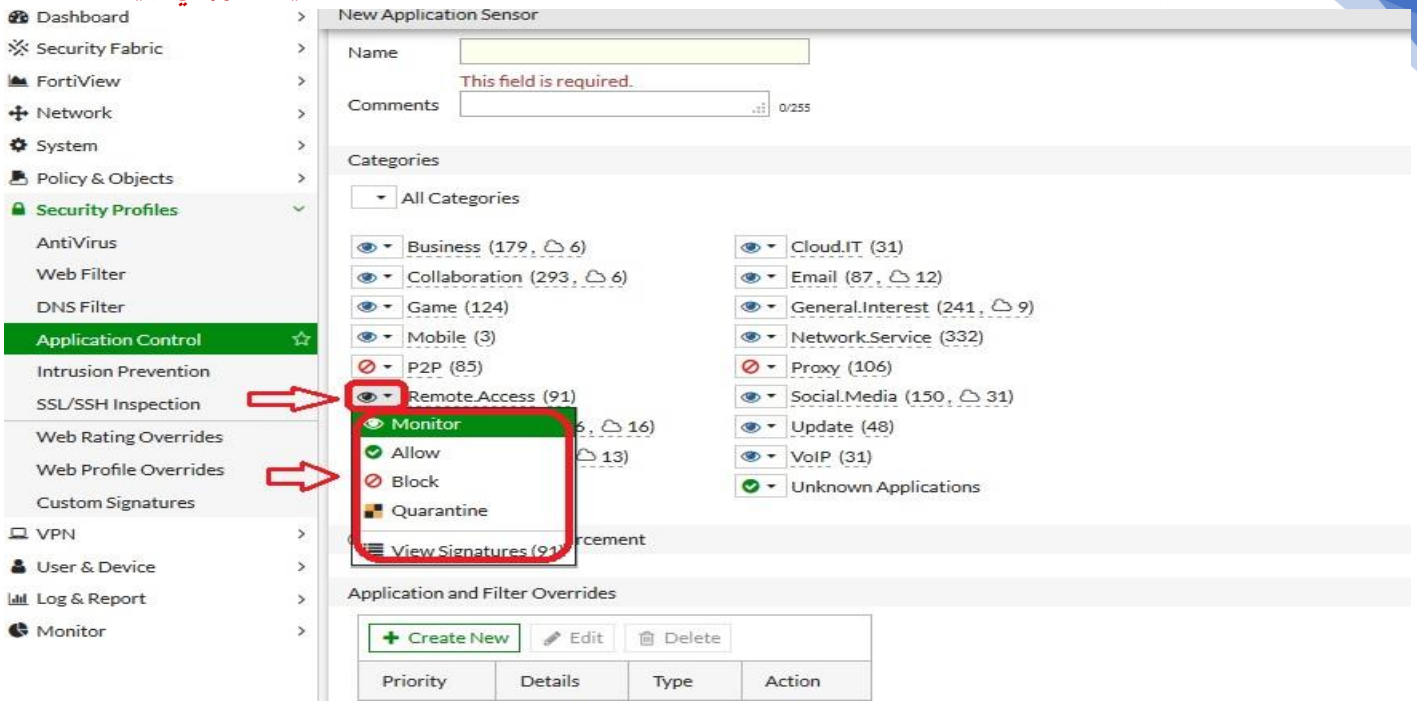
١- Categories :تحتوي على قوائم(تصنيفات)مقسمه بحسب النوع ..

حيث كمجموعة برامج(تطبيقات)يتم وضعها في التصنيف الخاص به مثلا تطبيقات الألعاب تكون مصنفه تحت games category ،وتطبيقات البروكسي وال vpn تحت التصنيف proxy category

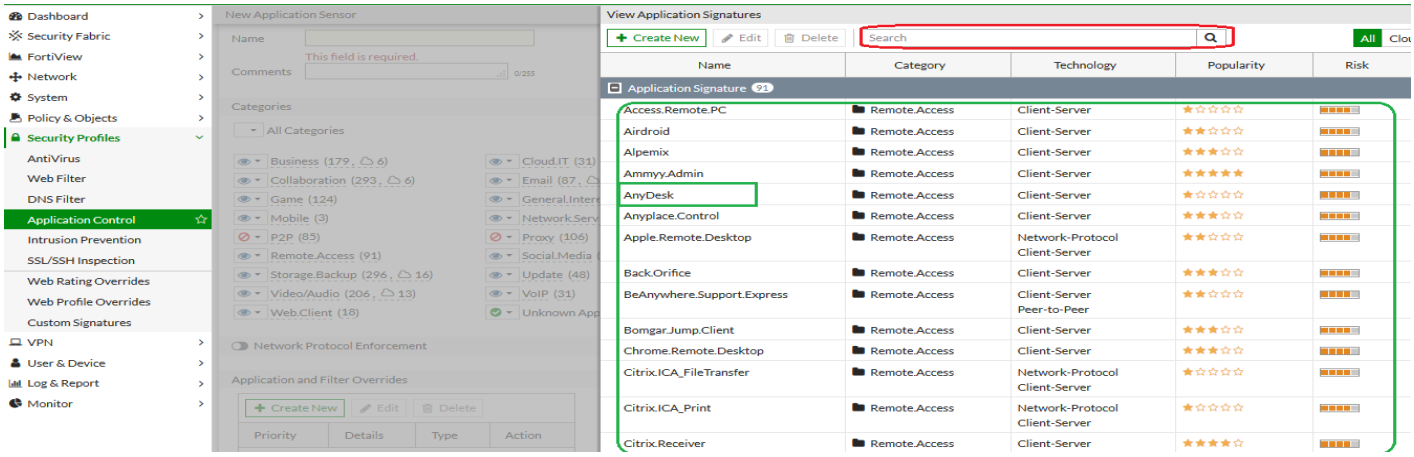
حيث ممكن ان تقوم لهذا التصنيف الـ action المناسب اما allow او Monitor او Block او quarantine و View signature ...



حيث يمكنك اختيار التصنيف المناسب للبروفايل المراد إنشاؤه ...



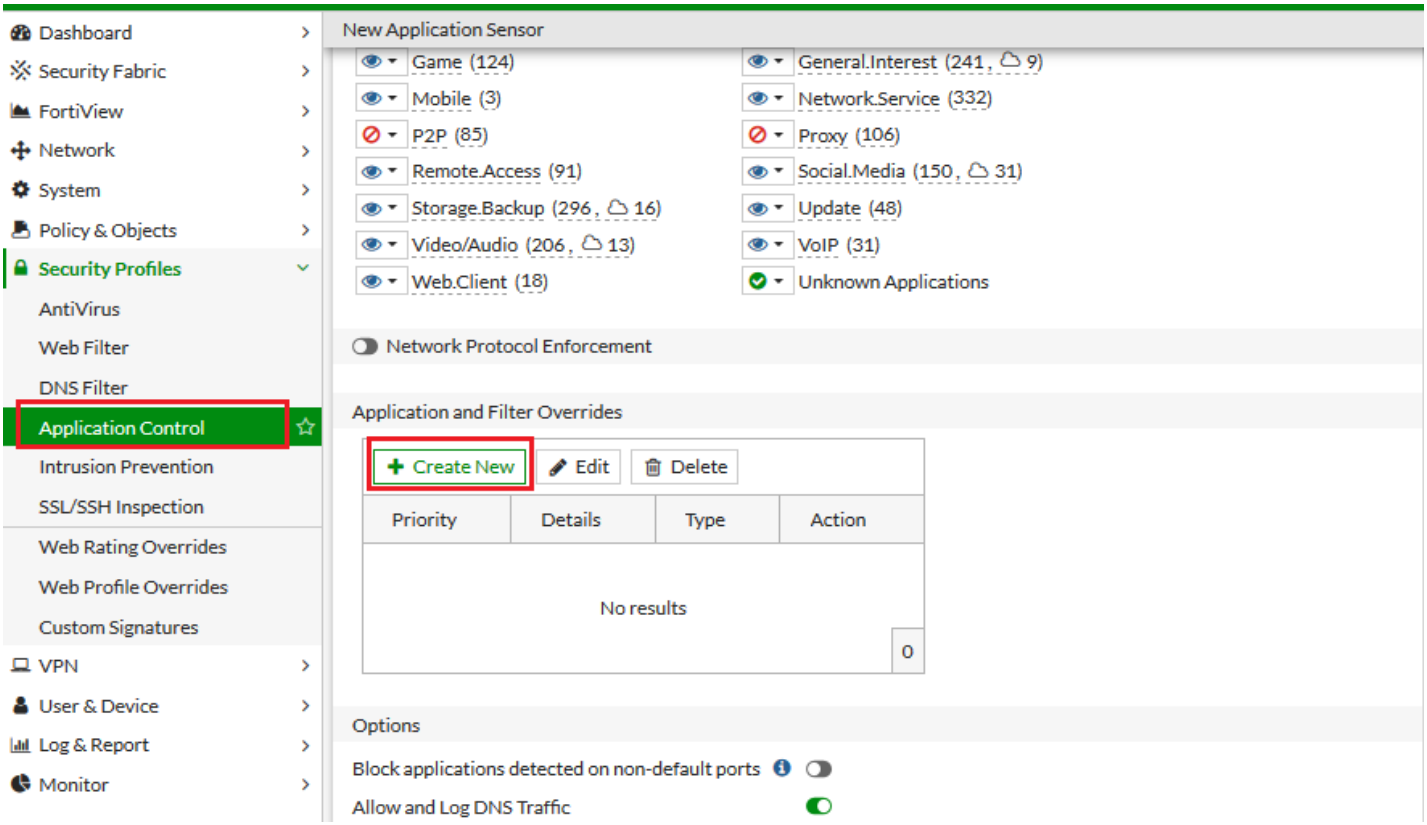
كما بالصورة أعلاه يمكنك اختيار الaction المناسب للتصنيف ... فأذا اردت مثلا معرفة على ماذا يحتوي هذا التصنيف فتقوم باختيار الخيار View Signatures وسوف تظهر لك البرامج التي تنتمي لهذا التصنيف ..



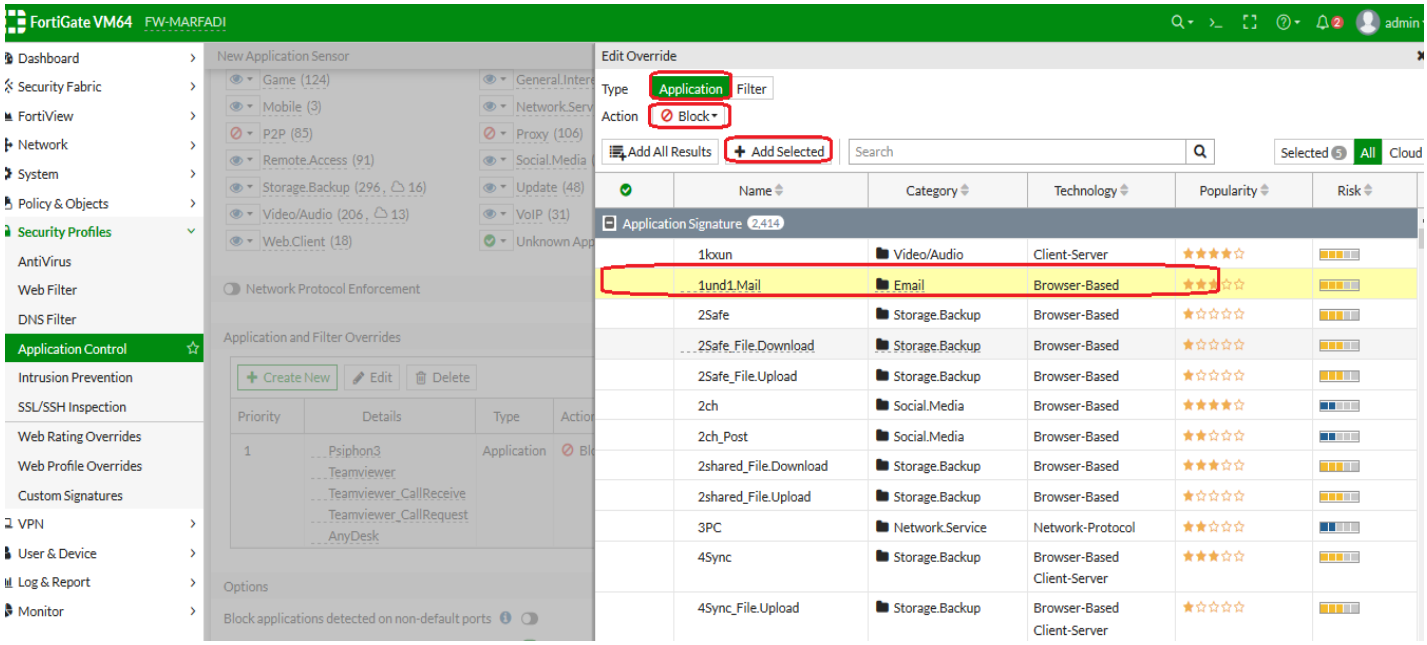
حيث ممكن البحث عن برنامج معين لتعرف هل ينتمي لهذا التصنيف وذلك عبر كتابه البرنامج في خانه search ثم الEnter لتظهر النتائج ...

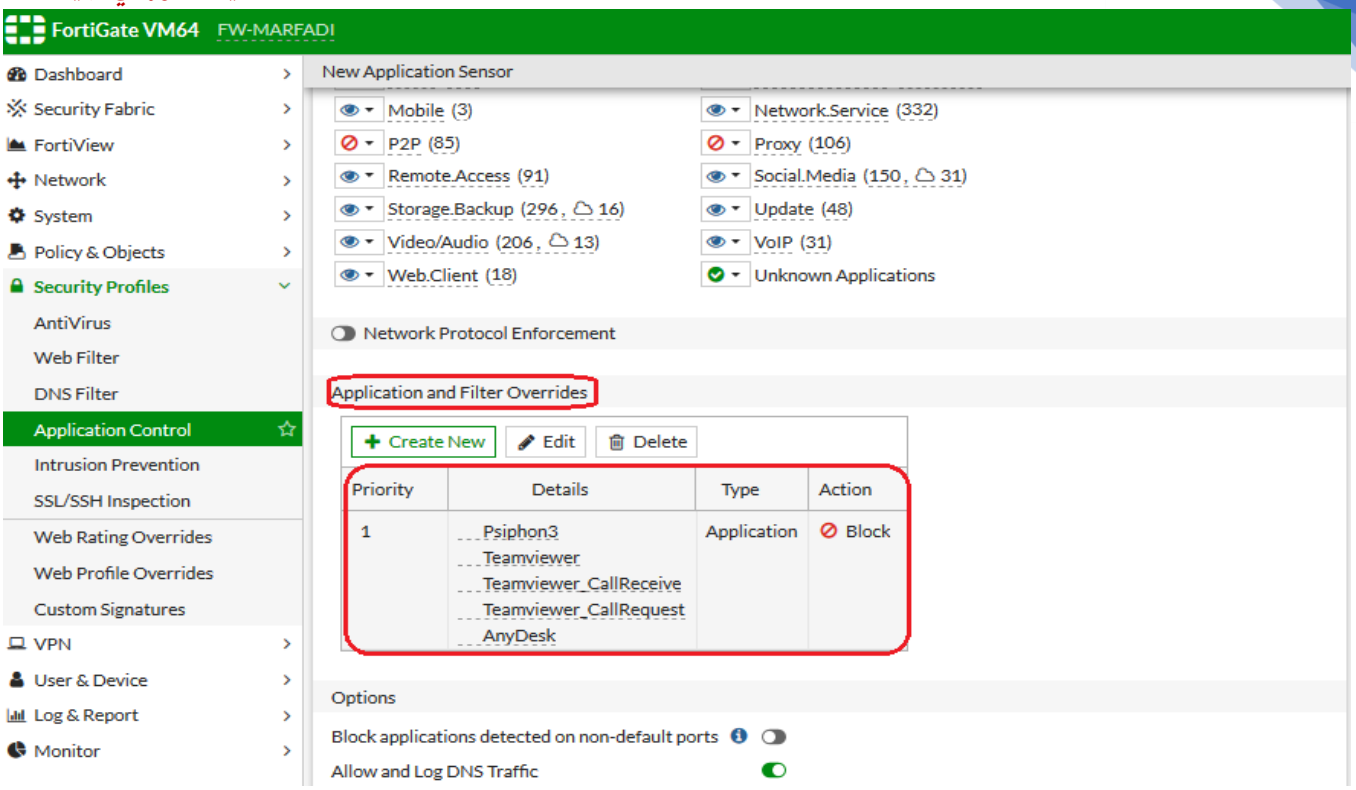
٢- Application overrides : ممكن بواسطته ان امنع او اسمح لتطبيقات معينه بعكس الخيار الأول الذي لا يمكنني ان اختار تطبيقات معينه بتصنيف معين ..

حيث في الخيار الأول اما اختار التصنيف كاملا او لا ...



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





نلاحظ كما بالصورة أعلاه تم اختيار تطبيقات معينه مثل Psiphon3 وTeamViewer وanydesk والـaction 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 بروفايل واحد فأنه يتم أولا تطبيق حسب الأولوية

١- Application overrides

٢- Filter overrides

٣- Categories

مثلا لو قمنا بالسماح لتطبيق الAnydesk في الخيار Categories

وبنفس البروفايل قمت بمنع التطبيق نفسه في الخيار Application overrides فأنه سوف يتم تطبيق المنع لهذا التطبيق لأن الأولوية لـ application override عن Categories .

ال ACTION :

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 فورتي جيت سوف يقوم بعمل ban (حظر)لهذا الايبي حيث بعدها لن يستطيع هذا الايبي ان يطلع انترنت لمده معينه يتم تحديدها مسبقا ..

٥- View Signature :معرفة التوقيع لهذا التنصيف

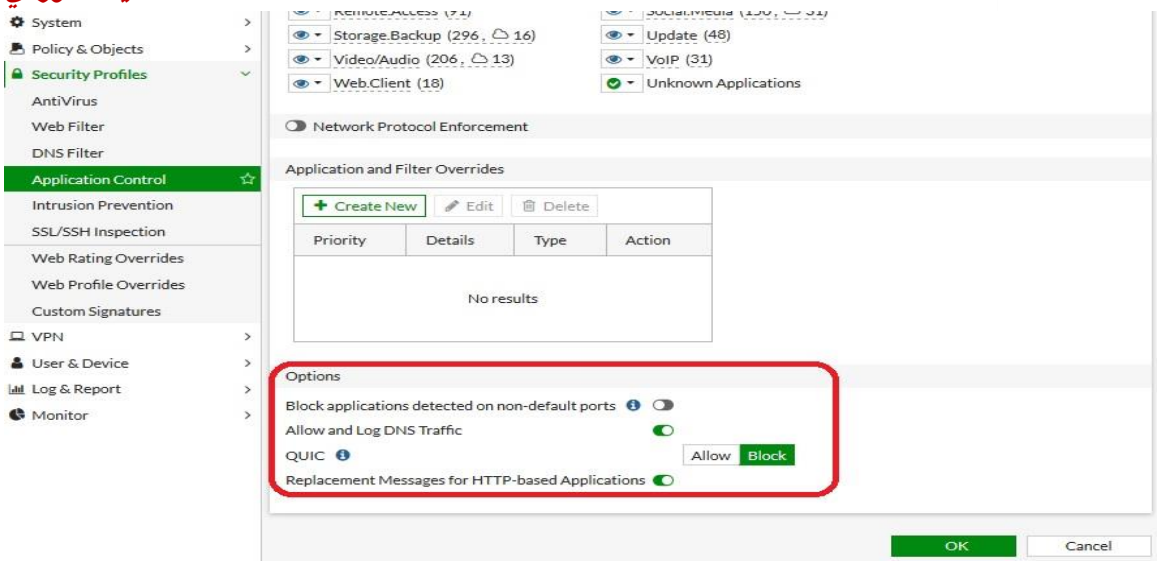
هناك بعض الخيارات :

١- Allow and log DNS traffic :

ينصح بتفعيله في بداية مرحله 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).



❖ Web Filter

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

❖ ما هو الـــfortiguard :

هي عباره عن اشتراك يتم ما بين الفورتي جيت و الفورتي جارد تيم من خلاله تم تقسيم URL الى مجموعات ،

بحيث تتم عمليه التقسيم عندما يقوم صاحب الموقع بإنشاء موقعه فأنه ملزم بأن يقوم بتصنيف الموقع هل سياسي اورياضي او...الخ

أيضا توجد خوارزميات في الفورتي جارد تعمل على تصنيف الـURL على حسب محتوى الموقع نفسه ...

❖ ماهي فكره الـــ Fortiguard ؟

عندما اليوزريطلب موقع مثل www.facebook.com فأن جهاز الفورتي جيت يرسل طلب الى الفورتي جارد لمعرفة تصنيف هذا الموقع وبعد ذلك يتم تخزينه(cache)على جهاز الفورتي جيت ..

بحيث لو قام يوزر اخر بطلب نفس الموقع فلا يحتاج الى عمل طلب الى الفورتي جارد ..

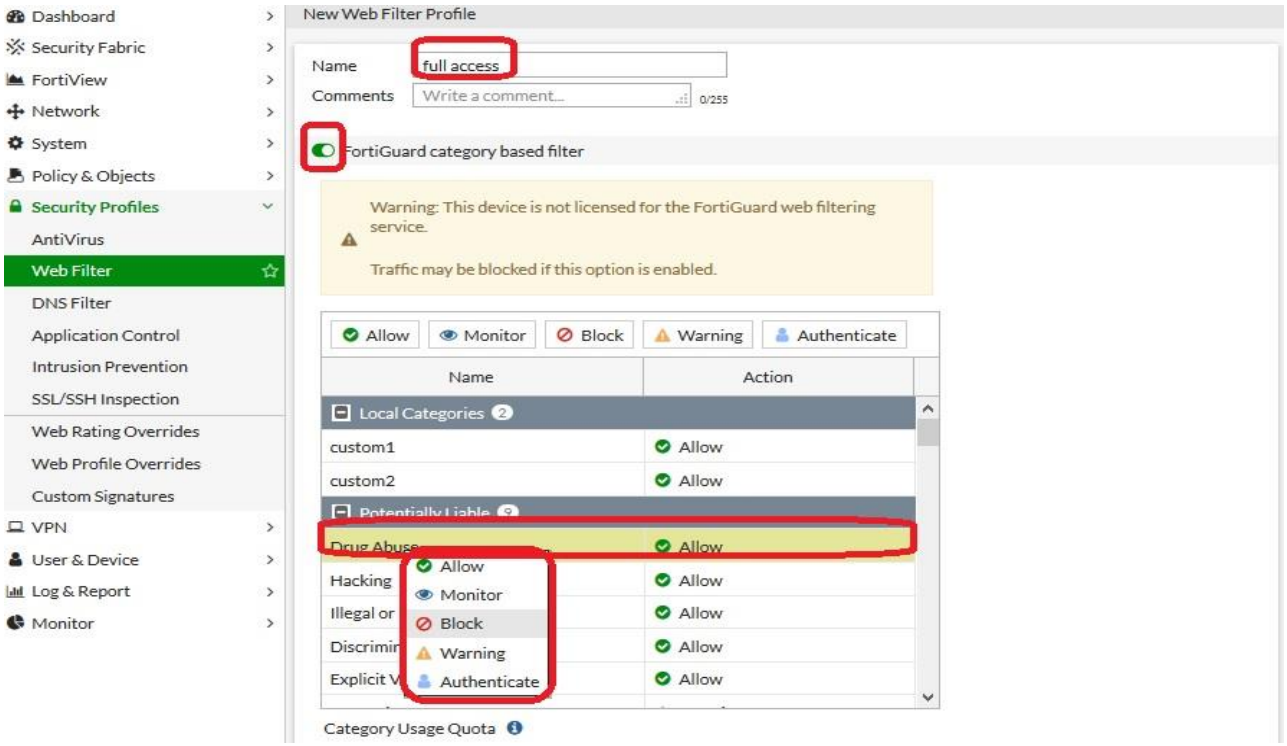
حيث بعد ما يحصل جهاز الفورتي على تصنيف الموقع فأنه يعمل له action المناسب ...

❖ طريقة انشاء web filter profile :

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

>fortiguard category based filter:enabled

حيث نحدد التصنيف(category)ثم بالزر الأيمن عليها ثم نختار الaction 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 و أضافته 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

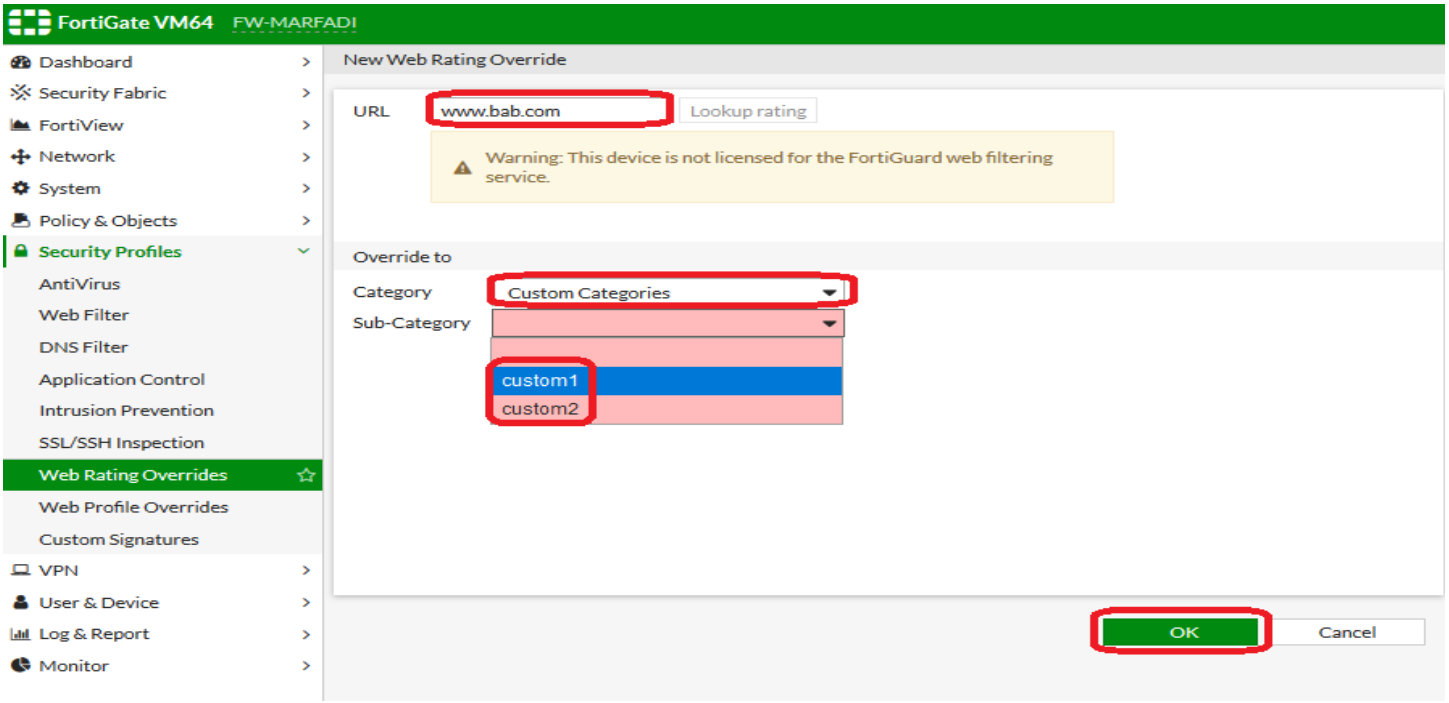
Override to :

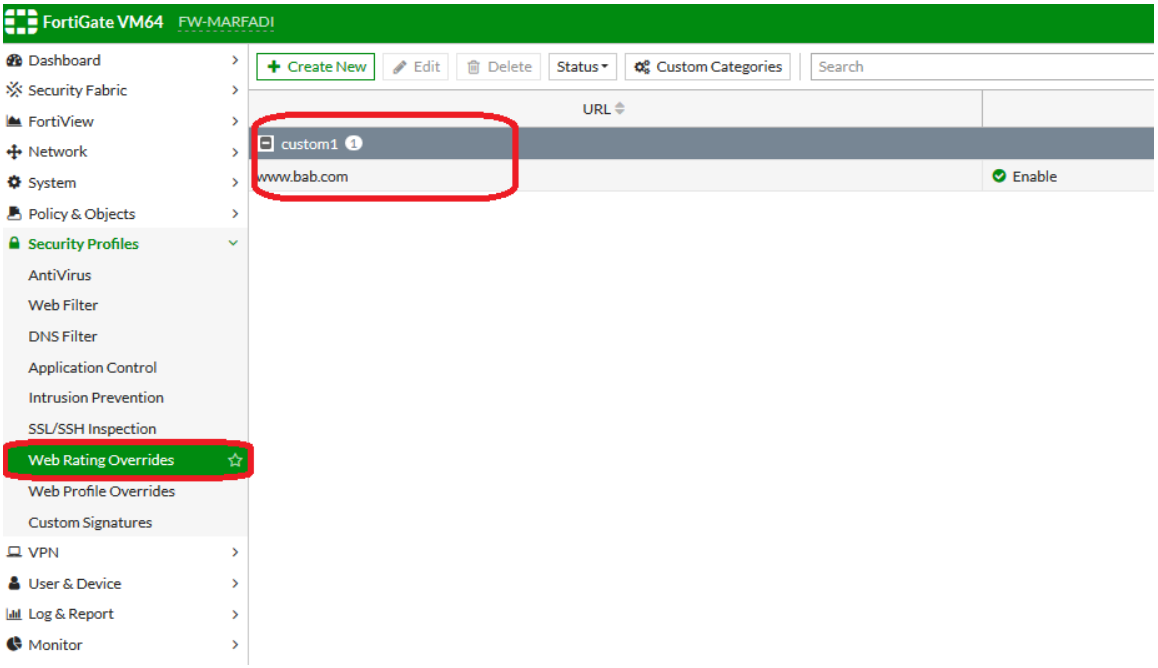
Category: custom category

Sub category: custom 1

ok

كما بالصورة ادناه ....





ثم نذهب الى

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

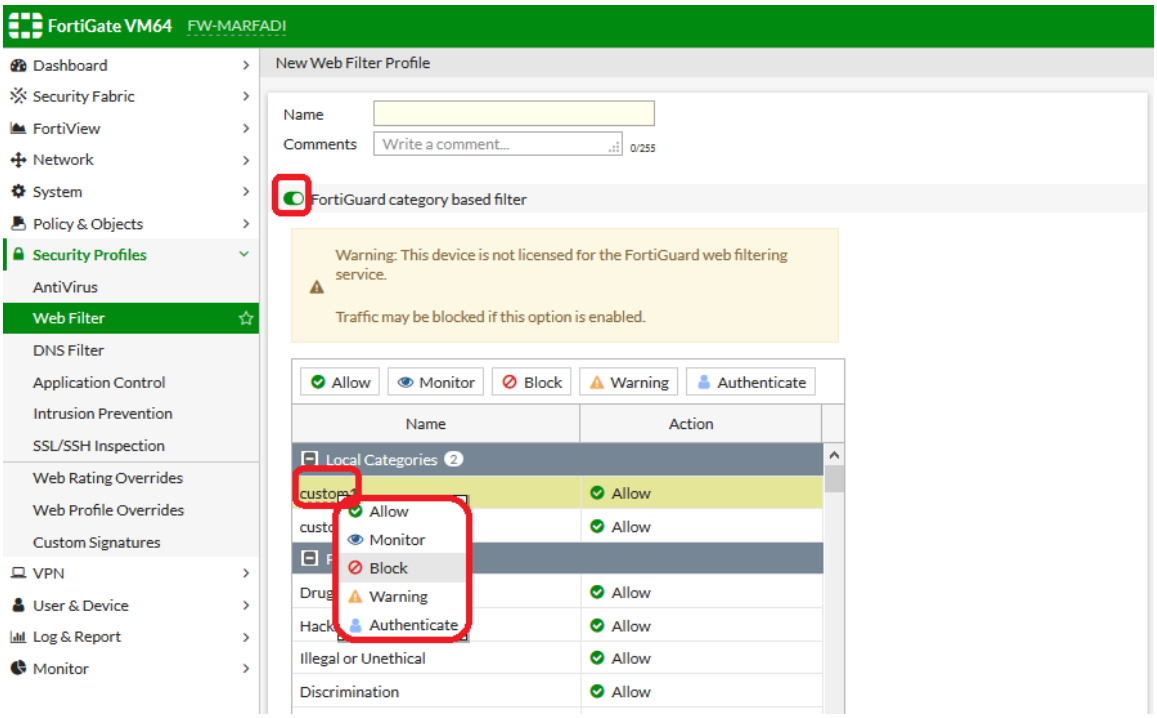
Local categories>نختار ثمcustom 1

حيث ننقر بالزر الأيمن على custom 1 ونختار نوع الـ action المراد تطبيقه على التصنيف custom 1

وبذلك سوف يتم تطبيق الـaction على قائمه الـURL الموجودة في ال custom 1..

الفكره :تقوم بتحديد المواقع المراد السمح لها في custom 1

والمواقع المراد منعها في الcustom 2



****

Static URL filter

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

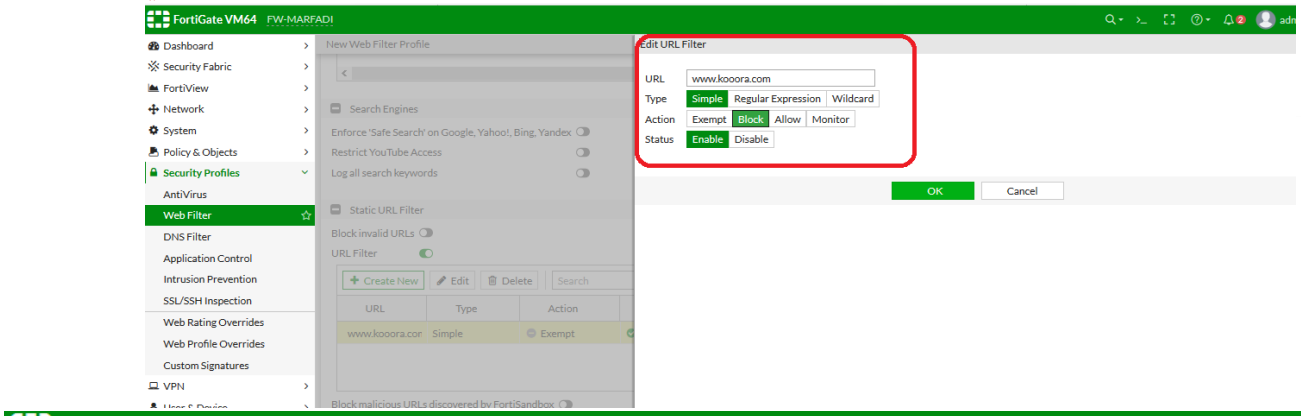
URL: www.kooora.com

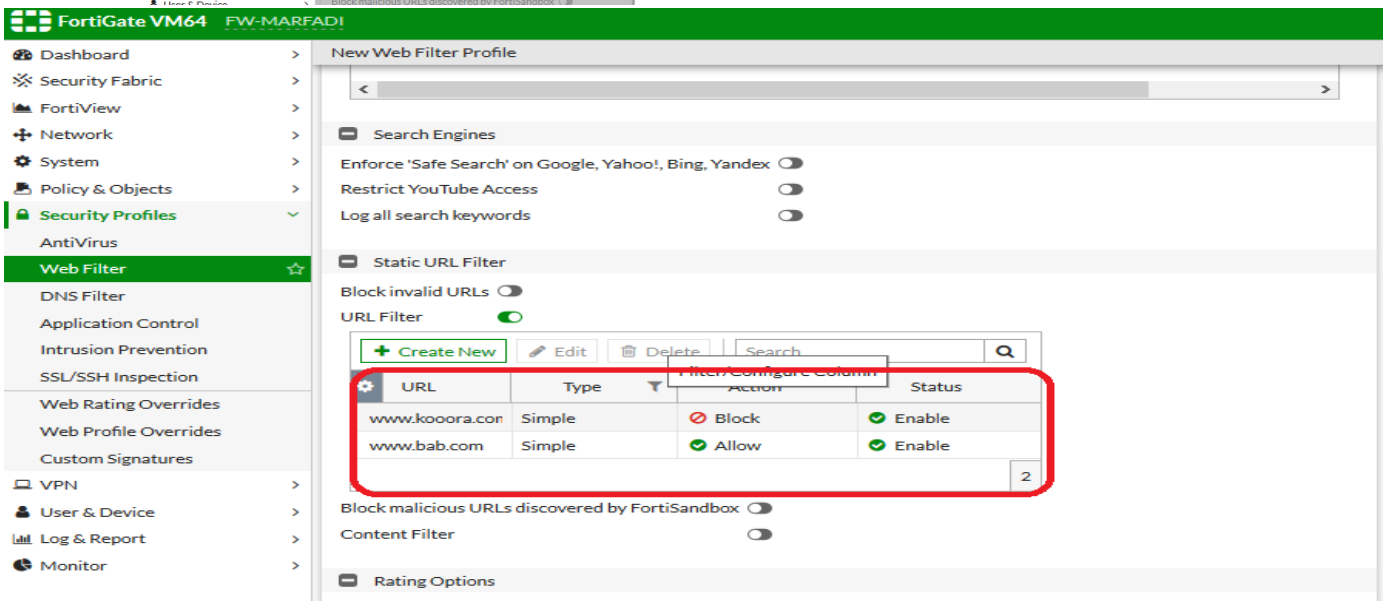
Type:simple

Action:block

Status:enable

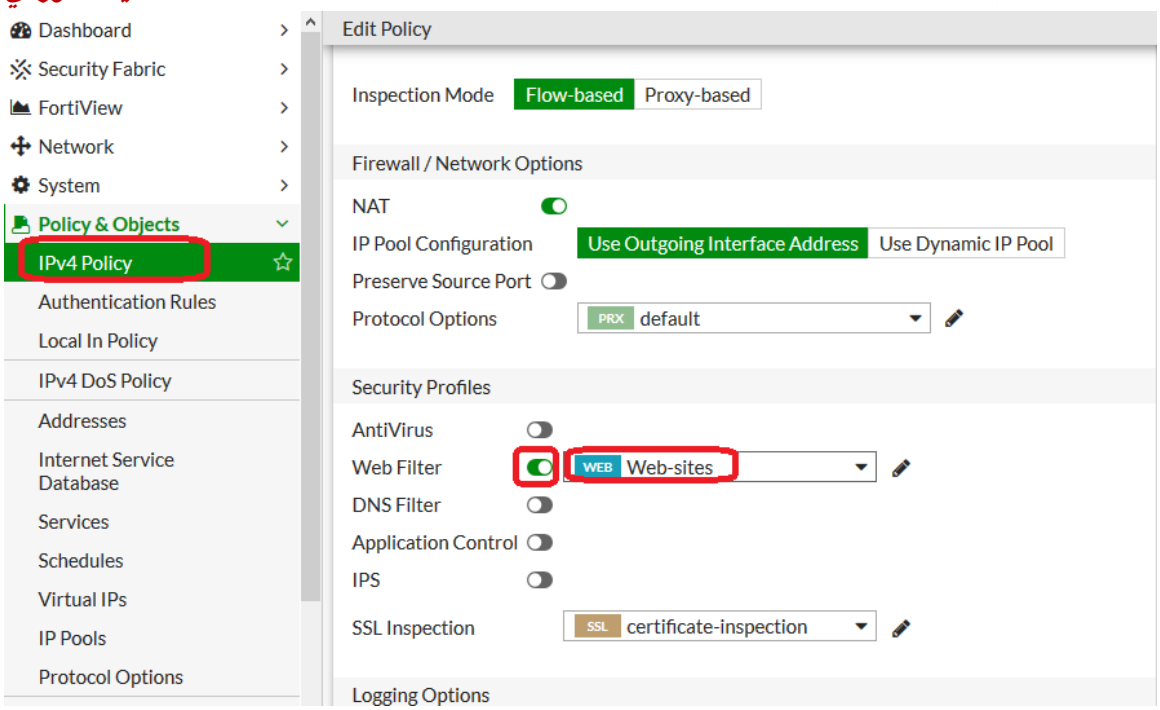
OK





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 ...



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

****

content filter

يتم عمل الـ action بحسب المحتوى لهذا الموقع وذلك كالتالي

security profiles>web filter>content filter:enable

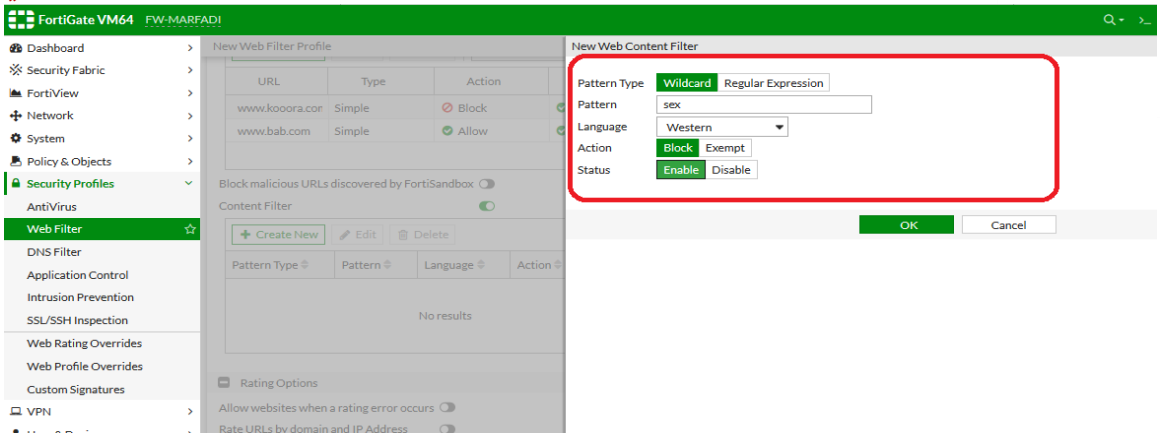
>create New>Pattern Type:WildCard

>patern :sex

>action:Block

Status:enable

OK



ملاحظة هامه :

الأولوية تكون حسب الترتيب التالي :

١- Static URl filter

٢- Fortiguard filter

٣- Web content filter

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

في حالة اردت ان تطبق الى web filter على المواقع https فأنه يجب تفعيل خاصيه ssl-certficate 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:*fcebook.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>

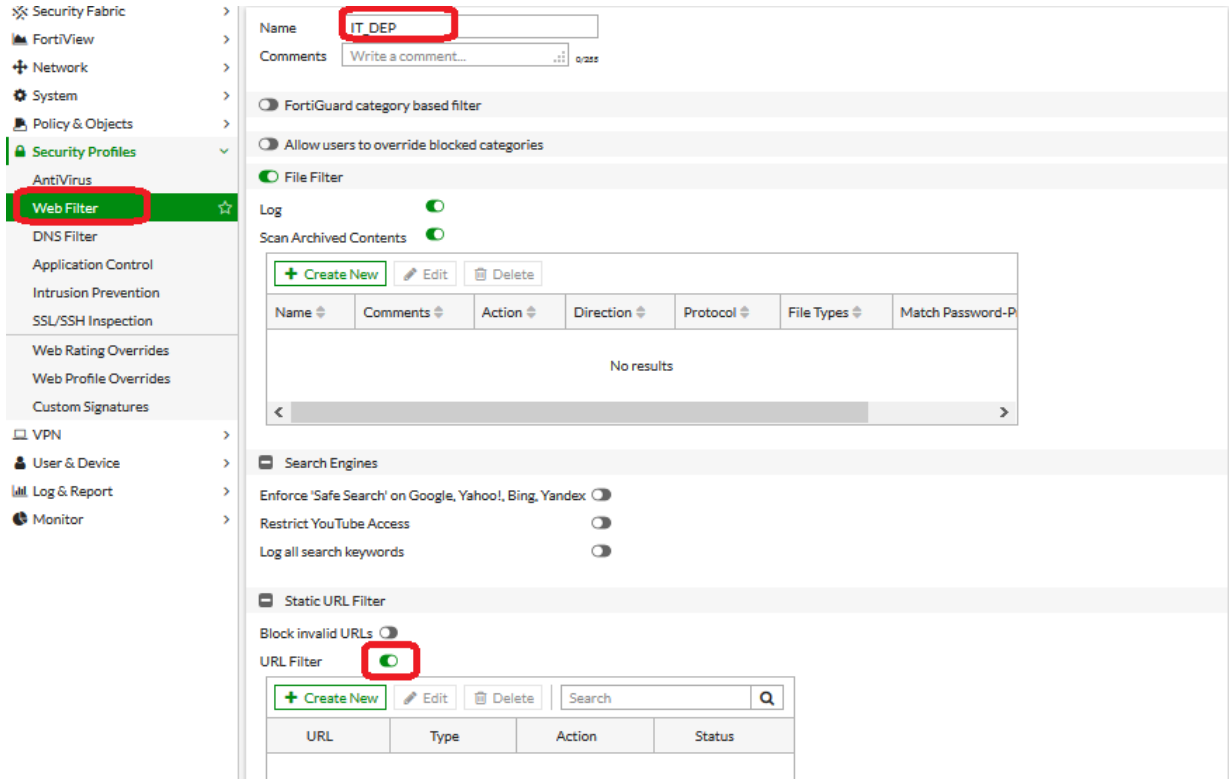
ثم من المتصفح في اجهزه الكلاينت نقوم با استيراد الشهادة

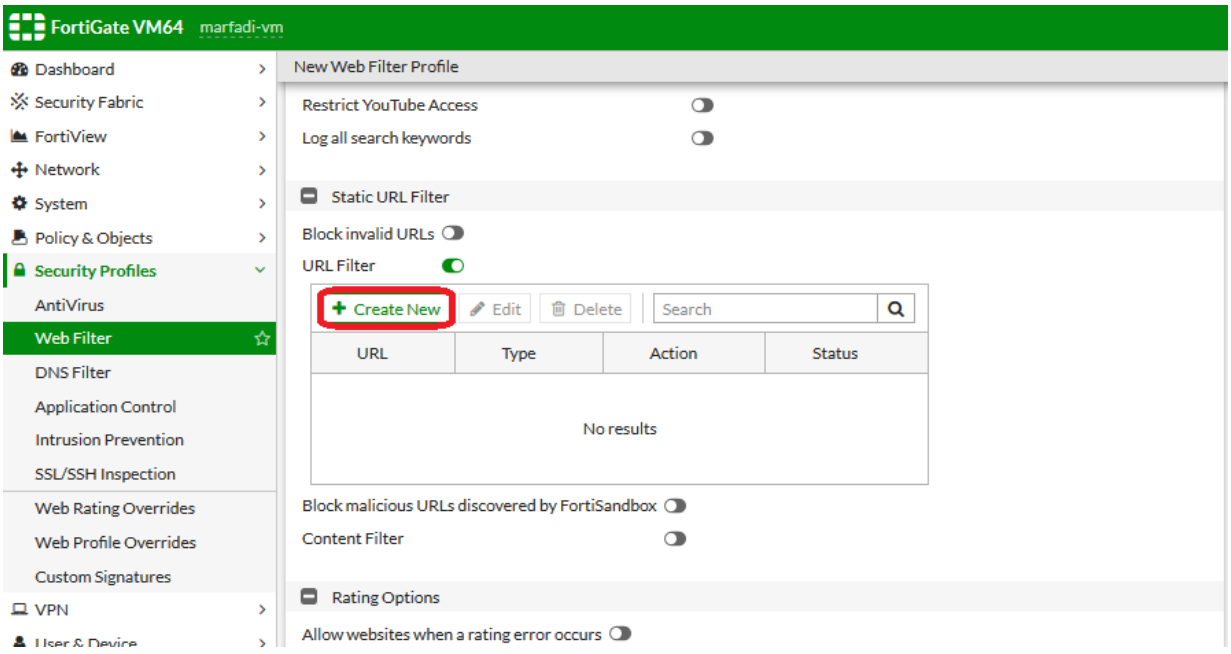
Option>privact&security>certificate>view certificates?authorities >import>trusted this CA to identify websites>ok

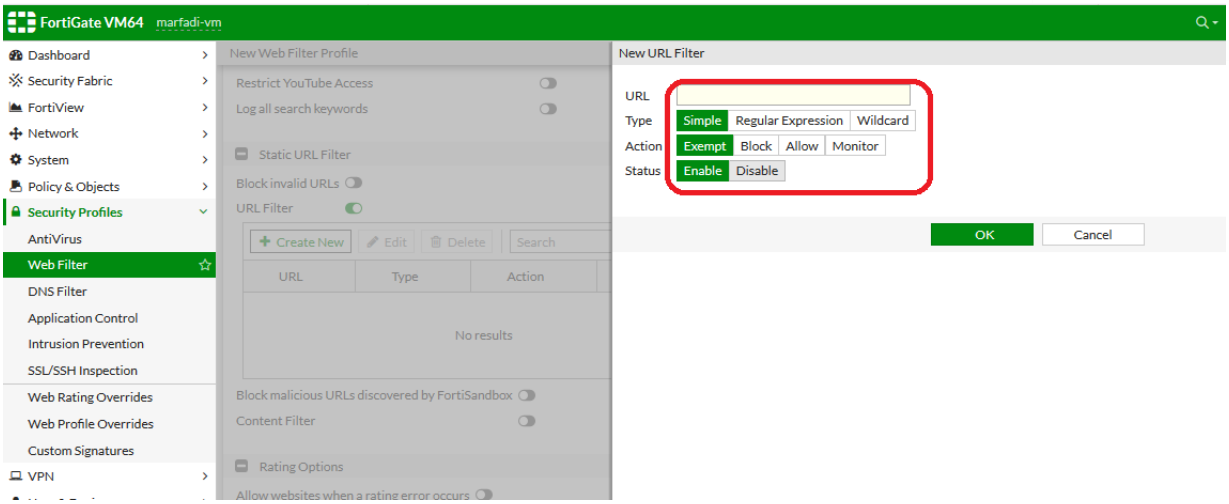
حيث بعدها نغلق المتصفح ونفتحه فأذا فتحت موقع https لن تظهر لك مجددا.

❖ بعض التمارين والأمثلة حول الـweb filter واستخدام static URL filter :

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







كما بالصورة أعلاه فأن URL ممكن كتابتها بأحدى الصيغ التالية :

Simple :سوف يقوم بتنفيذ مثلا الـaction=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 محبب .

Regular Expression : مثلا لو كان الـurl مكتوب facebook.com فأن أي رابط يحتوي على facebook.com سوف يتم تطبيق الـaction عليه فمثلا لو اليوزر كتب Login.facebook.com فأنه أيضا سوف ينطبق عليه الـaction وهكذا ..

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

Wildcard :

مثلا لو كتبت في url الموقع *facebook.com فأن اليوزر لو حاول يدخل على أي رابط يحتوي على facebook.com فأنه سوف يطبق عليه الـaction .

كمان ممكن ان تستخدم الطريقة *facebook* فأن أي موقع الرابط له بيحتوي على facebook سوف يتم تطبيق الـ action عليه ..

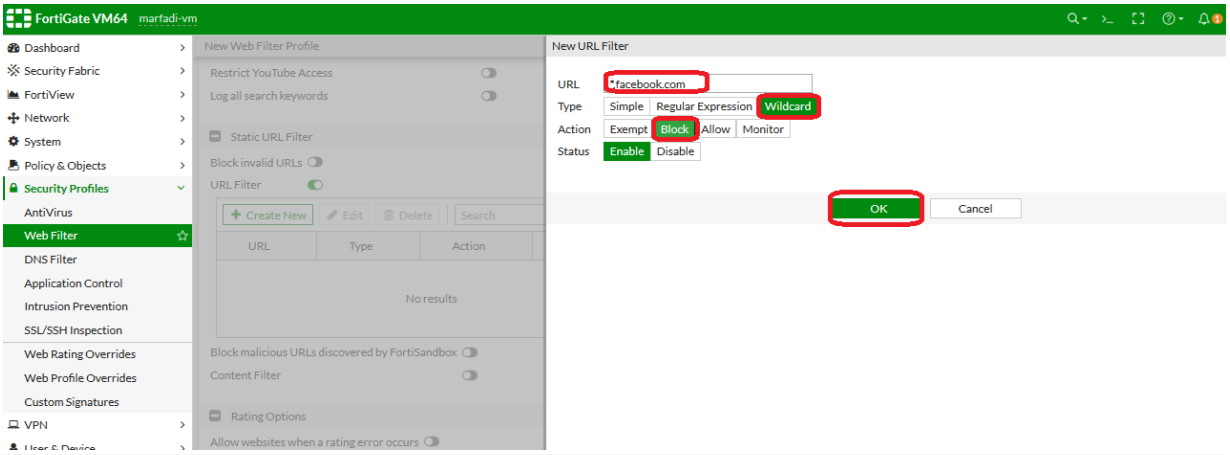
أنواع الـ action :

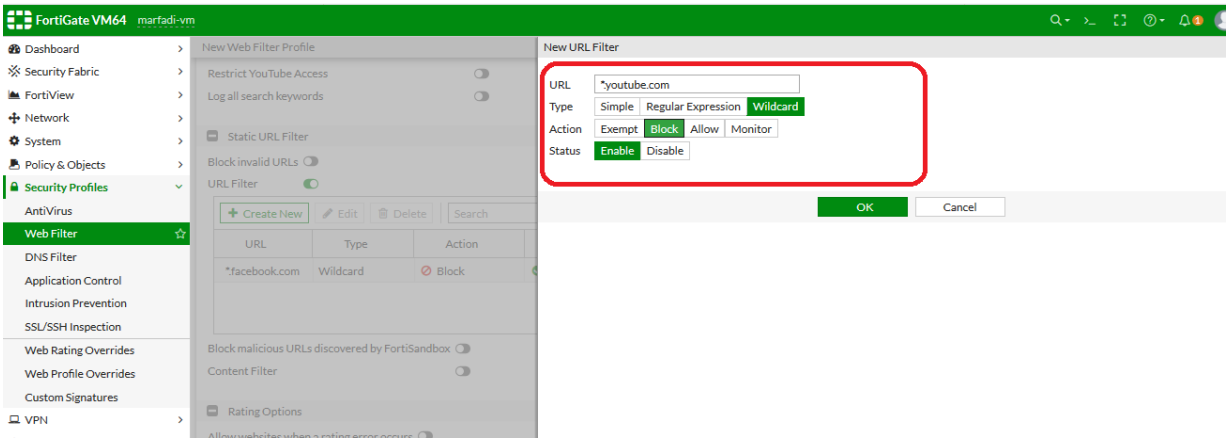
Exempt :يعتبر مثل الـ allow أي السماح للترافيك

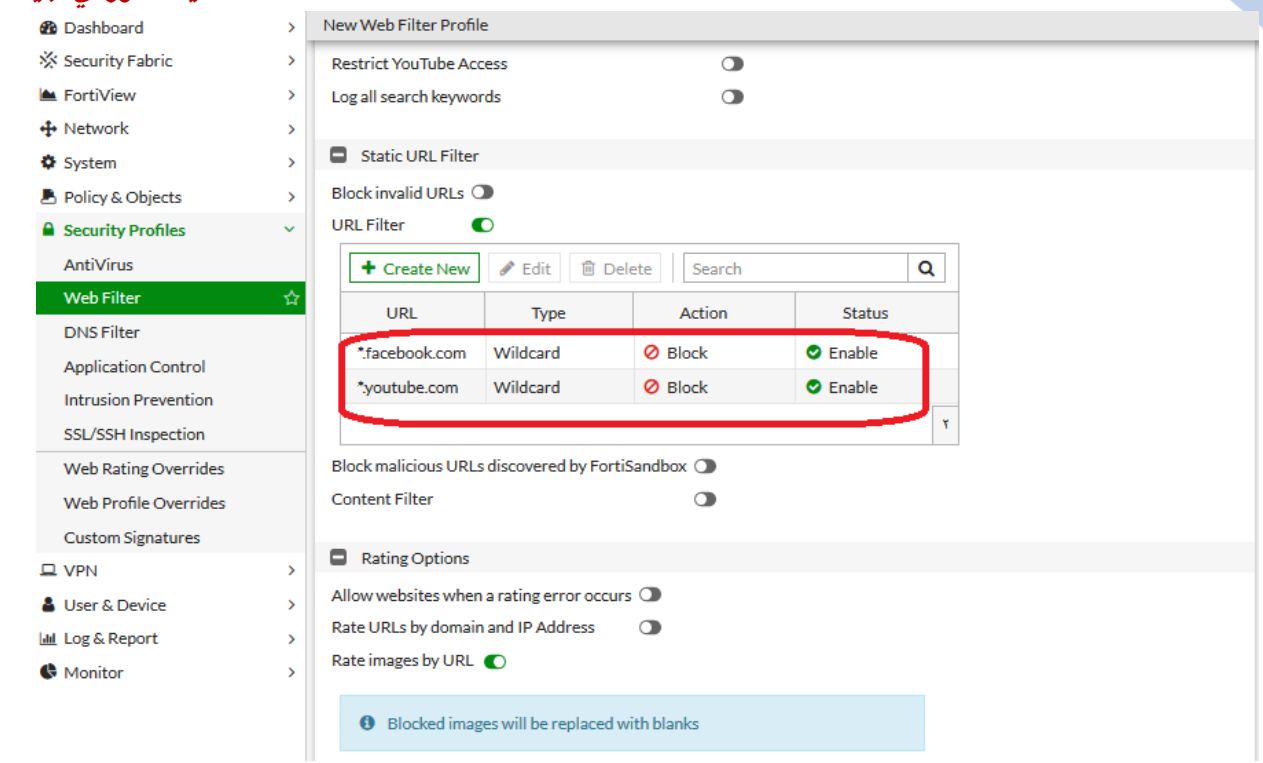
Allow : السماح للترافيك ولكن يتم تمرير الترافيك الى بروكسي سيرفر اخر...

Monitor : السماح مع عمل log للترافيك .

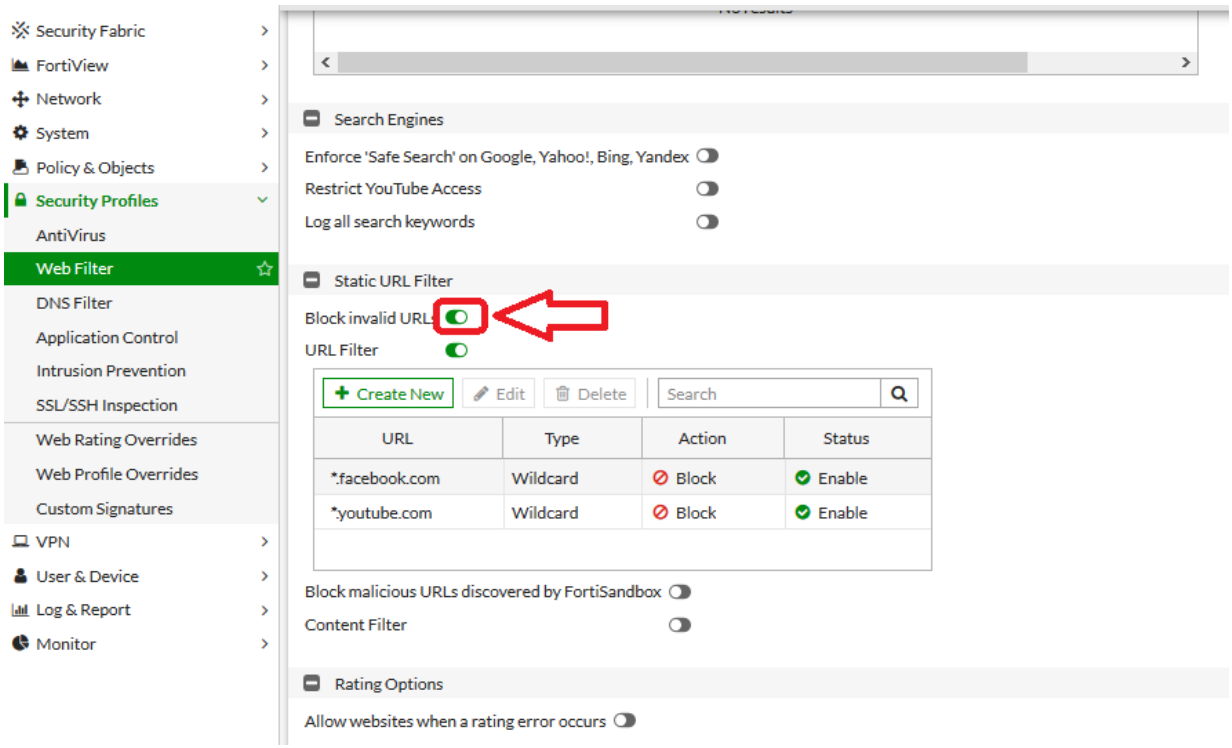
Block : امنع الترافيك ..



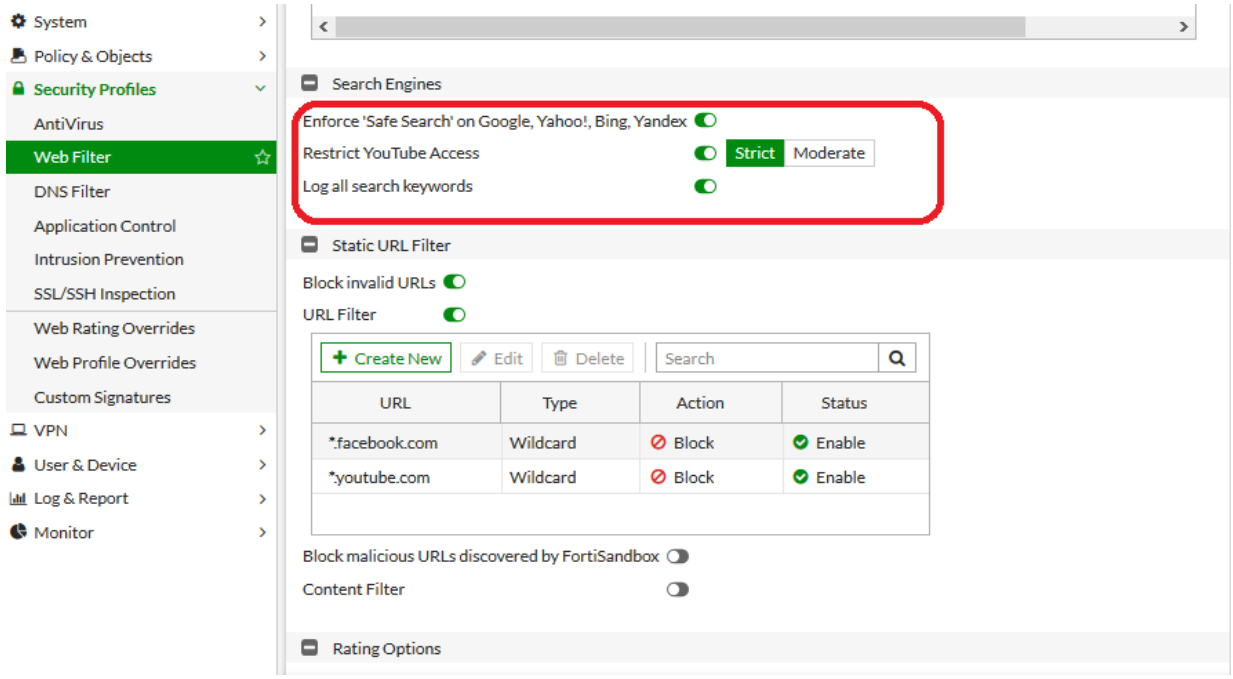




كما بالصورة أعلاه تم انشاء web filter security profile باسم IT_DEP يقوم باغلاق الفيسبوك واليوتيوب ..



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 فأنه سيتم عمل لها Block حيث يعتبر هذا الموقع invalid ويقوم بعمل منع للموقع.

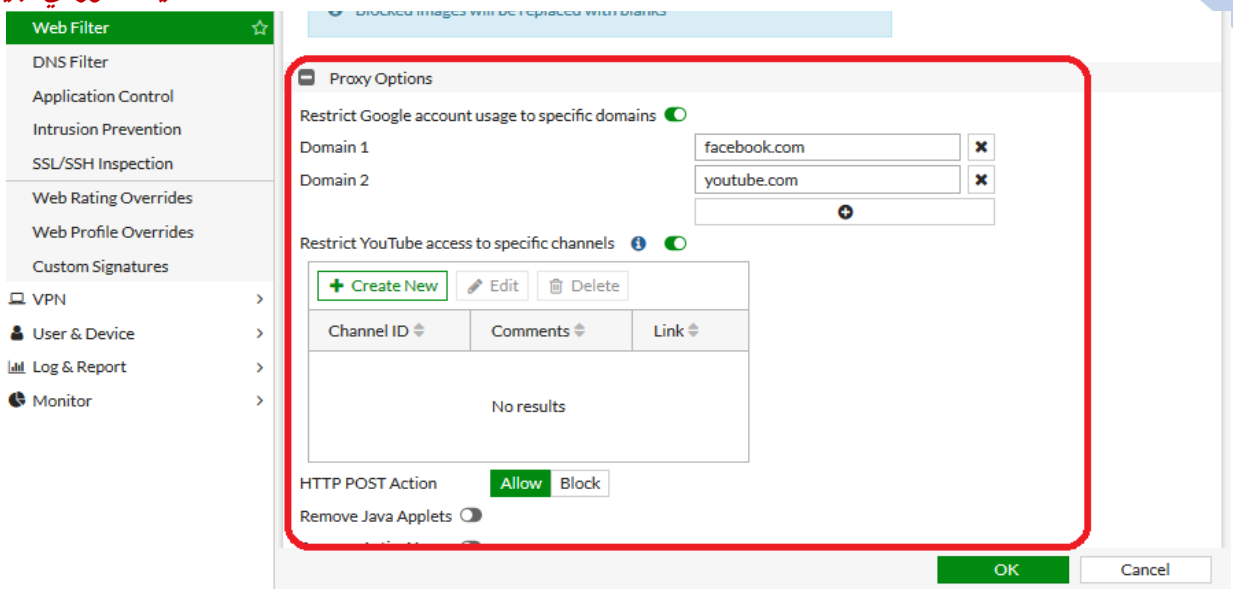


Enforce 'Safe Search' on Google, Yahoo!, Bing, Yandex : تجبر بان عمليه البحث الامن في محركات البحث جوجل وياهو وبينج وياندكس ..

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

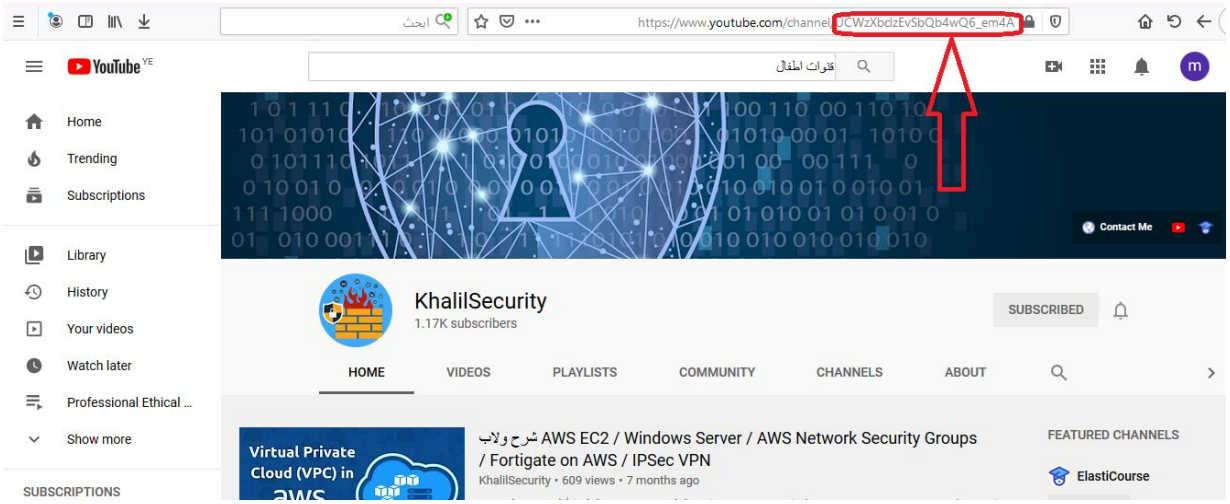
الـmoderate : يشغل جميع الفيديوهات ماعدا فيديوهات العري والـporn وغيرها .

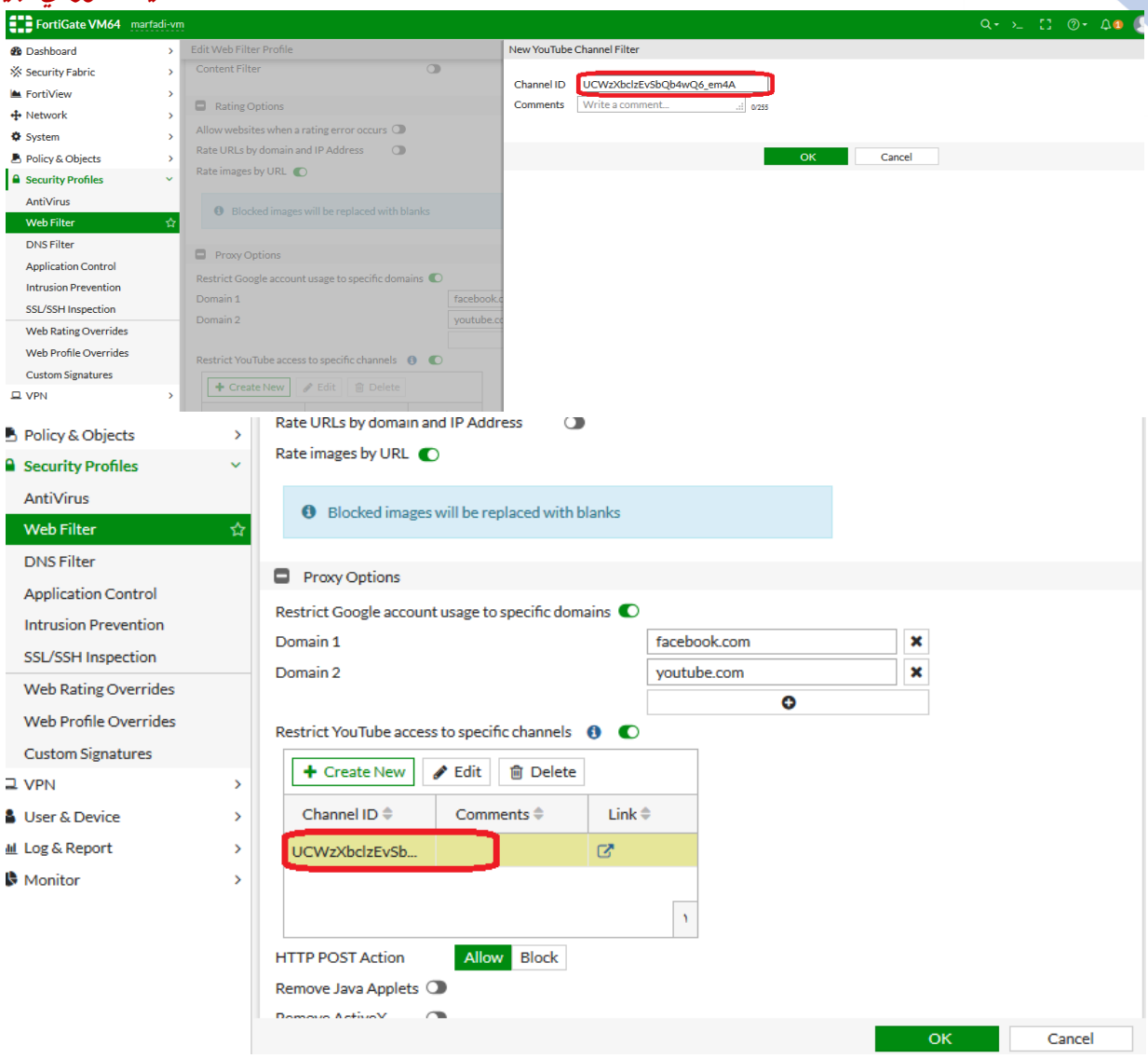
Log all search keywords : عمل تسجيل للـlogs لكلمات البحث على اليوتيوب .



Restrict Google account usage to specific domains : تقيد حسابات جوجل بحيث يمكن تستخدمها فقط في الشركة في التسجيل بفيسبوك ويوتيوب كما بالصورة أعلاه ..

Restrict YouTube access to specific channels : ممكن تحديد قنوات محدده على اليوتيوب فقط للسماح فيها مثلا نسخ رابط القناه

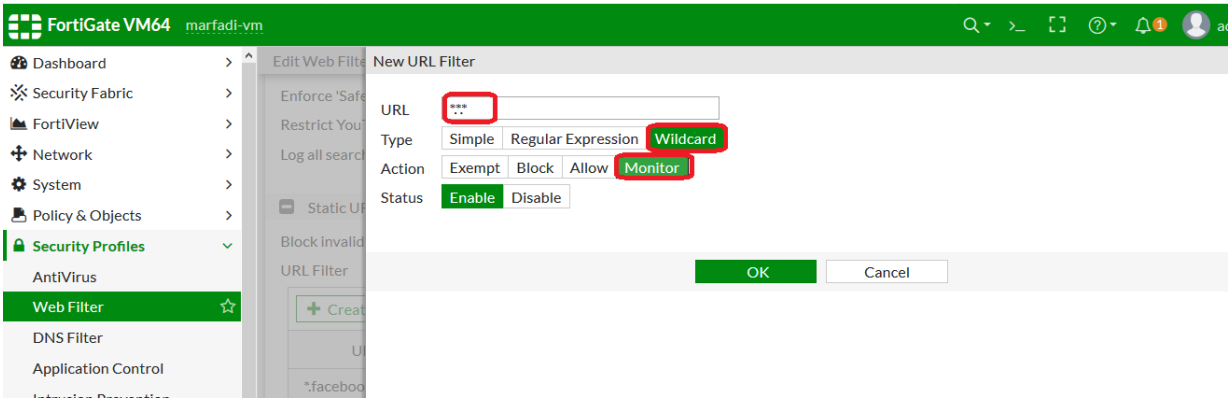




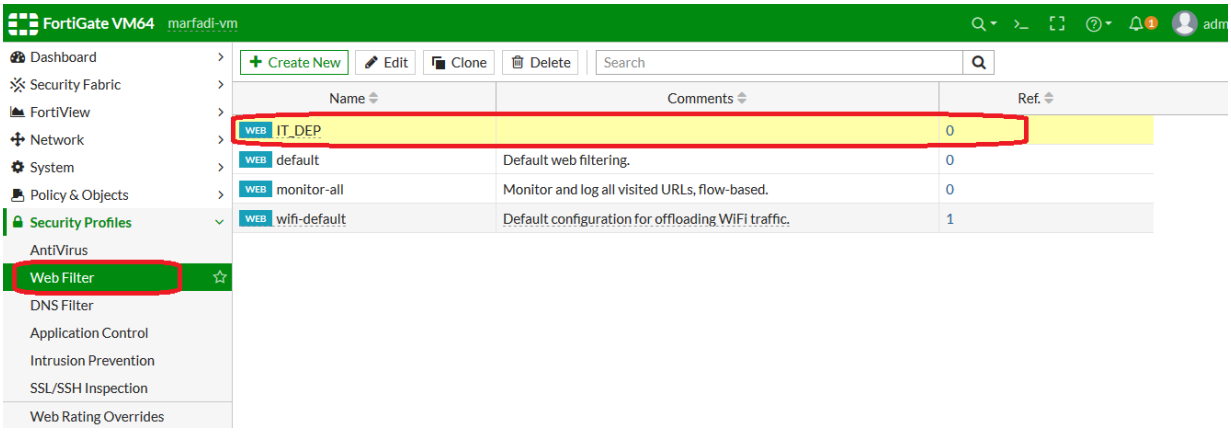
سيتم السماح لهذه القناه بالتحديد ...

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

..



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

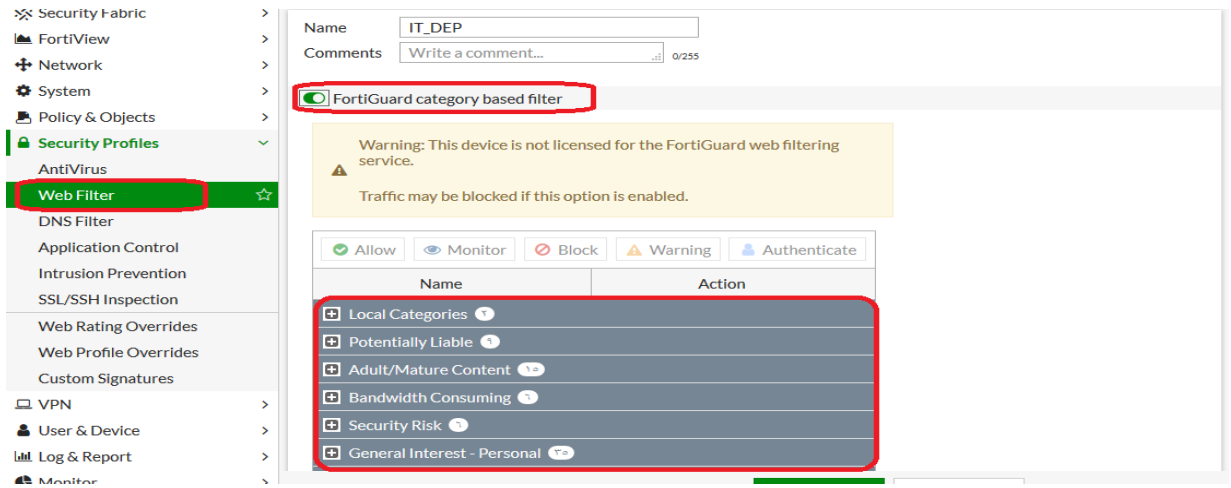


كما بالصورة أعلاه تم انشاء الـ web filter security profile باسم IT_DEP .

Web category based filtering :

الـcategory based filter تستخدم لتطبيق action معين على تصنيف معين من المواقع(مثلا تريد اغلاق كل مواقع الرياضه)، فبدلا من استخدام كتابه كل موقع على حده كما بالطريقة السابقة في Static URl filter فهذا صعب جدا .

فبواسطة الـ web category based يتم فقط اختيار التصنيف(category) المطلوب تطبيق الـaction عليه ....



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

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

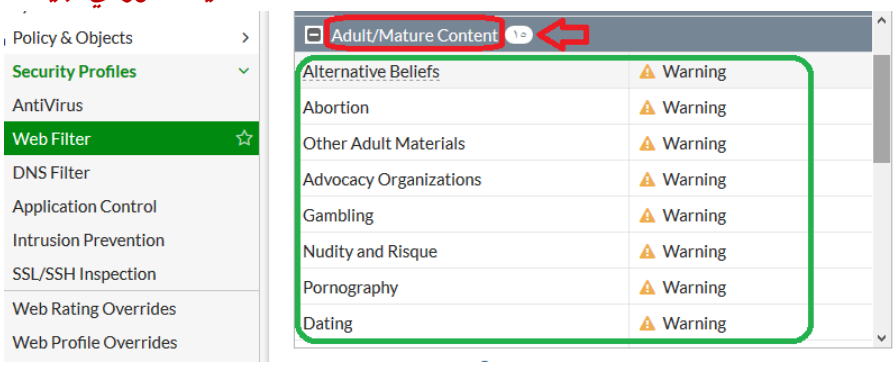
Traffic may be blocked if this option is enabled.

"

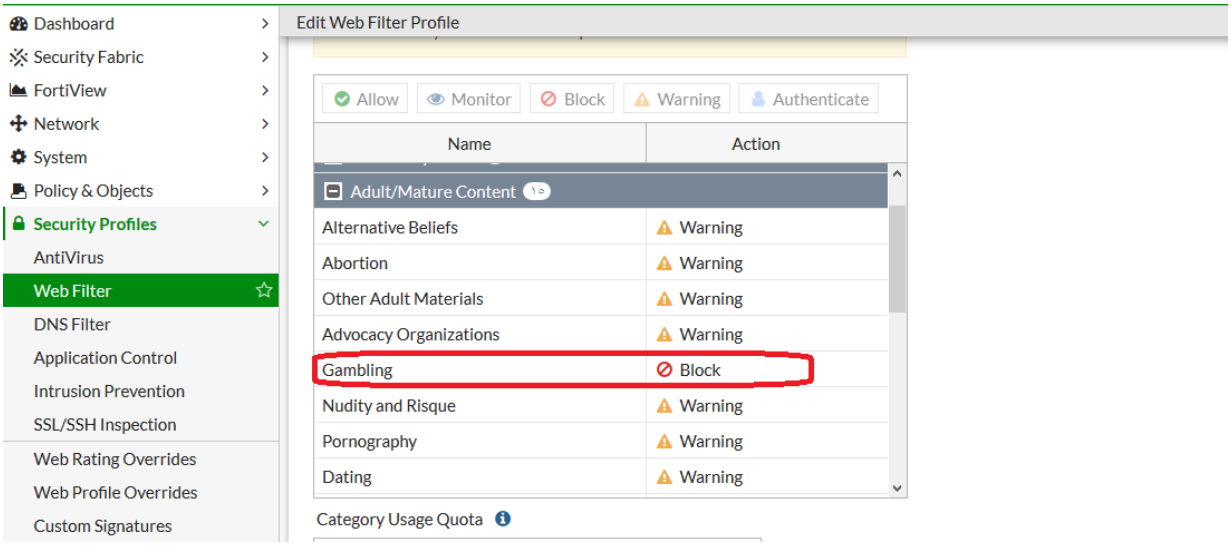
حيث الفورتي جيت مقسم الـcategory الى قسمين :

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

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

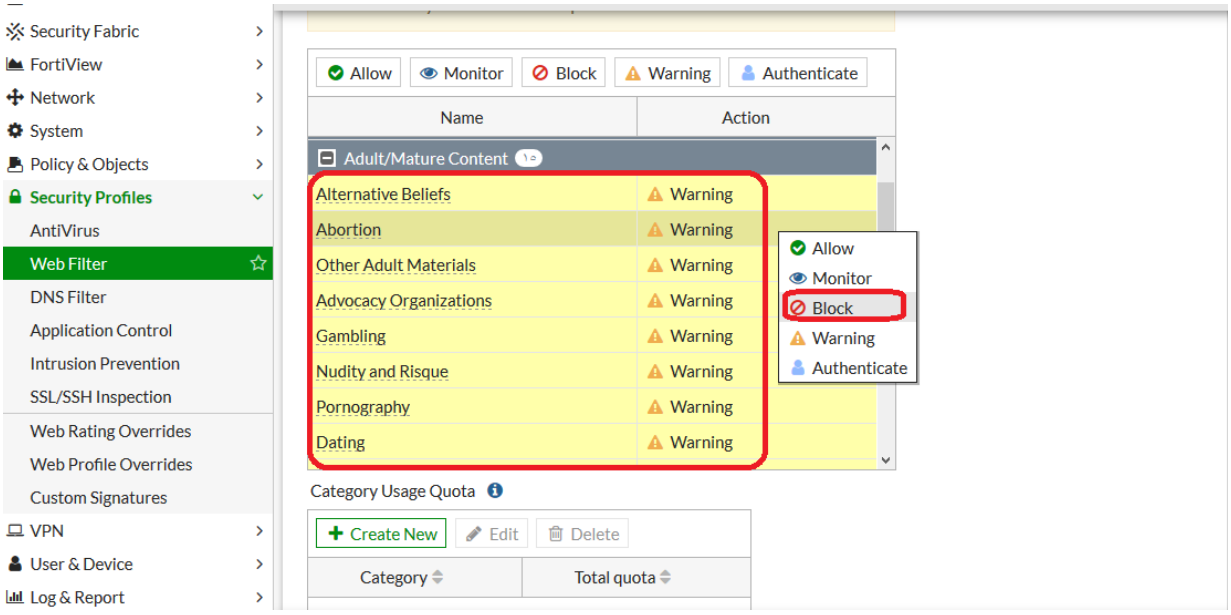


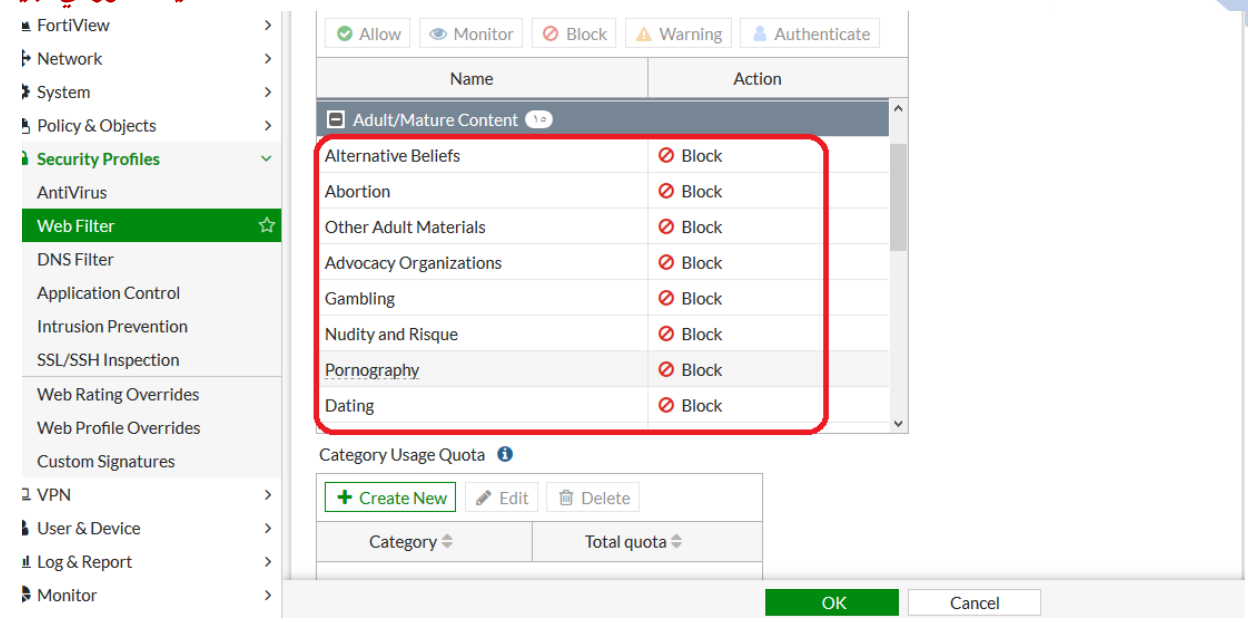
فيمكنك اغلاق مثلا مواقع القمار المسمى Gambling .



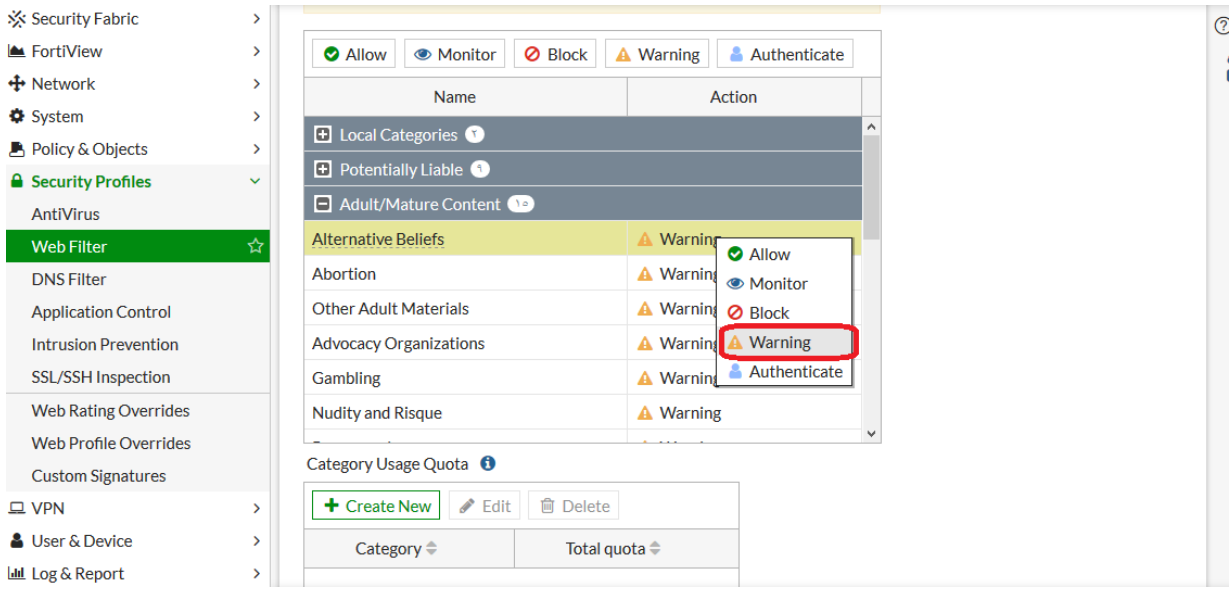
فلو تريد اختيار كل الـ sub category للتصنيف الرئيسي المسمى Adult/Mature

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



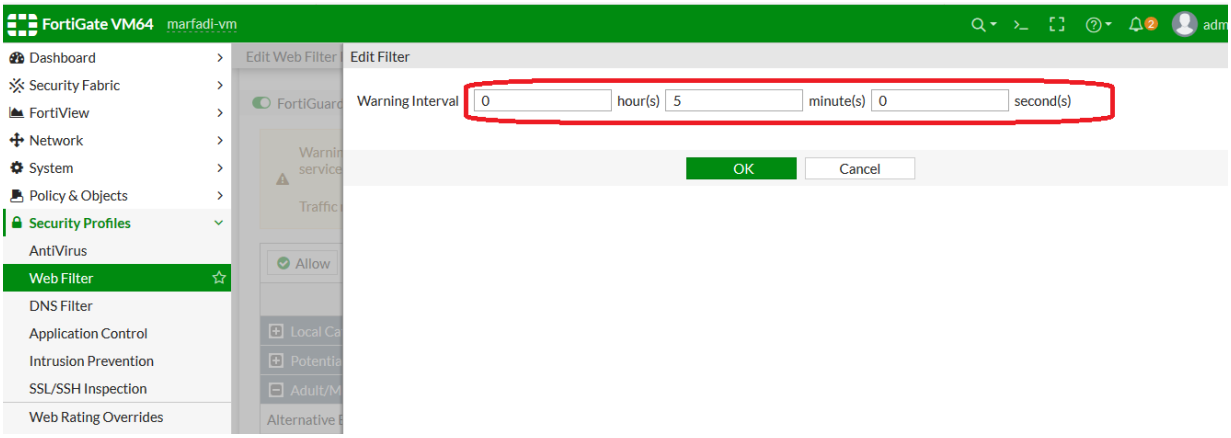

FortiView
Network
System
Policy & Objects
Security Profiles
AntiVirus
Web Filter
DNS Filter
Application Control
Intrusion Prevention
SSL/SSH Inspection
Web Rating Overrides
Web Profile Overrides
Custom Signatures
VPN
User & Device
Log & Report
Monitor
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Adult/Mature Content
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 :



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

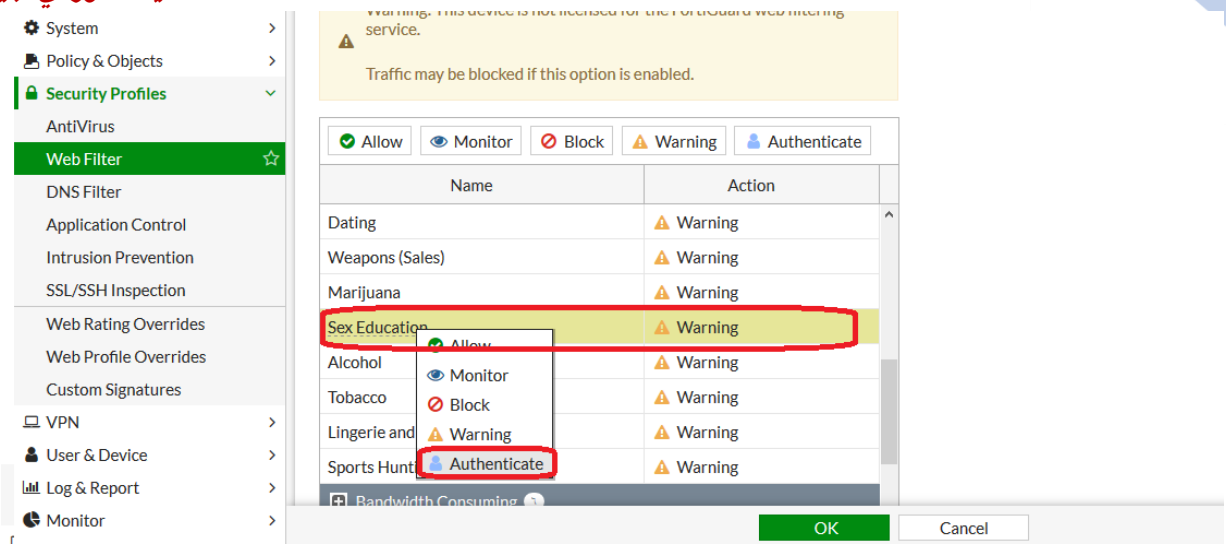
حيث بمجرد النقر على الزر warning تظهر لك الرسالة التالية

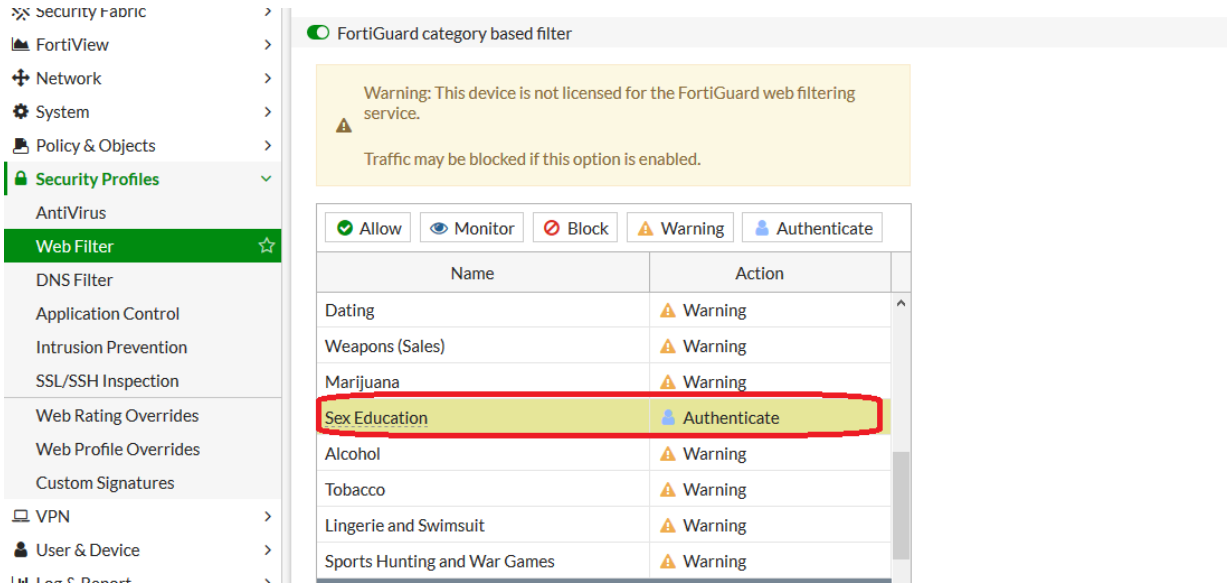


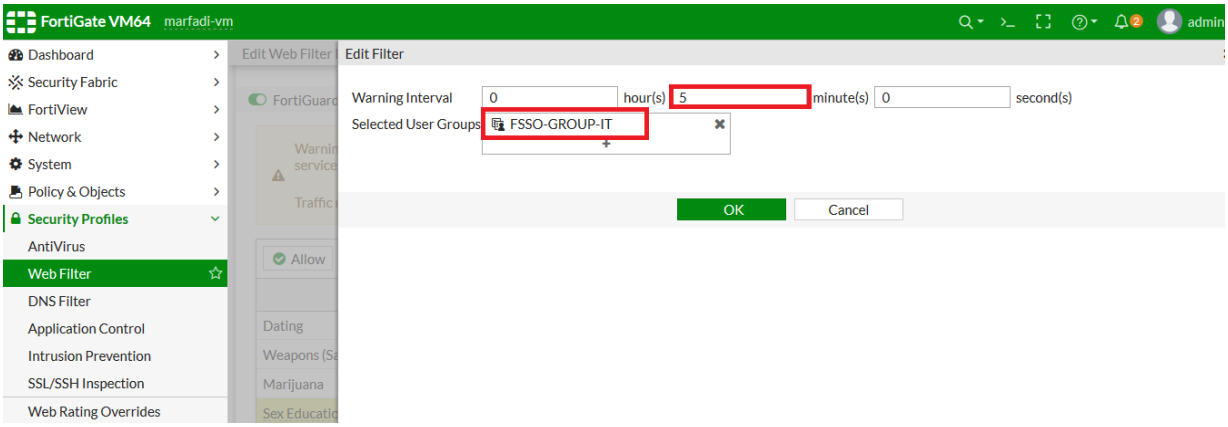
حيث ستظهر رساله التحذير مدتها 5 دقائق ...

الـ Authenticate action :

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

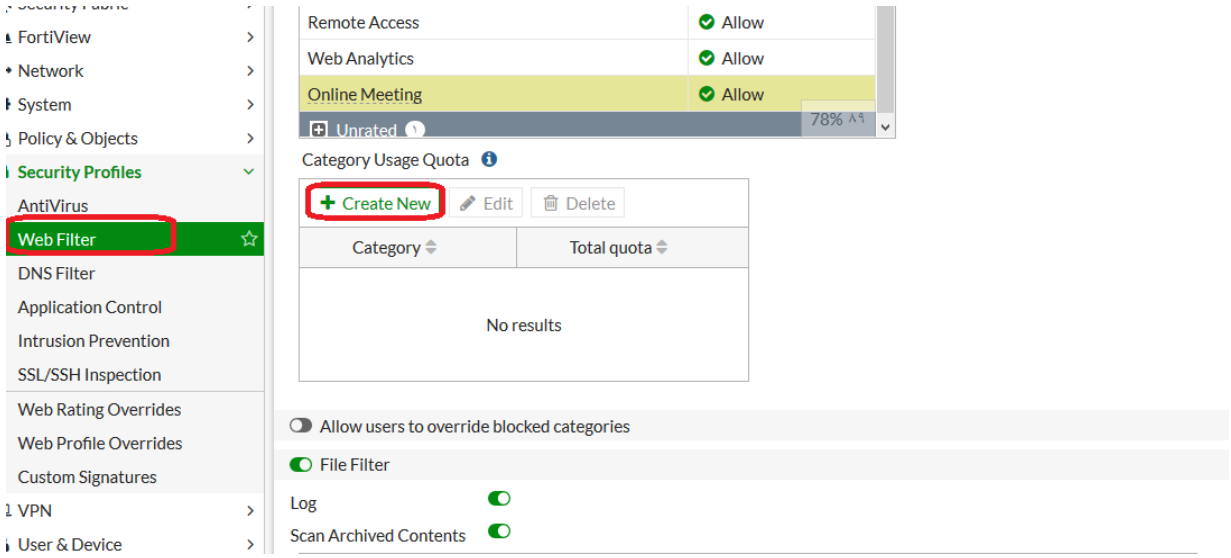


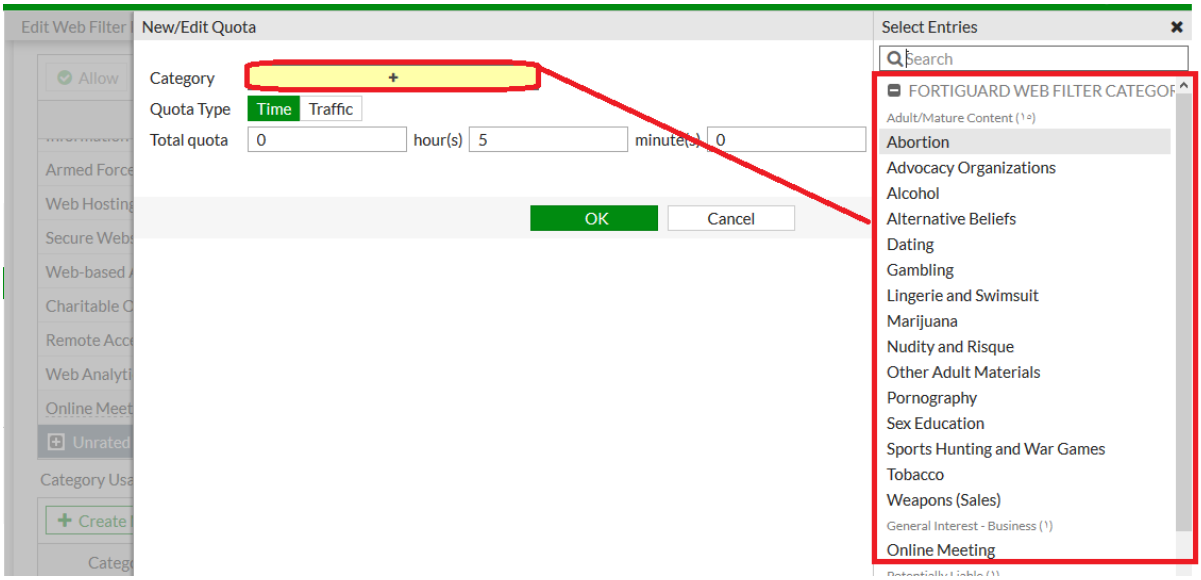




حيث تم أضافه جروب الـIT فيجب على اليوزر المراد فتح أي موقع تنتمي لـ sex education ان يكون ضمن الـIT group حيث يجب ان يقوم بإدخال يوزرنيم وباسورد لأي حساب ضمن الـIT group.

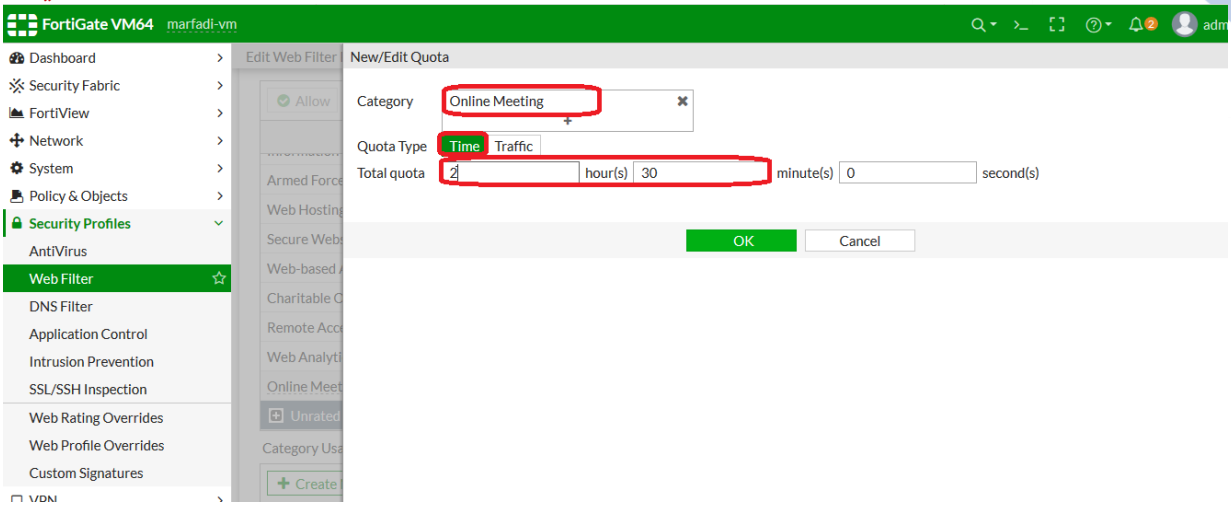
الآن سنقوم بعمل Quota لتصنيف معين وليكن الـ online meeting بحيث نحدد مثلا ساعه ونصف فقط وبعدها يتم الخروج من الموقع ..

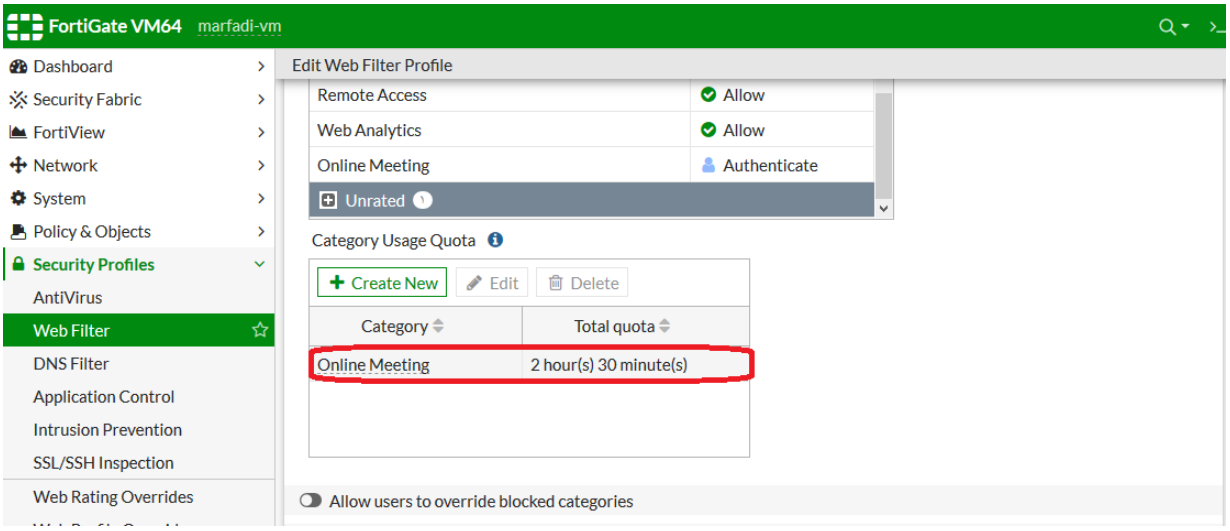




حيث لا يمكن عمل quota الا للتصنيفات المعمول لها Monitor او Authenticate او Warning في الـ FortiGuard web category filter ...

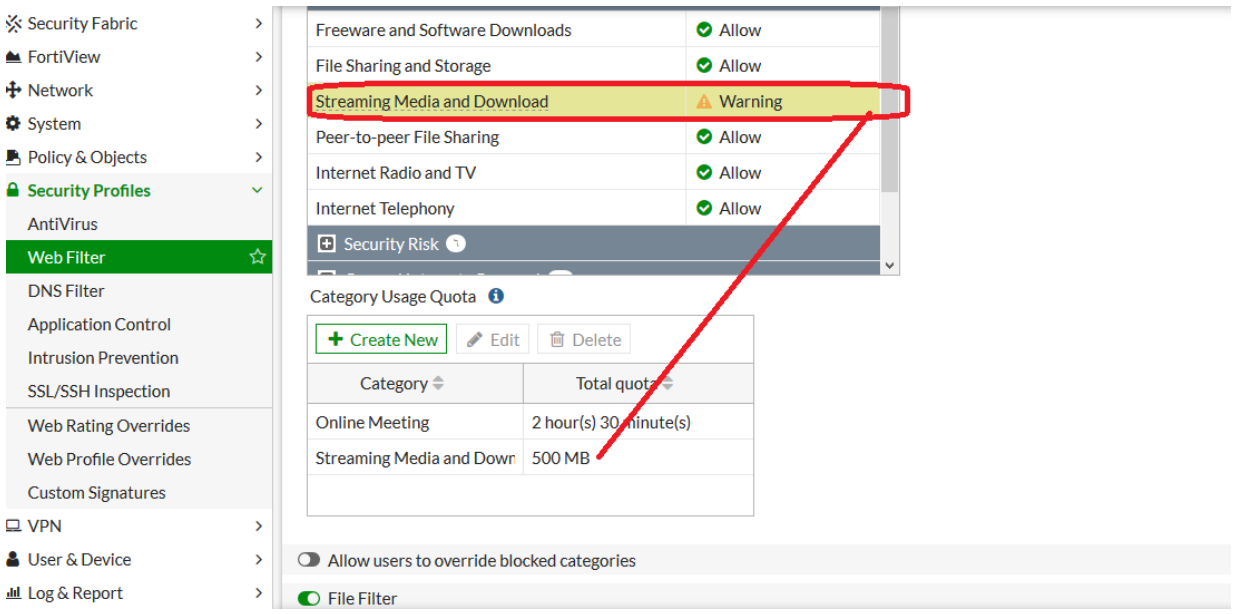
حيث يتم استخدام مواقع التصنيف Online meeting لمده ساعتين ونصف ومن ثم ظهور رساله الـ authenticate

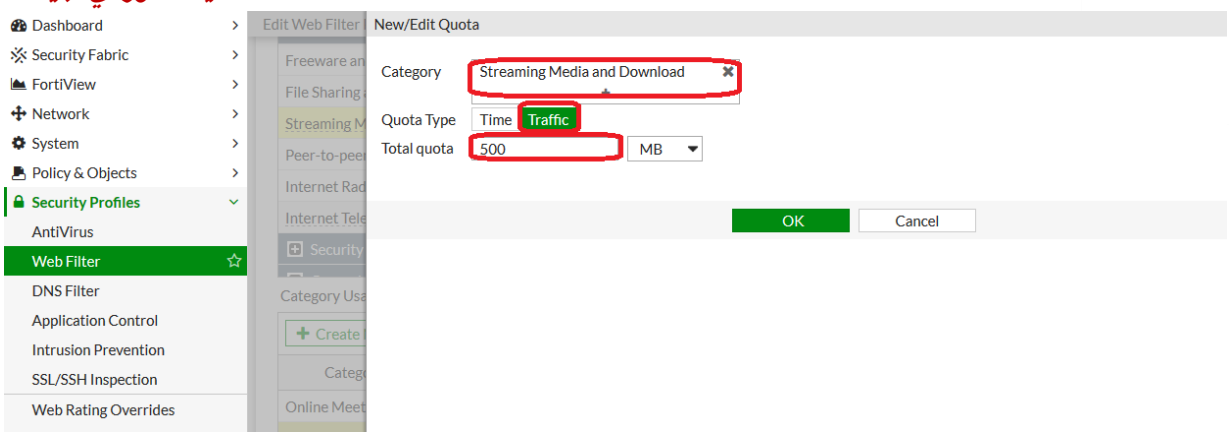




أيضا اريد ان اسمح ان يتم فتح مواقع ال streaming media and download

500 ميجا فقط ..

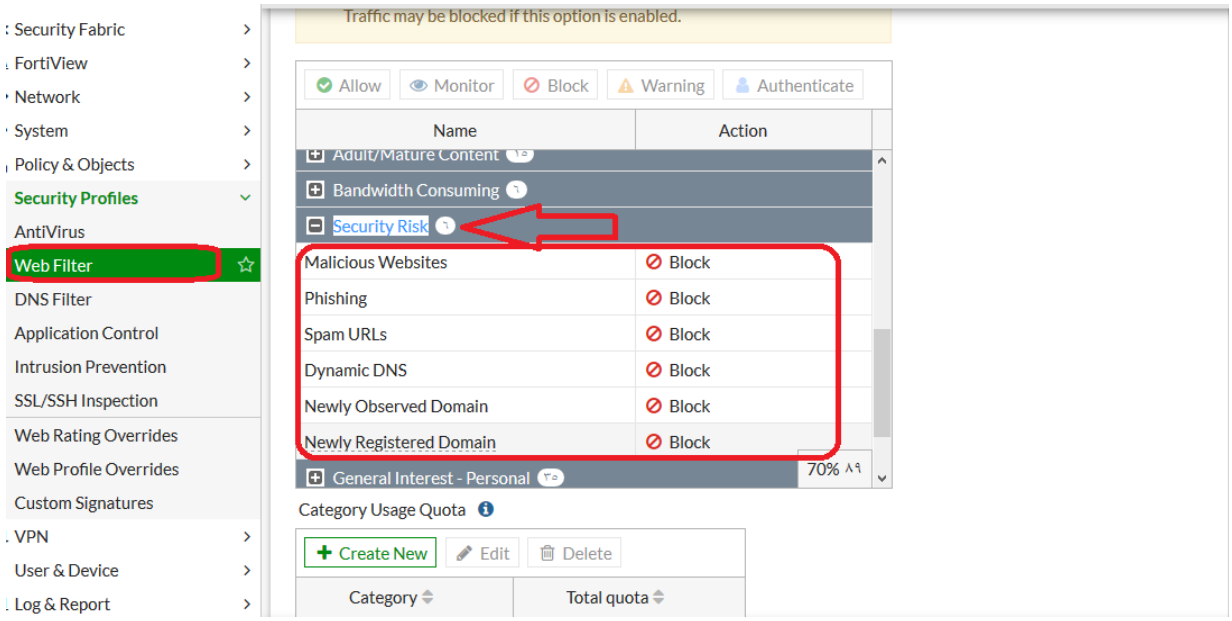


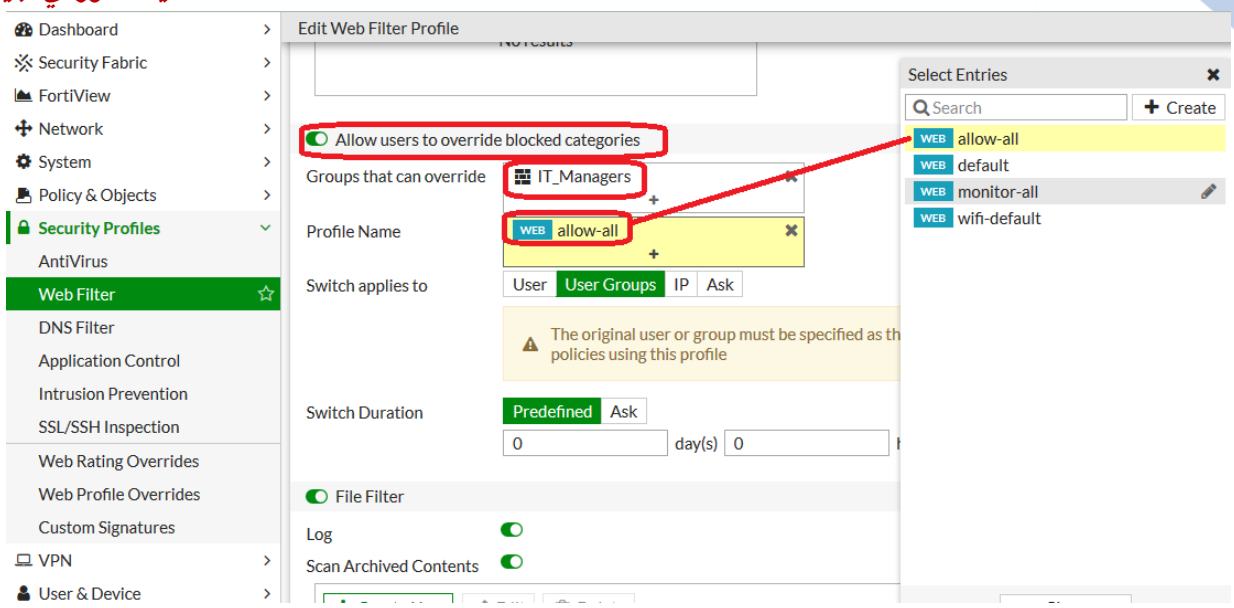


Web Category Based Filter Overriding :

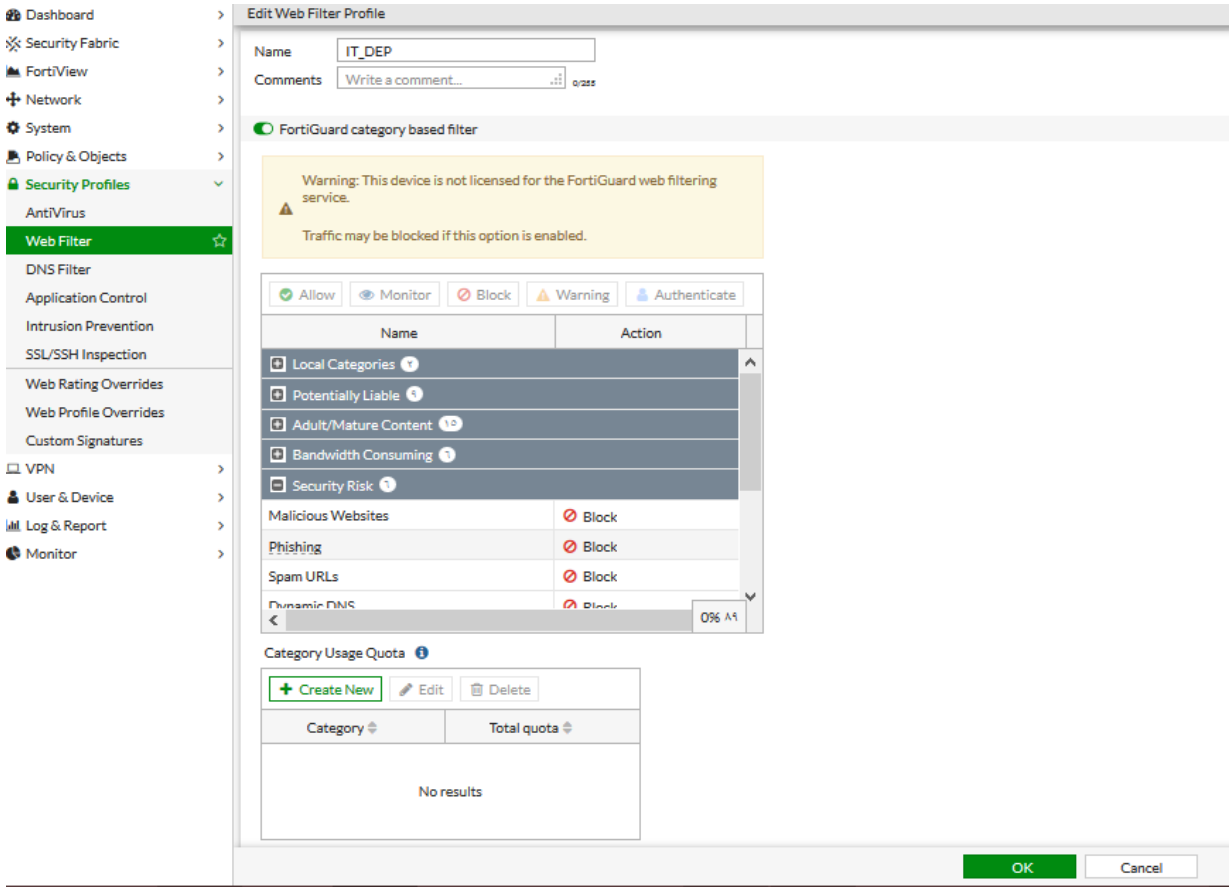
تعمل override(تجاوز) لأي تصنيف معمول لها block في الـFortiguard web category لـ group معين.

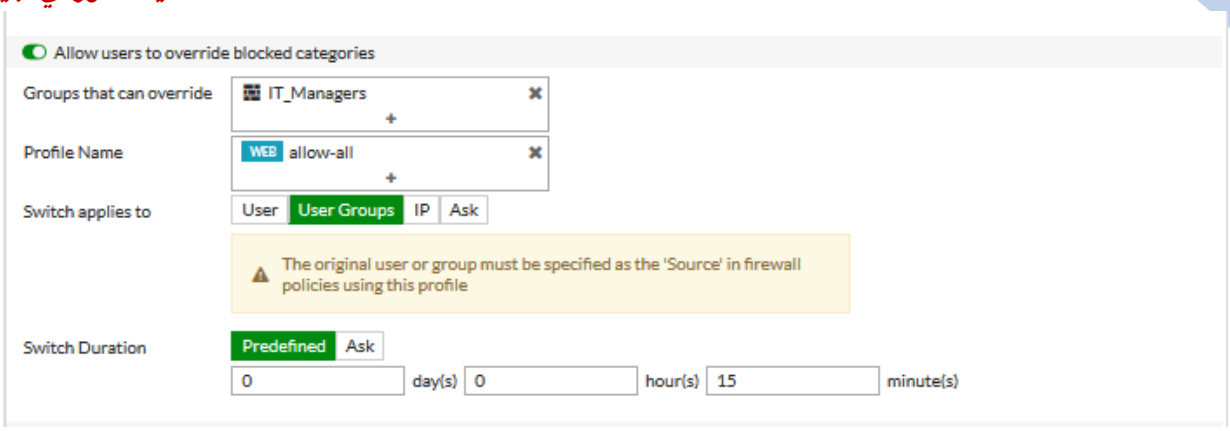
مثلا اريد انا اسمح لجروب اسمه IT_Managers بأن يتجاوز غلق مواقع الـSecurity Risk الذي تم اغلاقه في الـFortiguard web category ،وبهذا اليوزرات التي تحت الجروب IT_Managers سوف يسمح لهم بالوصول الى المواقع المدرجه تحت التصنيف Security Risk .





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

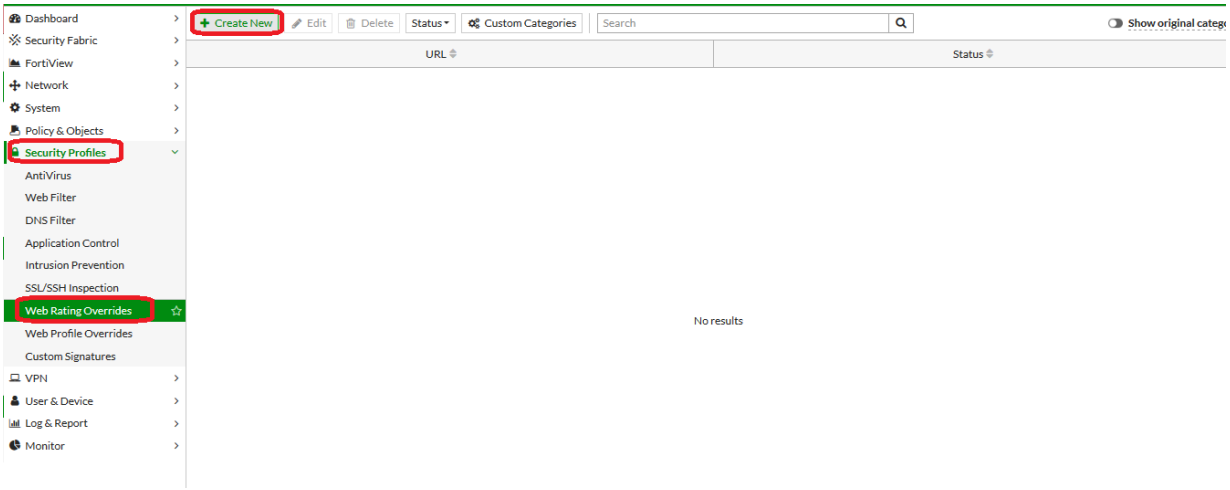


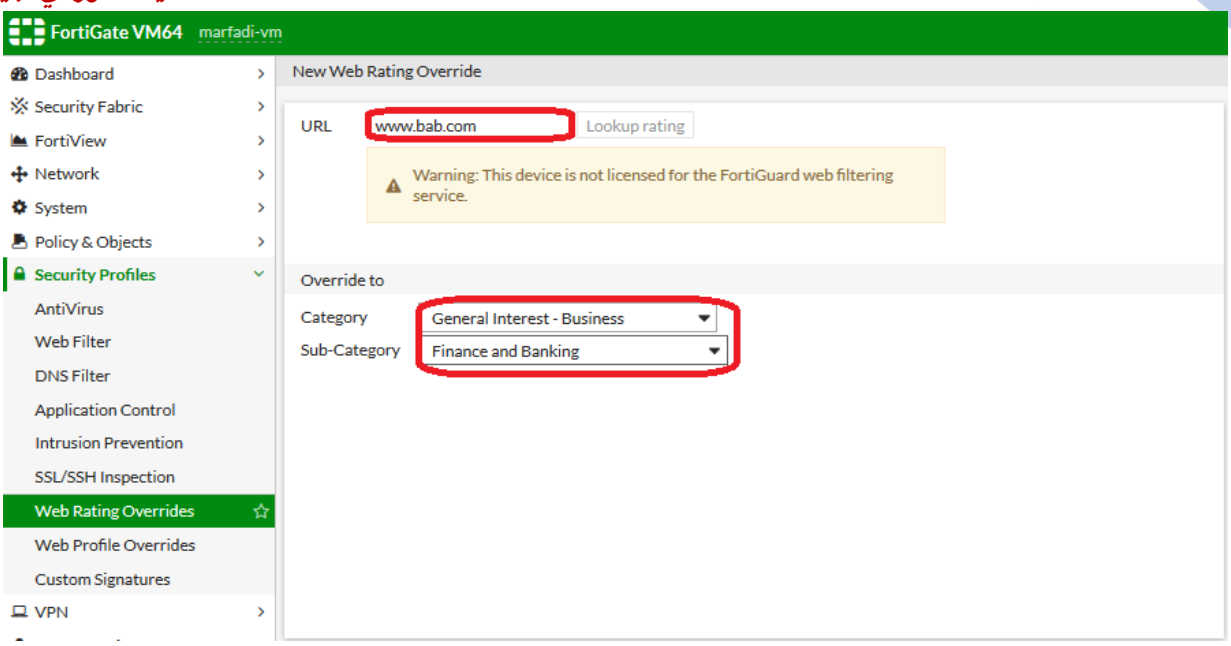


Web Rating Override :

في حالة كان لدينا موقع مثلا www.bab.com ونفترض بأن الموقع ليس له تصنيف معين او الفورتي جيت غير قادر على معرفة الـcategory التي يندرج تحتها .

او ان هذا الموقع موجود في category وتريد نقله الى category أخرى فأن بواسطة الـ Web Rating Override يمكن عمل ذلك .

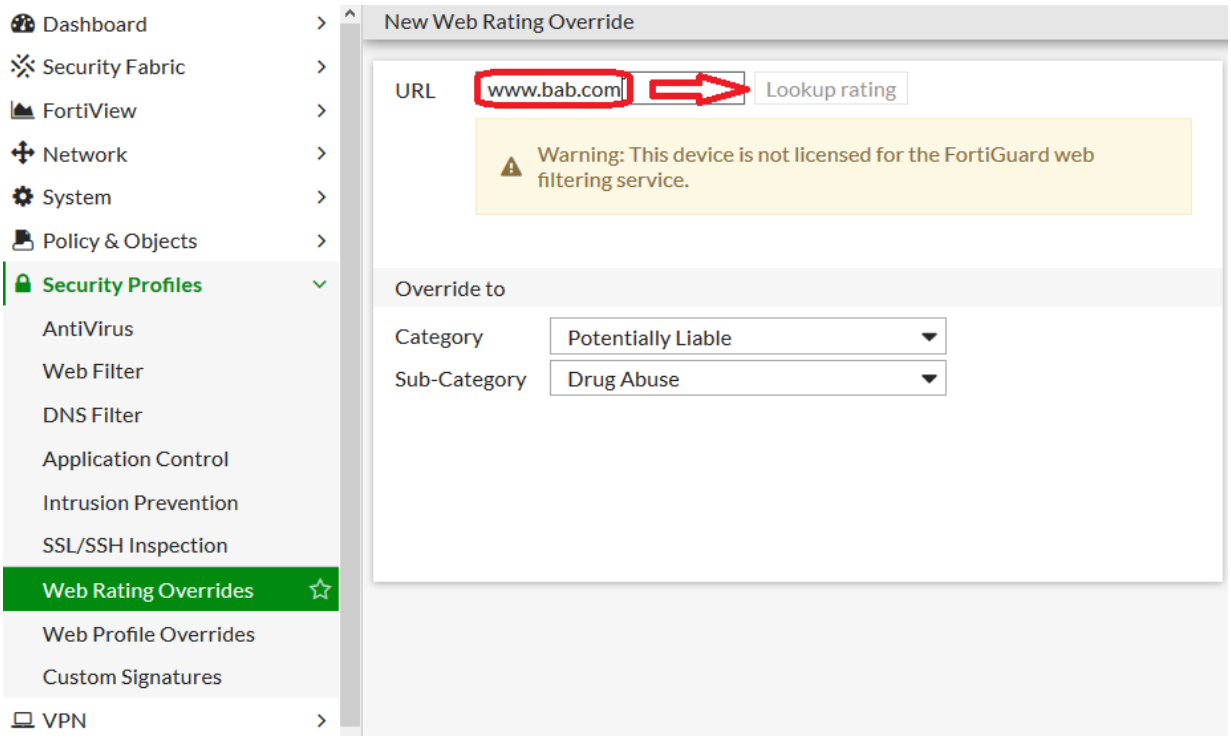




تم تصنيف موقع www.bab.com بانه ينتمي الى General Interest-Business

تحت التصنيف الفرعي المسمى Finance and banking .

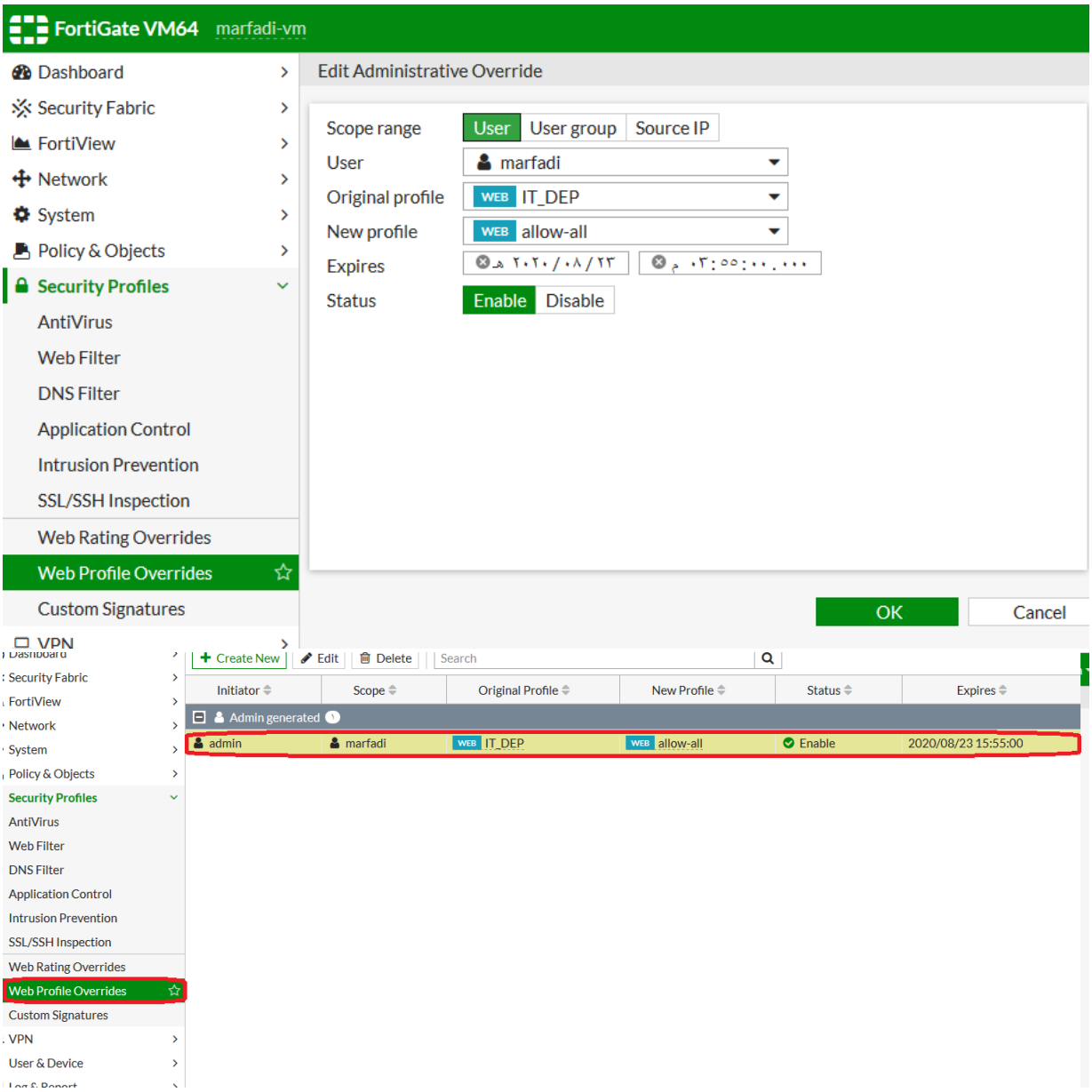
حيث أي موقع تريد معرفة الى أي تصنيف ينتمي نقوم بالخطوات التالية :



بالنقرعلى الزر Lookup rating سيتم معرفة التصنيف للموقع www.bab.com ولكن نظرا لأني اعمل ب fortigate vm ولا تحتوي على FortiGuard web filtering license فأني غيرقادرعلى الاستفاده من هذه الخاصية ..

Web Profile overrides :

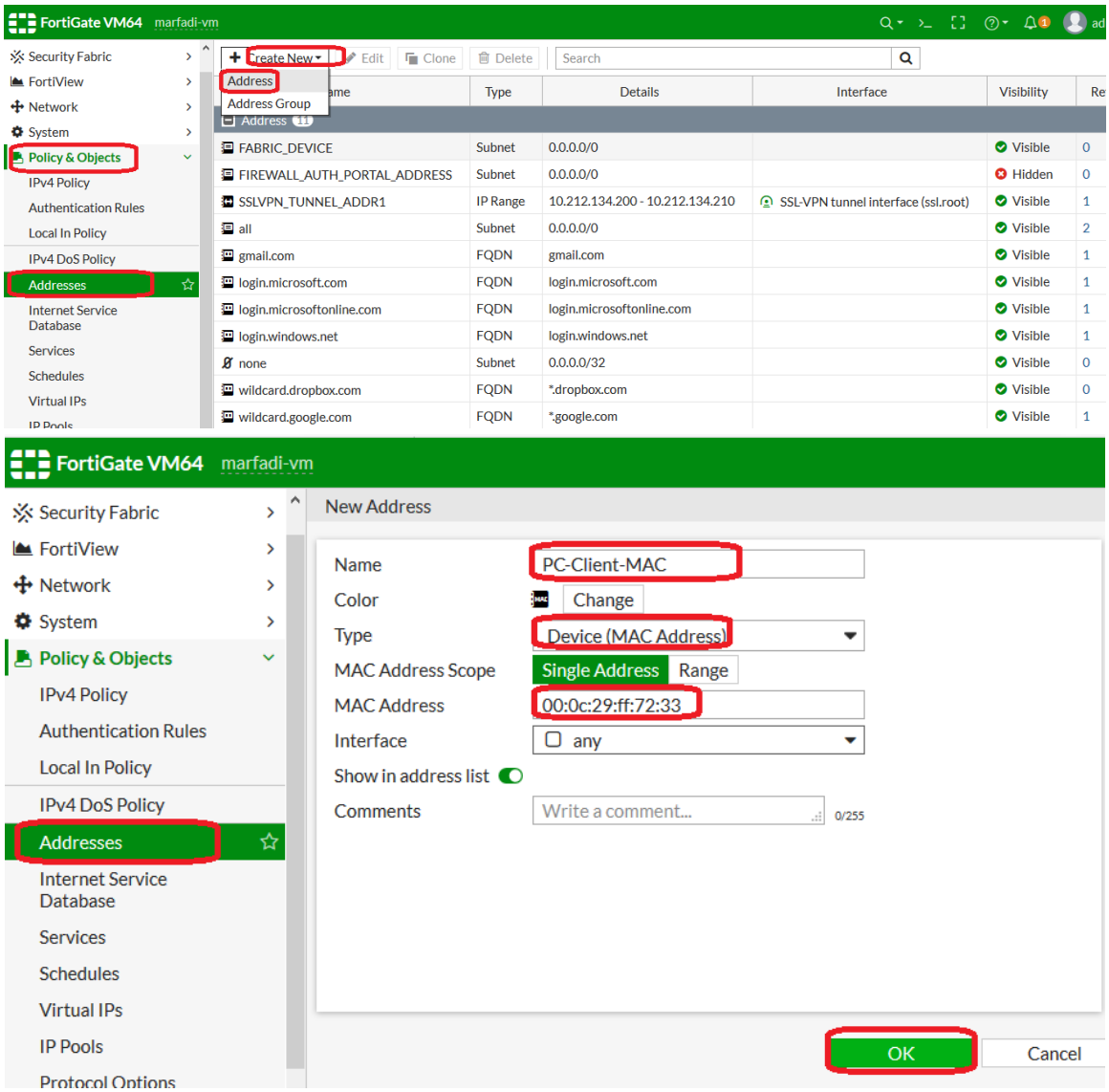
يستخدم في حالة وجود يوزر او جروب معين او ايبي معين مطبق عليه web filter profile معين وتريد في وقت معين ان يتطبق عليه web filter profile اخر...

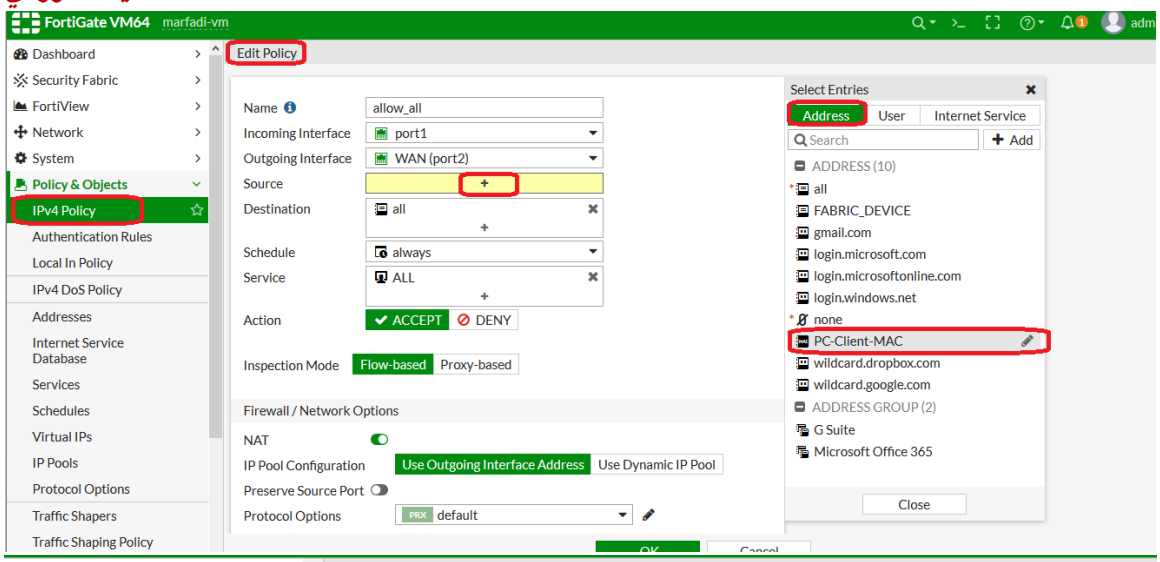


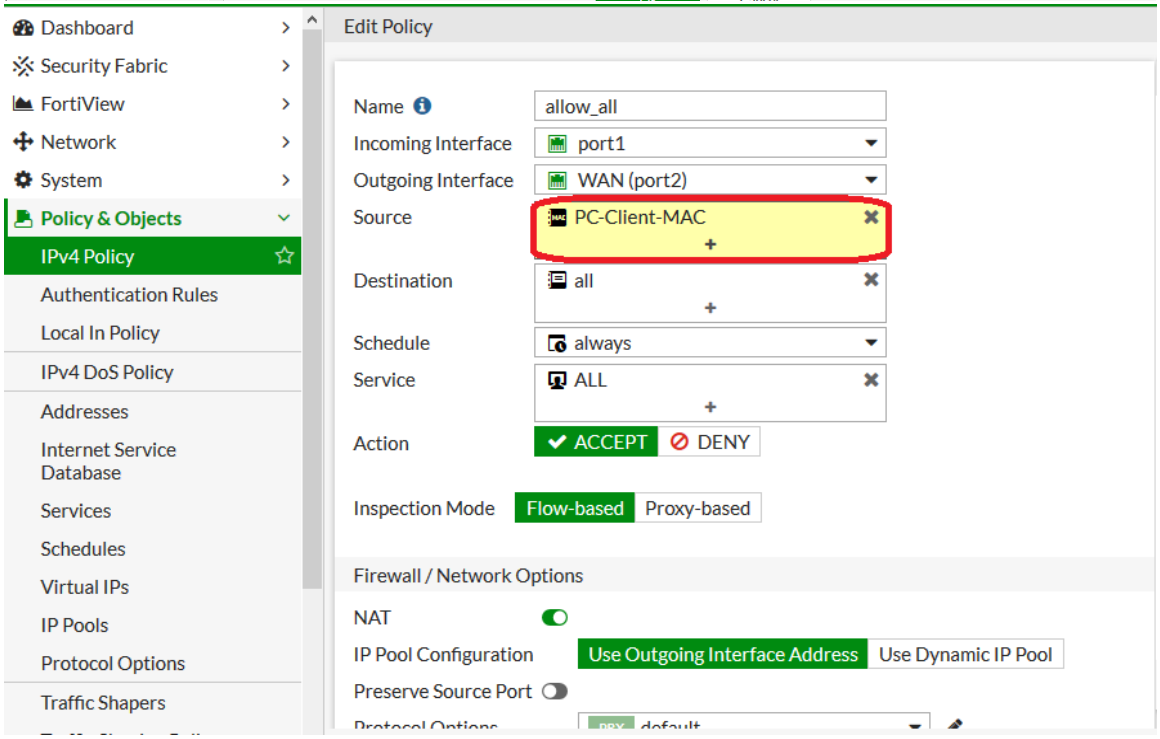
كما بالصور أعلاه يتبين بأن اليوزر المسمى marfadi الذي بالأصل ضمن الجروب IT_Managers والذي في الأصل مطبق عليها web filter profile =IT_Dep ولكن سيتم تطبيق الـallow-all= web filter profile في هذه الفترة الى تاريخ 2020-08-23 الساعة 15:55:00 .

:ADDRESS

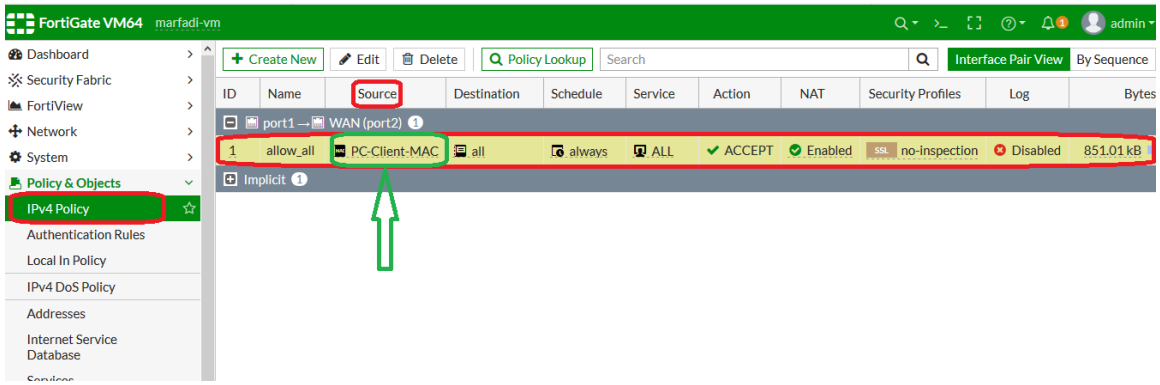
طريقة انشاء عنوان بحسب الماك ادرس للجهاز







تم تحديد هذا العنوان للجهاز بحسب الماك ادرس



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

❖ Fortinet solution

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

١- هاردويريسمى 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 الميل الخاص بك مثل سيرفر الـ exchange server

٢- Mail server : يعمل ك mail server مثله مثل الـ exchange server ويعتب اقوى ..

٣- Fortimanager :عباره عن جهازيعمل لك تحكم بكل اجهزه الفورتي التي عندك بالشبكة حتى 5000 جهازتحكم كامل بالسياسات والاعدادات واداره التحديثات ويعمل أيضا مع الجهاز fortianalyzer

٤- Fortianalyzer : جهاز يقوم بعمل تحليل الترافيك بشكل كامل وأيضا البروتوكولات التي تمر بالشبكة ويعطيك تقارير تفصيليه وبشكل رسومات عن الشبكة والـ logs حيث يعمل دمج كامل مع جهاز الـ 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 الكاسبر الذي بينزل على الجهاز الخاص بك (End point)حيث الفورتي كلاينت يعمل ك antivirus و web filter و فايروول ومن مميزاته بانه مجاني ولو عندك جهاز فورتي جيت فأنك ممكن ان تستفيد من ميزات إضافية ..

٨- Fortiswitch :هو عباره عن جهاز مثله مثل سويتشات سيسكو وغيرها

٩- fortiAP : عباره عن جهاز يعتبر من الحلول القوية والرائعة في اداره والتحكم بالوايرلس ..

❖Firewall :

الفرق بين الـ Firewall و Next Generation firewall و UTM

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

حيث الفايرول يوجد منه نوعين

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

مثل جهاز **fortigate firewall** من شركه فورتي 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- سوفتوير :مثل **Zonealarm** من شركه شيك بوينت و **pfsense** من شركه كومودو

Forefront من شركه مايكروسوفت مثل **TMG** والايزا

➢ تسلسل واشكال الفايروووول :

❑ **Firewall & UTM & Next Generation Firewall concepts**

Firewall	Concept
Transparent Firewalls Layer 2	✓ 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	✓ 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	✓ 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	✓ 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	✓ 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 اداره وتحكم للفايرول

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 الثالثه ..

يتعامل مع الـIP الا انه في network layer

يستطيع عمل فلتر على مستوى الباكت وأيضا يستطيع عمل NATING و VPN(ربط بين الشبكة الدخلية وشبكة أخرى)

3- Second generation :يعمل في الطبقة الرابعة وهي (transport layer) حيث يعتبر الجيل الثاني من الفايروول (لا يقصد بها next generation) لأن الـ next generation حاجه اعلى من الـ 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 الساعة (Application layer)حيث بدا التعامل مع على مستوى التطبيقات وظهر معانا أيضا IPSو bandwidth managementو web filterو application filter ..ومن عيوبه هو البطئ مقارنه بالأنواع السابقة لأنه كلما حققت حمايه وامان زياده فانه يكون على حساب السرعة.

5- UTM(Unified threat management) :

عباره عن جهاز لديه القدرة على تأدية عده مهام (خصائص) من خلال جهاز واحد حيث يتعبر فايروول و next generation firewallو يحقق لك الـ load balancingو data leak prevention (PLD) و gateway antispamو gateway Antivirusو app firewallو هذا هو النوع اللي سوف نشرحه ونتعامل معه حيث هذا الجهاز يحقق لك كل نقاط الحمايه في الشبكة من خلال جهاز واحد فقط وهو UTM .

Bandwidth ,Throughput ,Concurrent Sessions

مصطلحات مهمه :

1- Bandwidth : هو اقصى عدد للباكت تمر داخل القناه (اي القدرة الاستيعابية لهذه القناه) ..

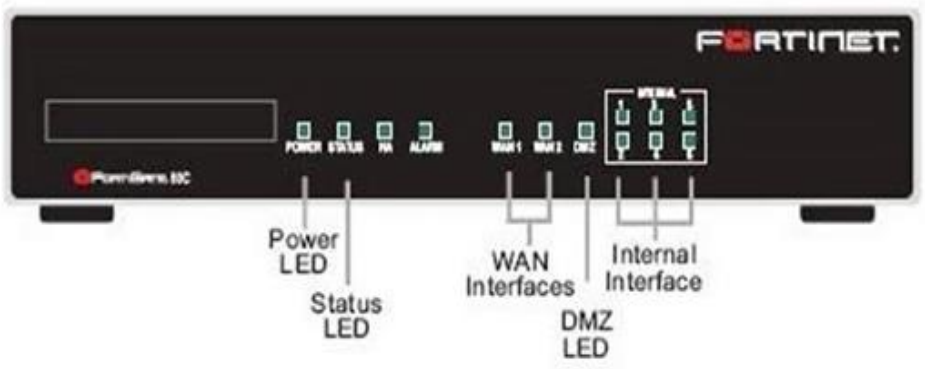
2- Throughput :هو عدد الباكت التي بيمر حاليا عندما الجهاز يتعامل(يتصل) مع جهاز اخر ...

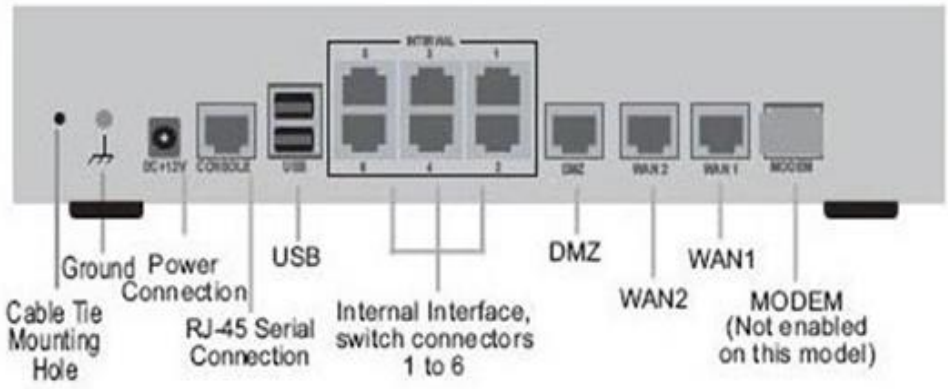
3- Concurrent sessions :هي عباره عم عدد ال connections(sessions) الذي يستطيع فيه الفايروول التعامل معها بنفس الوقت .

حيث عند فتح صفحة انترنت تعتبر جلسه او session

او فتحت برنامج سكايب يعتبر جلسه وهكذا ...


Bandwidth
Throughput





كما باصوره أعلاهلأحدى منتجات الفايروول فورتي 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 الUSB يستخدملأخذ نسخه باك اب من الاعدادات الخاصة بالجهاز او لو اردت أضافه firmware جديد للجهاز .
- Console port :يستخدم لعمل الاعدادات لجهاز الفورتي ويستخدم ذلك عندما تقوم بشراء جهاز فايروول جديد .

موديلات فورتي جيت :

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 تزيلها 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 الفورتي 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 فورتي جيت يكون في نفس المميزات(الخصائص) أعلاه تقريبا ...

Home lab Design

أي جهاز فورتي جيت فايروول (حقيقي وليس وهمي)يكون الايبي الافتراضي له هو 192.168.1.99 ويمكنك الوصول اليه عبر الPINGو HTTPو HTTPSوذلك عبر أي منفذ lan في الجهاز ...

حيث المنفذ lan1 يكون مفعل عليه DHCP أي بمجرد توصيل كيبل الشبكة للـport1 الى الابتوب الخاص بك فأن كرت الشبكة في الابتوب سوف يأخذ ايبي من نفس الرينج 192.168.1.0 .

بعكس لو قمت بتوصيل الكيبل بين الابتوب و port2,3,... فأنه يجب عليك ان تكتب ايبي لكرت الشبكة للابتوب من نفس الرينج 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 وتجددها سنويا من شركه فورتي جيت ..

لكي تتمكن من تنزيل الـvm fortigate يجب ان يكون لديك حساب على

https://support.fortinet.com

ولن تتمكن من انشاء حساب الا لو كنت مشتري جهاز من شركه فورتي جيت..

حيث عن طريق الرابط أعلاه يمكنك عمل تسجيل لجهاز الفورتي جيت التابع لك او عمل تجديد للترخيص للجهاز(أيضا يمكنك عمل هذا أيضا من خلال صفحة الويب التابع لجهاز الفورتي جيت نفسه)وأيضا يمكنك تنزيل الfirmware الجديد او قطع ticket للتواصل مع شركه فورتي في حالة مواجهه مشكله ما او عمل chatting معهم ..

عند شراء جهاز جديد يجب ان تعمل له تسجيل في موقع الدعم الخاص بفورتي نت وذلك لكي تقوم بتفعيل الجهاز الخاص بك وبهذا تسمح لجهاز الفورتي جيت الخاص بك بأن يستلم التحديثات من الفورتي جارد (fortiguard)الخاصة بـIPSو AVو Antispamو web filteringو application control .

وأيضا لكي تتمكن من عمل upgrade OS للجهاز..

ولكي تقوم بالتسجيل يجب ان يكون جهاز الفورتي جيت موصل بالإنترنت .

❖ طريقة عمل Registration لجهاز الفورتي جيت :

القوائم الرئيسية للفورتي جيت :

1- System : هي الاعدادات الرئيسية للفورتي جيت

2- Policy&objects :

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

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

3- Security profiles :

هي الاعدادات الأمنية مثل الويب فلتر او IPS

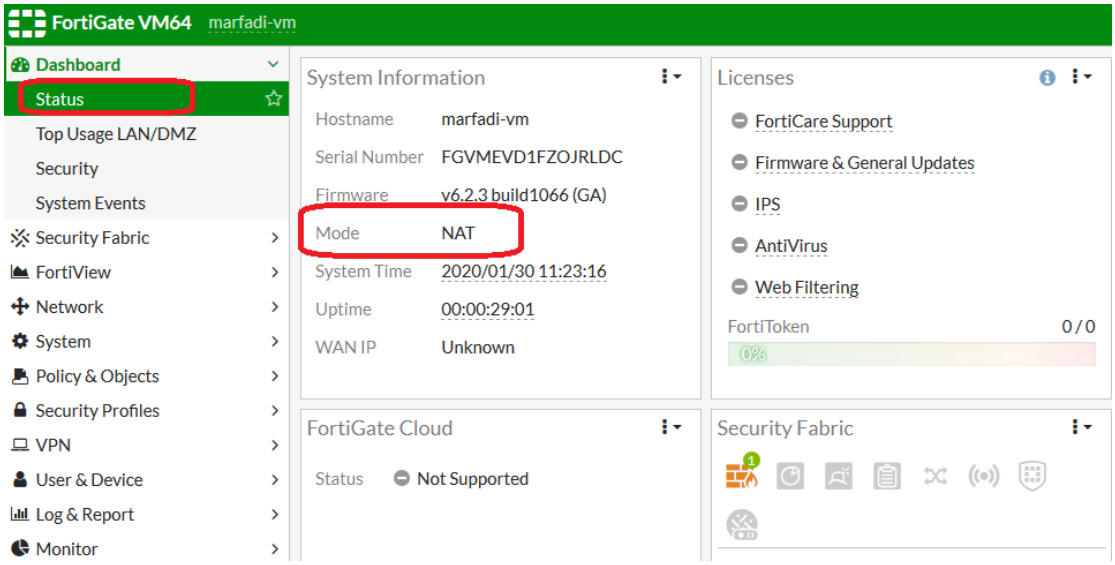
4- User& devises :

خاص بالمستخدمين والأجهزة التي سيتعامل معها الفورتي جيت.

5- Logs&reports :عباره عن التقارير والـ logs على أي شي يحصل لدي في الشبكة .

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

1- NAT mode



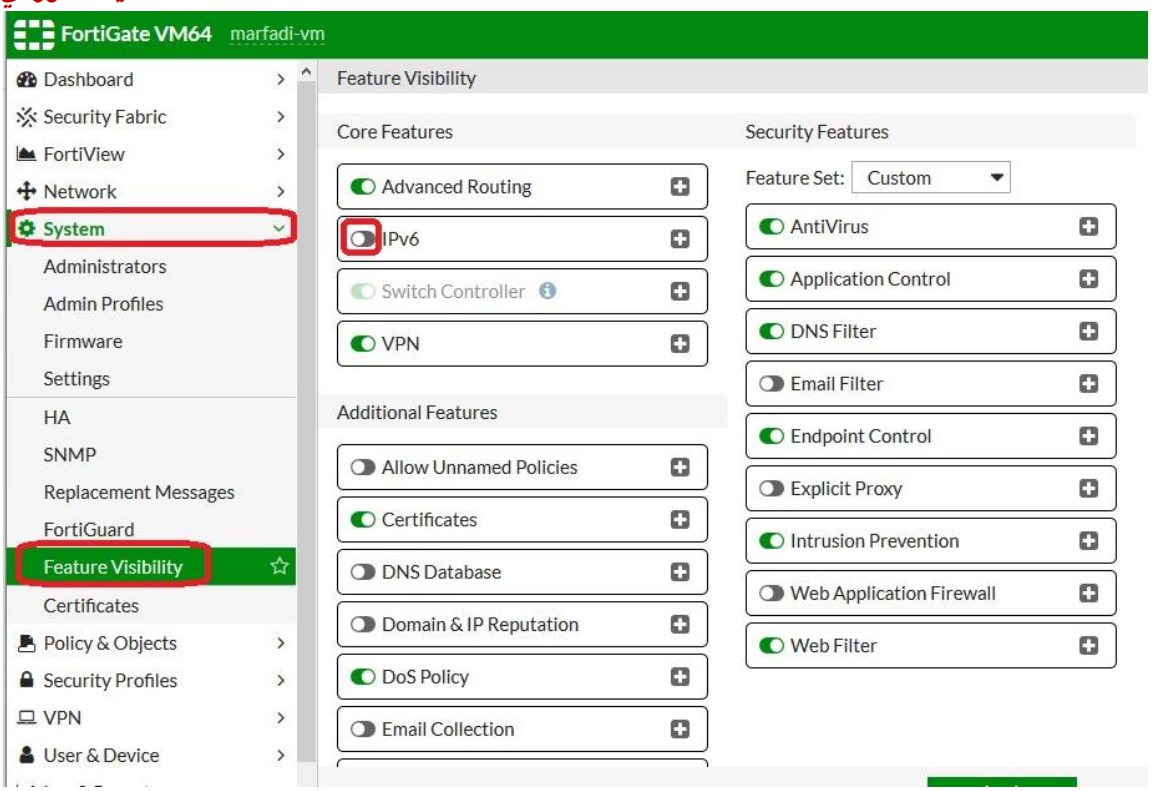
ملاحظة:

جهاز الفورتي جيت لا يحتوي على ازرار إيقاف التشغيل او اعاده التشغيل بل يمكنك ذلك من CLI او من GUI .

ماهي ال features :

هي الوظائف التي اجعل جهاز الفورتي 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 ..



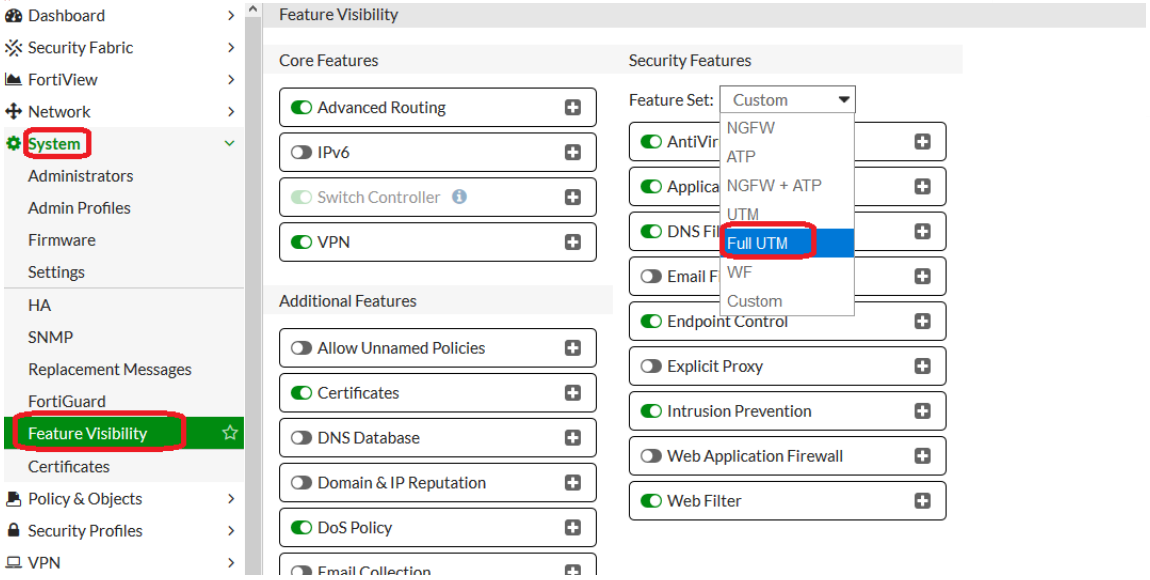
كما بالصورة أعلاه فأن جهاز الفورتي جيت لا يدعم IPV6 .

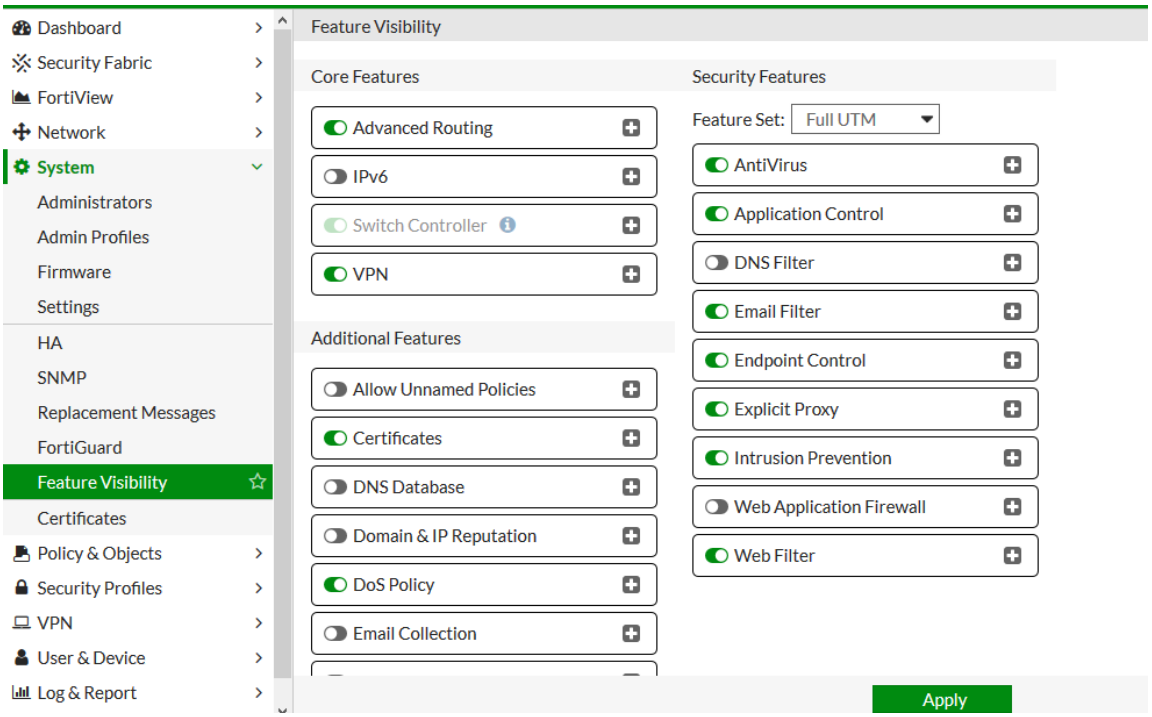
حيث الfeatures مقسمه الى جزئين :

1- Core Features :هي الخصائص الخاصة بالشبكة ليس لها علاقه بـsecurity مثل advanced routingو IPv6و VPN حيث استطيع تشغيلها بدون ترخيص (license).

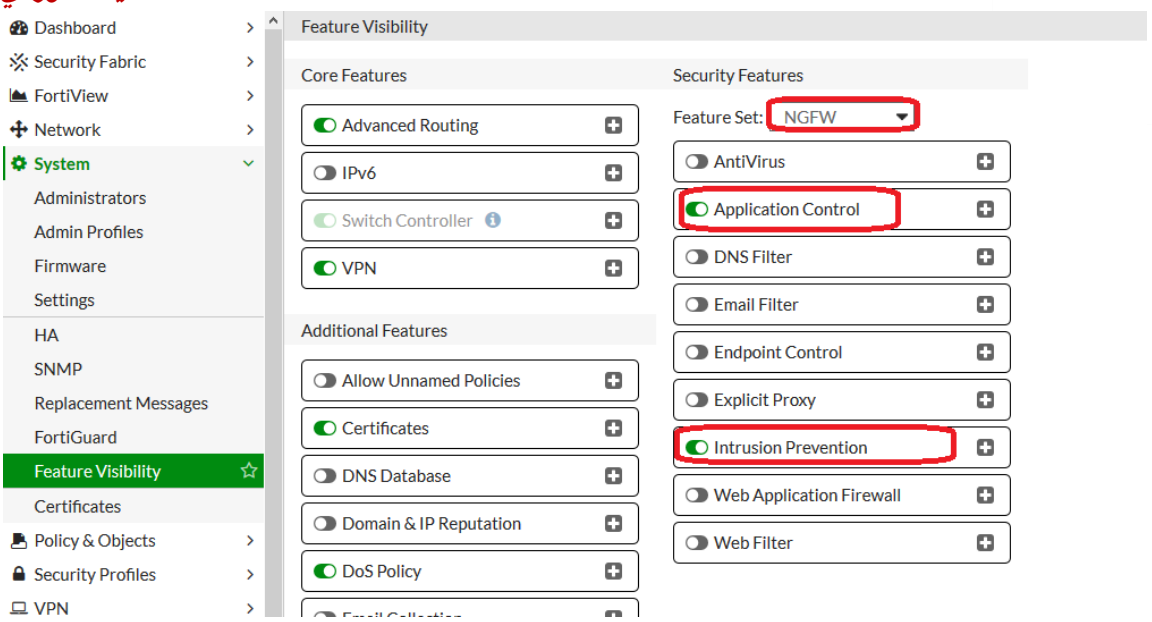
2- Security features : هي الخصائص الخاصة بالحماية مثل AV,application control,ips,web filter,email filter وهذه الخصائص لا تعمل الا بترخيص

ويمكن تعديل الخصائص من features set واختيار المناسب لك مثلا full UTM حيث سيقوم بتشغيل كل الخائص(features)



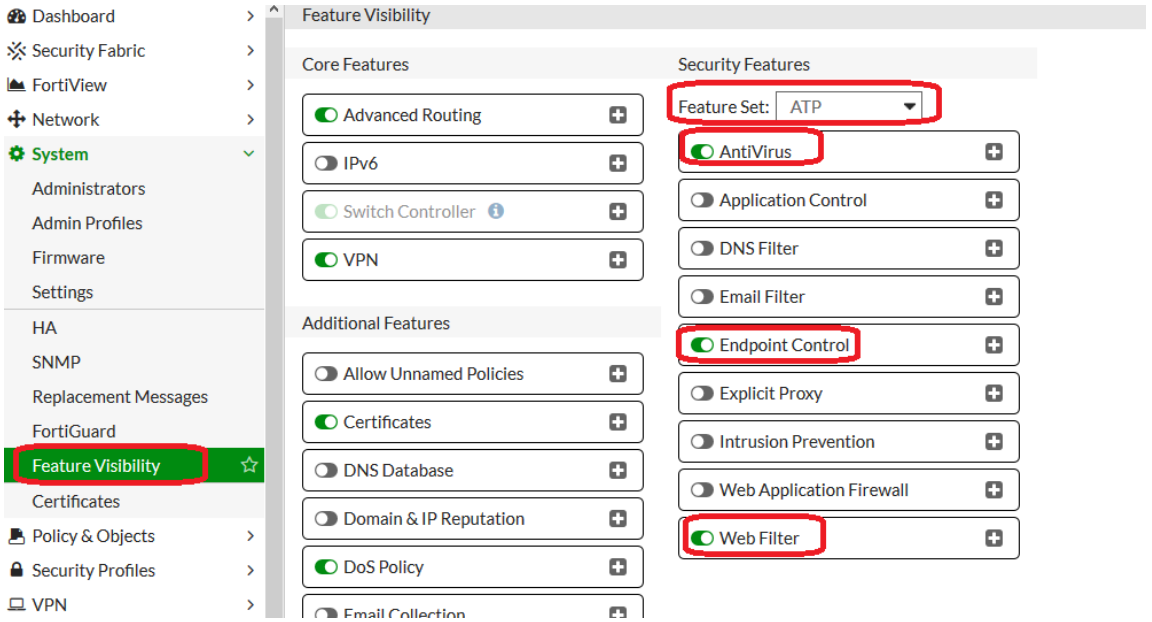


تم تحديد كل **security features** كما بالصورة أعلاه..



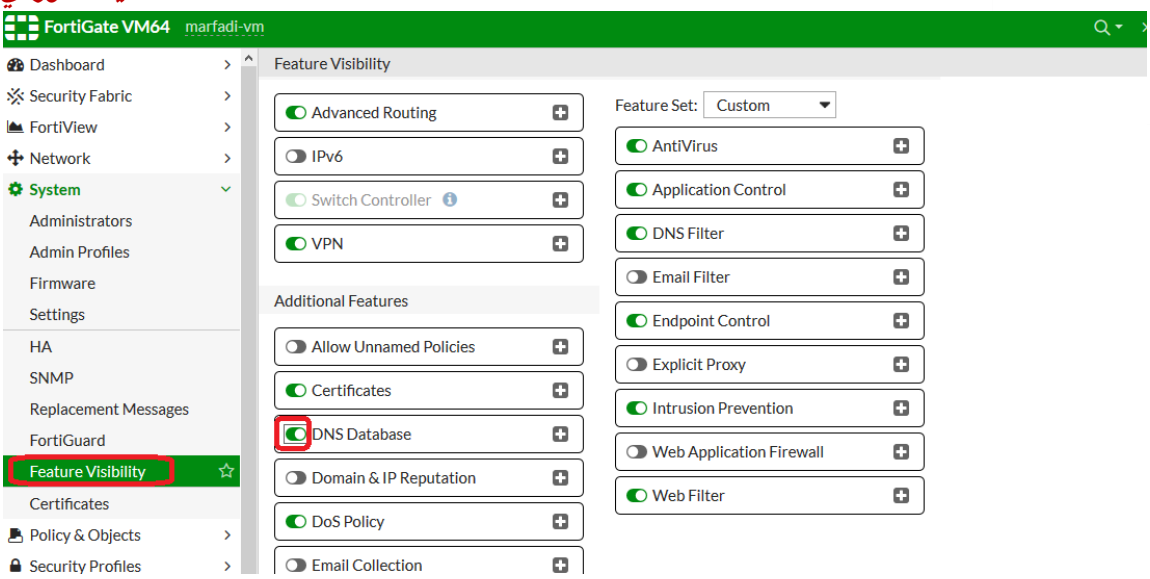
عند اختيار features set=NGFW .

ولدينا خيار يسمى ADVANCE THREAT PROTECTION=ATP



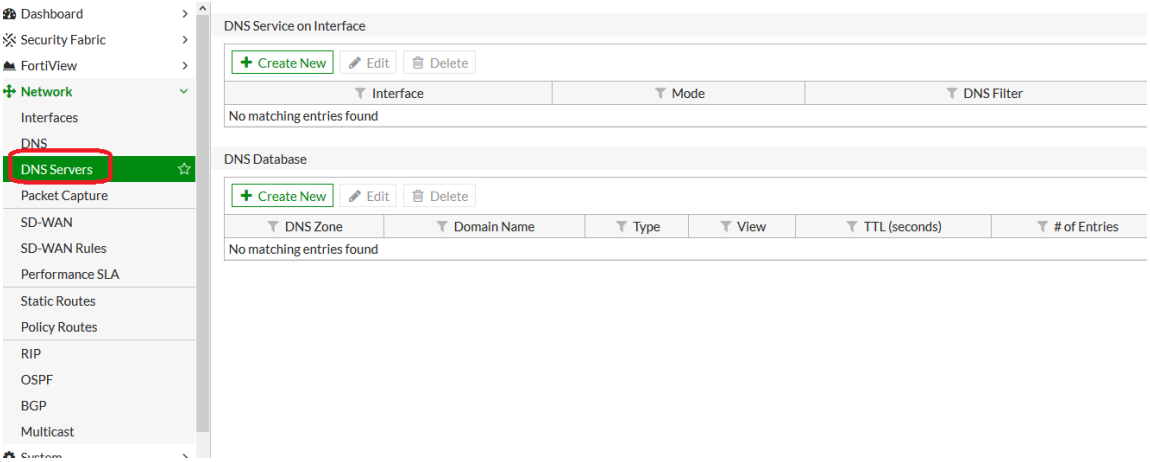
حيث هنا قمنا فقط بتفعيل الخاصية ولكننا لم نقم بعد بتطبيقها على أي احد بالشبكة (أي تطبيقها كرووول على اليوزرات او الاجهزه).

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



فبمجرد تفعيل DNS Database فأنه تظهر لك قائمه باسم

DNS SERVER كما بالصورة ادناه

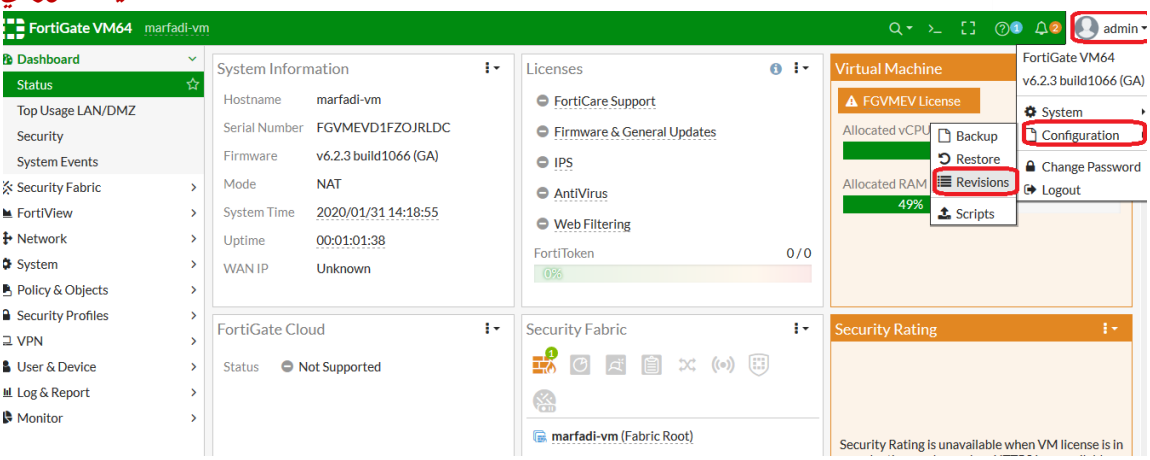


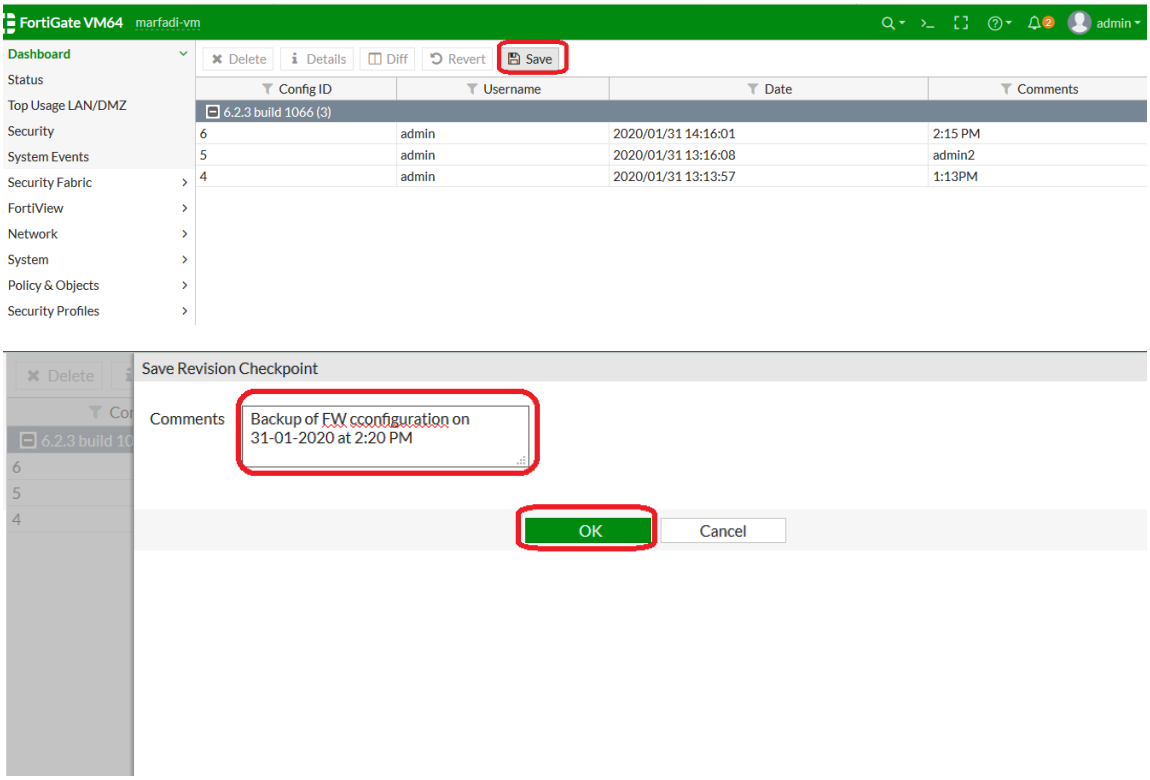
ما هو Revisions في الفورتي جيت :

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

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

واستطيع ارجاها باي وقت ...

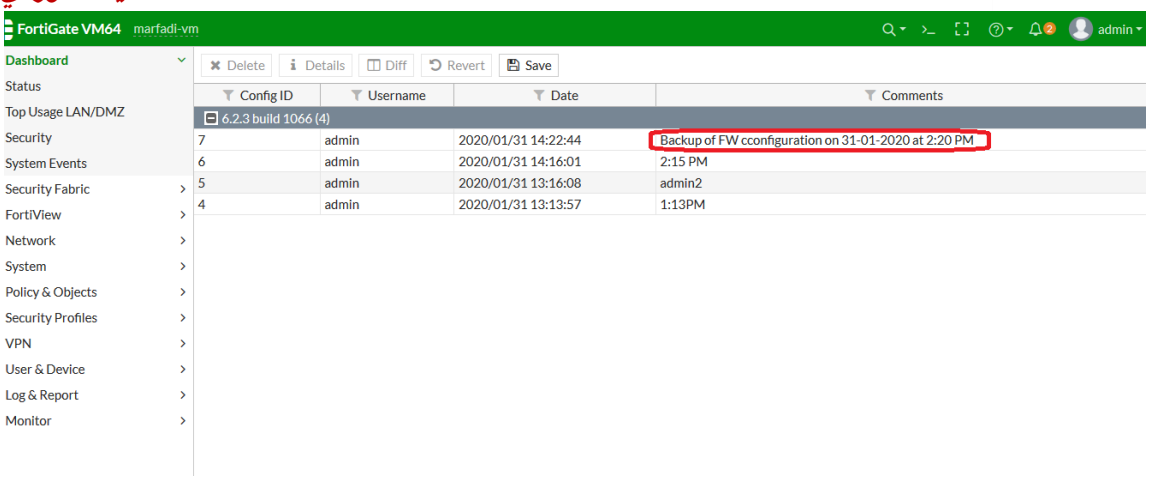


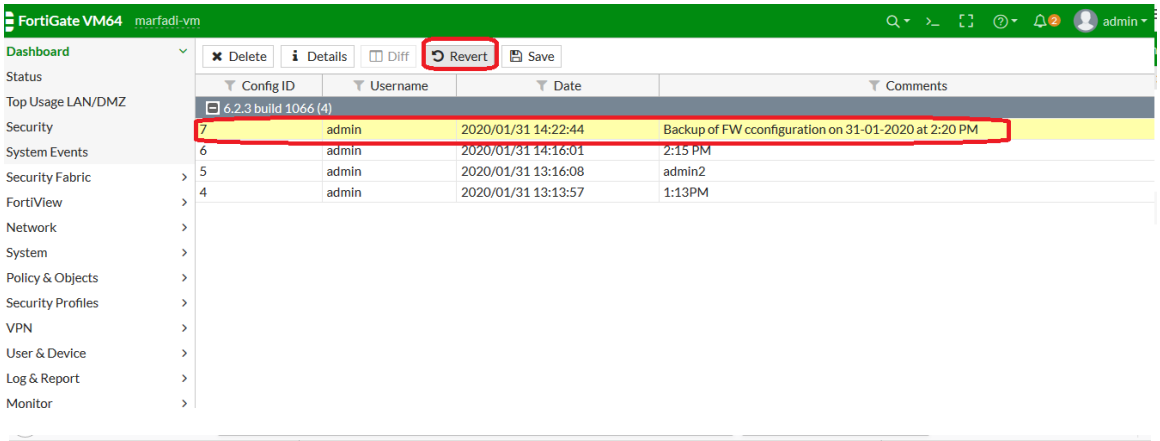


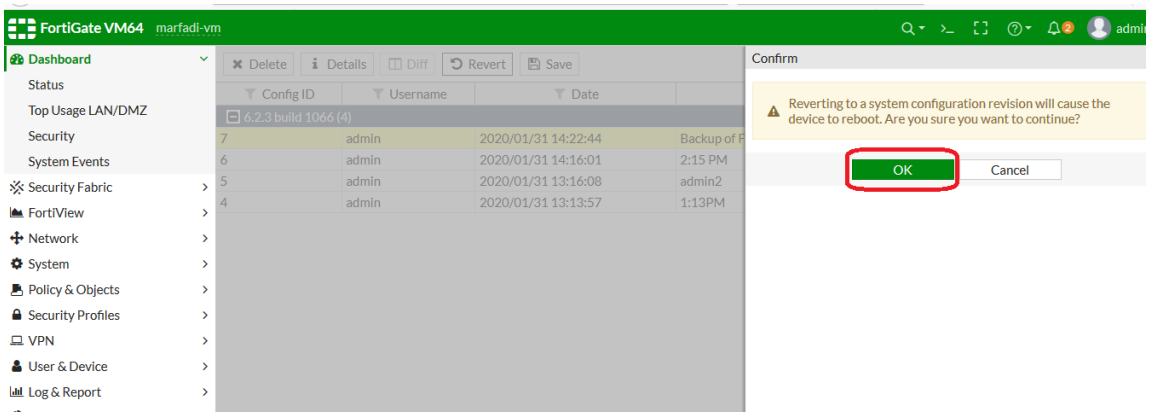
حيث كما بالصورة أعلاه تم عمل نسخه باك اب للإعدادات وتم حفضها على جهاز الفورتي جيت نفسه

...

الان سنقوم بعمليه الاستعادة لـcheckpoint كما بالصورة التالية





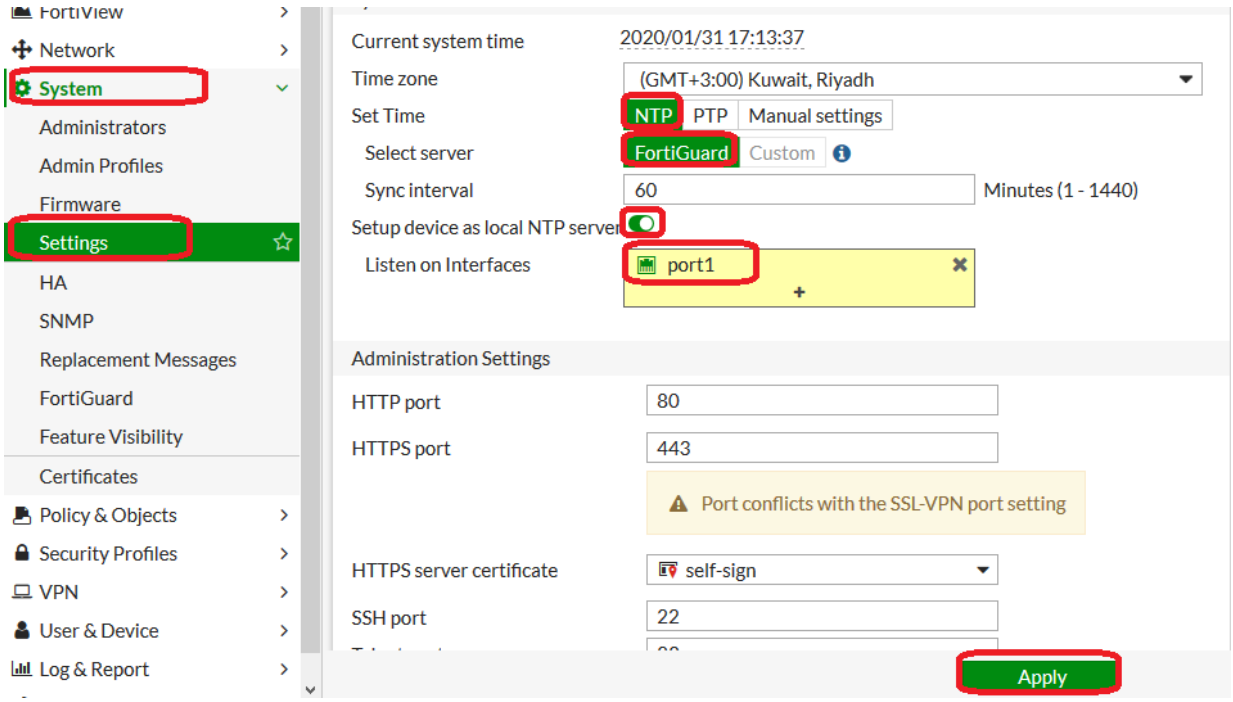


سيتم استرجاع النسخة بالاعدادات التي كانت عليها في تلك اللحظة بعد اعاده تشغيل الجهاز ..

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

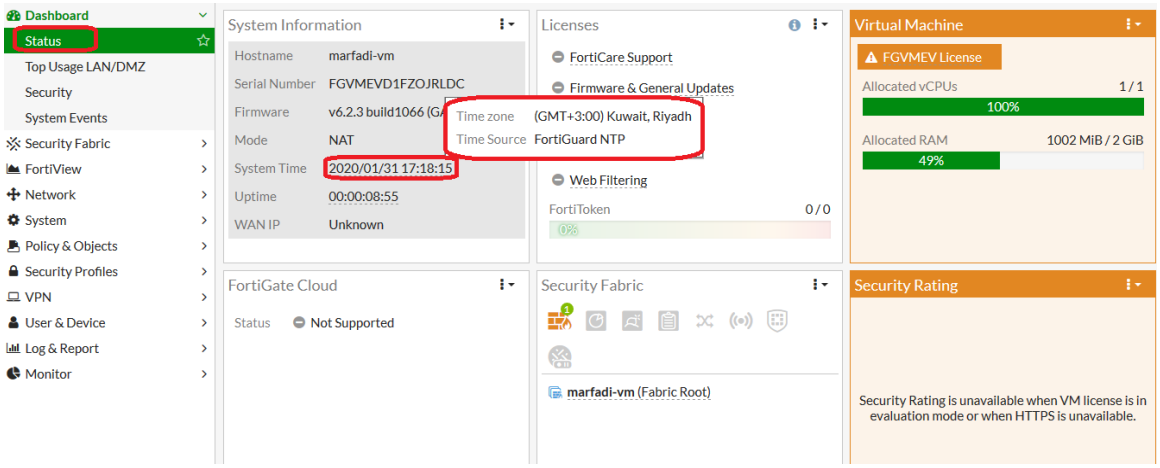
❖NTP server(Network time protocol)

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



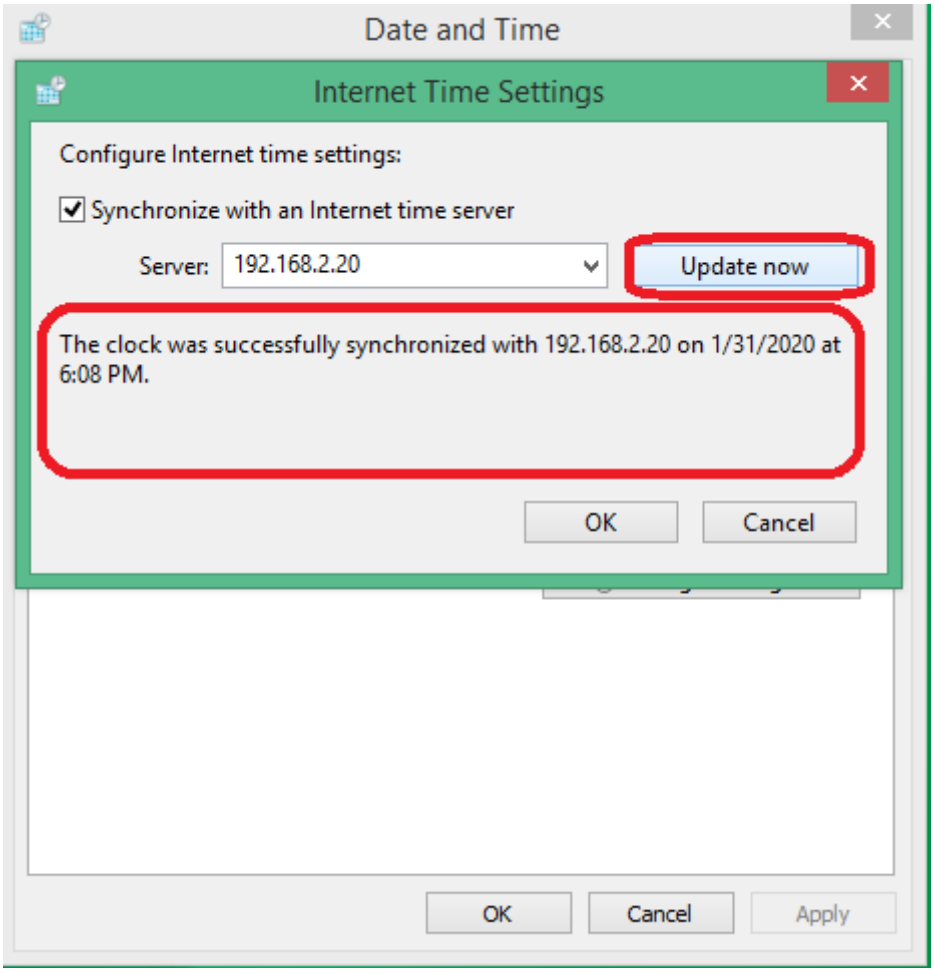
نقوم أولا بالتأكد بأن الوقت والتاريخ والمنطقة الزمنية على الفورتي جيت مضبوطة حيث سيتم عمل مزامنه للوقت والتاريخ بين جهاز الفورتي وسيرفر fortiguard ntp server كل 60 دقيقه.

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



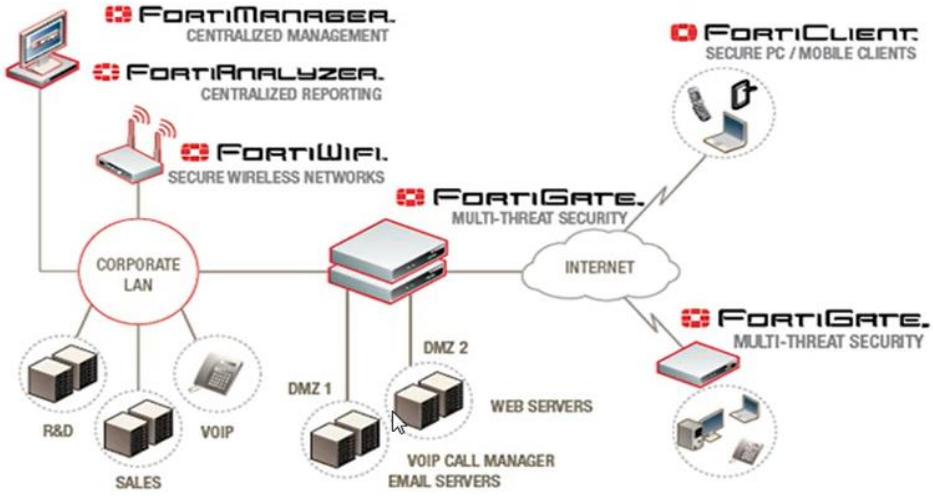
تم الحفظ بالإعدادات كما بالصورة أعلاه ...

ثم من على اجهزه الشبكة نقوم بتعديل الاعدادات لديهم بأن ال ntp server هو عباره عن ايبي 192.168.2.20 وهو port1 للفورتي جيت.



❖ تصميم الشبكة :

❑ FortiGate Network Design



الفورتي جيت سوف يكون Edge الحافه (حافه الشبكة).

كما بالصورة أعلاه فأن الفورتي 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 الفورتي جيت(الانترنت) والطرف الاخر خلف الفورتي جيت وهو الشبكة الداخليه(LAN).

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

حيث الـDMZ هي شبكة معزولة ومرتبطة بالفورتي جيت لكنها ليست LANولا هي internet هي ما بين الاثنين .

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

حيث هي مرتبطة بlan 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 .

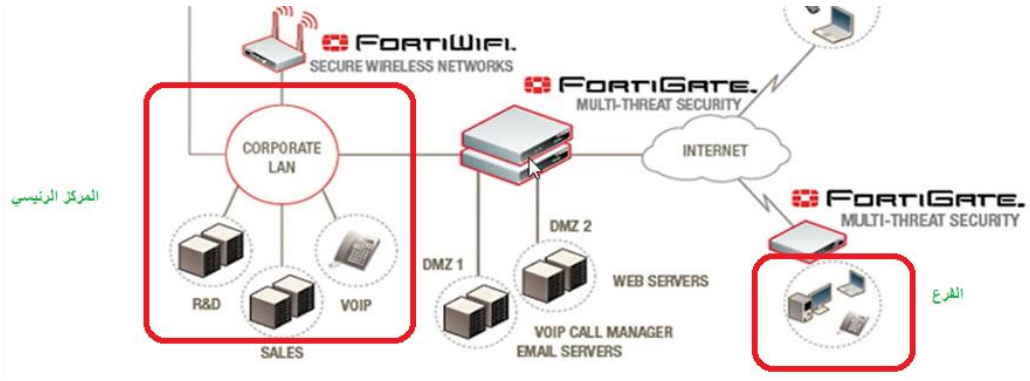
أي شي خلف الفورتي جيت يسمى LAN مهما كان اسمه سواء سيرفرات او اكسس بوينت او اجهزه عاديه او سويتشات ..الخ وجميعها سوف تكون تحت سيطرة الفورتي جيت .

ملاحظة:

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

سيناريوا اخر للتصميم الشبكة للربط بين الفروع :

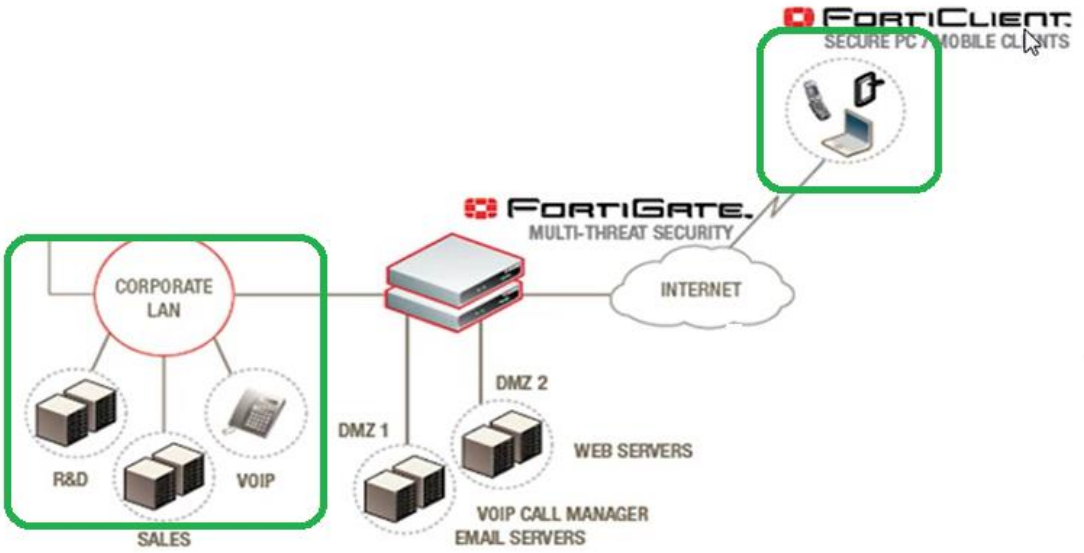
نفترض لديك مركز رئيسي وفرع اخر في مكان اخر وكل فرع يوجد لديه انترنت وايضا يحتوي على جهاز فورتي جيت .



حيث الفرعين متوصلين مع بعض عبر الانترنت عن طريق الVPN.

حيث يصبح الفرعين متوصلين مع بعض وكانهم شبكة واحده ..

وأيضا لو لدي جهاز موبايل او لابتوب موجود في دوله أخرى حيث استطيع ان اتحكم بهذا الجهاز عبر الفورتي جيت الموجود بالمركز الرئيسي عبر برنامج يسمى كلاينت ايند بوينت يتم نزوله على الابتوب او الموبايل..



Advice administration

طرق التعامل مع جهاز الفورتي جيت والتحكم فيه من اعدادات وغيرها ..

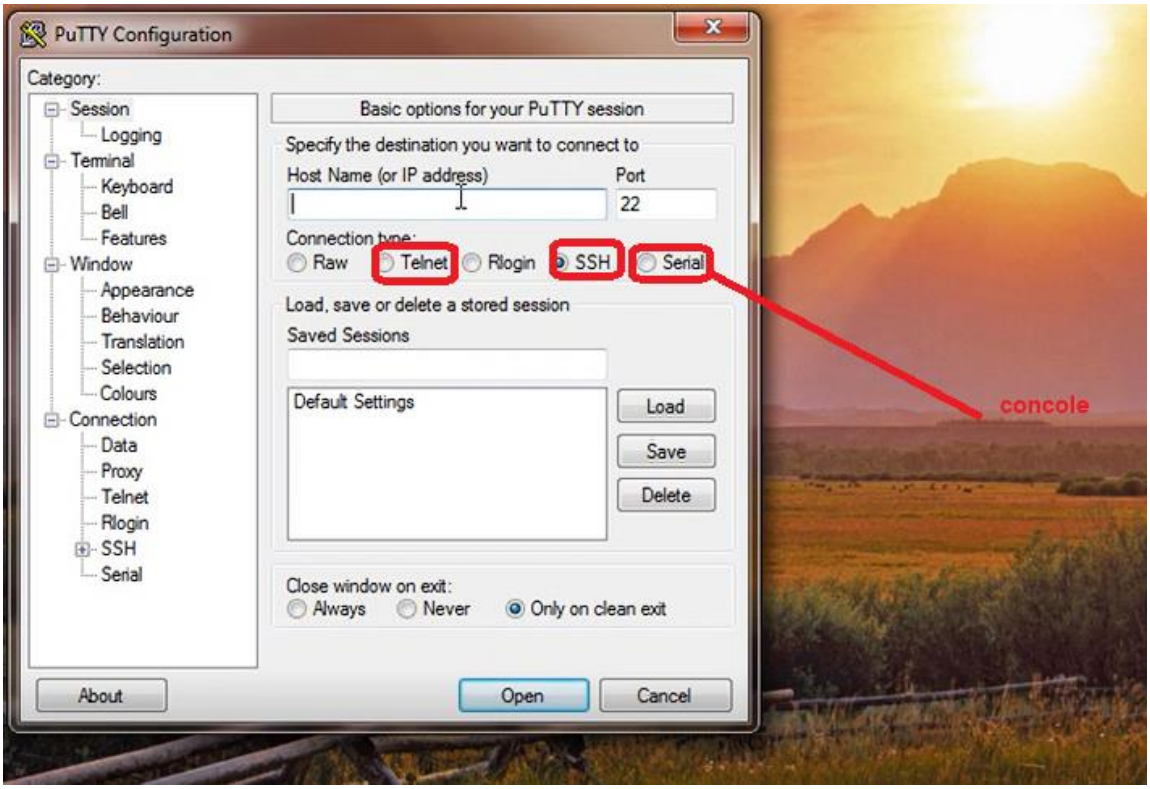
1- Web GUI(http,https) :يجب ان يكون لديك متصفح انترنت تدخل من خلاله بالايبي التابع للفورتي جيت.

2- CLI(console,Telnet,ssh,GUI widget) :هنا يتم التعامل مع جهاز الفورتي جيت بالاوامر command line باحدى الطرق التالية :

A – console: توصيل كيبل كونسول للابتوب وبواسطة برنامج مثل putty وبتوصل للفورتي جيت بدون ماتحتاج الى ايبي الفورتي جيت (حتى لو مش عارف الايبي للجهاز يتم استخدام هذه الطريقة).

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

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

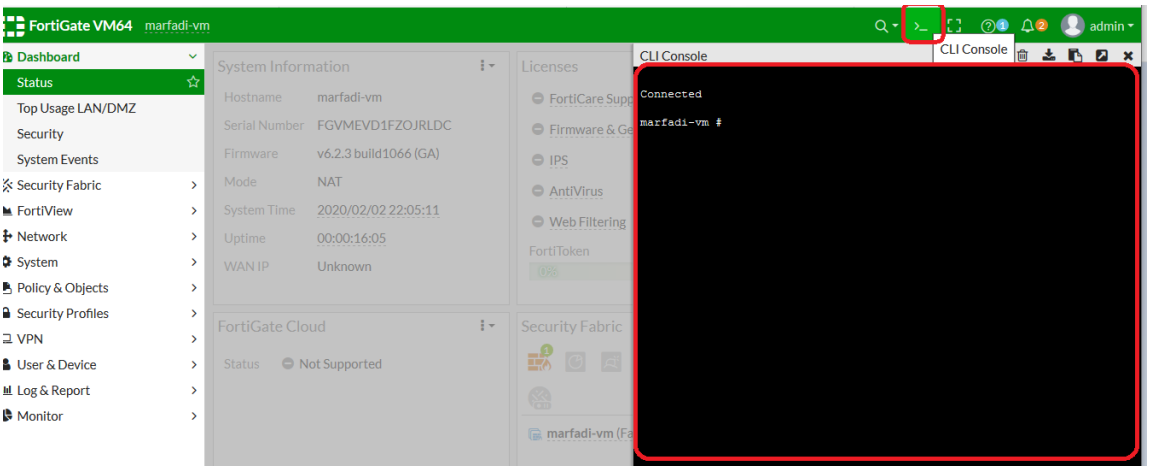


ملاحظة:لا يمكنك الوصول الى الفورتي جيت سواء ssh او telnet عبر برنامج الـ putty الا بعد عمل الامر

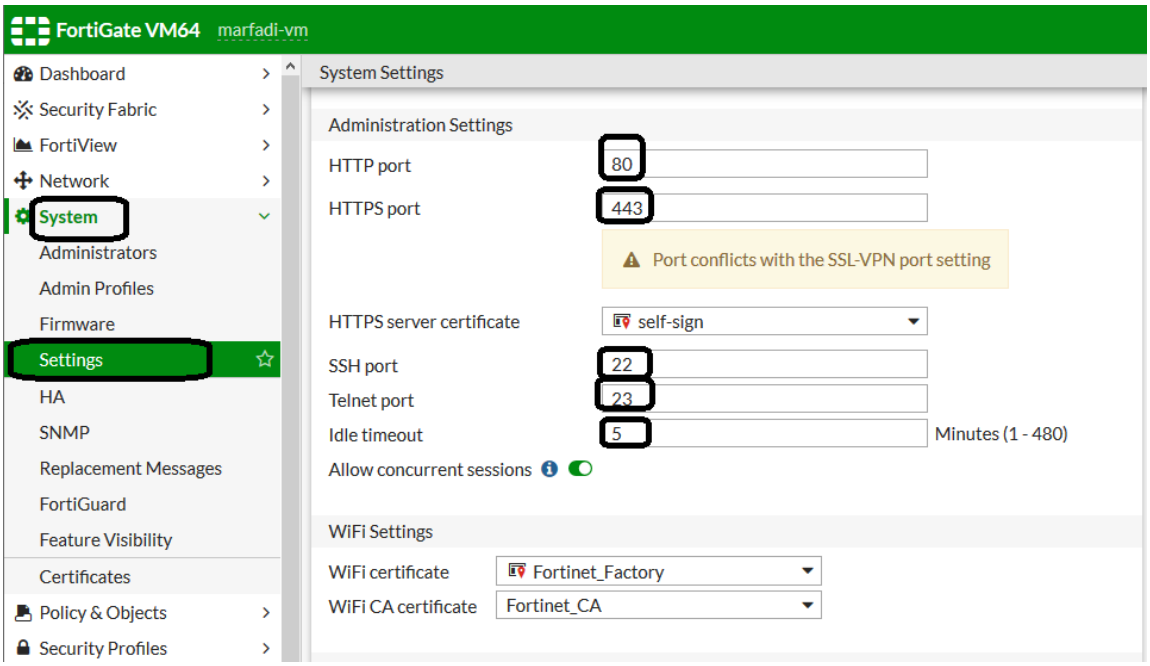
Set allowaccess ssh telent

لكرت الشبكة الخاص بالفورتي المراد الوصول اليه ..

D – GUI Widget :شاشه سوداء مثل CMD يتم الوصول اليها من GUI كما بالصورة ادناه .



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



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

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

192.168.2.20:4433

وهكذا ..

خيار idle timeout =5:هذه الخاصية بتجبر الفورتي جيت على عمل logout بعد مرور 5 دقائق وبعدها تجبر اليوزر بإدخال اليوزرنيم والباسورد مره أخرى كنوع من الأمان .

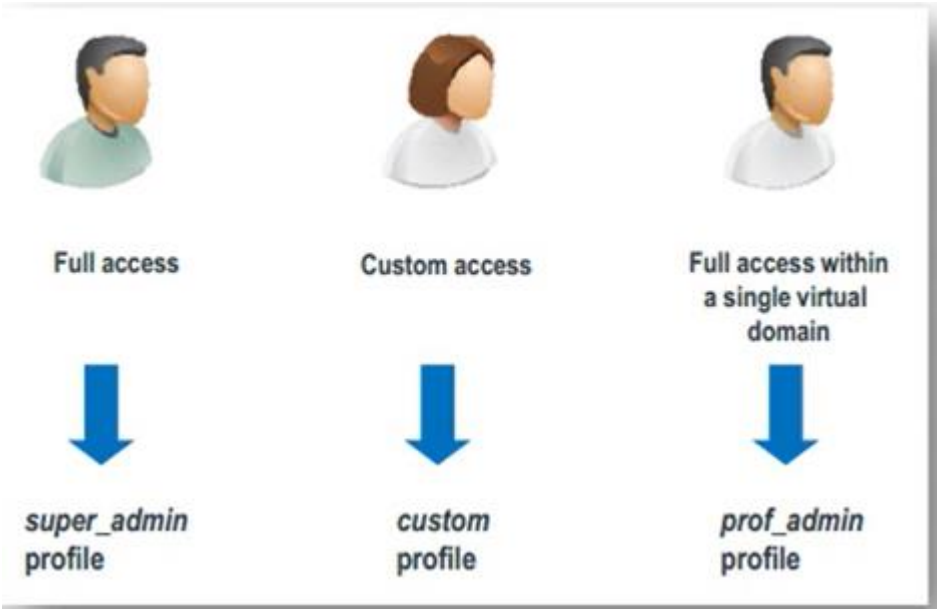
Device administration

Administrator : الأشخاص الذي لهم صلاحيات للدخول للفورتي جيت والتعامل معه وعمل اداره للجهاز وأنواع الـ administrator هي:

1- Full admin (super admin) :هو الذي له صلاحيات على كل الفورتي جيت بدون أي تقييد

2- Prof admin : هو نوع من الـ administrator الذي لديه صلاحيات عاليه جدا ضمن بيئه اسمها (SVD) single virtual domain

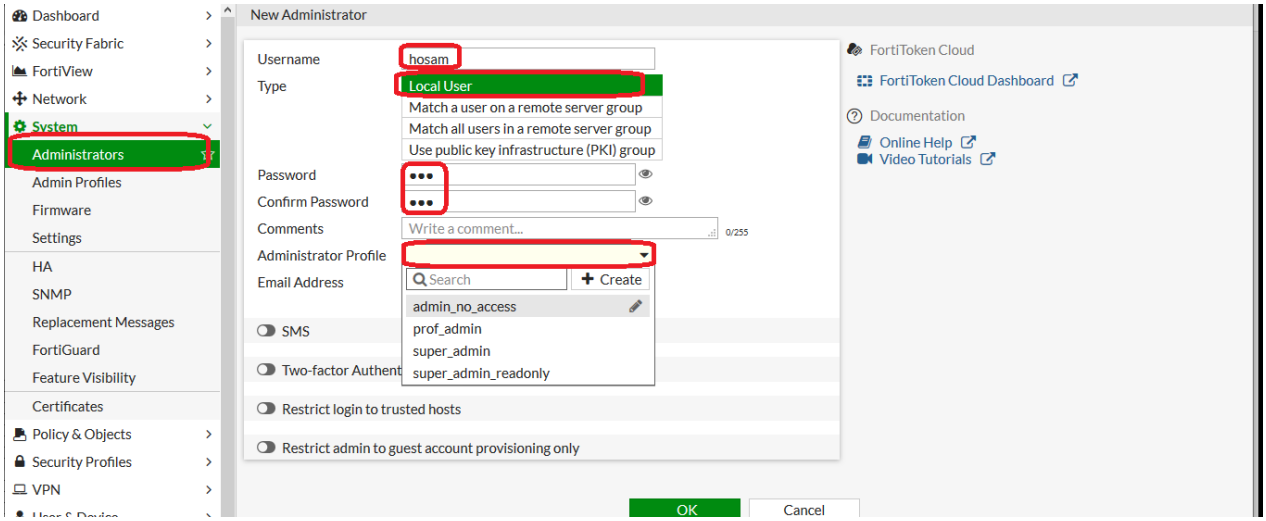
3- Custom profile :الوصول الى صلاحيات محدده حيث أقوم بتحديدها انا له.



Admin profile : هي الاعدادت التي أقوم بإعدادهاالأحدى الـadministrator أعلاه لكي يصل اليها ..

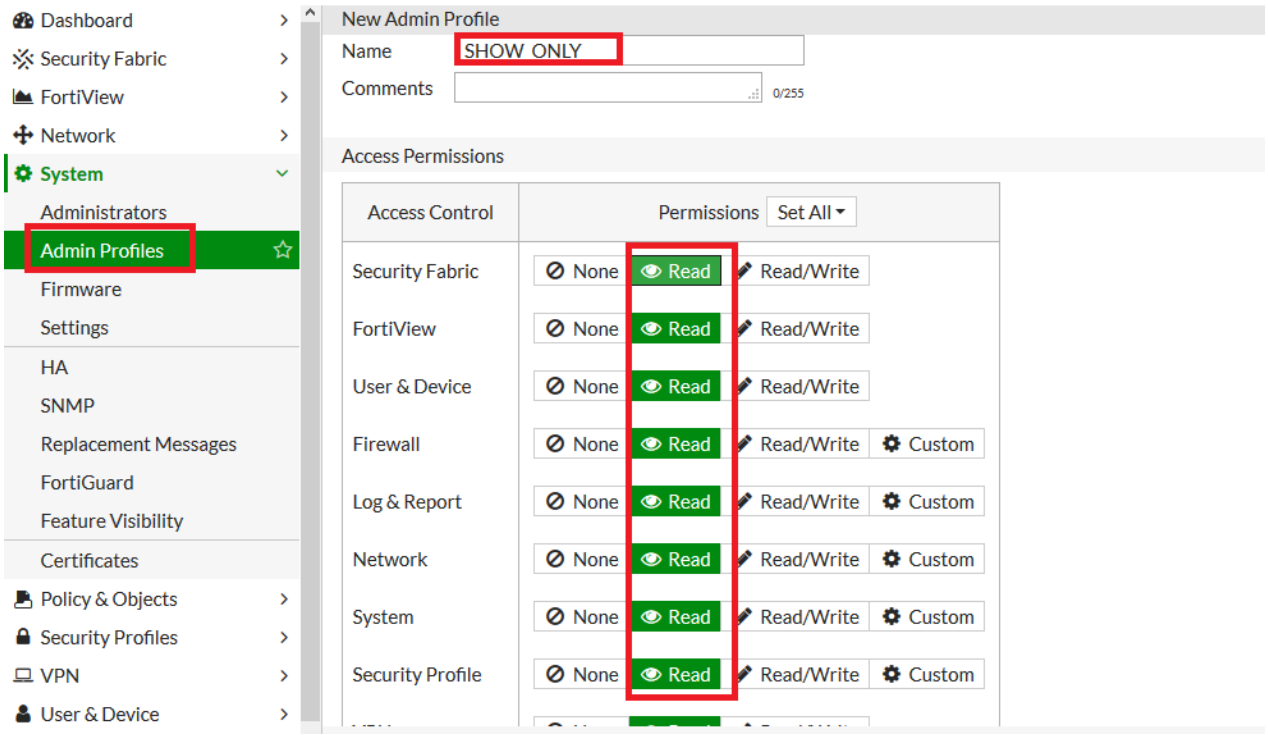
Permission : هي الصلاحيات (read,write,none) التي سيتم تحديدها للـadministrator .

طريقة انشاء administrator جديد :



اسم الـadministrator 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 الصوره ادناه

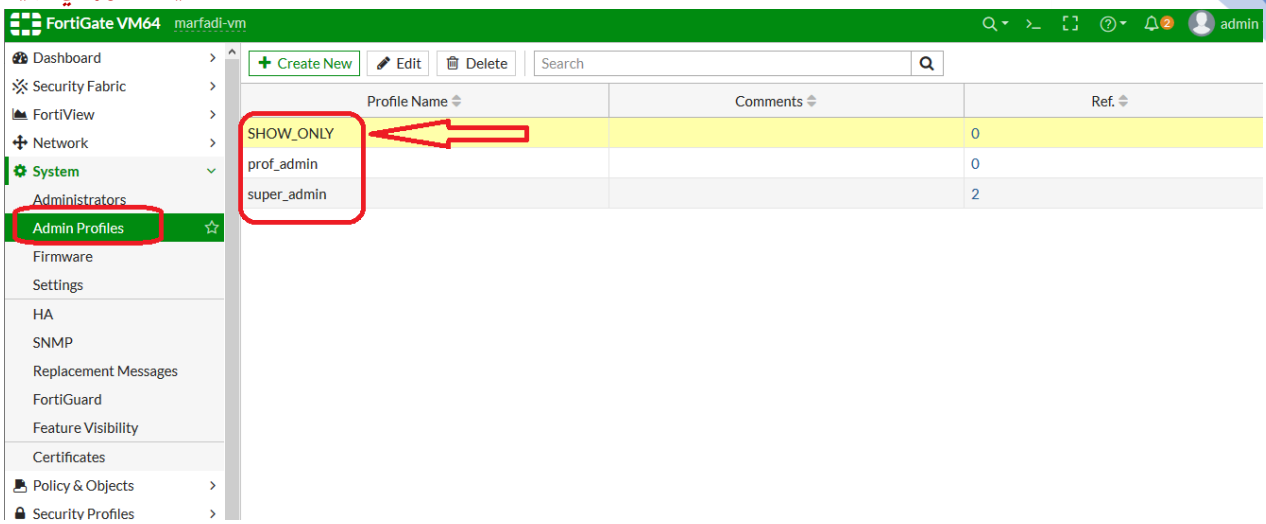


حيث اسم البروفايل هو show_only وله صلاحيات القراءه فقط على كل الأشياء(الأشياء)التي سوف اتعامل معاها كما بالصورة أعلاه ..

حيث صلاحيه الnone معناها بأن هذه الشاشة لن تظهر نهائيا لليوزر.

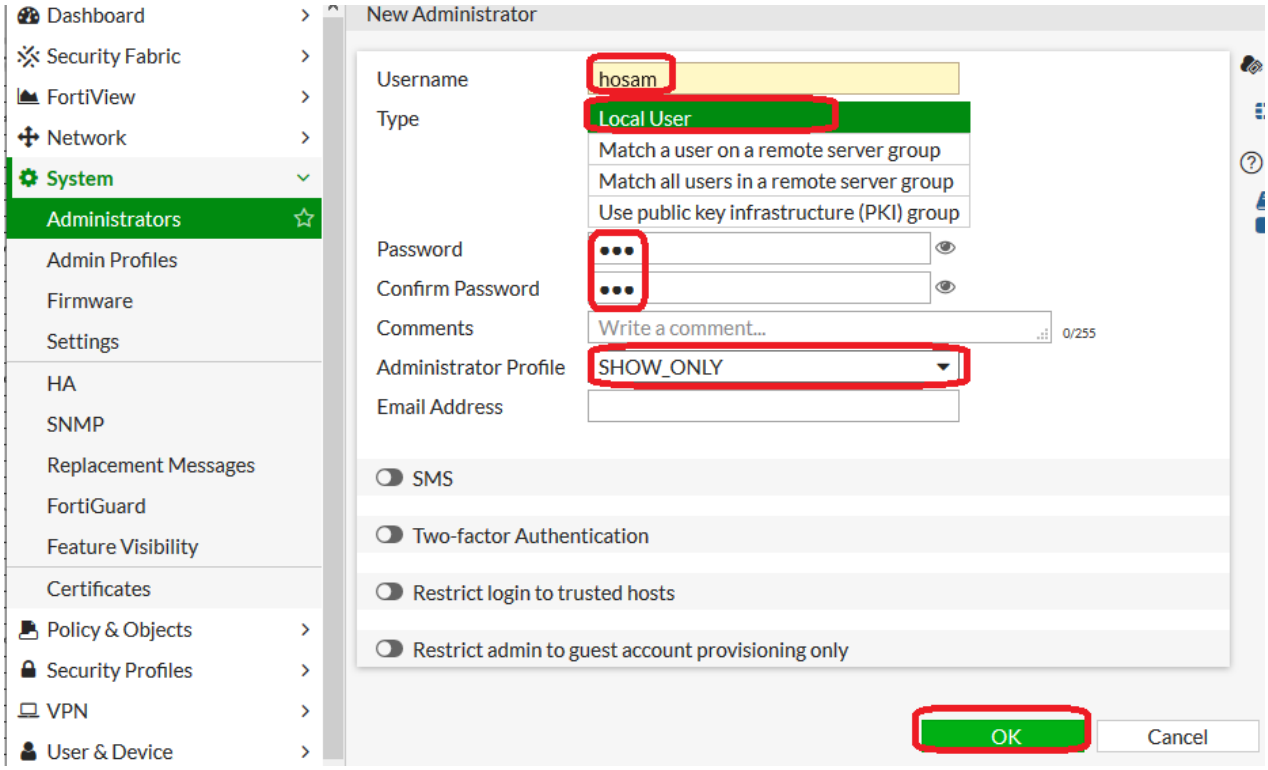
و read :للقراءه فقط ولا يمكنك التعديل عليها ،

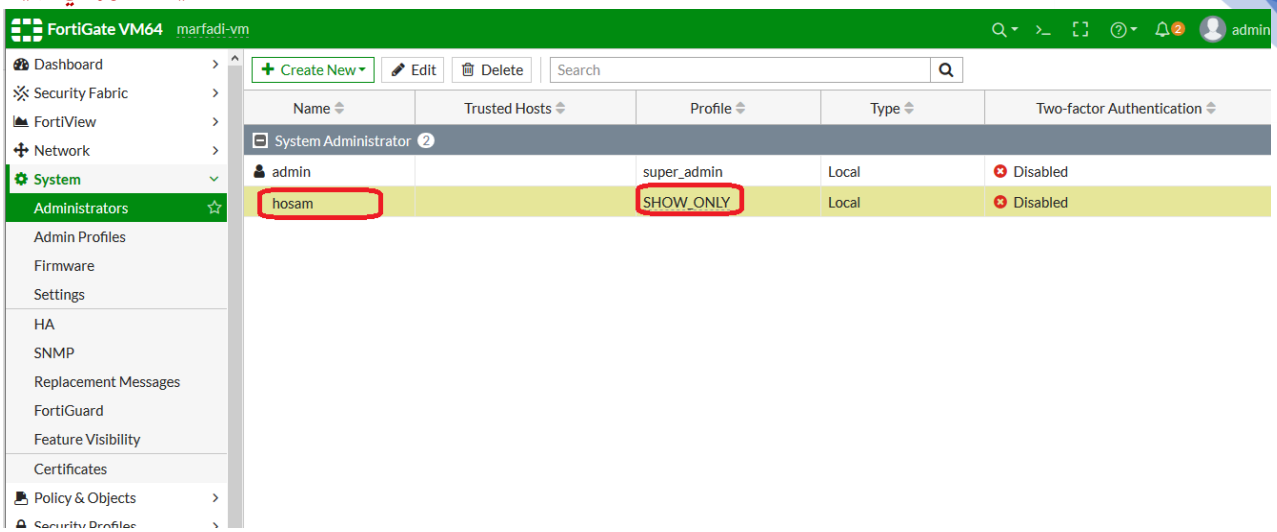
و read/write :يمكنك التعديل على الشاشات ..



يوجد لدينا الان 3 بروفايلات كما بالصورة أعلاه ...

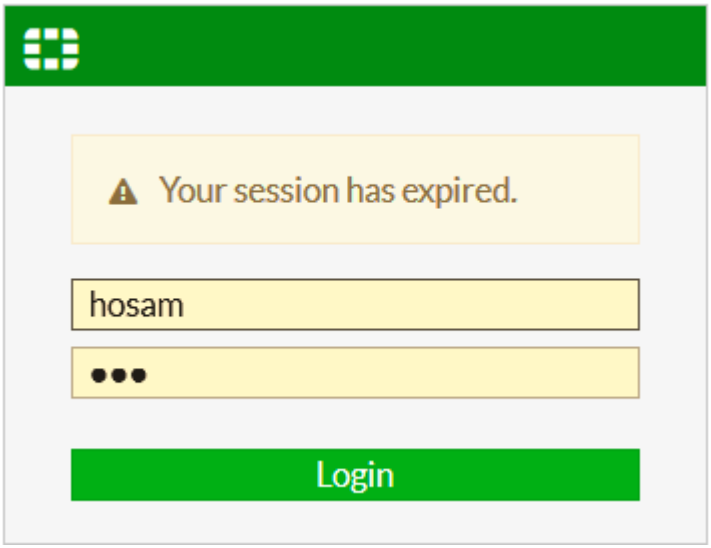
الآن يمكننا تحديد البروفايل المناسب مثلا show_only لليوزر hosam كما بالصورة ادناه

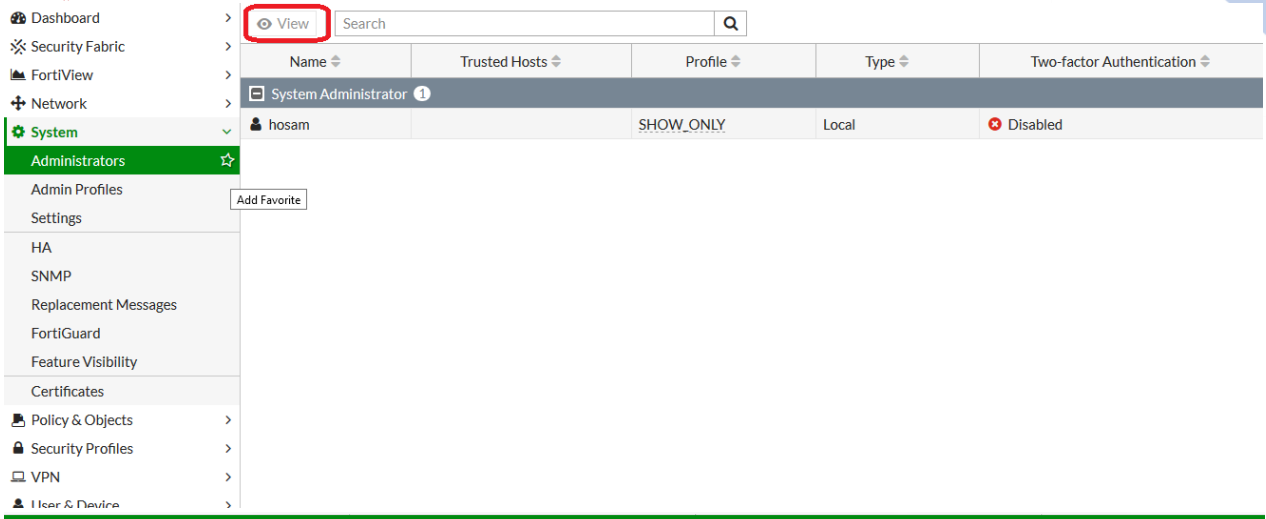


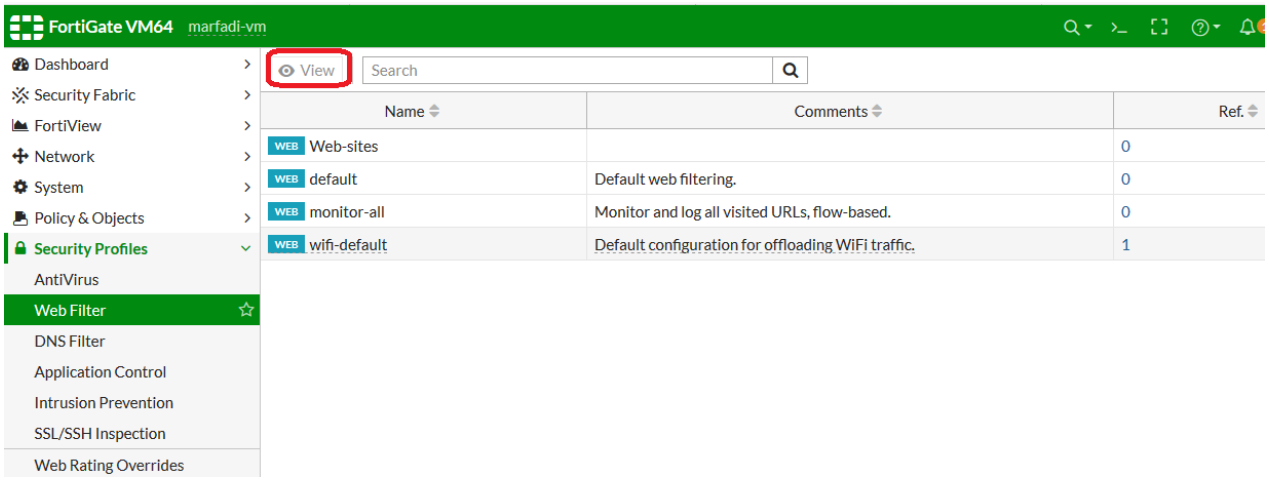


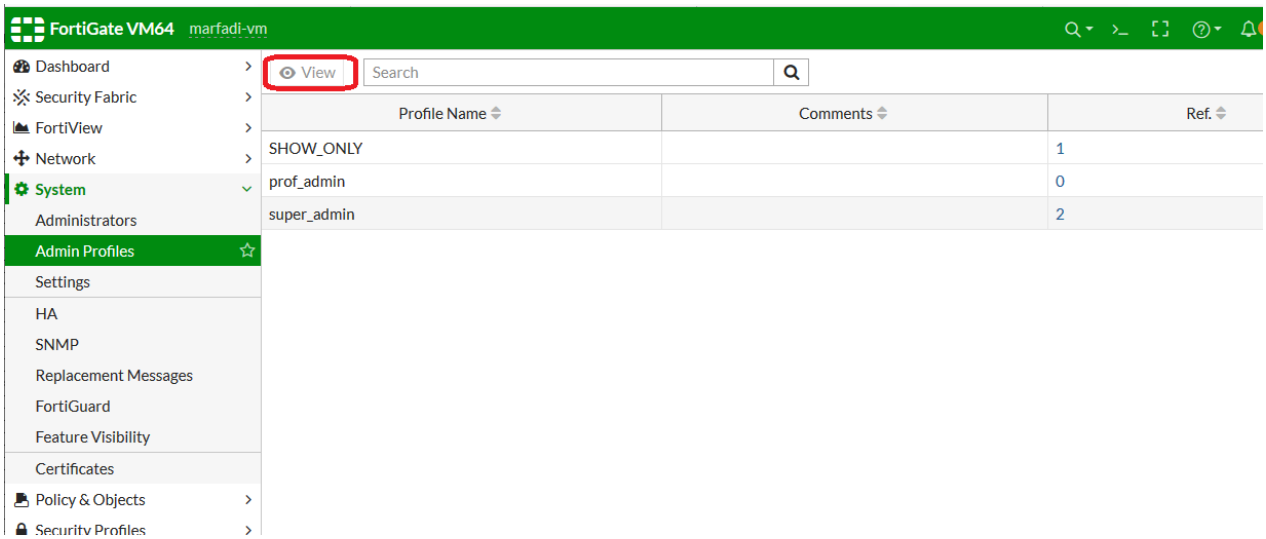
كما بالصورة أعلاه يوجد لدينا 2 يوزرات ..

الان سوف ندخل للفورتي جيت من خلال اليوزر الذي أنشأناه سابقا





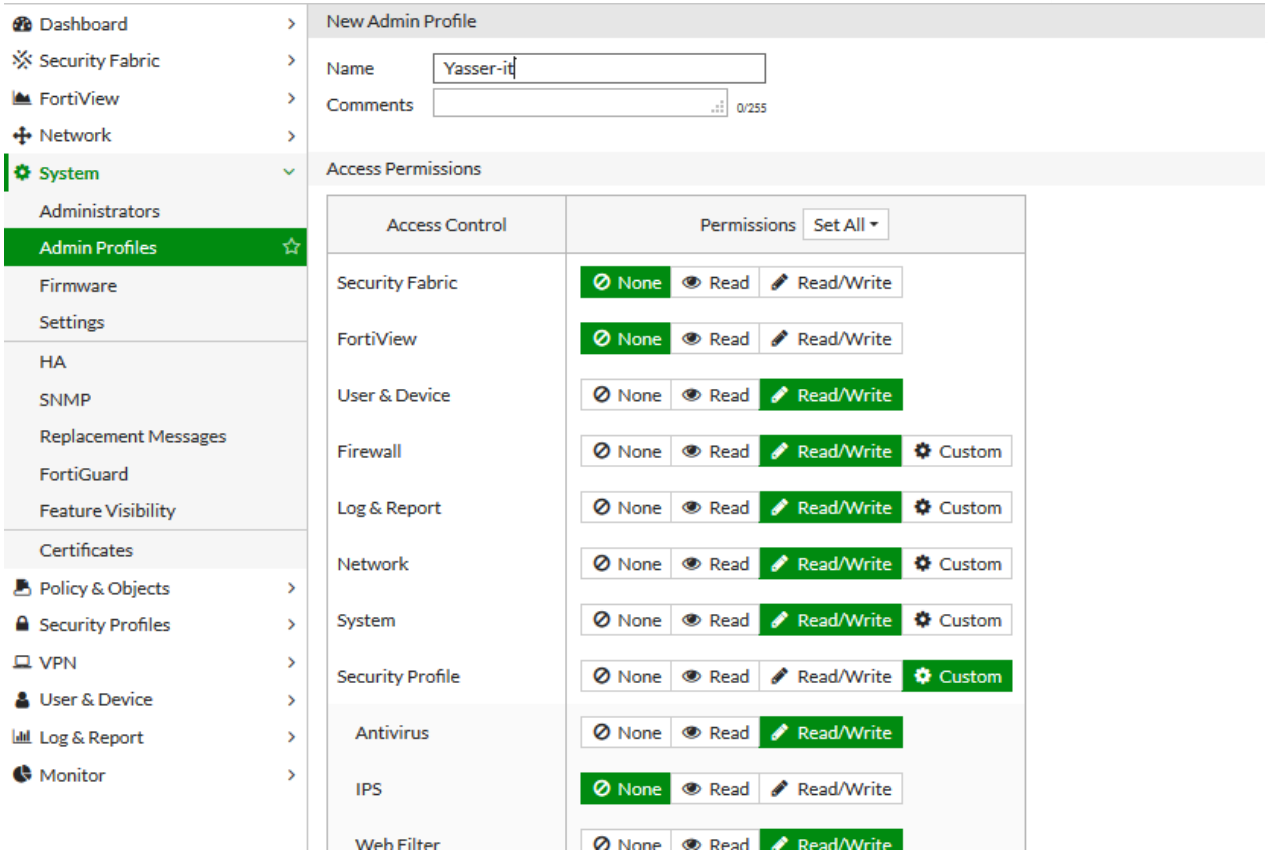


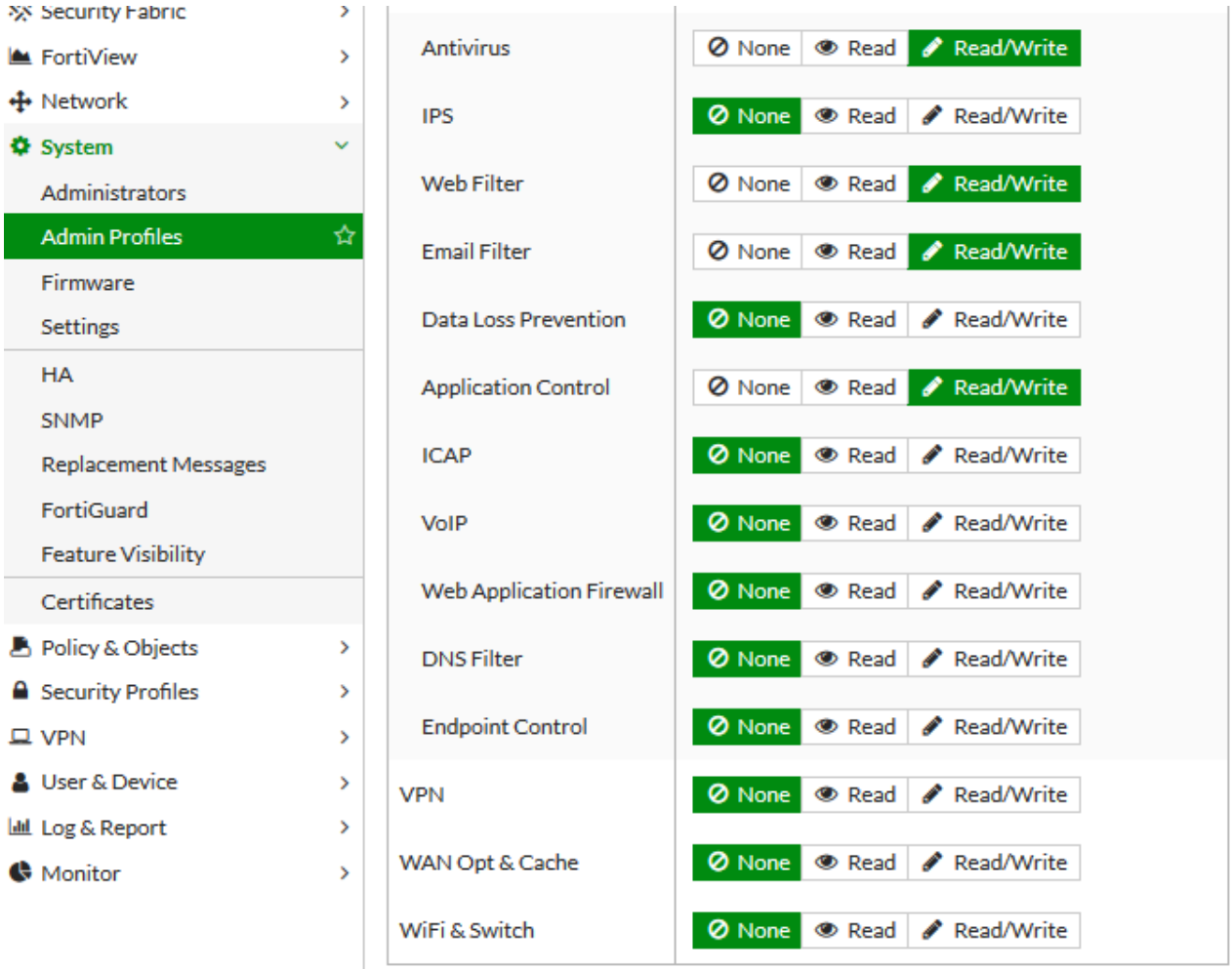


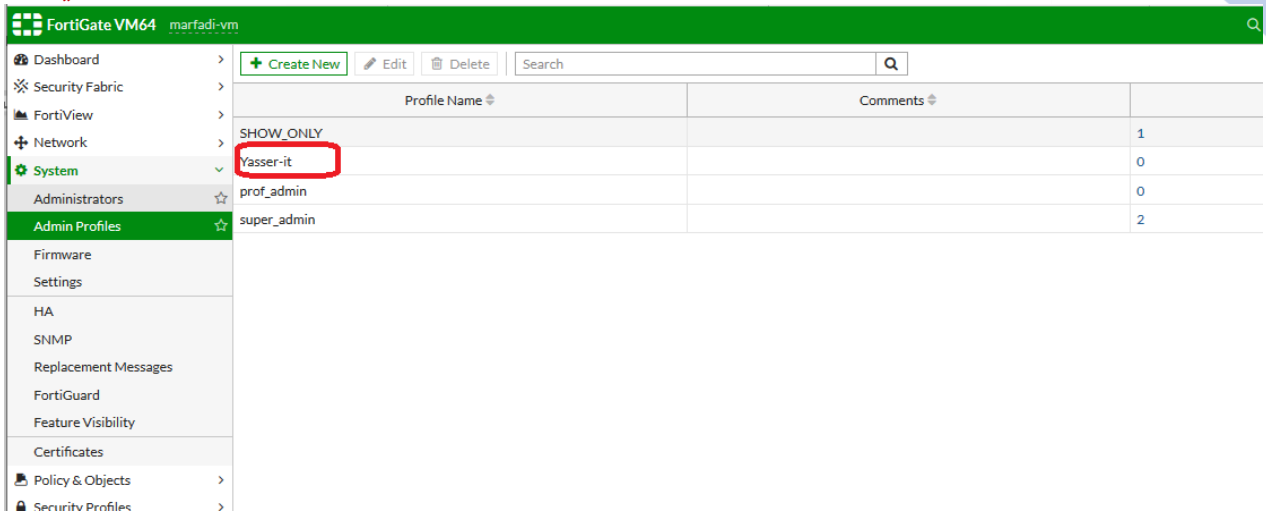
لاحظ بان الشاشات بهذا اليوزر هي read only ولا يمكن لهذا اليوزر التعديل ...

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

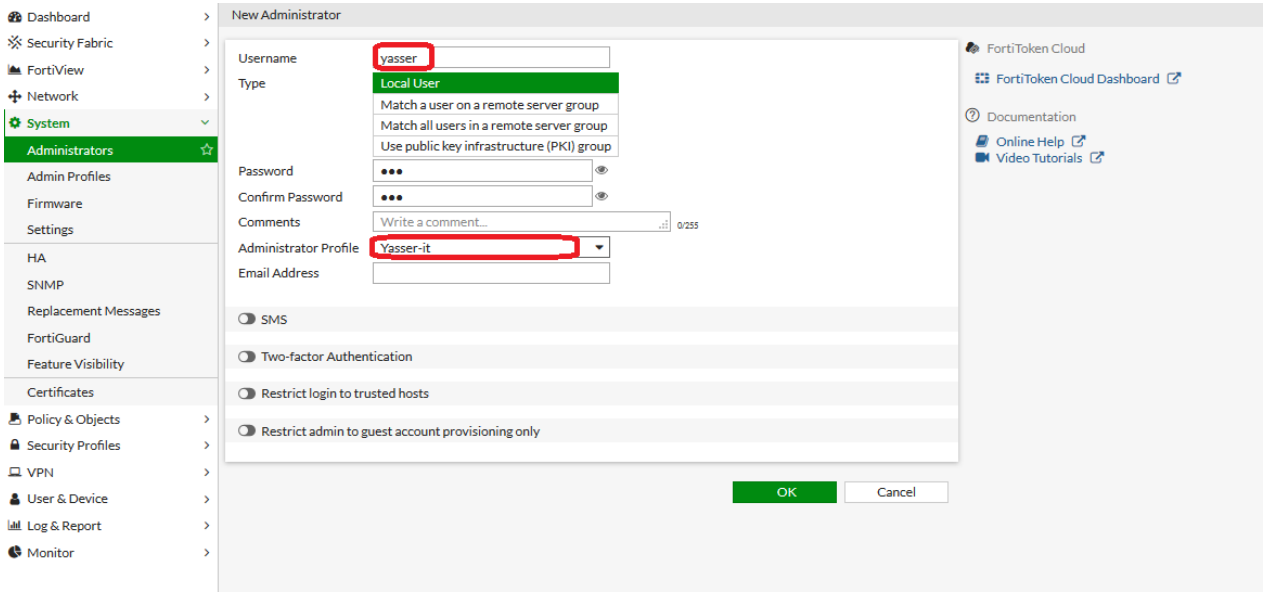
كما تم تحديد صلاحيه read/write بعض الشاشات وتخصيص بعضها كما بالضور ادناه :

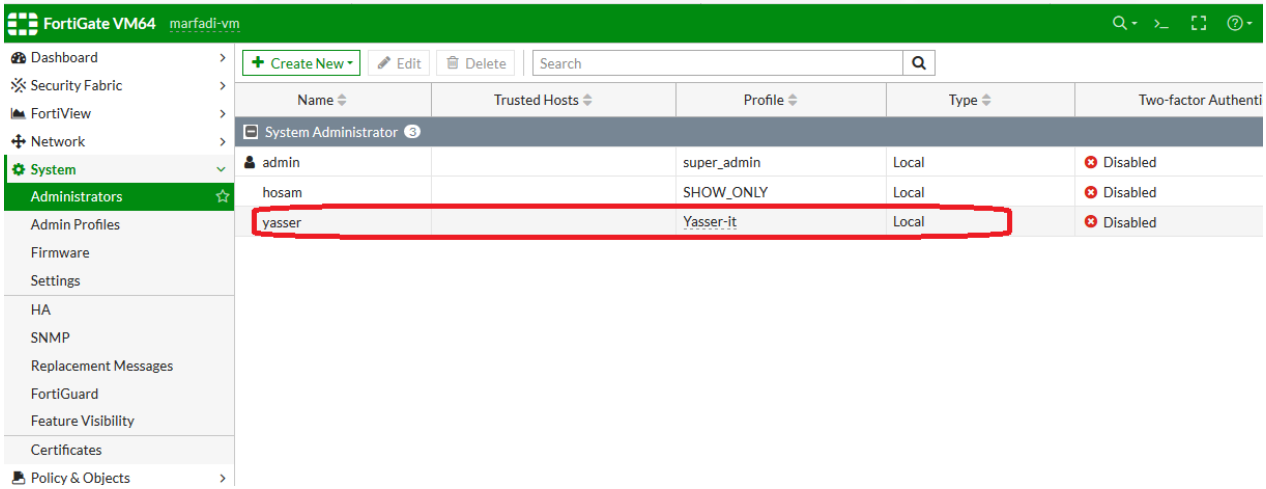

Dashboard
Security Fabric
FortiView
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
New Admin Profile
Name
Yasser-it
Comments
0/255
Access Permissions
Access Control
Permissions
Set All
Security Fabric
FortiView
User & Device
Firewall
Log & Report
Network
System
Security Profile
Antivirus
IPS
None
Read
Read/Write
Custom

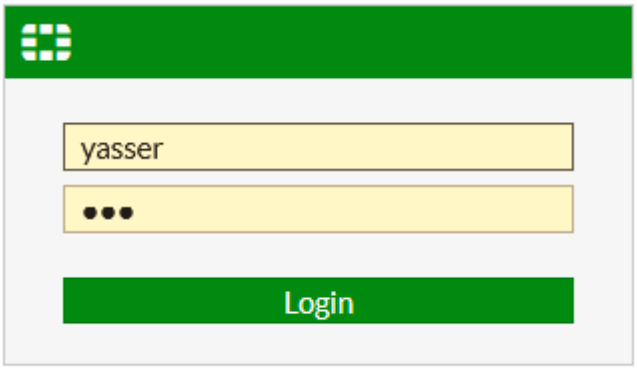

Security Fabric
FortiView
Network
System
Administrators
Admin Profiles
Firmware
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Policy & Objects
Security Profiles
VPN
User & Device
Log & Report
Monitor
Antivirus
IPS
Web Filter
Email Filter
Data Loss Prevention
Application Control
ICAP
VoIP
Web Application Firewall
DNS Filter
Endpoint Control
VPN
WAN Opt & Cache
WiFi & Switch
None
Read
Read/Write



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





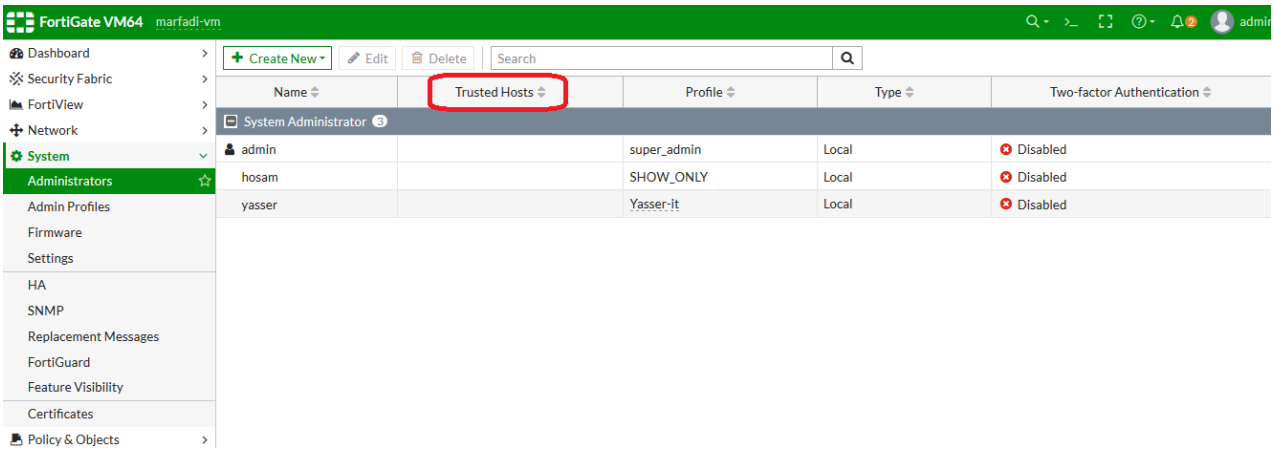


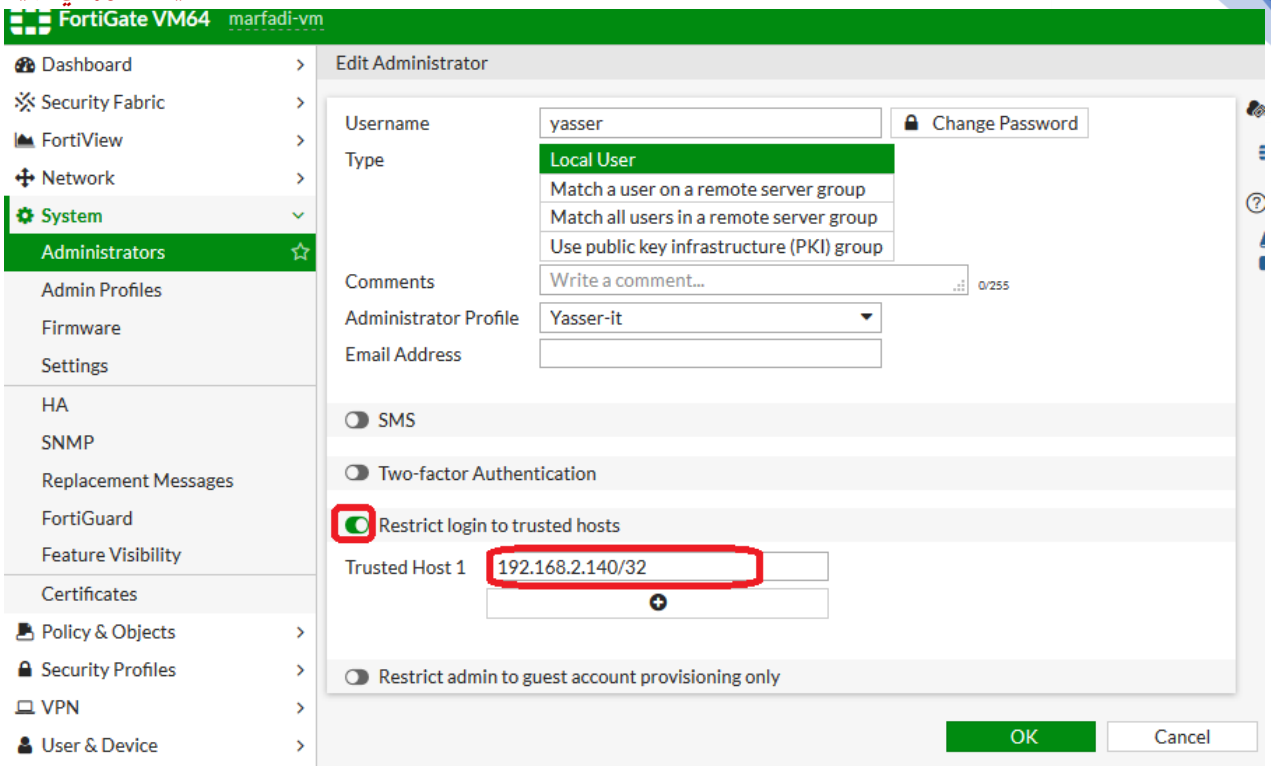
سيتم الدخول لهذا اليوزر بالصلاحيات والشاشات التي تم تحديدها بالبروفايل Yasser-it .

❖ ملاحظة :

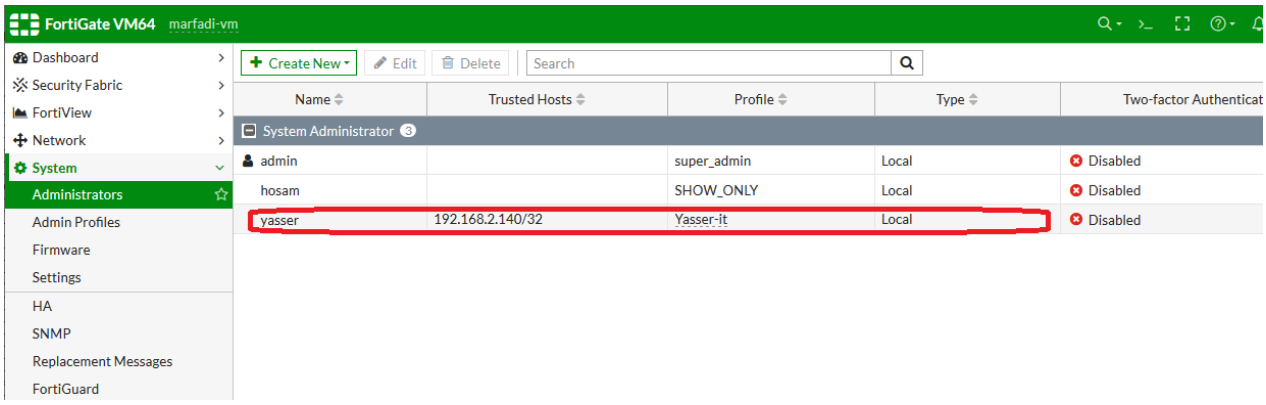
ممكن تعطي يوزر معين بأن يكون له صلاحيات لـ vpn connection بالشركة فقط فلذا ليس له داعي ان يفتح كل الصلاحيات ويعدل عليها وبهذا انارفعت مستوى الأمان وقمت بعمل تخصيص للأعمال ..

➢ ما هو Trusted hosts :



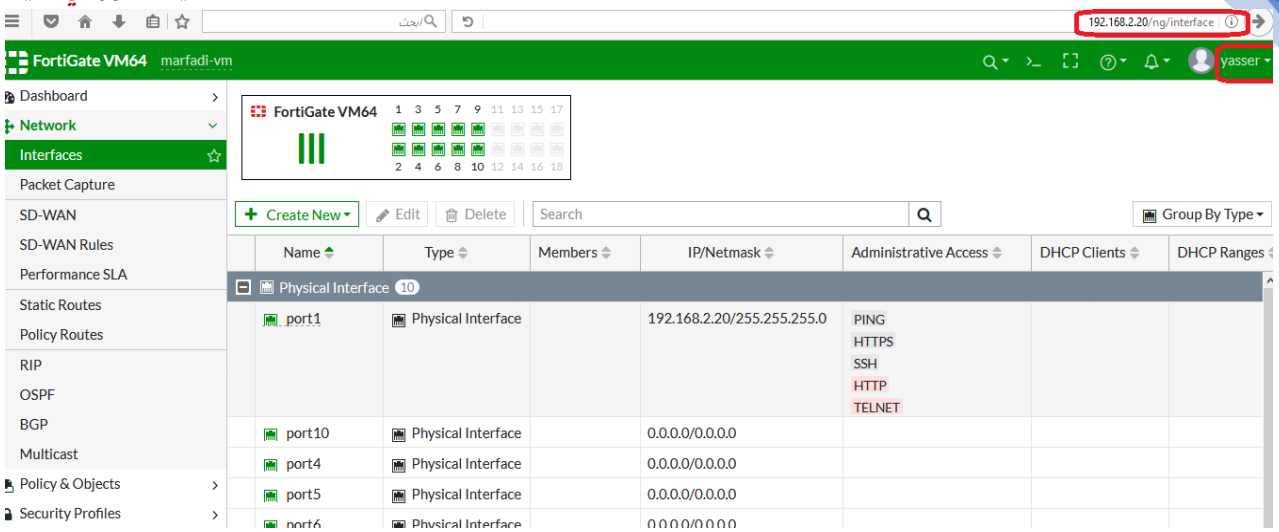


هذا الخيار معناه قم بتقييد اليوزر المسمى Yasser بأنه لا يمكنه الدخول الى الفورتي جيت الا عن طريق اجهزه معينه (جهاز موثوق فيه)مثلا احدد جهاز معين عندي بالشبكة فقط وليكن 192.168.2.140/255.255.255.255 حيث لو حاول هذا اليوزر بالدخول الى الفورتي جيت من أي جهاز اخر فأنه لن يستطيع ذلك .

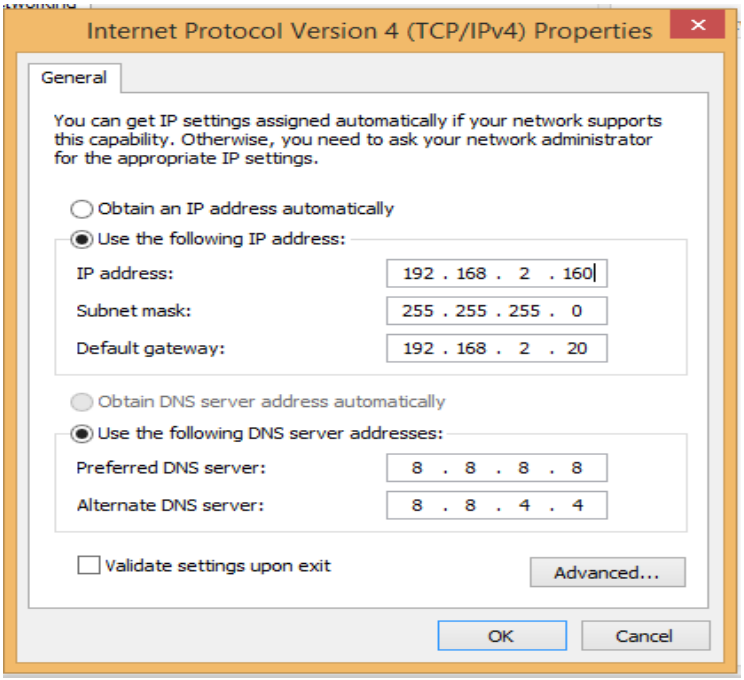


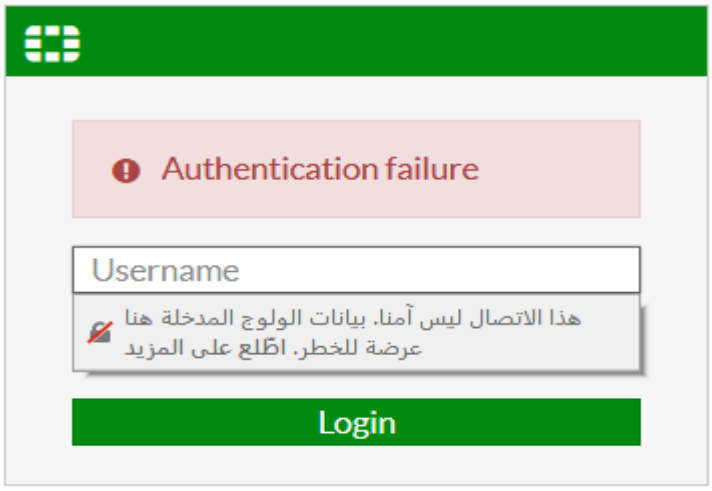
أي ان اليوزر Yasser لن يستطيع الدخول الى الفورتي جيت الإ من الجهاز 192.168.2.140 حتى وان كان لديه اليوزر نيم والباسورد ..

قمنا بالدخول الى الفورتي جيت من خلال جهاز 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 الفورتي جيت بالرغم من ان اليوزر نيم والباسورد صحيحين ..

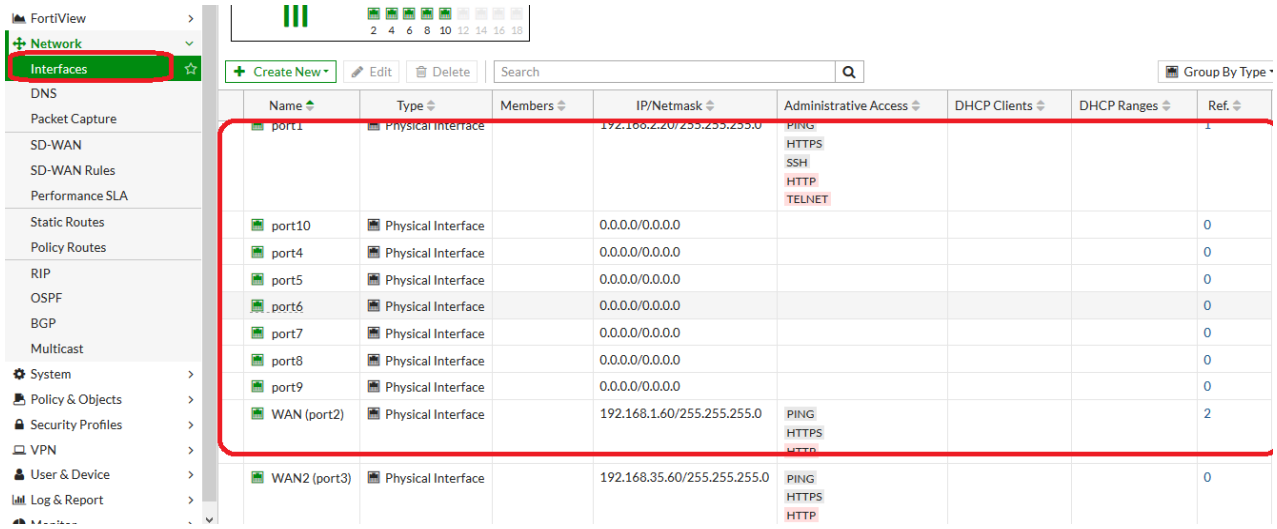




❖ Interface ip address

للتعامل مع الـ interfaces التابعه للفورتي جيت كما بالصورة التالية

حيث يظهر لك كل الـ interfaces لجهاز الفورتي جيت

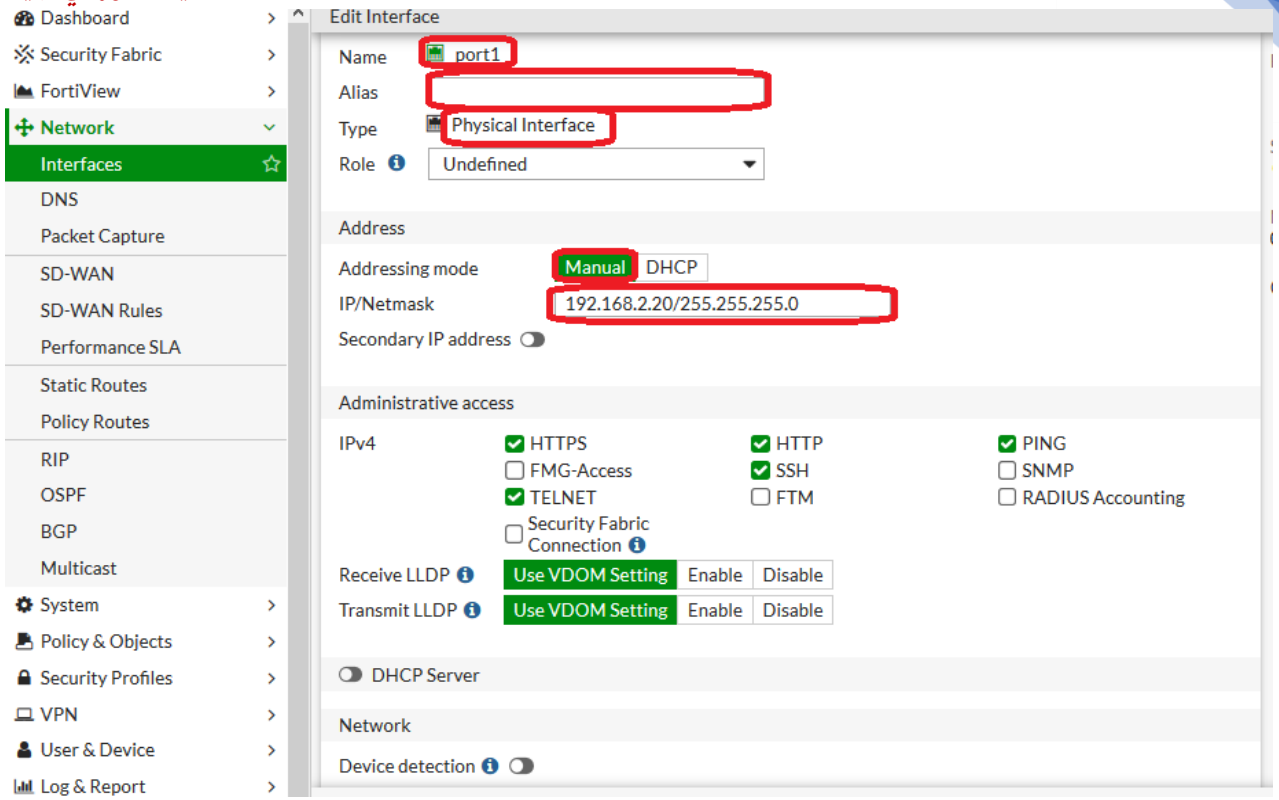


حيث بتوضح اسم الـ interfaces ونوعه والايبي وطريقة الوصول اليه(administrative access) ...

حيث في الـ vm يتم تسميه الـinterfaces ب port ويمكن التعديل على تلك الأسماء كما تريد ،

اما بجهاز الفورتي الحقيقي يكون اسمه internal او wan1او wan2 او dmz .

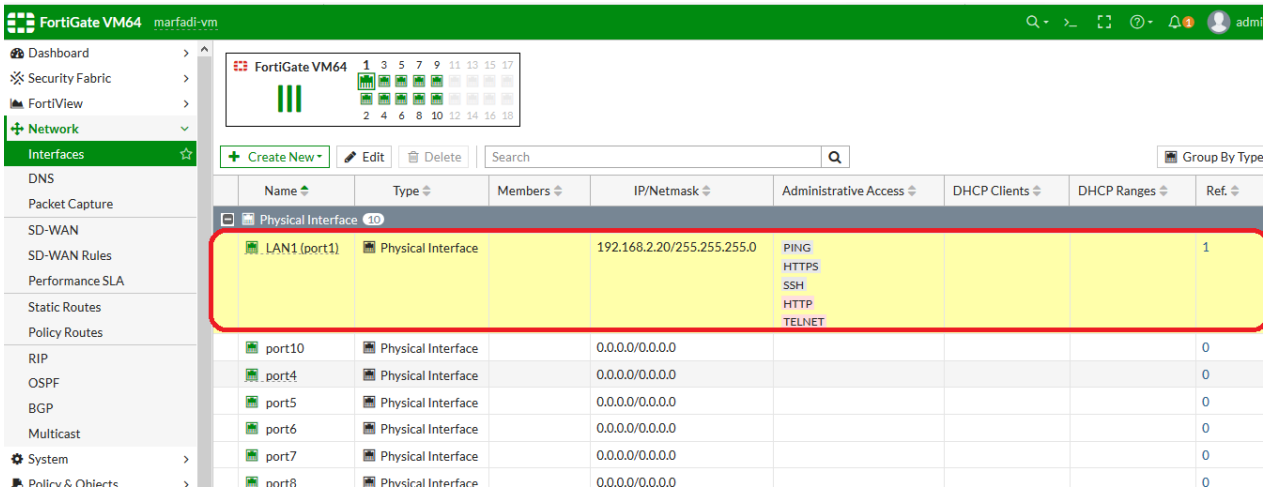
فعندما تريد ضبط اعدادات interface معين وليكن port1 فأننا ننقر عليه نقرتين فتكون كما بالشكل التالي



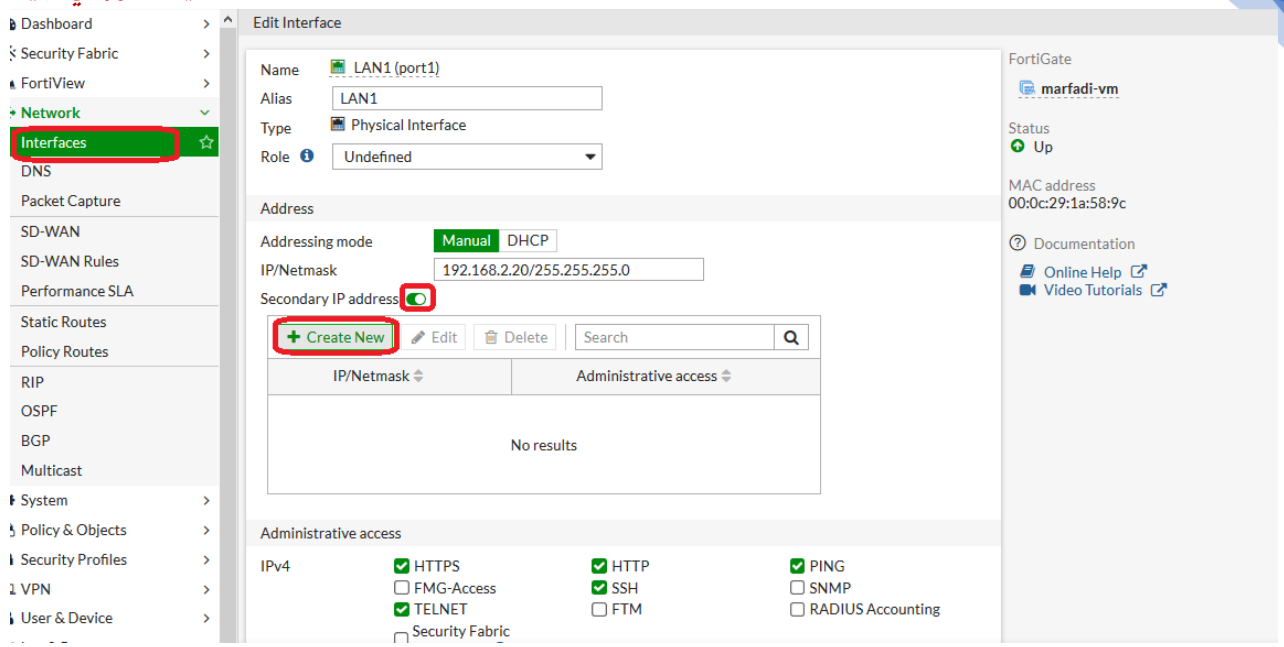
اسم الـinterface هو port1 ويمكن عمل له alias باي اسم تريد ان تعبر عن هذا المنفذ مثلا lan1 ونحدد طريقة تحديد(تعيين) الايبي للـinterface هل manual or dhcp

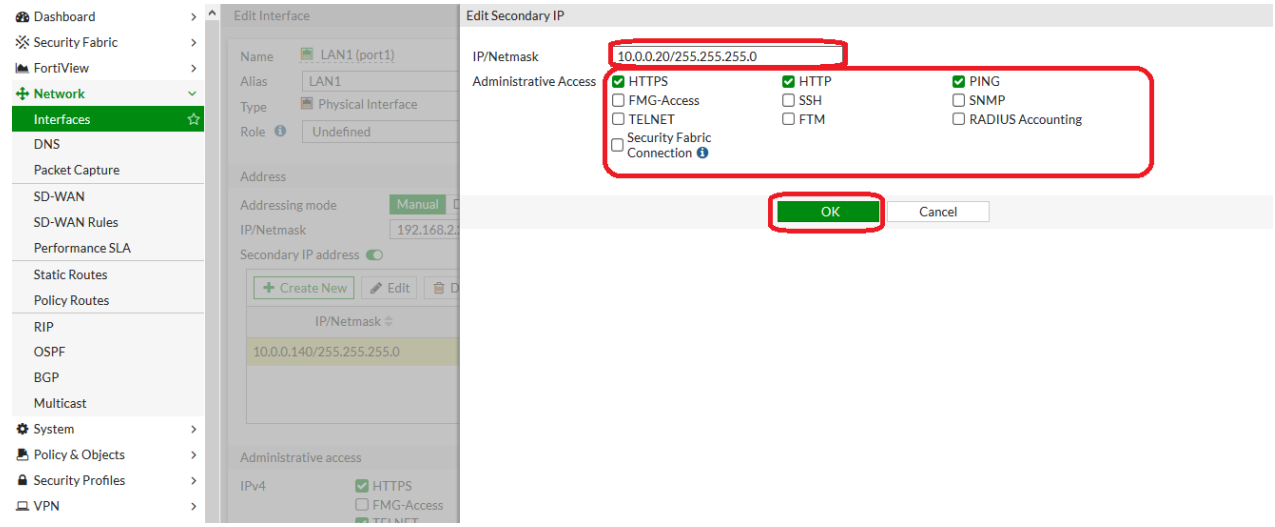
حيث يفضل في الـlan يكون manual اما للـwan يكون dhcp

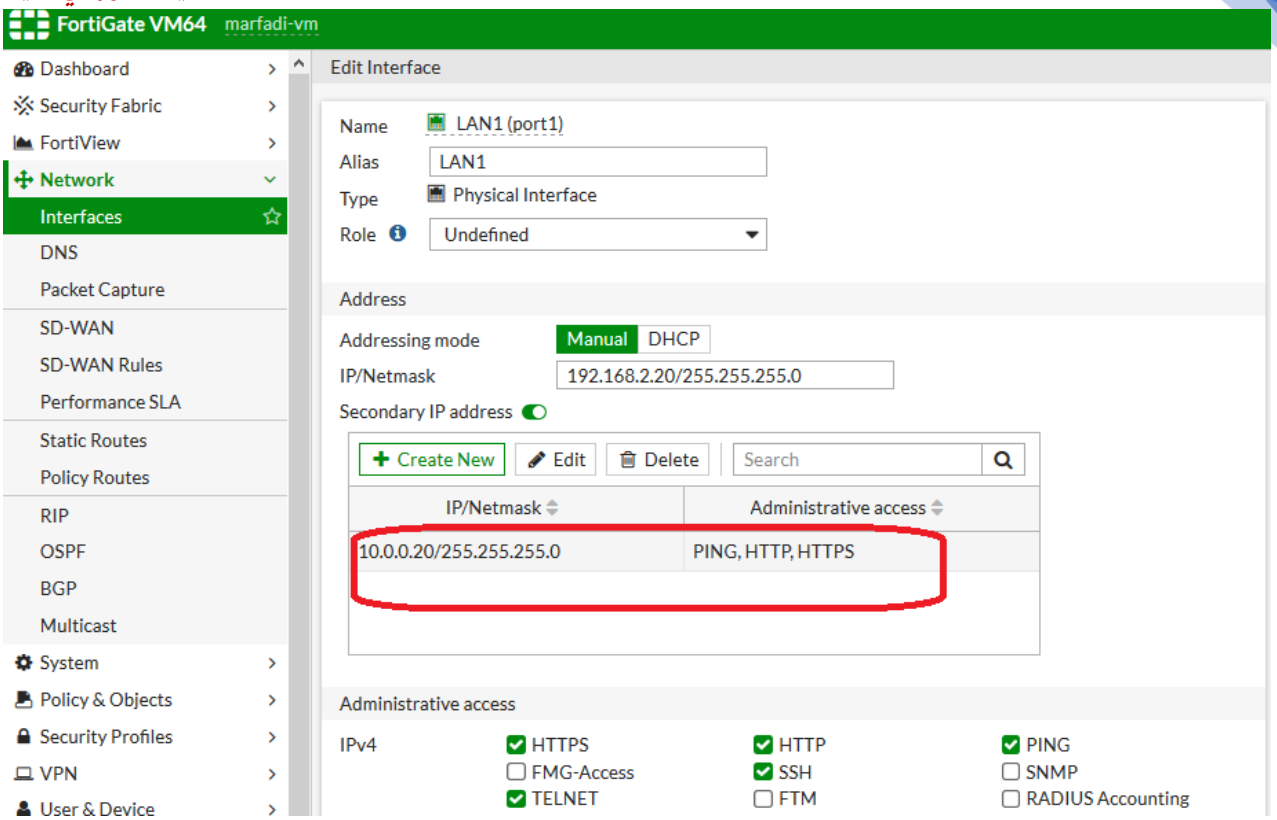
ولاحظ بأن طريقة الوصول كما بالصورة أعلاه لهذا interface عن طريق https http ping telnet ssh



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


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
Create New
Edit
Delete
Search
IP/Netmask
Administrative access
No results
Administrative access
IPv4
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
TELNET
FTM
RADIUS Accounting
Security Fabric
FortiGate
marfadi-vm
Status
Up
MAC address
00:0c:29:1a:58:9c
Documentation
Online Help
Video Tutorials

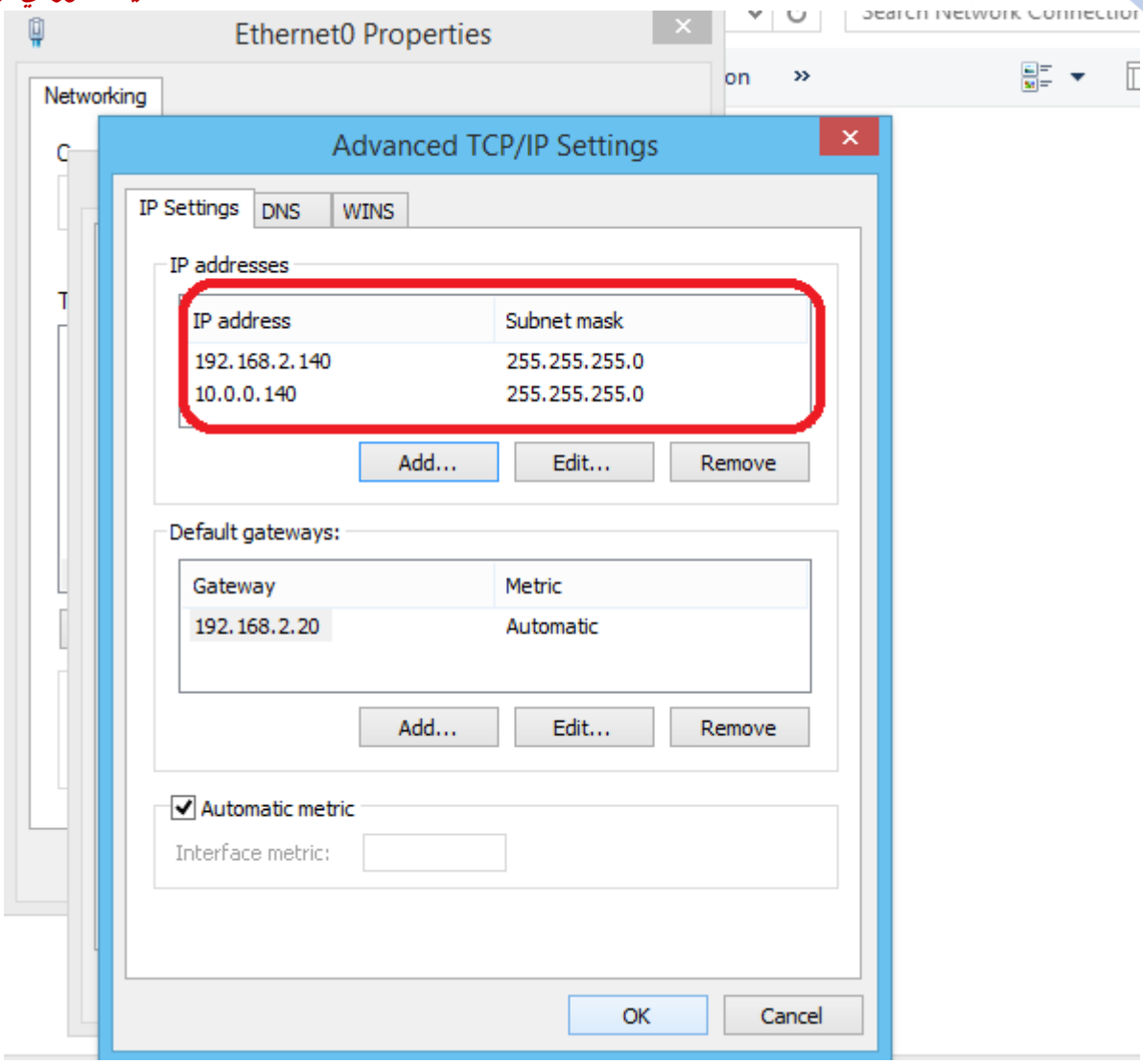

Edit Secondary IP
IP/Netmask 10.0.0.20/255.255.255.0
Administrative Access
HTTPS
HTTP
PING
FMG-Access
SSH
SNMP
TELNET
FTM
RADIUS Accounting
Security Fabric Connection
OK
Cancel

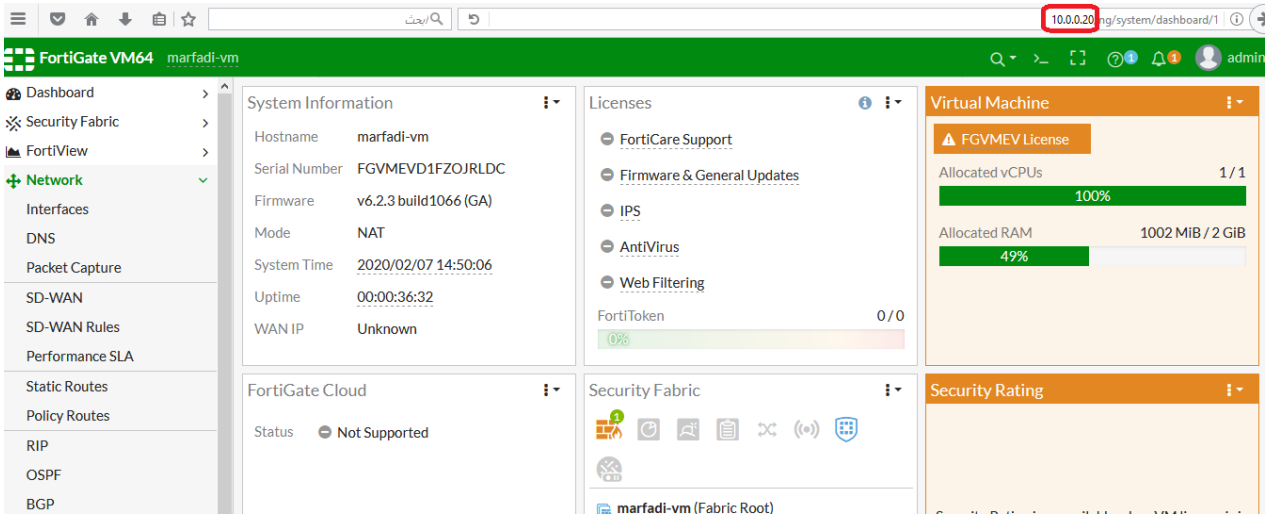


حيث اصبح لدينا 2 ايبي للinterface المسمى lan1وهما

192.168.2.20و 10.0.0.20

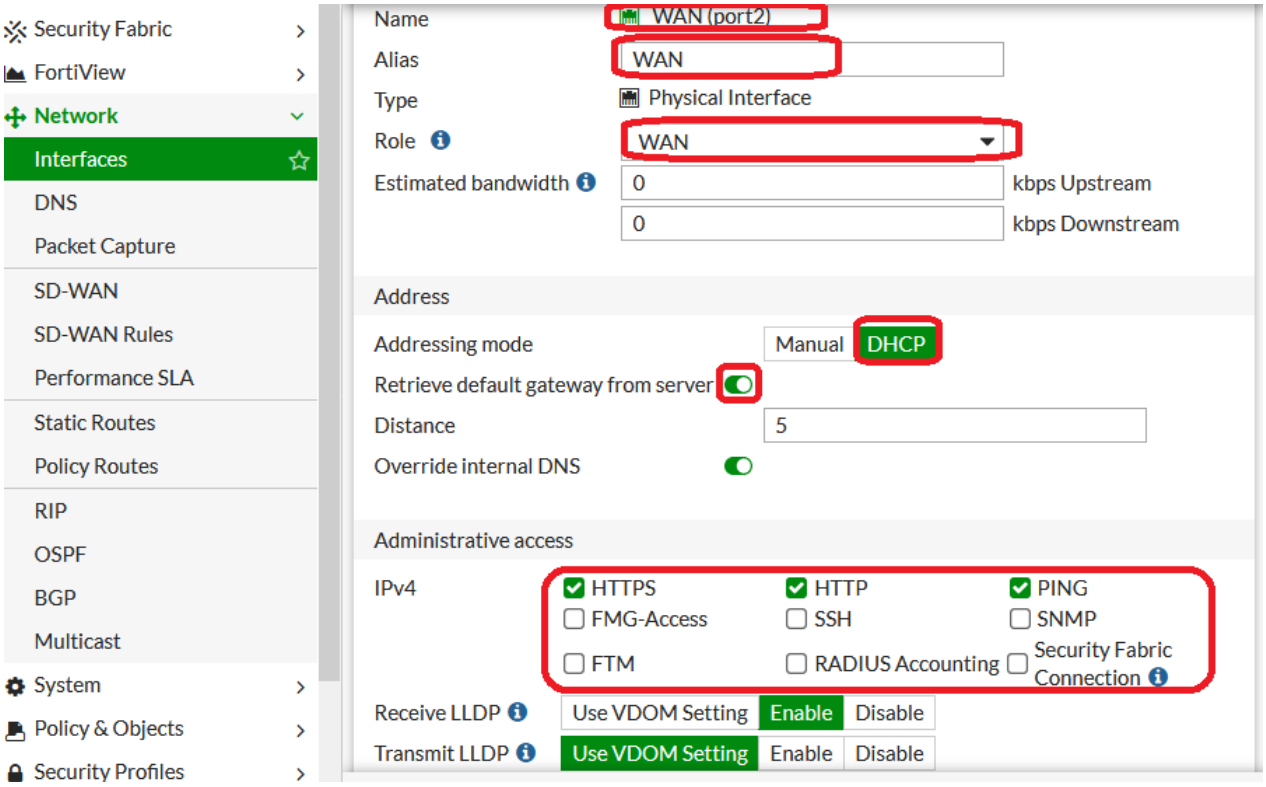
حيث نقوم بالدخول على جهاز الكلاينت 192.168.2.140 ونظيف لكرت الشبكة ايبي إضافي من نفس الرينج مثلا 10.0.0.140



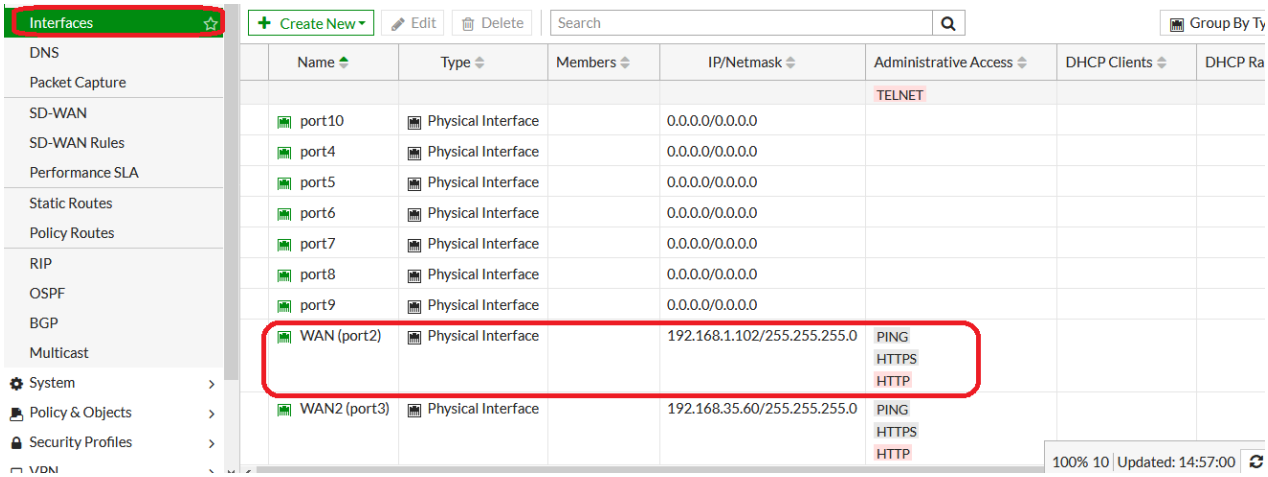


كما بالصورة أعلاه تمكنا بالدخول الى الفورتي عبر الايبي 10.0.0.20 طبيعي جدا ..

اما في الـ interface الذي سنجعله ك wan فأننا سنجعله يأخذ الايبي من dhcp server وهو الروتر(المودم) لأننا ليس بحاجه ان ادخل الى الفورتي جيت من خلاله في الواقع لذا ليس من الضروره ان تقوم بجعله static ip



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



كما بالصورة أعلاه تم اخذ الايبي 192.168.1.102 من الروتر(المودم)الخاص بي في البيت ..

ملاحظة:في حالة dhcp فأنه لا يحتوي على خاصيه secondary ip address .

❖ Static route(default gateway)(static gateway)

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

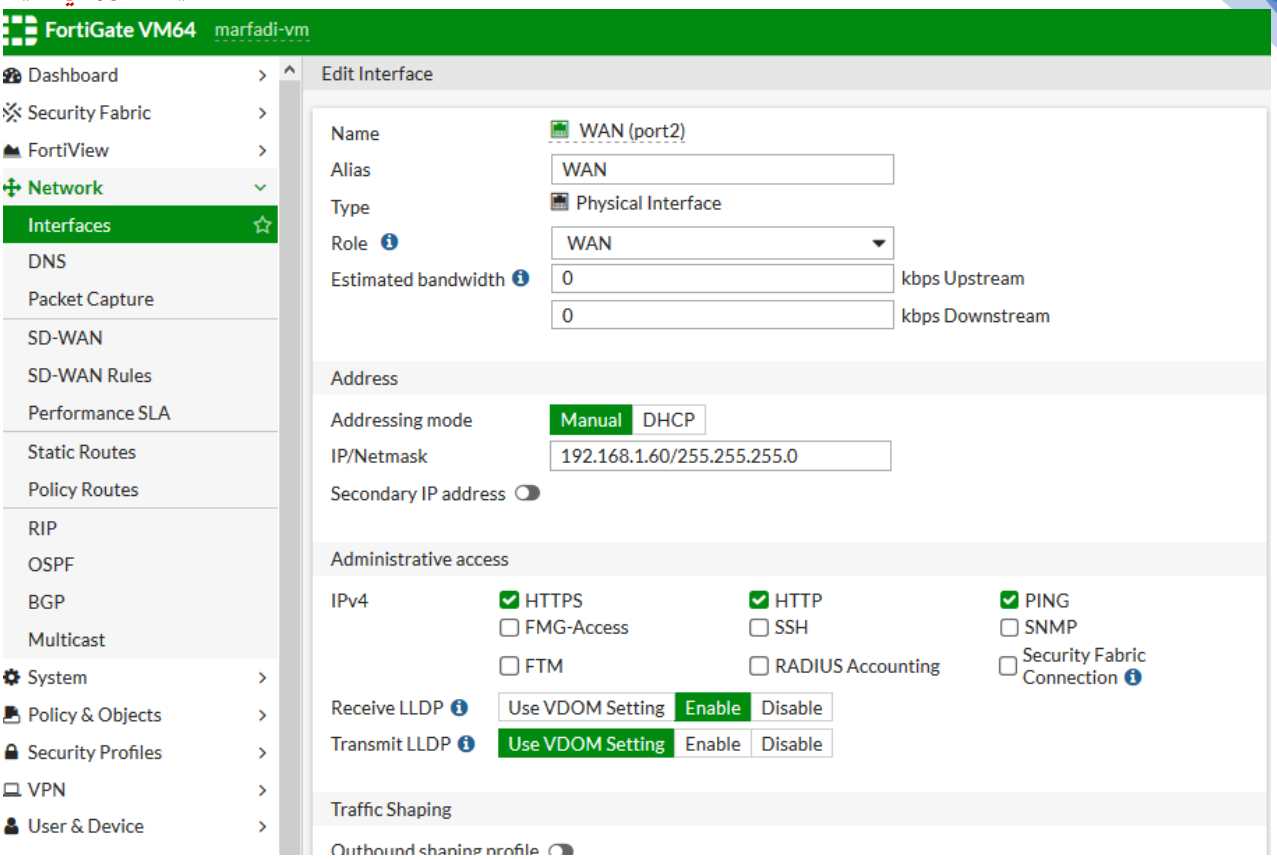
لماذا نريد ان يحصل جهاز الفورتي جيت على الانترنت :

1 – لأن الفورتي جيت هو البوابه للشبكة الداخليه فلو كان الفورتي جيت غير قادر على الوصول الى الانترنت فأكيد جميع الاجهزه بالشبكة الداخليه لن يوصلوا الى الانترنت .

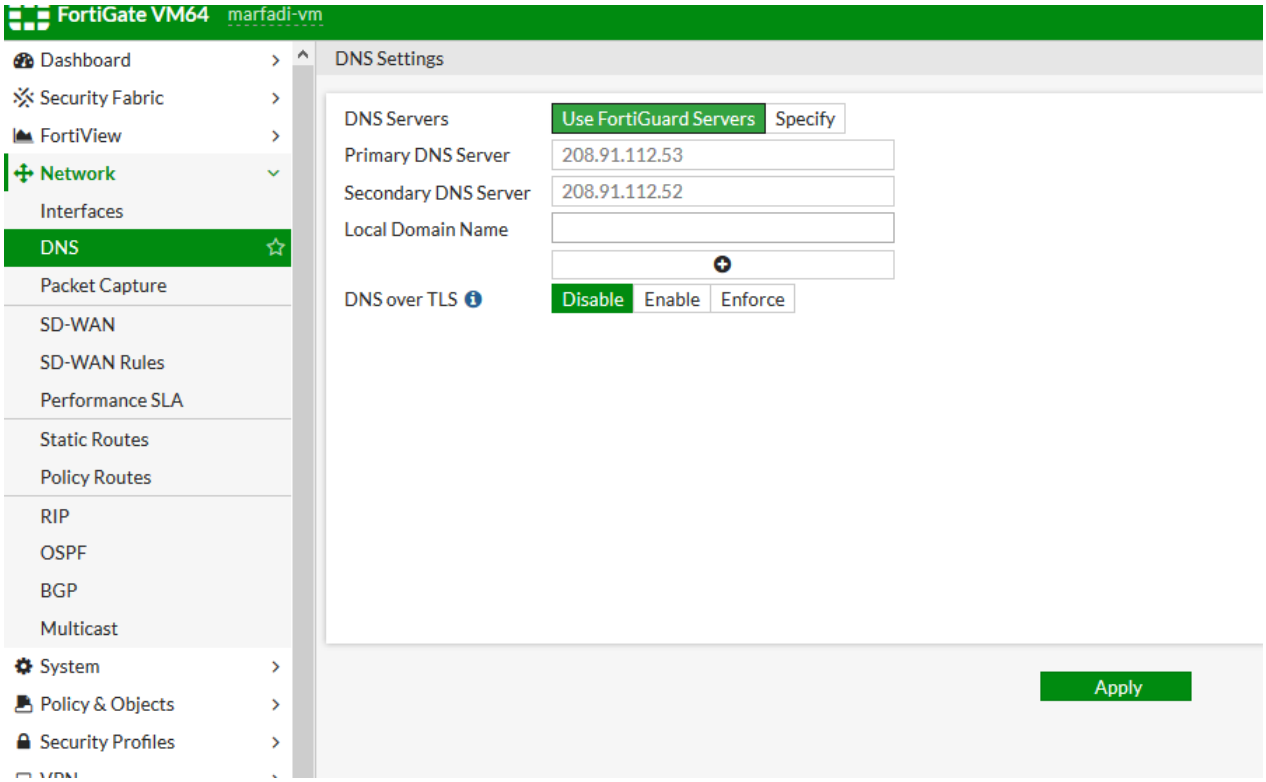
3- جهاز الفورتي جيت يجب ان يكون واصل له انترنت لكي يحصل على التحديث من الفورتي جارد فبدون انترنت لا يمكن للفورتي جيت تجديد الايسنزولا يستطيع تحديث قواعد بيانات كل من الAV وIPS وWeb filtering و ...الخ

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

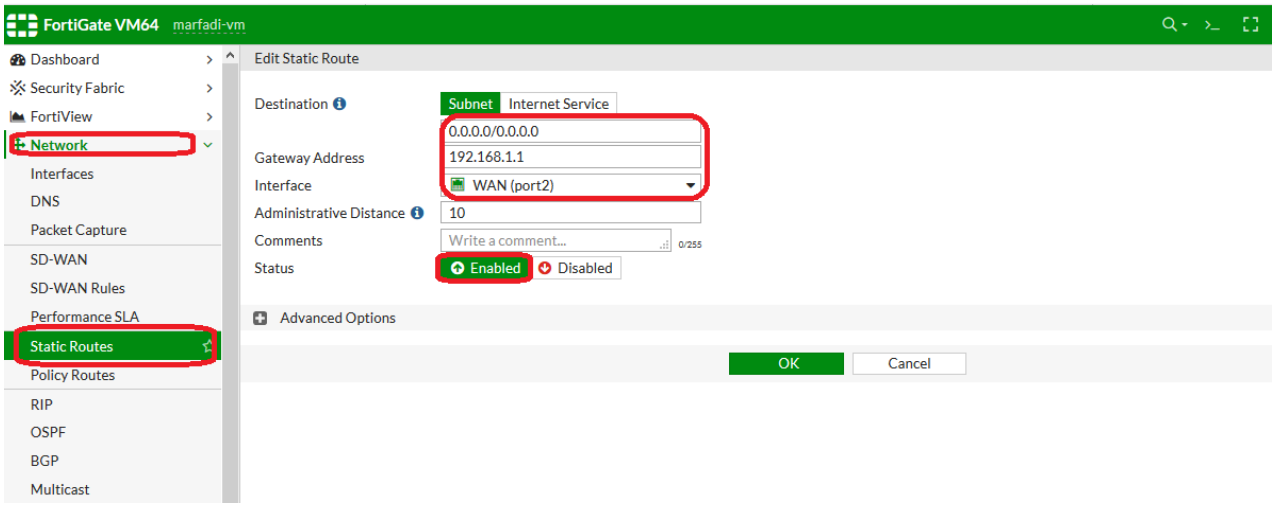
أولا نقوم بتعيين ايبي لكرت الـ wan من نفس رينج الروتر او نجعله يأخذ من DHCP .

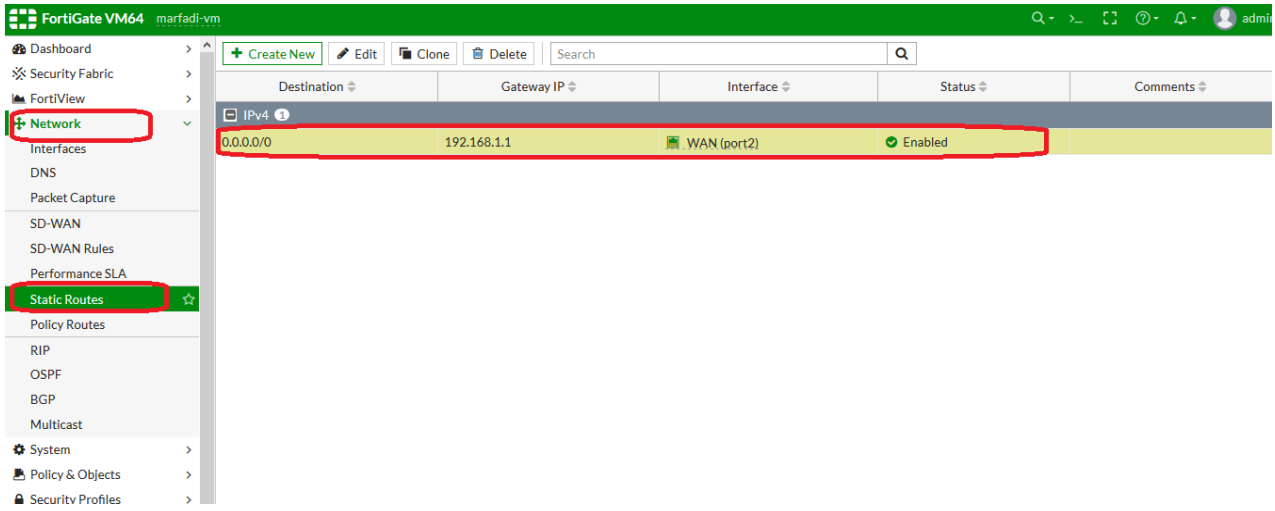


ثم نتأكد فقط من اعدادات الdns للفورتي جيت بالرغم ان بشكل افتراضي تكون مفعله fortiguard DNS



أخيرا يجب ان نقوم بتحديد الـstatic route





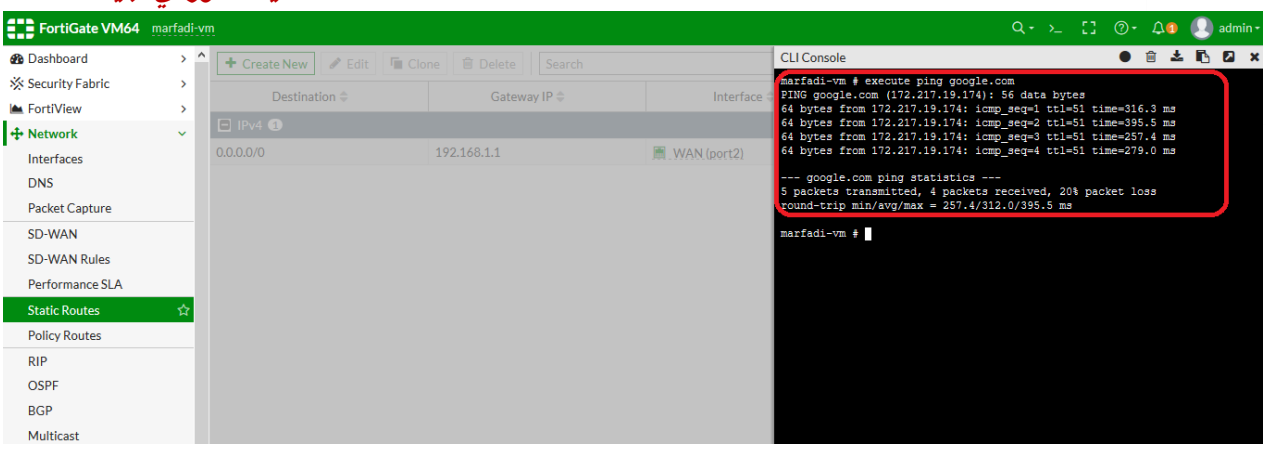
حيث قمنا بإنشاء static route

حيث قمنا بعمل التالي :

لو أي شخص يريد الوصول الى ال0.0.0.0/0.0.0.0 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 الفورتي حصل على الانترنت ام لا

Execute ping google.com

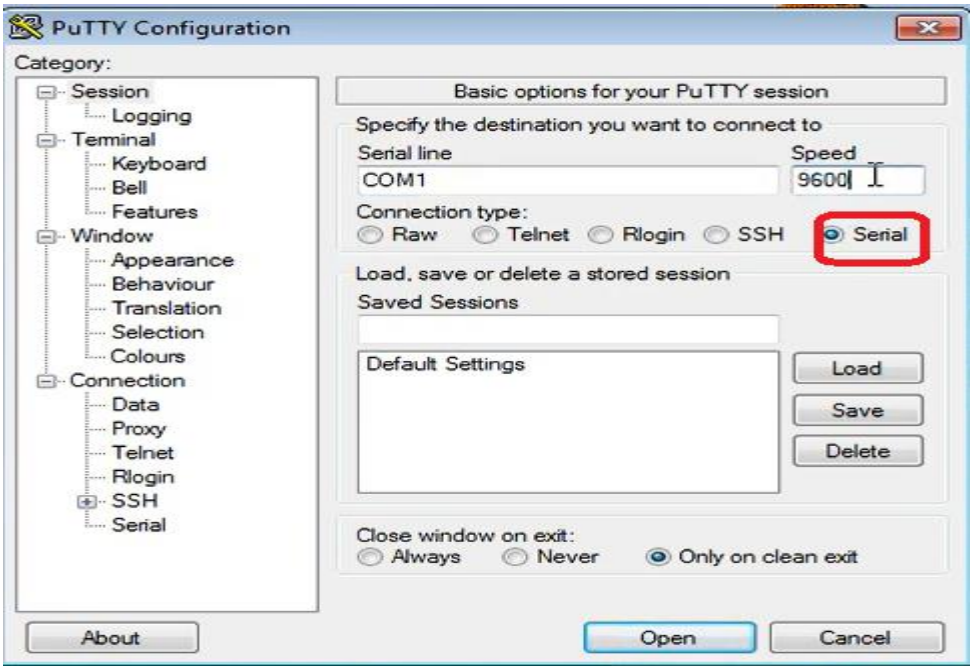


كما بالصورة أعلاه توضح بأن الفورتي جيت حاصل على الانترنت حاليا...

Password recovery: طريقة لاستعاده الباسورد في حالة نسيان الباسورد التابع للـ admin وذلك كالتالي:

1- ندخل عن طريق الكونسول بواسطة تركيب كيبل الكونسول للفورتي 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 بتعين باسورد جديده ليوزر الadmin

حيث في هذا الوضع سوف اكتب اليوزرنيم هو maintainer

والباسورد هو السيريال الخاص بجهاز الفورتي جيت

ثم اكتب الأوامر التالية :

```
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 الفورتي بواسطة الامر

#execute reboot

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

ملاحظة:هذه الطريقة يجب أن يكون maintainer mode يكون enabled لكي استطيع ان اطبق هذه الطريقة وللعلم هذا الmode مفعل بشكل افتراضي فلو قمت بجعلها DISABLED فلن تتمكن من تطبيق هذه الطريقة ..

ملاحظة:في شاشه الmaintainer mode يعطيك فقط 14 ثانية فقط لإدخال اليوزرنيم والباسورد لذا يجب ان تكون سريع في كتابه maintainer والباسورد ..

❖ طريقة عمل DISABLE لـ MAINTAINER MODE كما بالأوامر التالية :

#config sys global

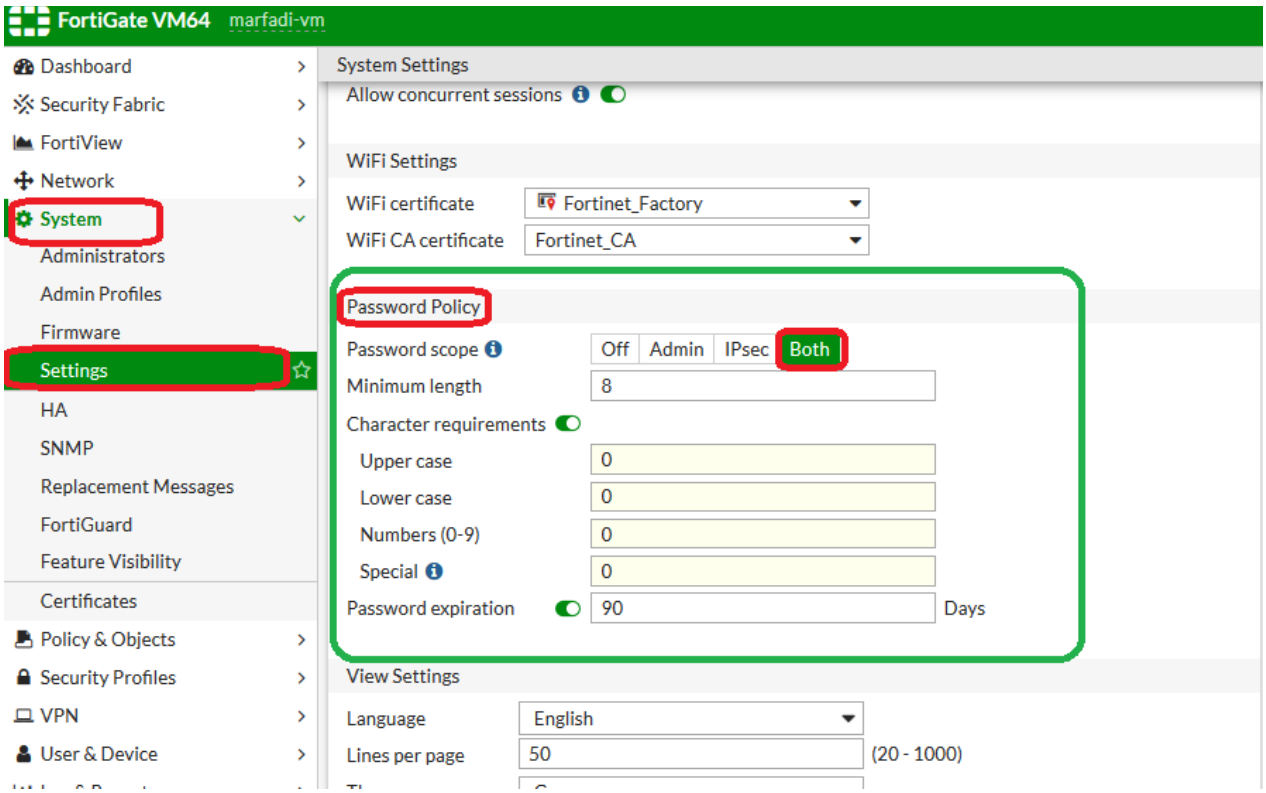
#set admin-maintainer disable

#end

ولو تريد تفعيها 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 الـadministrator ان يقوموا بتعيين باسوردات معقده



كما بالصورة أعلاه

1- تم تفعيل password policy ليكون ليوزرات الadmin الذي يقوموا بعمل اداره لجهاز الفورتي جيت وايضا لـpre-shared key الخاص ب IPsec الخاص بـvpn (وهو الباسورد الذي يكون بين الكلاينت والسيرفر في حالة الاتصال بطريقة vpn).حيث ممكن تحديد مستوى الpassword policyلأحداهما فقط وليس لكليهما .

2- طول الباسورد يكون على الاقل 8 حرف

3- ثم حسب ما تريد هل تريد ان تجبر الادمن ان يجعل الباسورد يحتوي على حروف كبيتل و اسمول وأرقام ورموز وأيضا ان تجعل مده انتهاء الباسورد هي 90 يوم بعدها يطلب من الادمن تغيرها اجباري ...

مثلا :

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

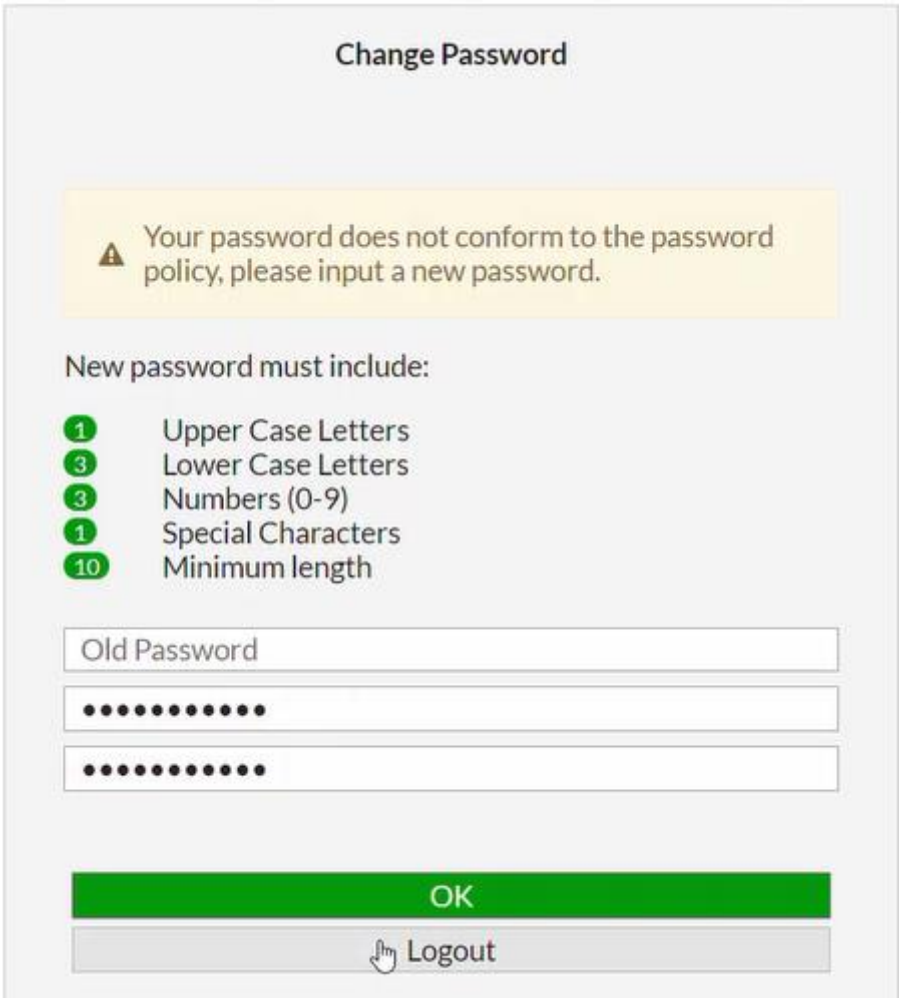
على الأقل يجب ان يكون هناك حرف واحد كبتل في الباسورد

على الأقل يجب ان يكون لديك 3 حروف سمول في الباسورد

على الأقل يجب ان يكون لديك 3 ارقام في الباسورد

يحتوي على الأقل رمز واحد (special)مثلا ! @ $ #

يجب خلال 60 يوم ان تقوم بتغيير الباسورد



لاحظ كما بالصورة أعلاه بأنه عند مطالبتي بتعيين الباسورد تم الاشاره الى تعقيدات الباسورد ..

مثلا :

M@rfadi123

❖ كيف تفعيل DHCP server على الفورتي جيت بحيث الاجهزه بالشبكة تأخذ الاعدادات (IP،Gateway،DNS) من جهاز الفورتي جيت :

❑ DHCP Concept

✓ **DHCP** working method

1- Discover message

Source IP / **0.0.0.0** Source MAC / **NIC address**

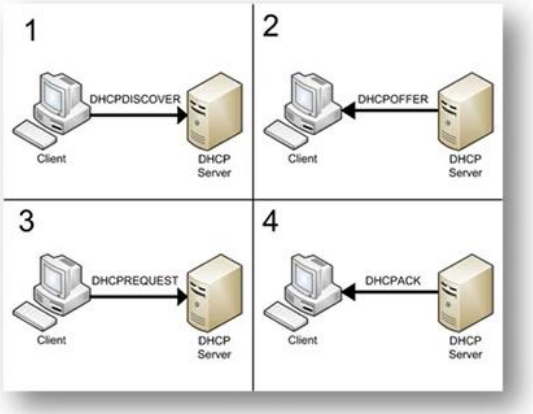
Dest IP / **255.255.255.255** Dest Mac / **FF-FF-FF-FF-FF-FF**

2- Offer message (DHCP server on demand)

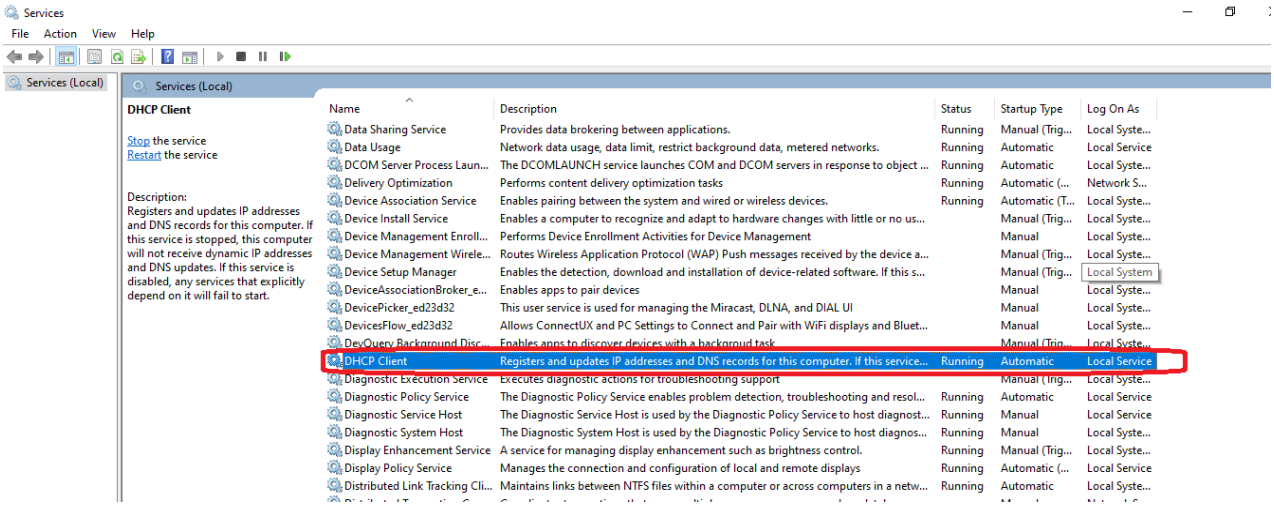
3- Request message (need TCP/IP configuration)

4- ACK message (hand over)

Note : all DHCP traffic at first time are broad Cast

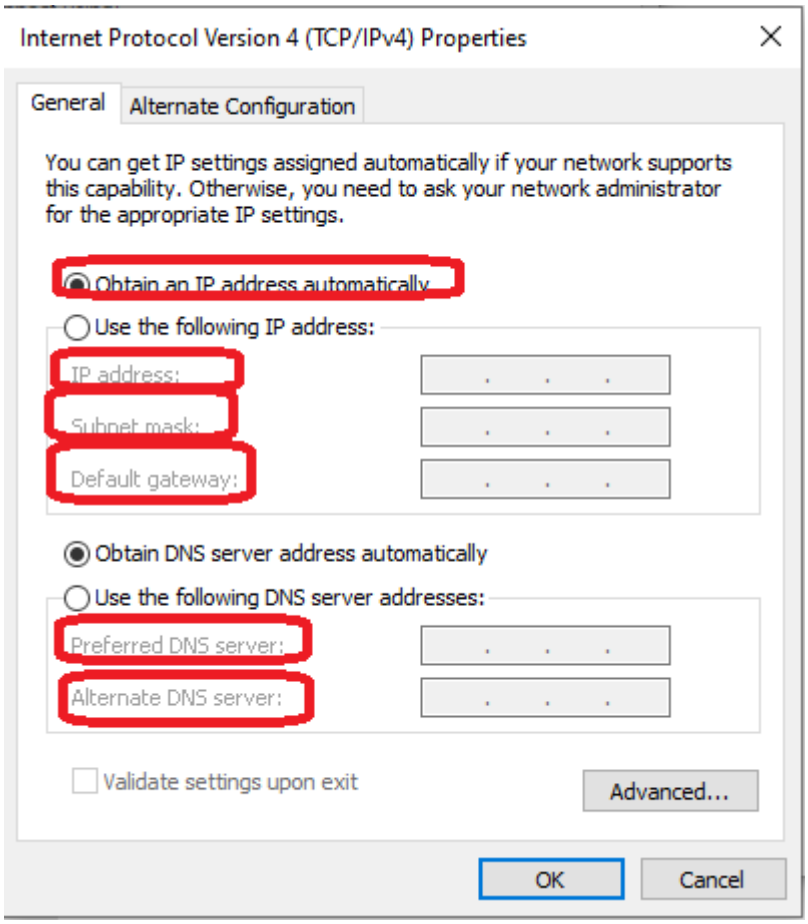


Dhcp client :هي الservice التي بتتيح لك بأن تستفيد من خدمات السيرفر (Dhcp server)حيث يجب ان تكون startedو enabled في جهاز الكلاينت(by default).



*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 الشبكةلاجهزه الكلاينت فأن الdhcp server سيقوم بتوزيع الاعدادات كما بالصورة أعلاه اما في حالة عدموجود dhcp server شغال بالشبكة فأن اجهزه الكلاينت ستأخذ ايبي من apipa(automatic private ip address)وهذارينج من الايبيهات يبدا من 169.254.0.1 -169.254.255.254 حيث سياخذ الكلاينت هذا الايبي الى ان يصبح الdhcp server متاح بالشبكةويوزع ايبي للكلاينت ..

حيث ساقوم بتفعيل الdhcp server في جهاز الفورتي جيت على الـ interface lan1لأن هذا الكرت الذي متوصل بالشبكة الداخليه لكي يوزع الاعدادات لكل اجهزه في الشبكة الداخليه ...

ملاحظة :

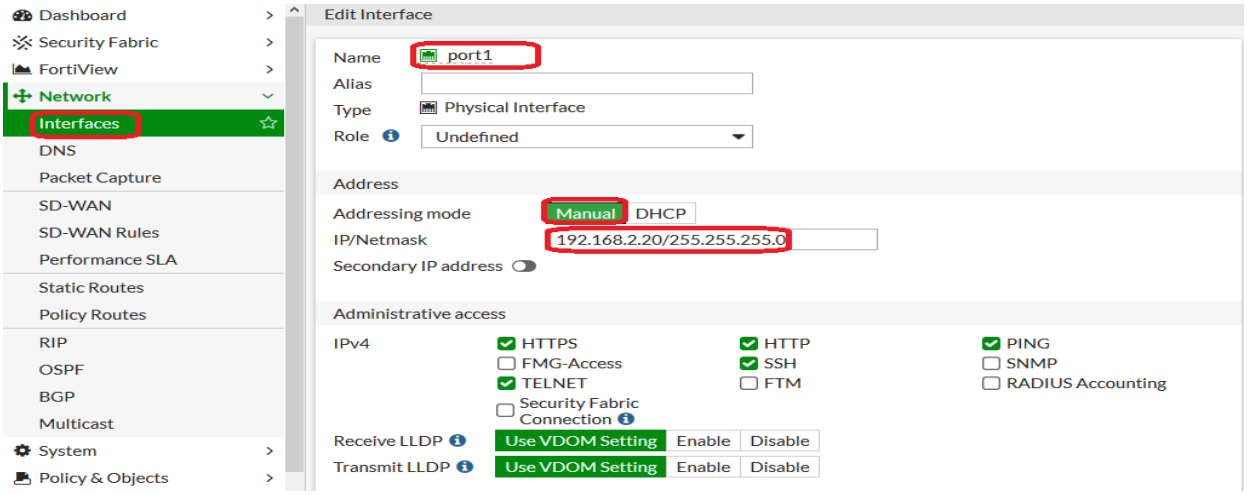
بمجرد ان تقوم بتفعيل الخيار Obtain an IP address automatically في كروت الشبكةلاجهزه الكلاينت فأن جهاز الكلاينت هو الذي يطلب الاعدادات من الـ dhcp server وذلك عن طريق عمل رساله broadcasts في الشبكة لكل الاجهزه،

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

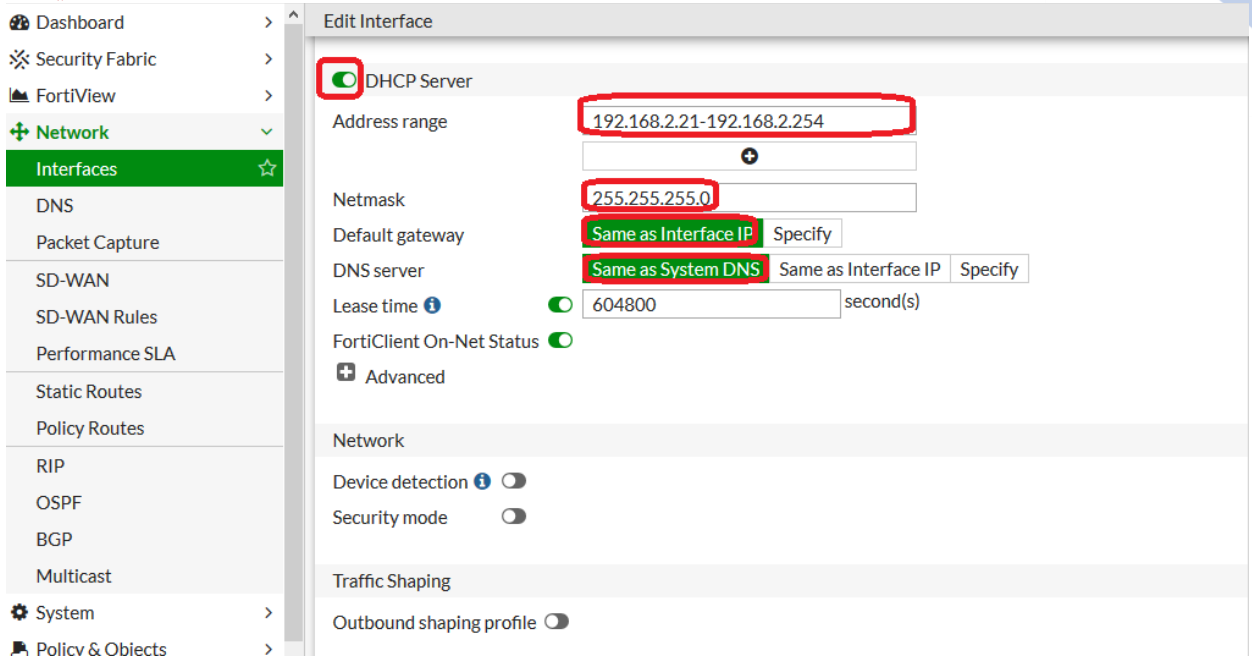
حيث نفترض بان leased duration =7 days فأن بعد 7 أيام سيفقد الكلاينت الاعدادات المرسله من dhcp server ويجب ان يقوم بعدها الكلاينت بعمليه الطلب مره أخرى ..

الآن سنقوم بعمل الاعدادات على جهاز الفورتي جيت :

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



كما بالصورة ادناه قمنا بتفعيل الdhcp server



وأيضا الرينج من الايبيهات التي سيتم توزيعها سوف تكون 192.168.20.21-192.168.20.254 حيث كل اجهزه الكلاينت سوف يكون الايبي التابع لها من نفس هذا الرينج ..

وأيضا سيقوم بتوزيع الmask=255.255.255.0

و Default getwat=Same as interface ip والذي سيكون نفس ايبي كرت الlan1=192.168.2.20

DNS server= Same as system DNS والذي سيكون نفس ايبي كرت dns التابع للفورتي جيت والذي قمنا بتحديده سابقا في قائمه الdns كالتالي 8.8.8.8 8.8.4.4

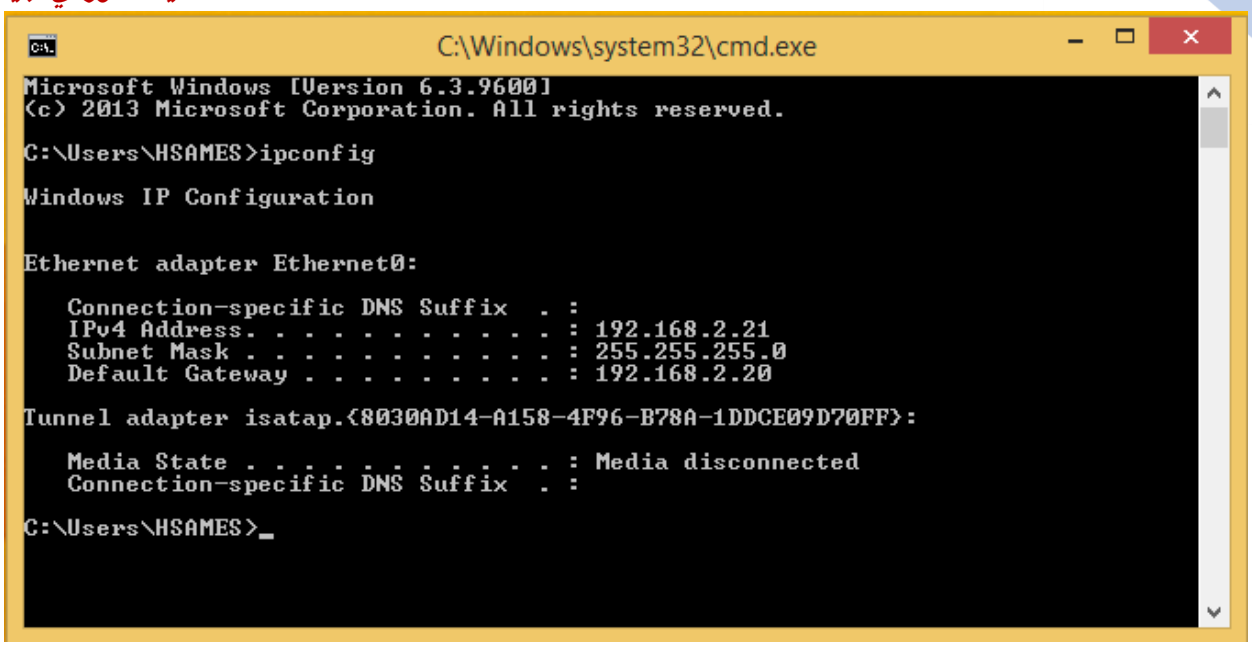
او تختار Same as interface ip وسوف يكون هو ايبي الlan1 للفورتي جيت

ويمكنك تخصيص أي ايبي تريده وذلك بتحديد الخيار Specify وتكتب الايبي المطلوب توزيعه ك DNS مثلا ايبي الدومين DC .

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

Ipconfig

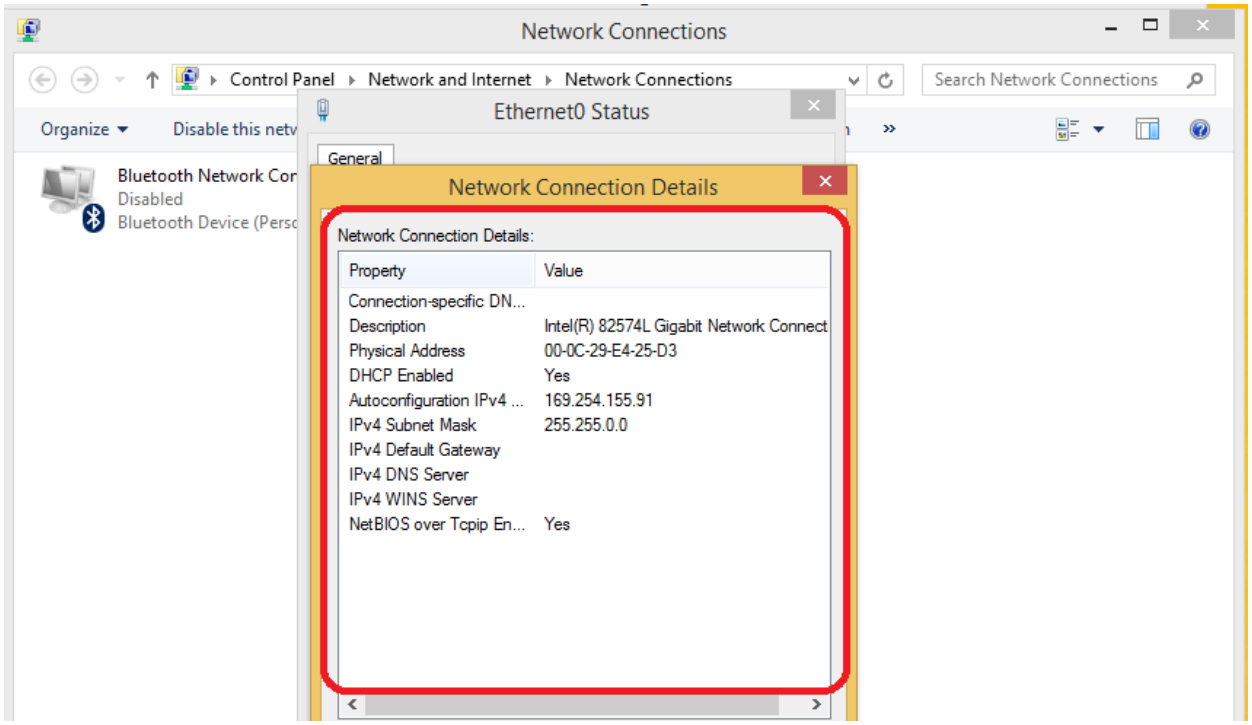
امر يقوم باستعراض كل الاعدادات لكروت الشبكة من mask, ip,gateway,dns



Ipconfig /release

معناها افقد (تخلص)من الايبي اللي عندك (على جهاز الكلاينت)

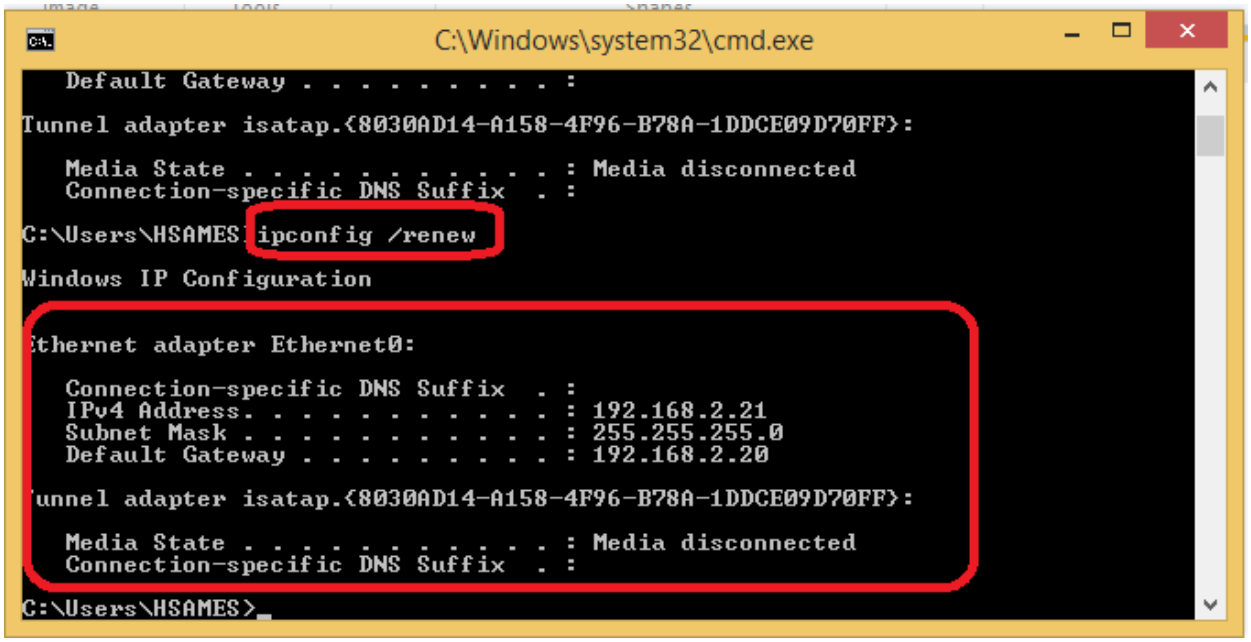
حيث يصبح كرت الشبكة للكلاينت بلا أي ايبي ولا أي اعدادات.

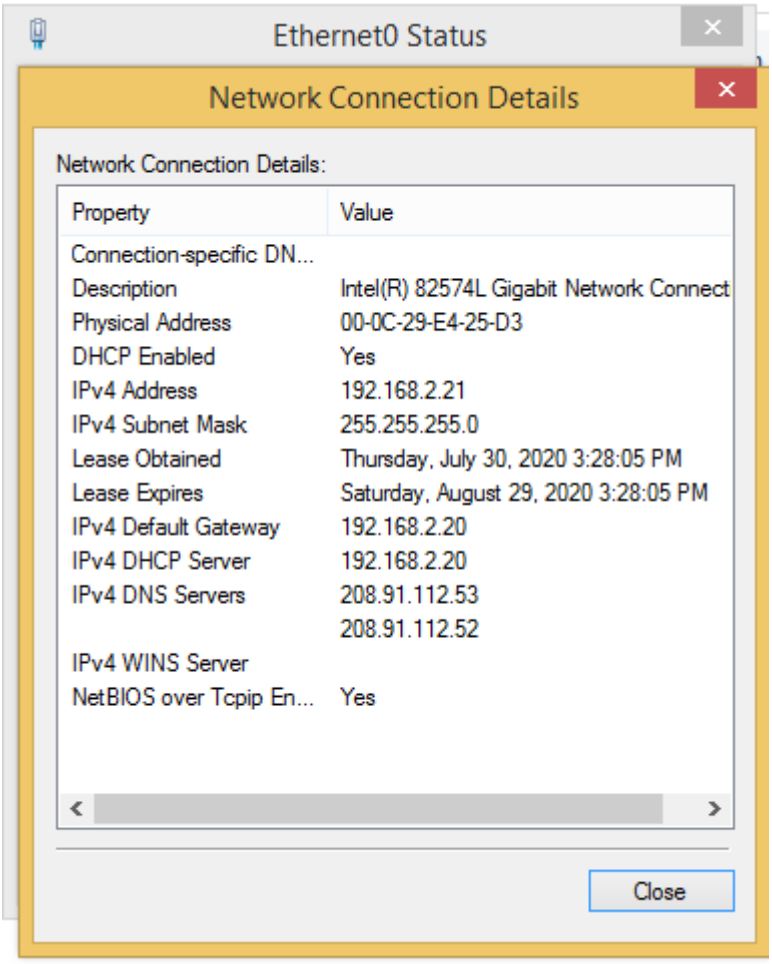


Ipconfig /renew

معناه ابحث لي عن اعدادات جديده من أي dhcp server

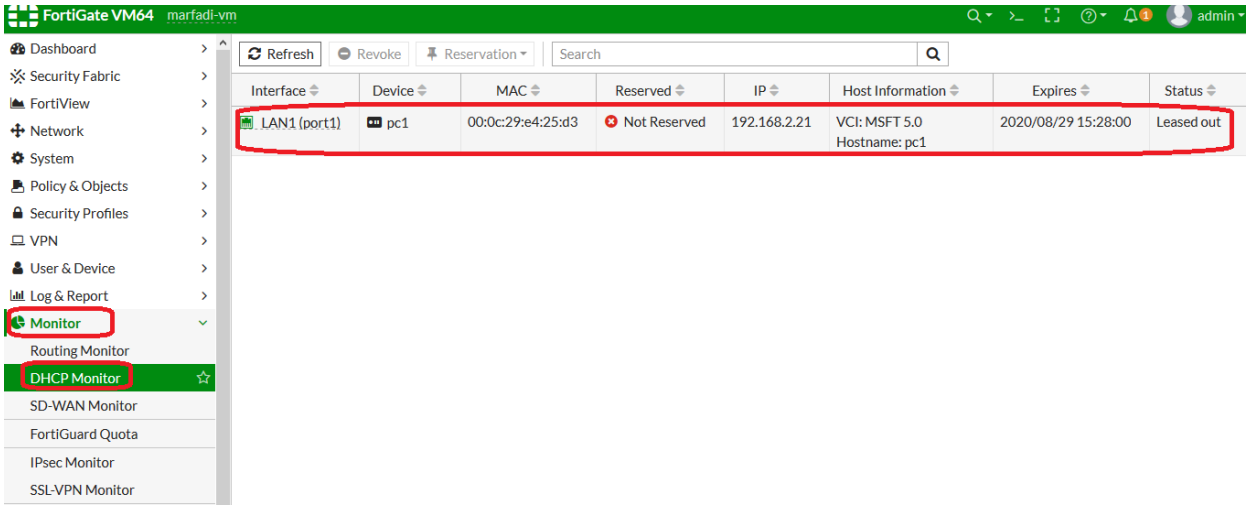
او ممكن عمل disableو enable لكرت الشبكة على جهاز الكلاينت بدلا عن هذا الامر ..





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

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



حيث اسم الجهاز الكلاينت هو pc1 والماك ادرس موجود والايبي الذي اخذه هذا الجهاز وأيضا leased duration

❖ طريقة تعديل الـ leased duration في الـ dhcp server :

القيمة الافتراضي لـ leased duration هي 7 أيام حيث يمكن تعديل هذه القيمة من خلال CLI في الفورتي جيت كما بالتالي:

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 ثابته في الشركة بعكس اجهزه الموبايل و الابتوبات التي ممكن تتغير كل فتره وفتره..

لذا بحسب السيناريو عندك بالشركة فلو كانت اجهزه pc فالأفضل ان تقوم بزياده فتره leased duration لكي نقلل من الـtraffic

الان سنبدأ عمليه التعديل من خلال للفورتي جيت:

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

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

وفي حالة اردت ان تكون الفترة غير محدودة فنكتب القيمة 0

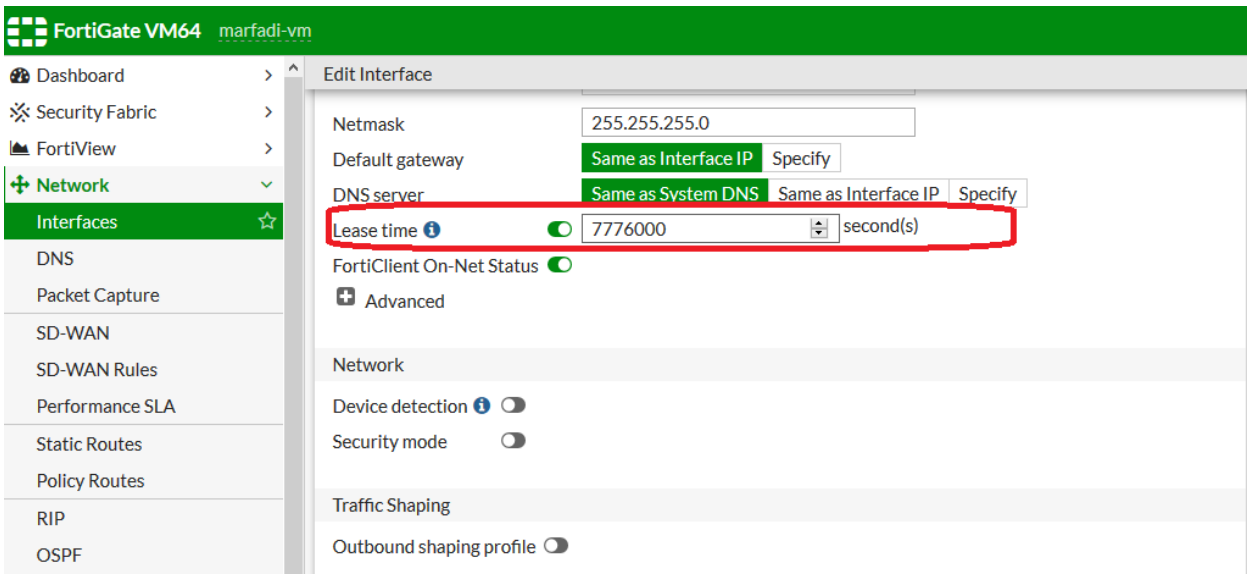
حيث لحساب عدد الثواني مثلا لـ30يوم

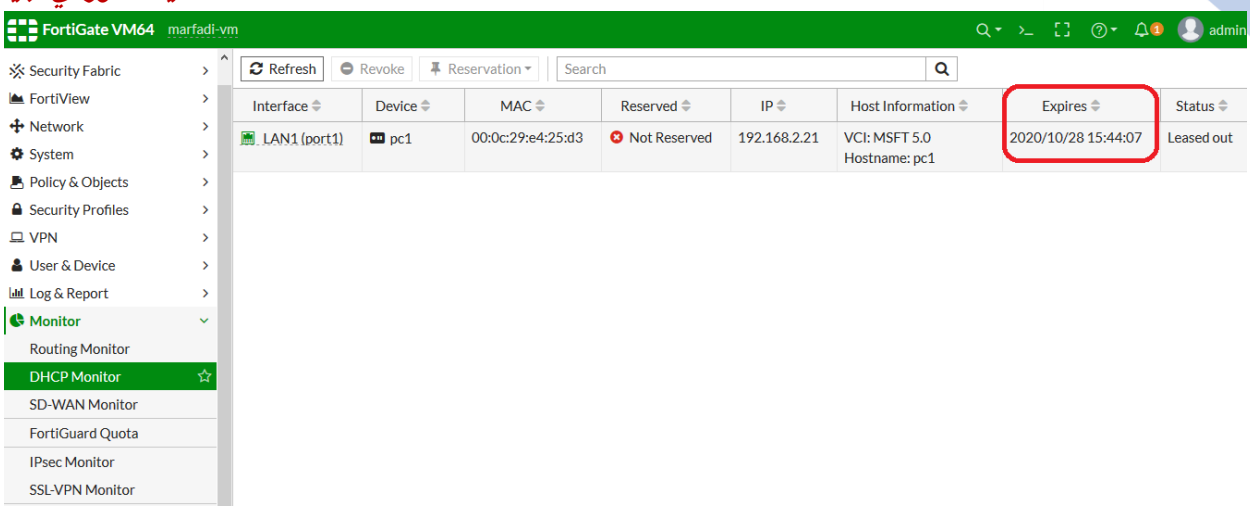
24 hours x60 min x60 sec x 30 days= 2592000 sec

ثم سنقوم بتنفيذ الامر ipconfig /renew على جهاز الكلاينت وسنلاحظ 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 الـ lease time الى 3 اشهر =7776000 ثانية ..





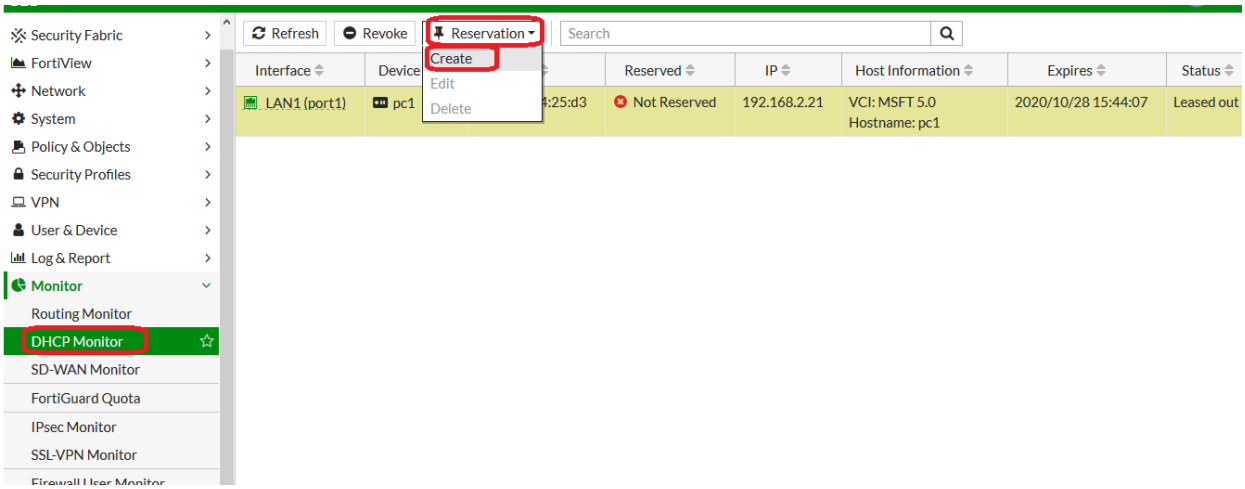
وأيضا كما بالصورة أعلاه من الفورتي جيت بأن ال leased duration هو 3 اشهر..

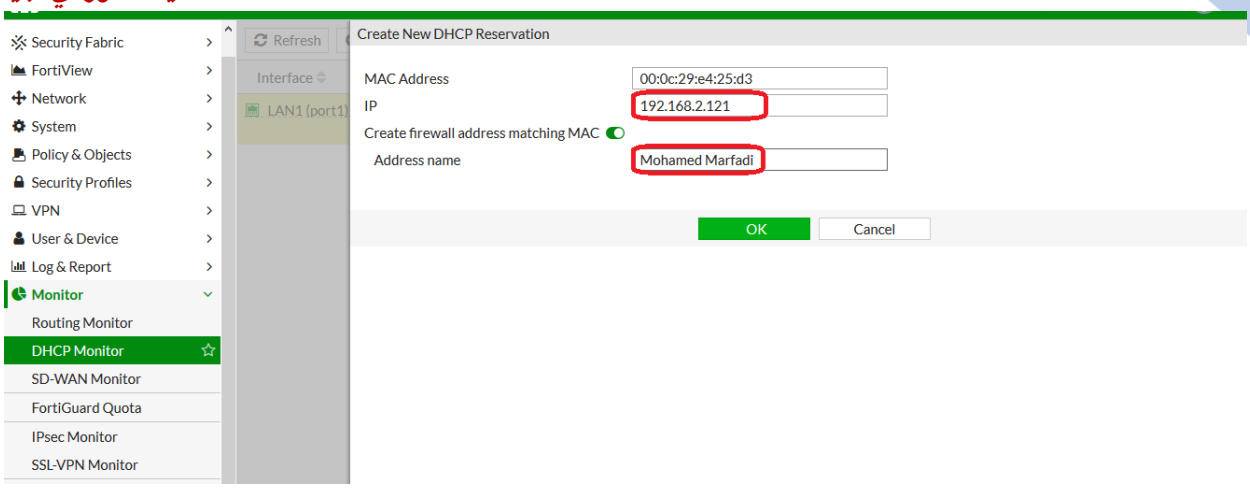
فلو اردنا عمل تعيين ايبي محدد لجهاز ما وليكم PC1

نقوم بالدخول الى dhcp Monitor ثم نحدد الجهاز المراد تخصيص ايبي محددوليكن مثلا 192.168.2.21 ومن ثم نختار التبويب المسمى Reservation

ثم create ثم

ملاحظ بأن الجهاز الكلاينت المسمى pc1 كان اخذ ايبي 192.168.2.21والان سوف نجعله دائما يأخذ الايبي192.168.2.121



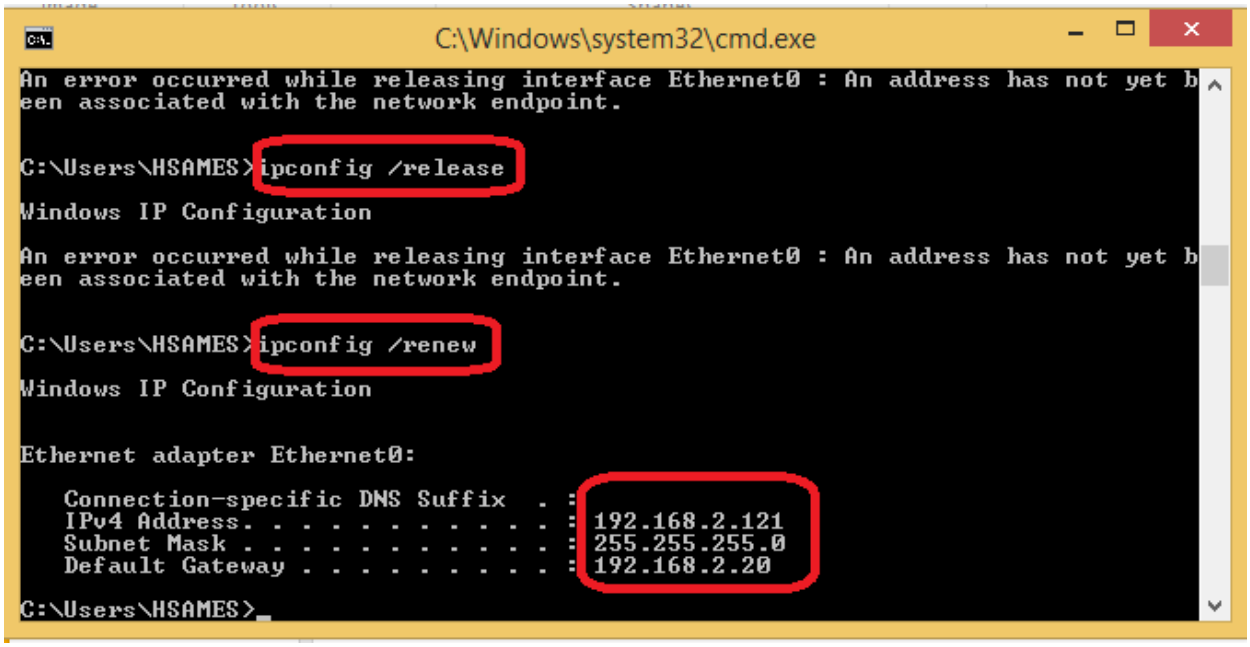


تم تحديد بأن الجهاز PC1 صاحب الماك ادرس أعلاه يجب تخصيص له الايبي 192.168.2.121 .

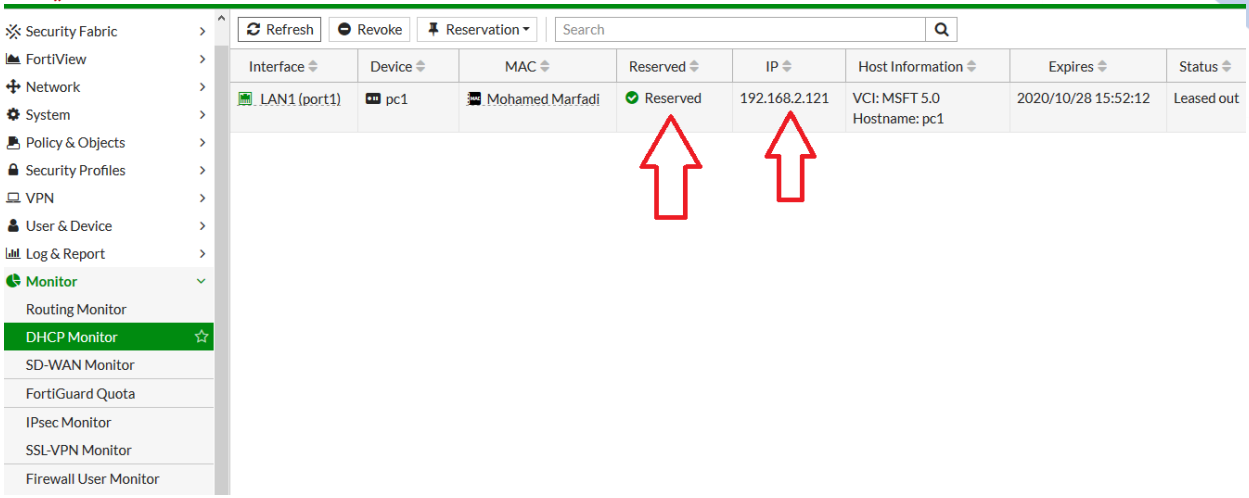
الان سوف ندخل على الكلاينت ونعمل له الامر

Ipconfig /renew

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



وايضا في الفورتي جيت لاحظ بأن الجهاز اخذ reserved كما بالصورة ادناه الايبي192.168.2.121



DNS(domain name service)

الـ dsn عباره 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 فأن الـ dns يقوم بعمل resolve من الاسم الى الايبي لأن الشبكة-الأجهزة- لا تعرف تتعامل مع الأسماء بل مع الايبيهات 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(ip(host to name from records

او from ip to name (ptr)

حيث الفورتي جيت يشتغل ك dns forwarder او dns server .

حيث لو كانت ال database موجودة على جهاز الفورتي جيت فهذا يعمل كdns server

ام الخيار dns forwarder فهذا يعني بان الفورتي جيت لا يوجد لديه database لـ dns ولكنه بيسال dns server اخر .في حالة يوزر طلب موقع مثلا ياهو فأن الفورتي جيت اكيد غير مخزن ال database لكل المواقع بالعالم لذا سيتم بتحويل الطلب الى dns forwarder الذي قمنا بأعداده سابقا 8.8.8.8 , 8.8.4.4

اما ان قام يوزر بطلب الوصول الى طابعه او أي resources بالشبكة فأن ال database تكون موجودة و مخزنه على الفورتي جيت وهنا سوف يكون dns server .

الخلاصة:

لو أي احد سال الـ dns التابع للفورتي جيت عن أي شي غير موجودة عنده على الـ database فأنه سوف يقوم بتحويله الىdns forwarder

وهوgoogle dns server

8.8.8.8 ,8.8.4.4

FortiGuard Concept

الفورتي جارد:(FDN) هي عباره 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

DDNS -8

على اجهزه الفورتي جيت المشتركه عند الفورتي جارد.

حيث بمجرد ما تشتري جهاز الفورتي 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 لتهديهات 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: عباره عن نظام موجود على جهاز الفورتي جيت تقدر من خلاله التحكم بأكثر من 1000 تطبيق على اجهزه الكلاينت

Antivirus: عباره عن نظام موجود على الفورتي جيت ويحتاج الى لايسنز لكي يتمكن الجهاز من عمل التحديث من الفورتي جارد

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 الرياضية 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 الكونفجيراشن والباتشات

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

DDNS: هي عباره عن خدمه تستفيد منها بمجرد الاشتراك مع فورتي جارد بتسمح لك ان تكون لديك dnsاكثر امانا بالإضافة الى الحصول تلقائيا على web filtering حتى لو لم تقم بعمل web filter على جهاز الفورتي جيت..

حيث الخدمات الثمانيه المذكورة أعلاه لو تقم بتجديدها فأن جهاز الفورتي جيت سوف يعمل كروتر و vpn لكن ك security profile لن يعمل الا بتجديد الاشتراك في الفورتي جارد

حيث يوجد علامات توضح حالة الخدمات التي لديك كما بالشرح ادناه :

الرمادي: بأنك مشترك بالخدمة ولكن يوجد مشكله بالاتصال مع الفورتي جارد فييجب 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 للفورتي جارد.

حيث بمجرد اقتراب موعد انتهاء الاشتراك تقوم شركه فورتي جيت بأرسال ايميل بقرب انتهاء الاشتراك..

Fortiguard distribution network (FDN)

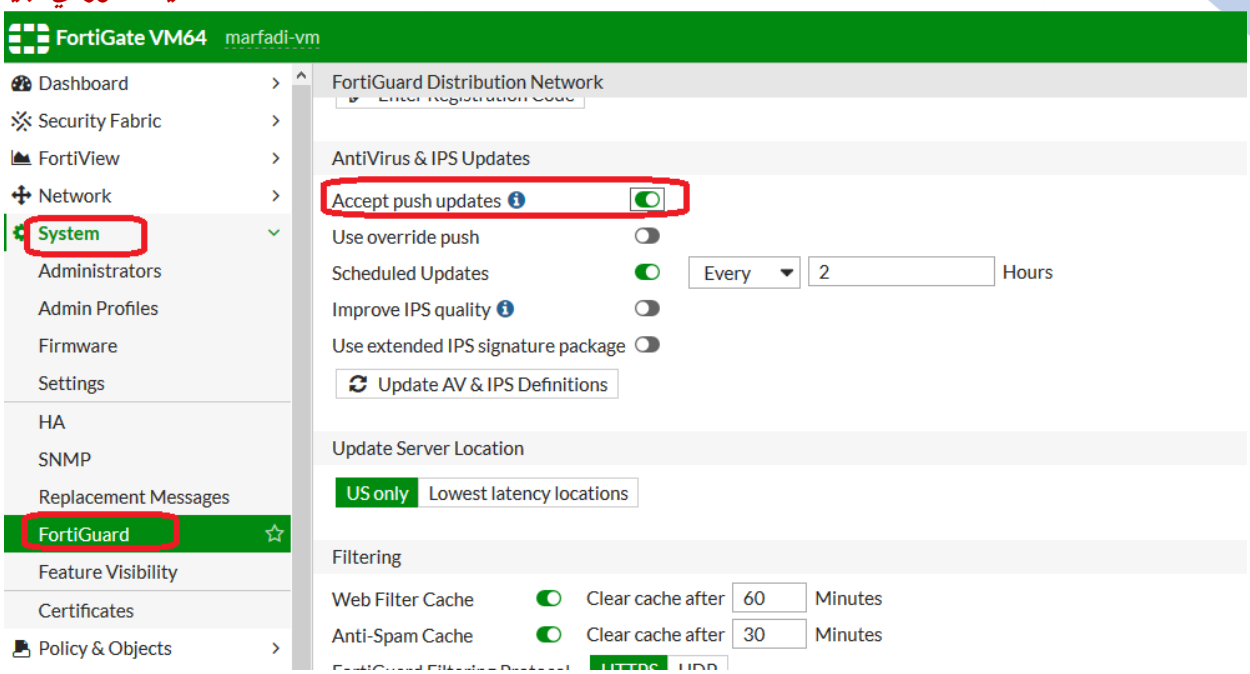
من خلال هذه الشاشة يمكنك متابعه العقد(الاشتراك)الخاص بك مع الفورتي نت متى ينتهي ومن الشخص الذي قام بتسجيل العقد والايميل أيضا..

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

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

فلو اردت ان تقوم بعمل تحديث من الـ IFDN تلقائي بمجرد وجود تحديث جديد بشرط ان يكون جهاز الفورتي جيت متصل بالإنترنت نقوم بالخيار التالي:

Accept push updates



ولو تريد ان تعمل تحديث الان نقوم بالنقر على الزر Update AV&IPS Definitions حيث ينفع هذا الخيار في حالة جهاز الفورتي جيت كان متوقف عن التحديث لأي سبب فتريد ان تقوم بتحديثه حالا...

وبعد كذا سوف يقوم بتزيل أي تحديث جديد بشكل اوتوماتيكي لأن الخيار الاخر قمنا بتفعيله

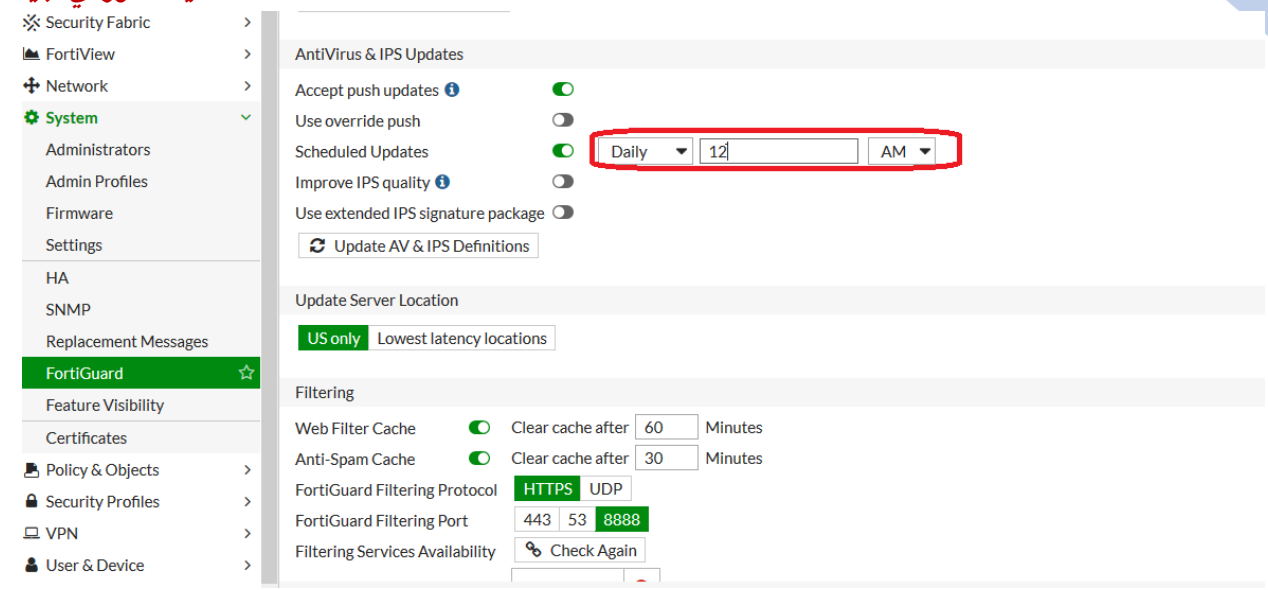
Accept push updates

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

Schedule updates

ونحدد الوقت واليوم لعمليه التحديث...

كل يوم الساعة 12 صباحا بيتم البحث عن التحديثات من الـ FDN



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

في خيار اخر على مستوى web filter cache وantispam cache

الكاش هو التخزين،

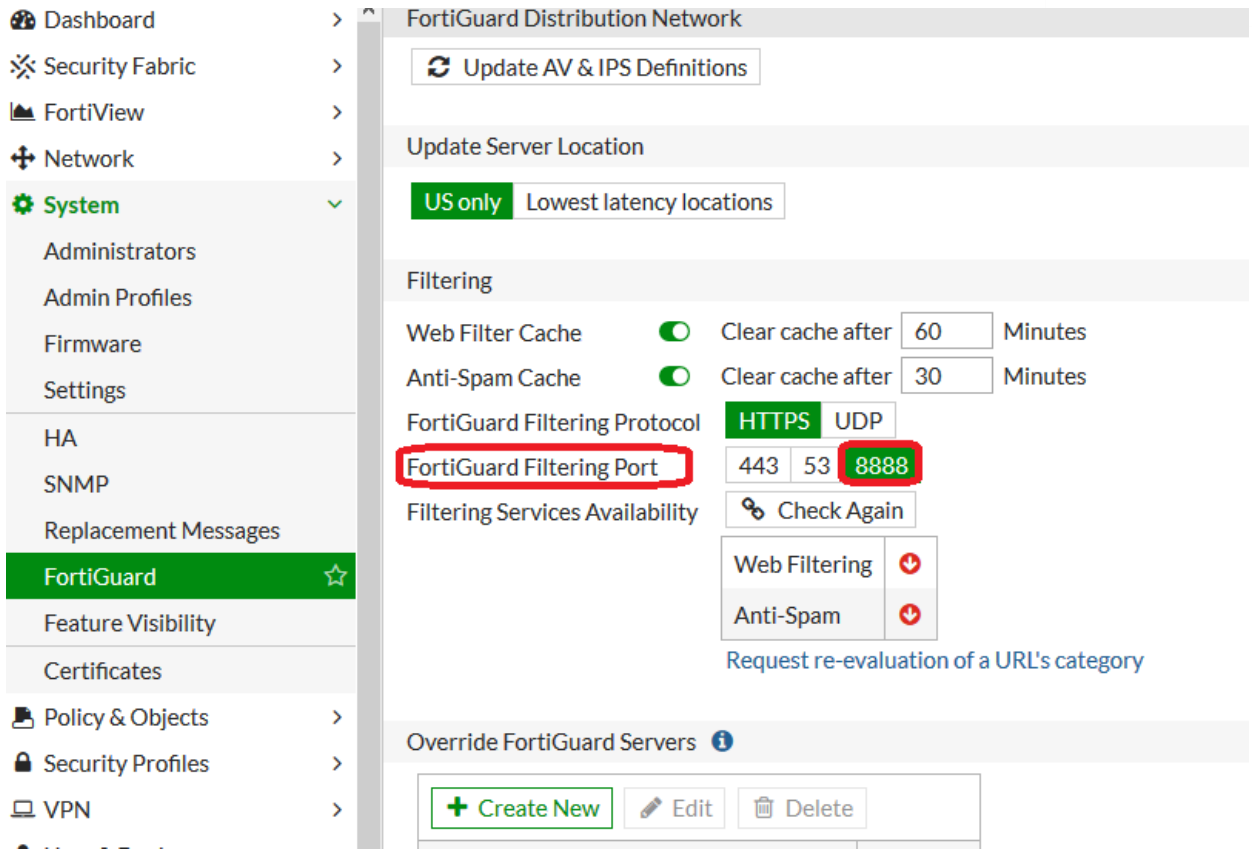
حيث جهاز الفورتي جيت بيستلم طلبات كثيره من الاجهزه الموجودة بالشبكة الداخليه لموقع معين او على ايبي معين ترسل له ايميل فالذي يحصل كالاتي ان جهاز الفورتي جيت بيتصل مع الـ FDN بيقول له لدي طلب وصل لي بخصوص الموقع الفلاني هل الموقع هذا في القائمة السوداء او يوجد فيه مشكله فأن في كلا الحالتين يجب ان يقوم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

حيث لو أي جهاز كلاينت طلب نفس الموقع خلال تلك الفترة فأن الفورتي جيت لا يقوم بالذهاب الى الـ FDNمره أخرى بل جهاز الفورتي جيت هو الذي يرد على جهاز الكلاينت مباشره فبذلك قمنا بتوفير الترافيك والوقت بين الفورتي جيت والـFDNوبهذا يتمزياده 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 الفورتي جيت الى الفورتي جارد هو 8888 كما بالصورة اداناه



FortiExplorer

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

حيث تقوم بتوصيل منفذ USB MGMT بالابتوب ومن ثم بواسطة التطبيق fortiExplorer الذي يمكنك تنزيله مجانا.

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

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

ملاحظة :لا يمكن تطبيق FortiExplorer على fortigate VM بل على فايروول حقيقي

Fortigate firewall policy

حيث سنستخدمه في عمليه الترافيك و الـ vpn و traffic shaper و securityوغيرها..

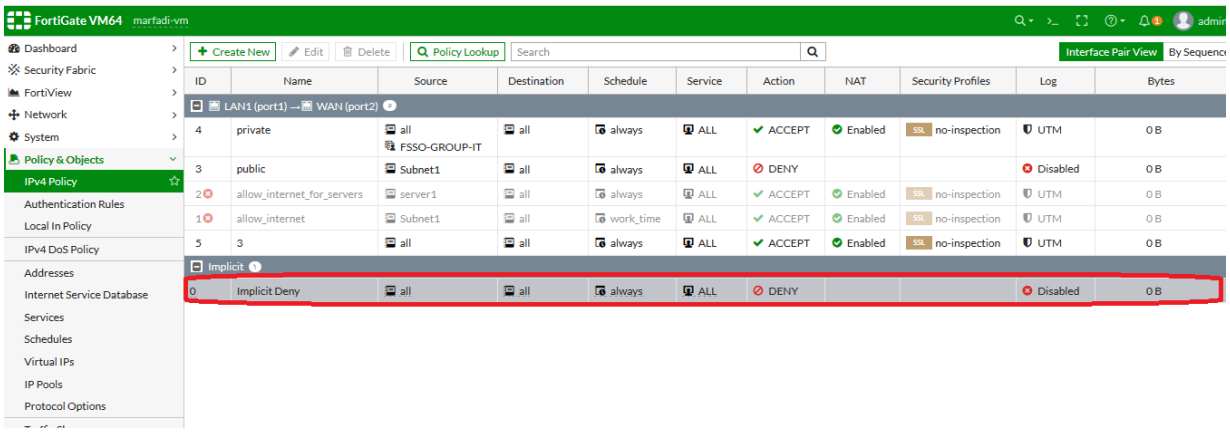
ماهي البوليسي:

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..

اذا البوليسي هي سلاحك في أي فايروول تستخدمه...

ملاحظة:أي فايروول 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...



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

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

لو في أي sourceورايح الى أي Destination في أي وقت وبأي خصائص و services قم بمنعها .

أي امنع كل شيء .

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

❖ ماهي انواع الـــ objects الأساسية (الضرورية)

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

حيث الـ interface له أنواع ممكن يكون physical interface اوvirtual interface

طريقة عمل: virtual interface

Create New>interface >

تم إعطاء اسم للكرت باسم vlan1وعنوان له مثلا virtual interface 1 ونوعه Vlan أي انه كرت وهمي وليس حقيقي لذا يجب ان يكون جزء من كرت حقيقي)ابن من الكرت الحقيقي (ولذ تم اختيار LAN1 وبعدها تم إعطاء الكرت الايبي 192.168.3.100/255.255.255.0 واعطائها administrative access لـ https pingحيث بعد ذلك يصبح هذا المنفذ المسمى VLAN1 كانه 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 حاجه..

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.

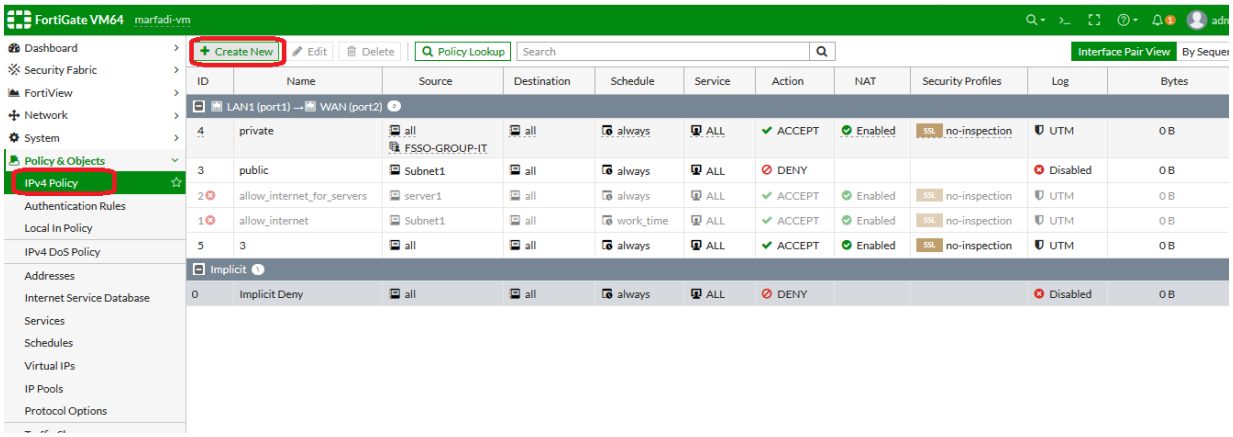
حيث لو اخترت بروتوكول معين وليكن https فهذا يعني بأنه هو فقط الذي سيتطبق عليه البوليسي اما لو اردت كل البروتوكولات يتم التطبيق عليها فنختار. All

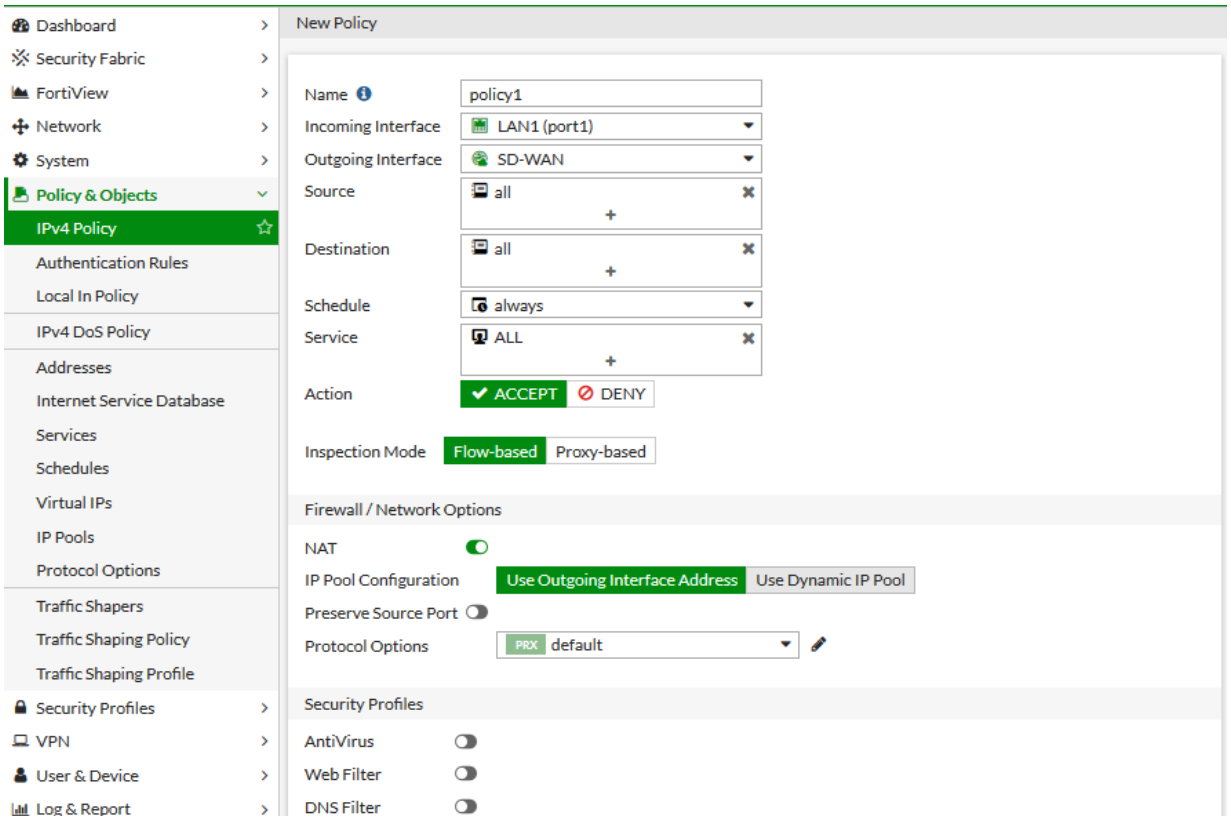
3- Sechdual : متى تريد تطبيق هذه البوليسي!! هل في أوقات معينه او مره واحده فقط فلو اخترت الخيار Always يعني باي وقت.

4- Action : تسمح allow لهذه البوليسي

Deny تمتع هذه البوليسي..

❖ طريقة انشاء البوليسي:





ثم نقوم باختيار الـ objects كما تكلمنا عنها سابقا

Name : اسم البوليسي

Incoming interface : الـinterfaceالذي سيمر منه الترافيك

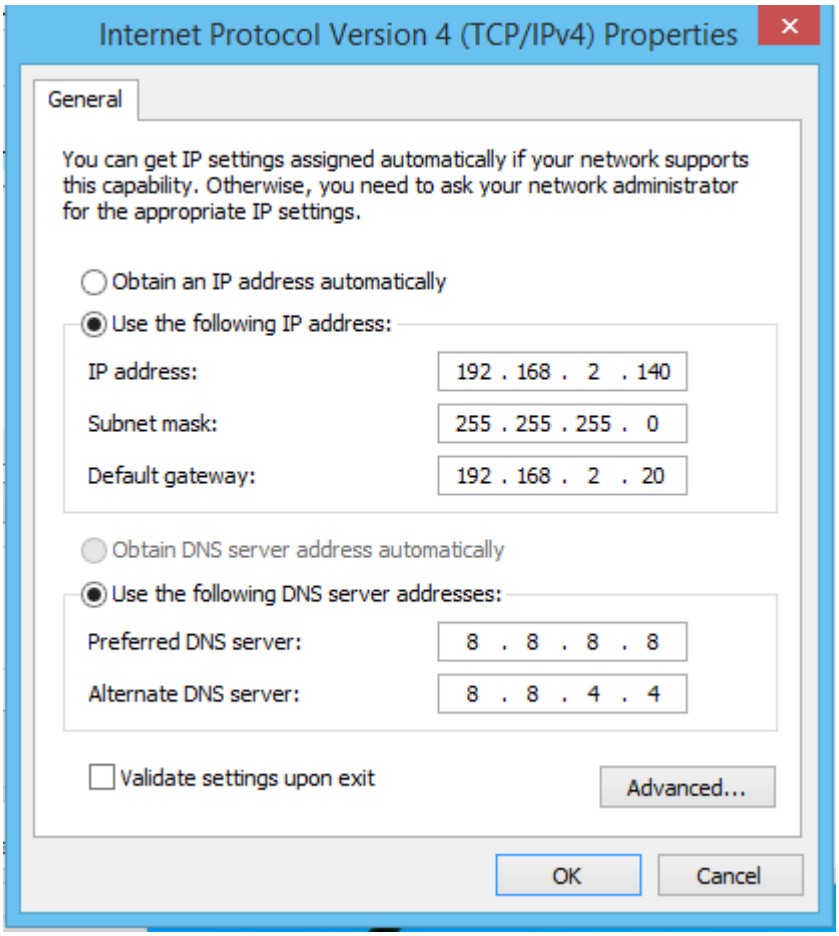
Outgoing interface : الـ interfaceالذي سيمر اليه الترافيك

Source :

تصميم الشبكة لدينا كما بالرسمة التالية:

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

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



كما بالصورة أعلاه لأحد اجهزه الكلاينت في الشبكة الداخليه الذي يوضح اعدادات كرت الشبكة من ايبي وبوابه افتراضيه و.. DNS

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

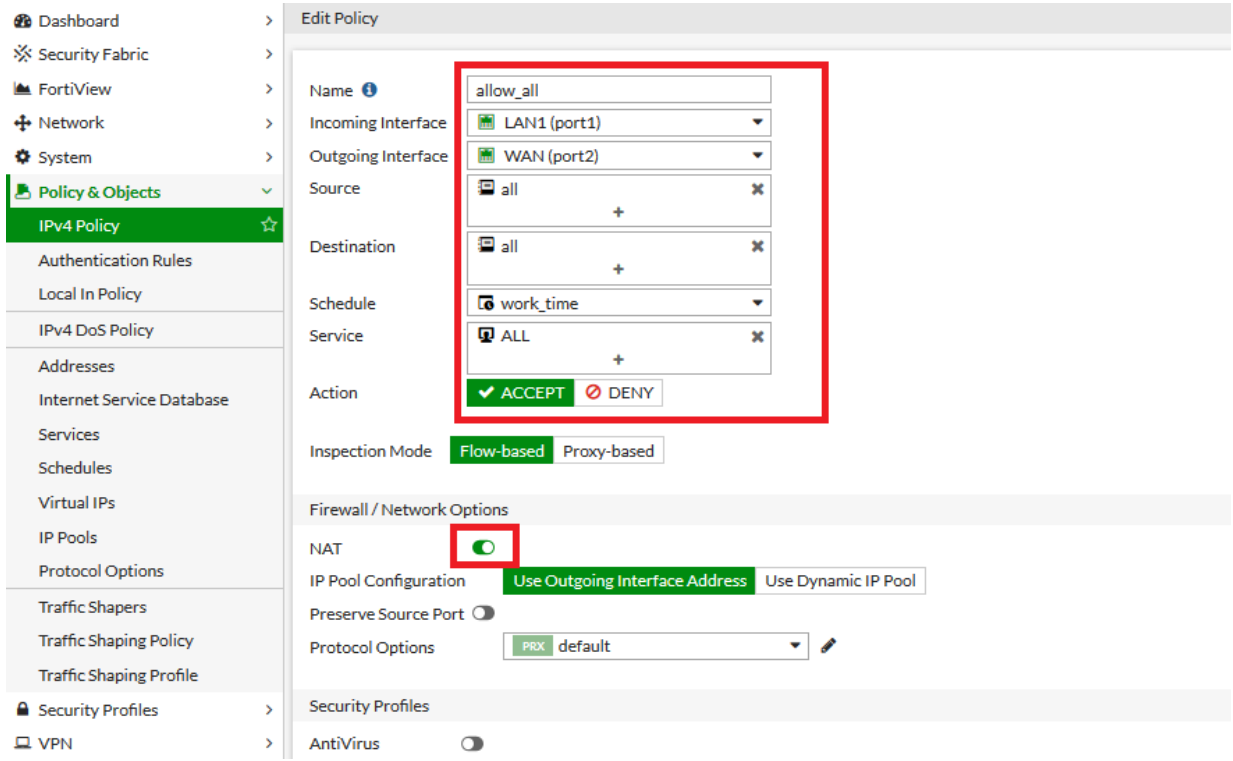
اسم البوليسي(الرول)allow_all:

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

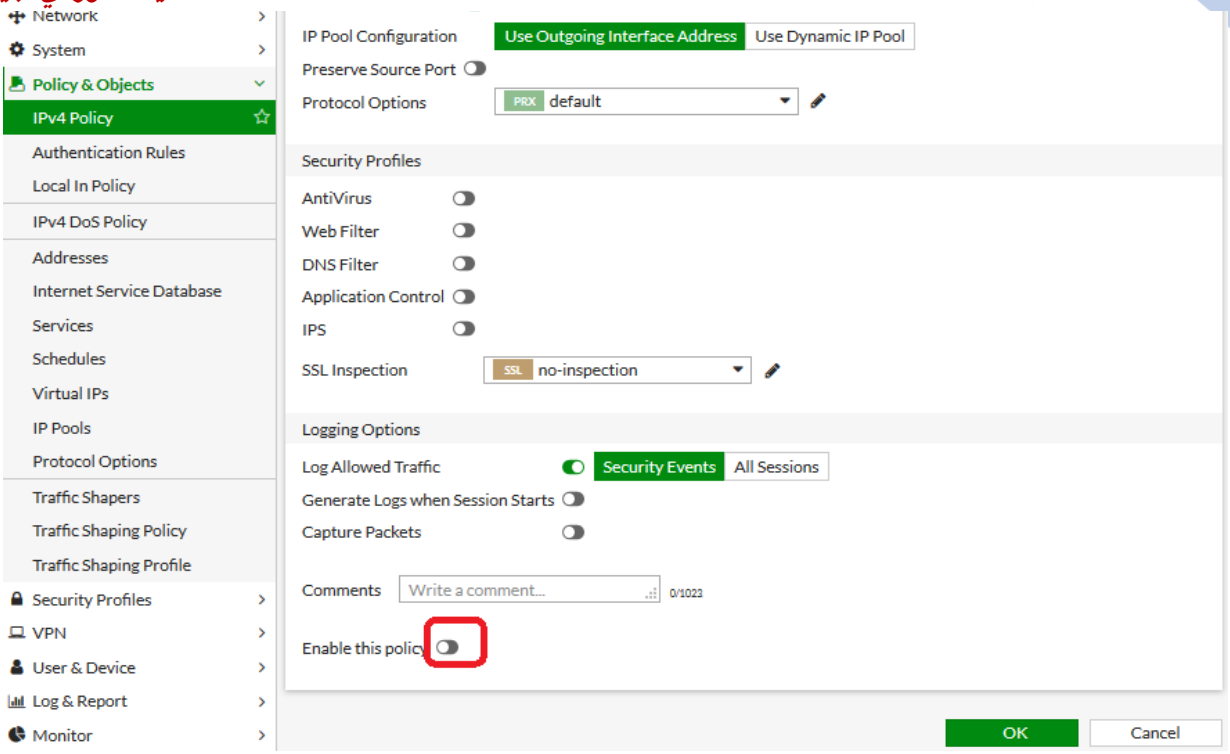
يجب ان تقوم بتفعيل الخيار NAT لأنه طالما أي شبكة تريد ان تتواصل مع شبكة أخرى بـ subnet مختلفه فلازم يكون هناك عمليه الـ NATلذا يجب تفعيل هذا الخيار لكي يعمل NAT بين الشبكة الدخلية(LAN) وبين الانترنت..(WAN)

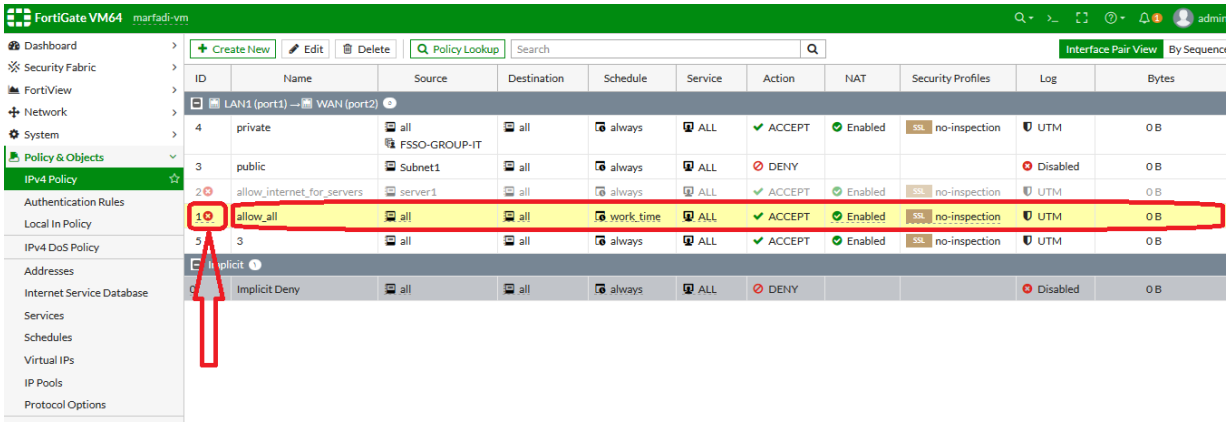
ثم موافق...

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



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 اريد تفعيلها فاننا نقوم بعمل الخيار. Enable this policy=off





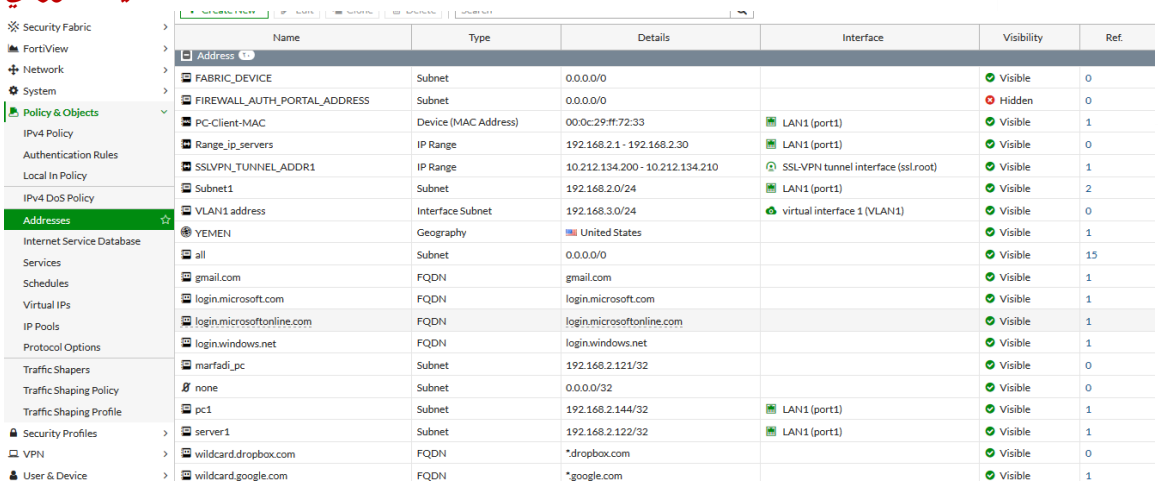
لاحظ بالصورة أعلاه بان البوليسي allow_all معمول لها disabled .

Firewall objects

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

: Address

لاحظ بالصورة ادناه بأن هناك مجموعة من العناوين التي موجودة بشكل افتراضي..



ولأنشاء عنوان جديد نقوم بالخطوات التالية:

Subnet :

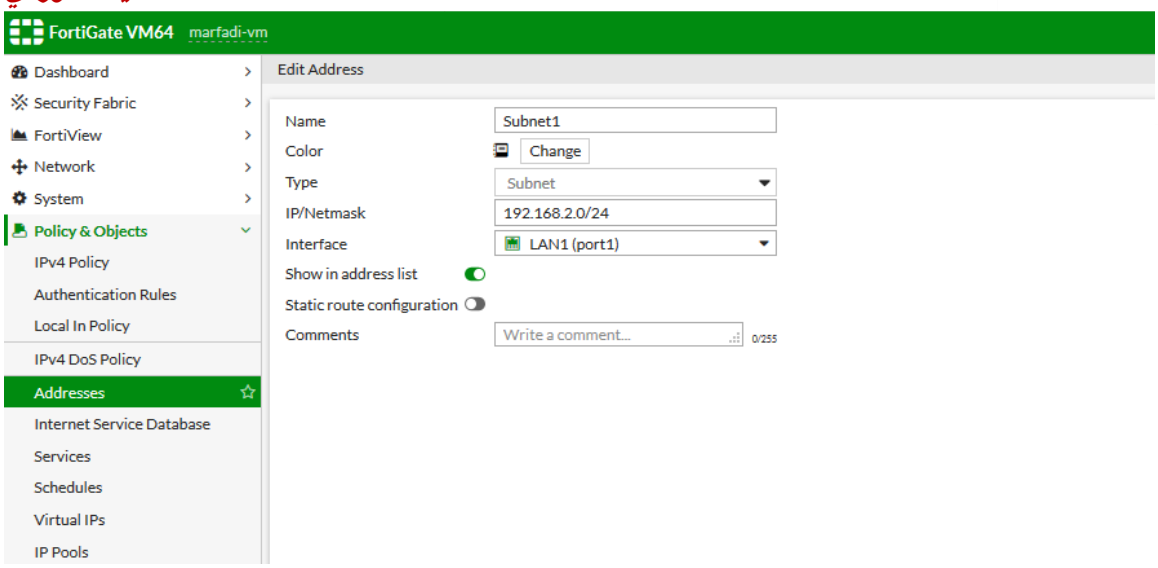
هذا النوع بيعبر فيها عن الشبكة(Subnet) Network

او تعبر فيها عن جهاز معين) ايبي محدد(

او تعبر فيها عن كل العناوين(all ip's)

الطريقة الأولى:

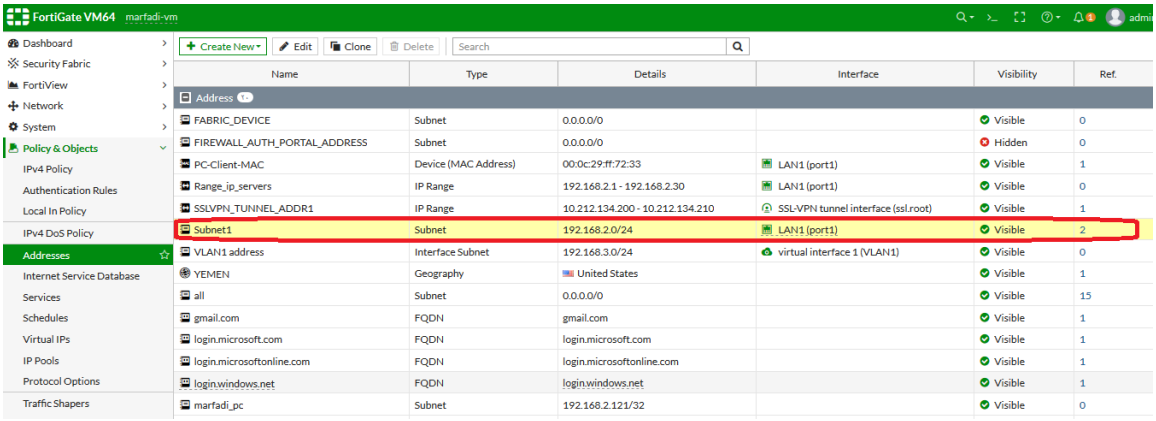
التعبير عن شبكة كامله(شبكة معينه)



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

المسماة subnet1 بكرت الشبكة LAN1.

لاحظ كما بالصورة ادناه بان العنوان تم اظهاره...



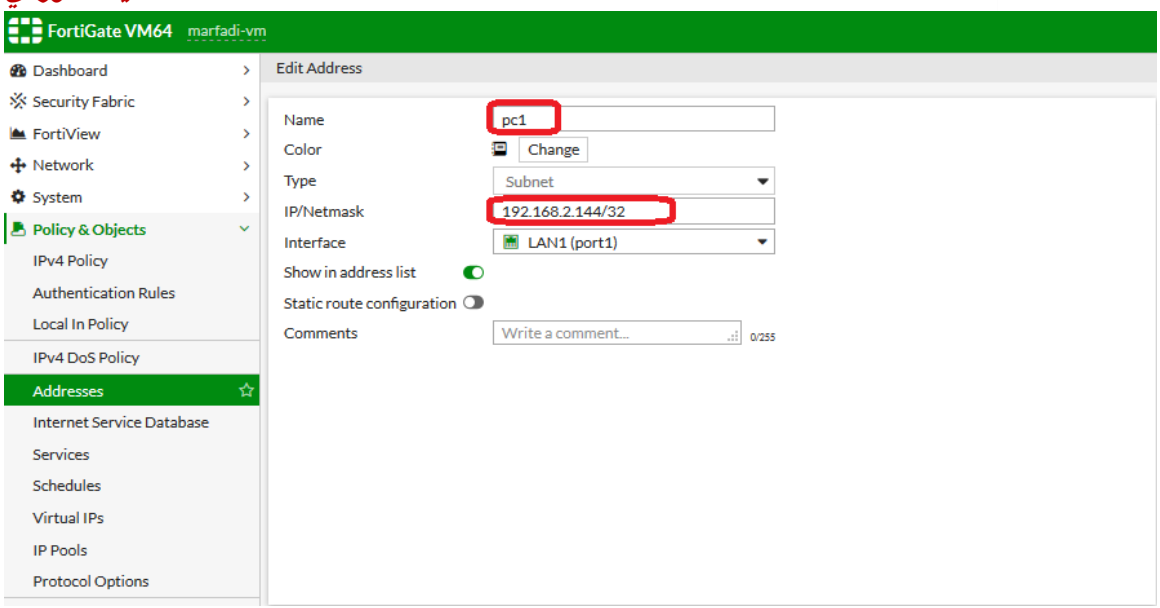
الطريقة الثانية:

التعبير فيها عن جهاز معين- ايبي محدد-

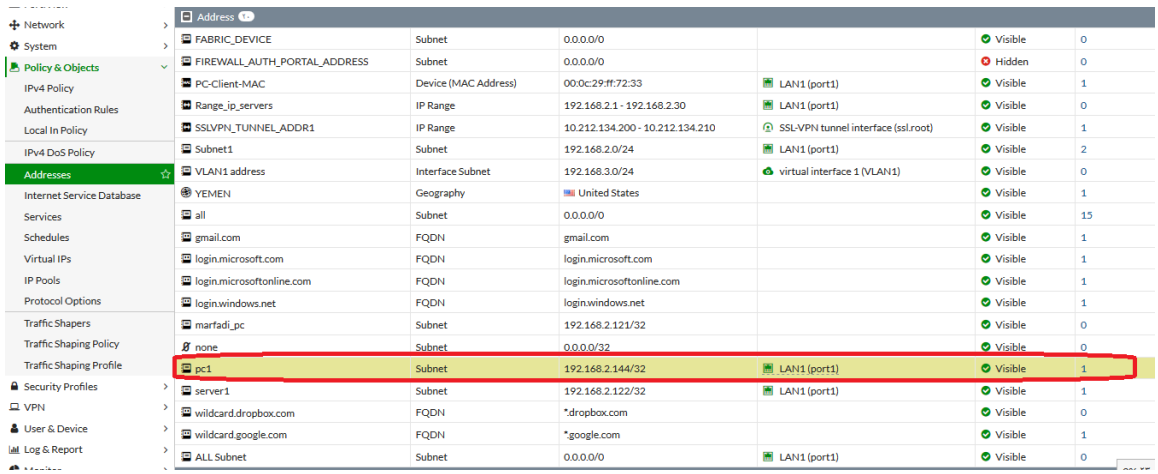
اما اني اكتبه بالطريقة التالية

192.168.2.144/32او192.168.2.144/255.255.255.255

لكي اعبر عن جهاز معين) ً(Single host



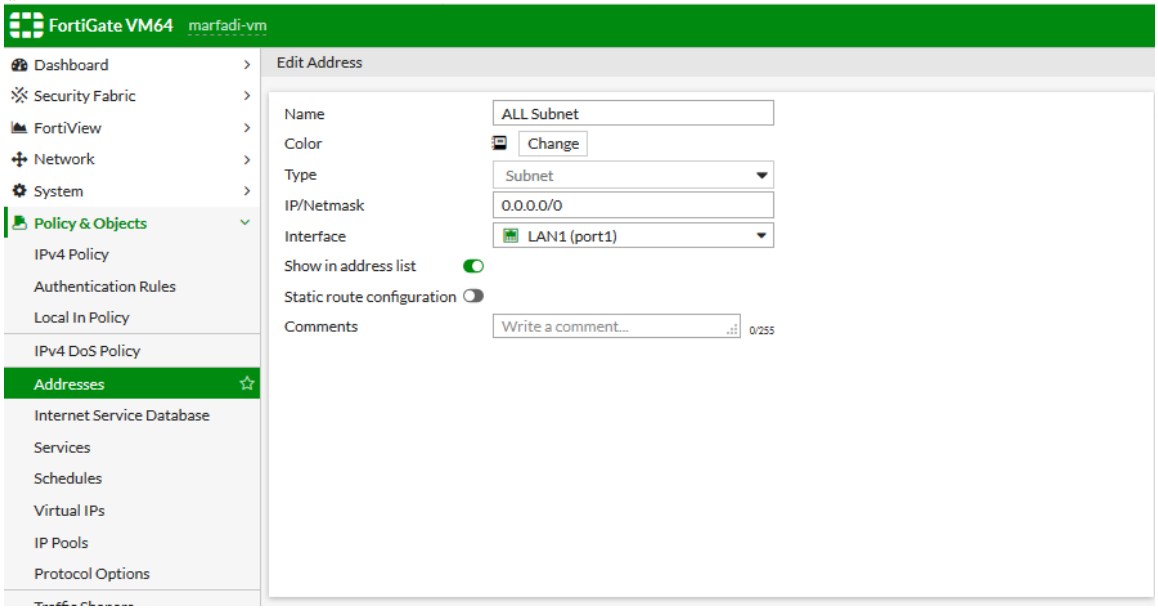
لاحظ بأن العنوين المضلل يعبر عن جهاز معين اسمه pc1وله ايبي. 192.168.2.144



الطريقة الثالثه:

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

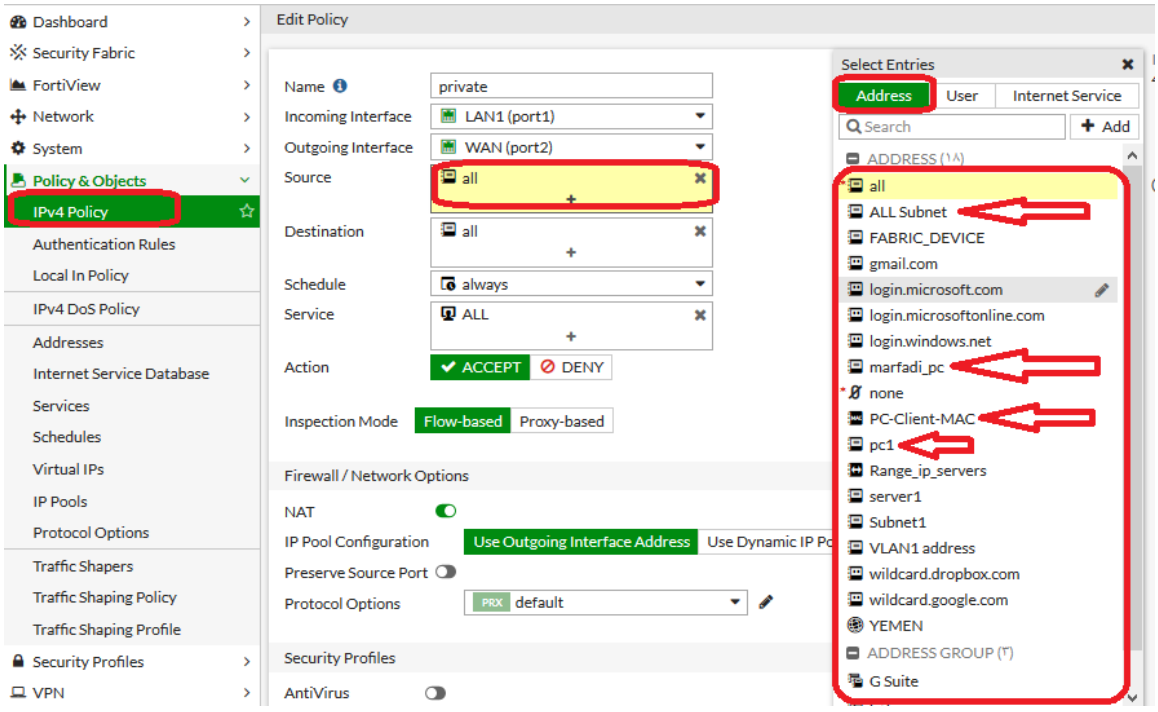
حيث يتم كتباتها كالتالي 0.0.0.0/0.0.0.0 أي كل الشبكات.



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

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

كما بالصورة ادناه



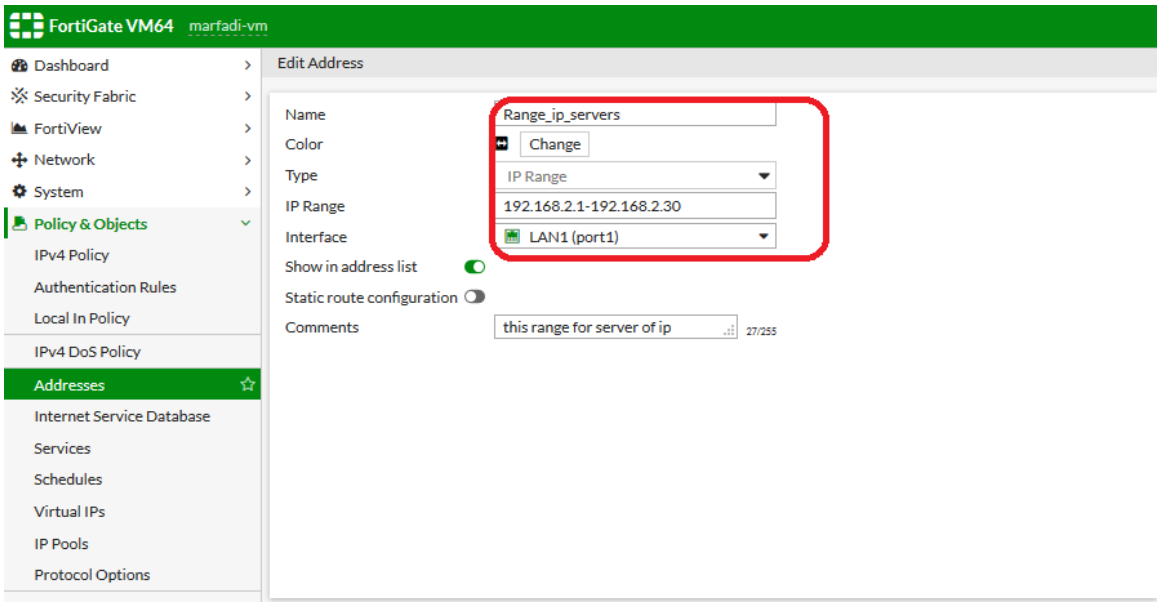
فلو اخترت العنوان pc1والذي له الايبي المحدد192.168.2.144

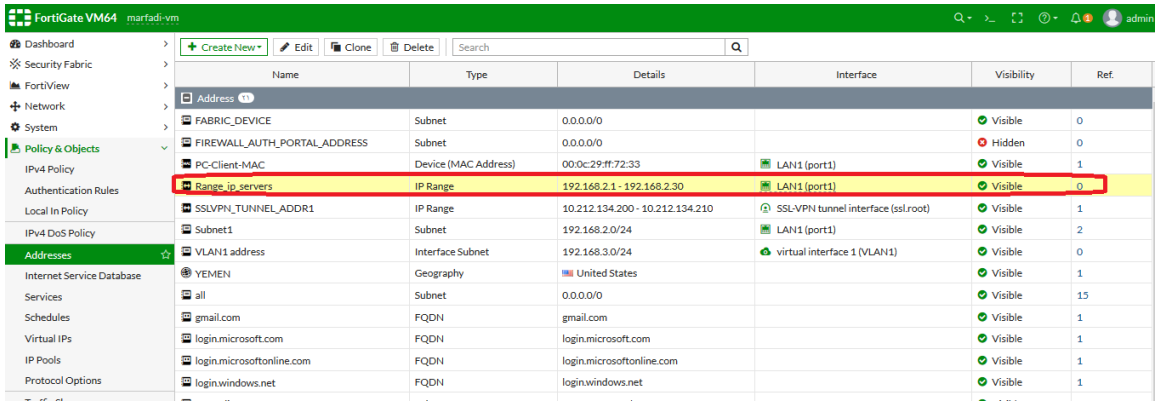
فان فقط الجهاز صاحب الايبي 192.168.2.144/32 هو الذي سيستطيع ان يحصل على الانترنت فقط من اجهزه الشبكة الداخليه..

: Ip range

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

على سبيل المثال لدينارينج ايبهات مخصصه للسيرفرات من192.168.2.30- 192.168.2.1





حيث يمكنني ان اطبق عليهم بوليسي معينه..

حيث يتم استخدام الـ ip range مع VPN فأذا كان لديكvpn clients

ويريدوا ان يصلوا الى الشبكة الداخليه عبر الفورتي جيت من خارج الشركة) من المنزل مثلا(فستقوم بتوزيع مجموعة ايبيهات 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 استطيع 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(

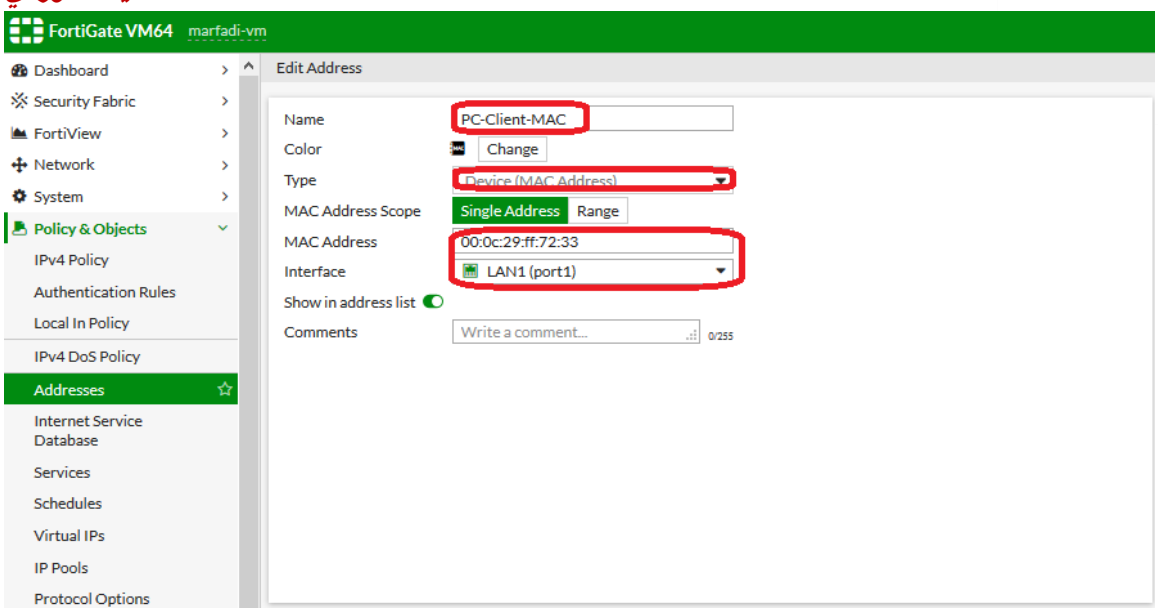
مثلا لديك موظفين موجودين في مصر ويدروا الدخول الى الشبكة الداخليه التي عندي عبر الفورتي جيت بواسطة الـvpn

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

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

1- MAC DEVICE :

عمل عنوان بحسب الماك ادرس للجهاز

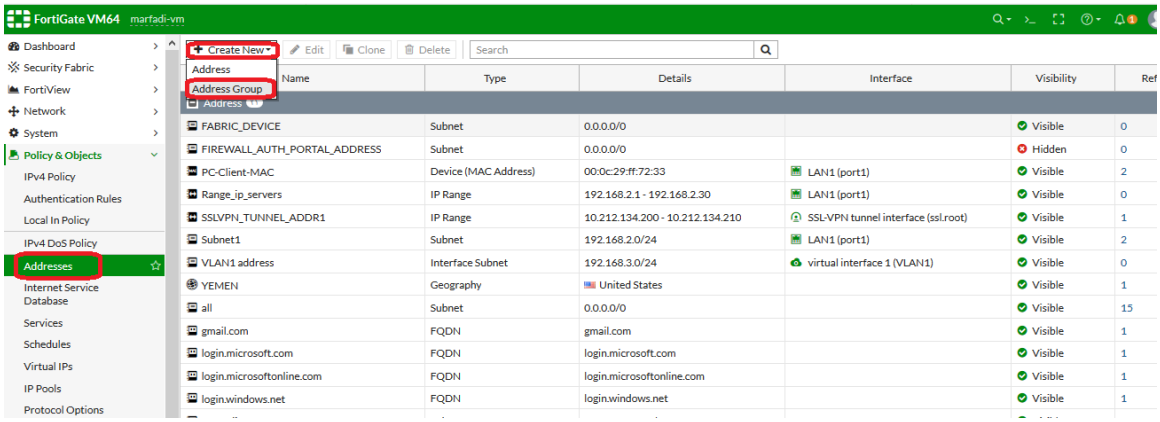


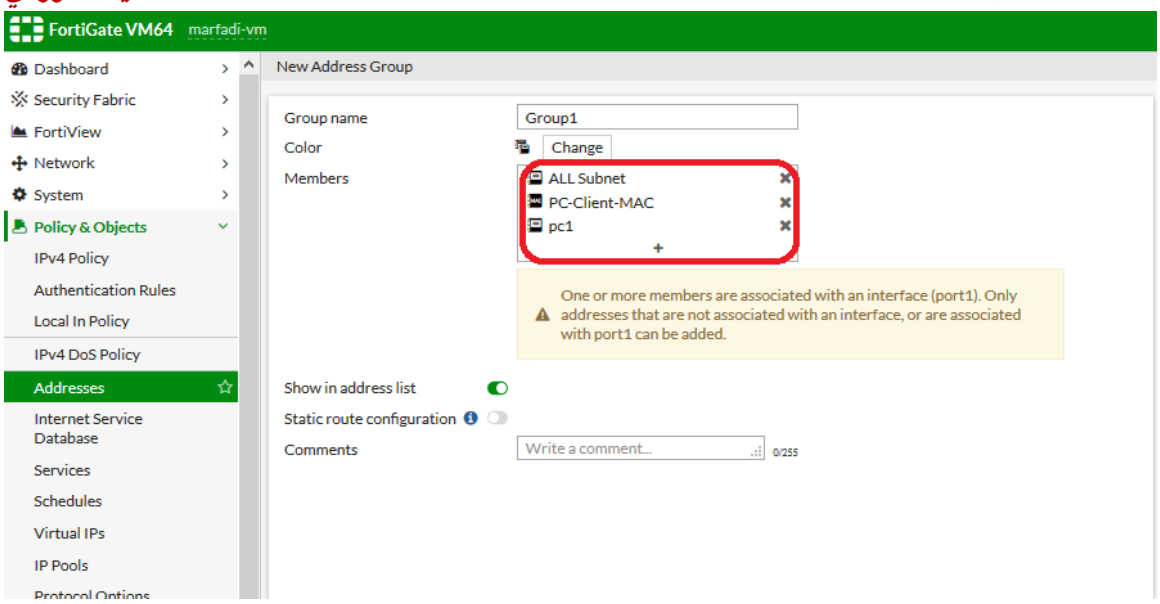
ماهي فكره الـ Address group

الجروب هي مجموعة من العناوين..

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

طريقة انشاء Address group





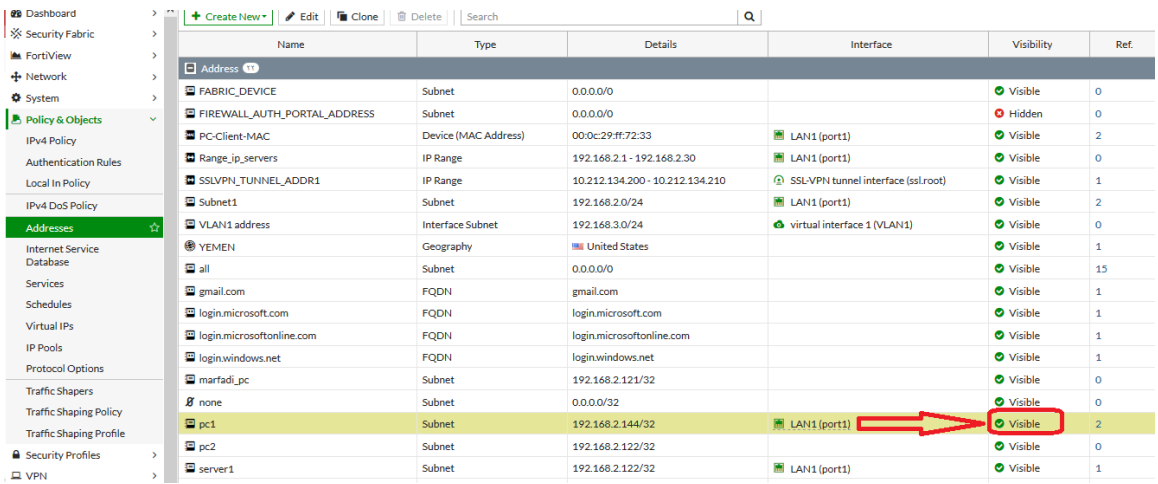
❖ شرح بعض اعمده الـ address list :

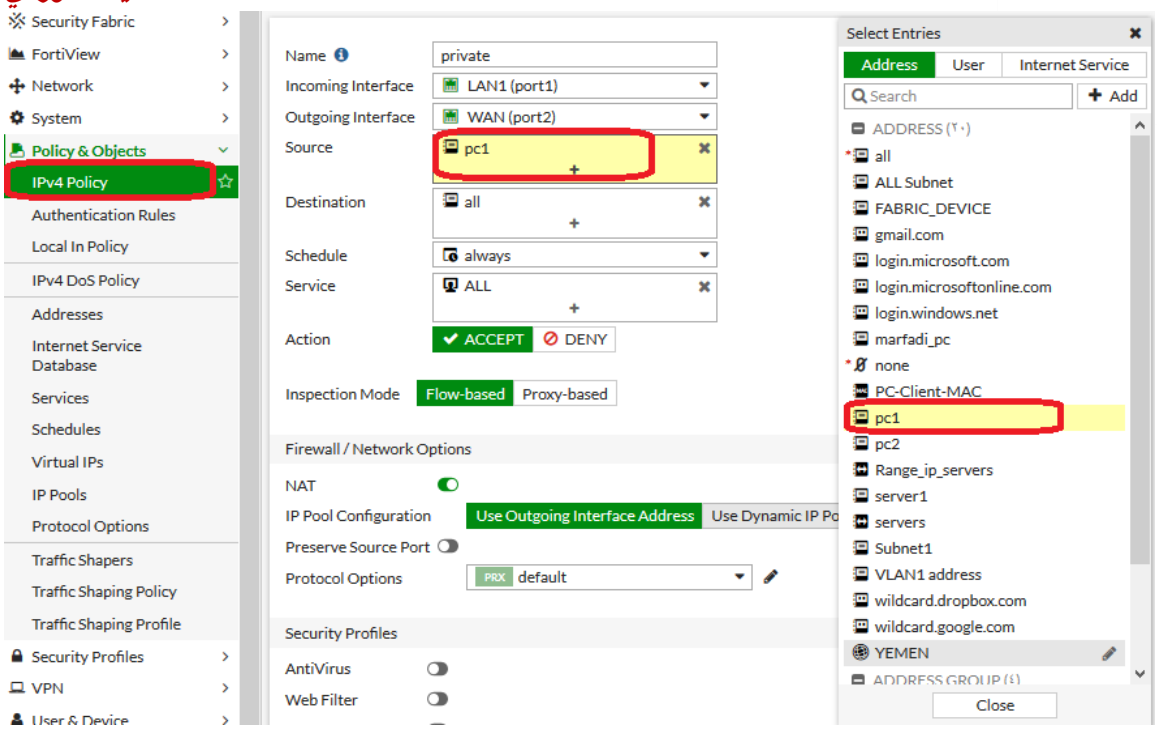
Visibility : هو عمود يوضح بأن العنوان المحدد متاح (visible) او مخفي(Hidden) وهذا معناه بأن هذا العنوان سوف يظهر او لا في البوليسي ..

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

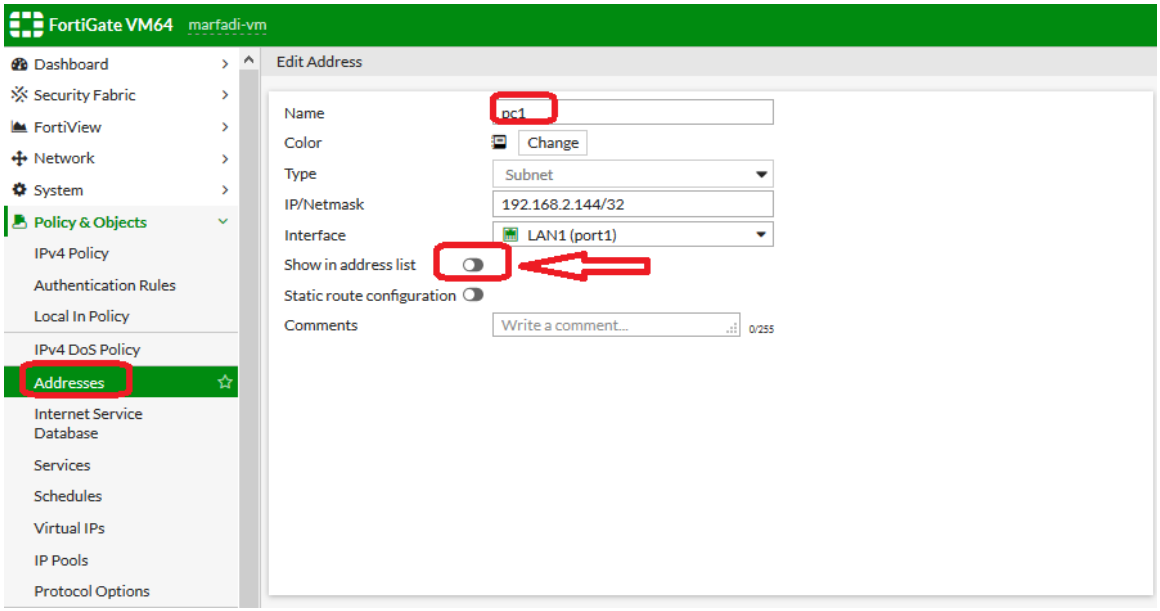
اما لو كان معمول له X فهذا يعني بأن العنوان لن يظهر في البوليسي .

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

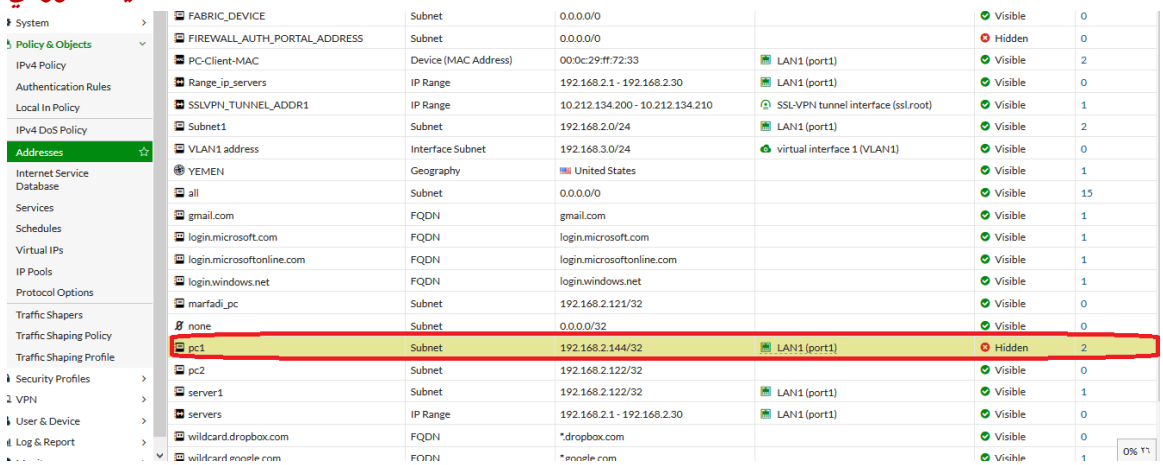




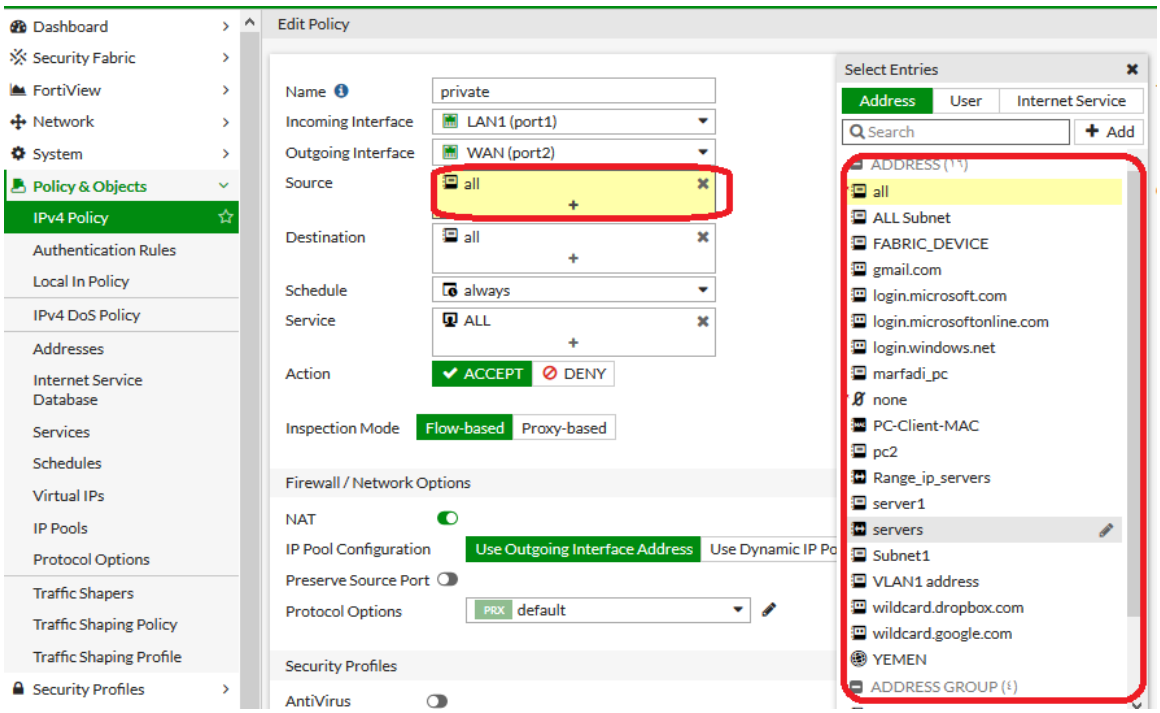
فلو قمنا بتغيير الخاصية الى Hidden للعنوان pc1 كما بالصورة التالية:



فلاحظ بان الخاصية في address list للعنوان pc1 أصبحت Hidden.



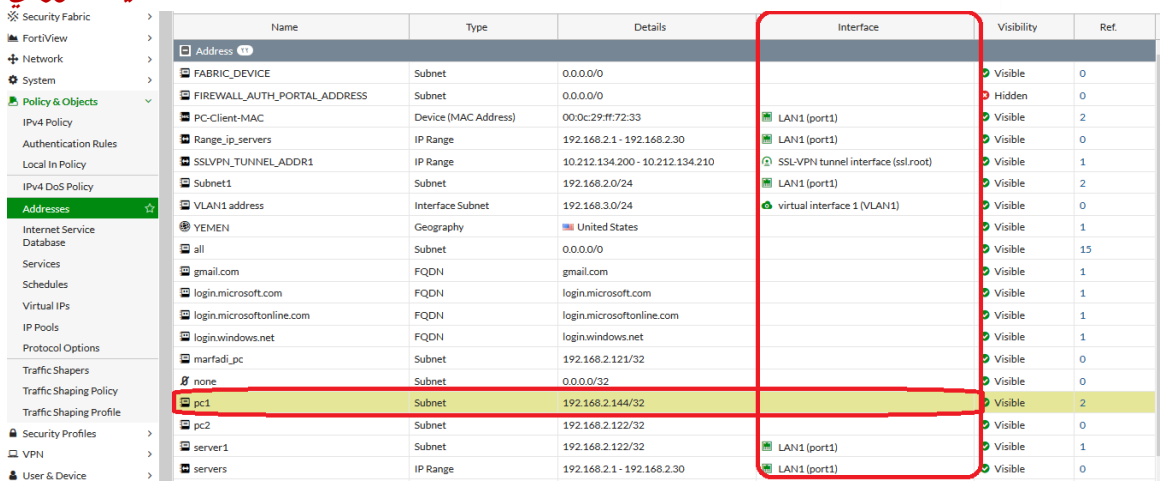
لذا عند محاوله اختيار العنوان pc1 في البوليسي فانه لن يظهر أصلا



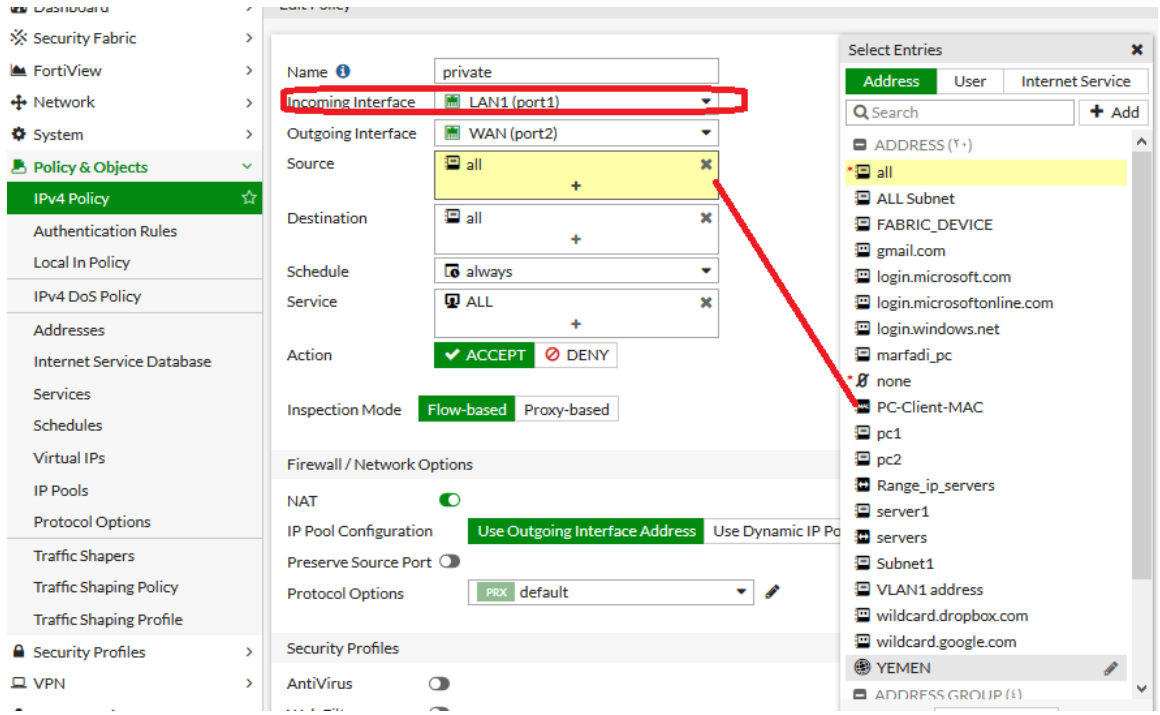
لاحظ كما بالصورة أعلاه بأن العنوان PC1 غير متاح حاليا...

Visibilityمرتبط بـ interface.

مثلا العنوان pc1 في عمود الـ interface غير مكتوب فيه أي شيء فهذا يعني بأن العنوان pc1 مرتبط مع any interface اي سوف يظهر لأي interface سواء lan او wan.

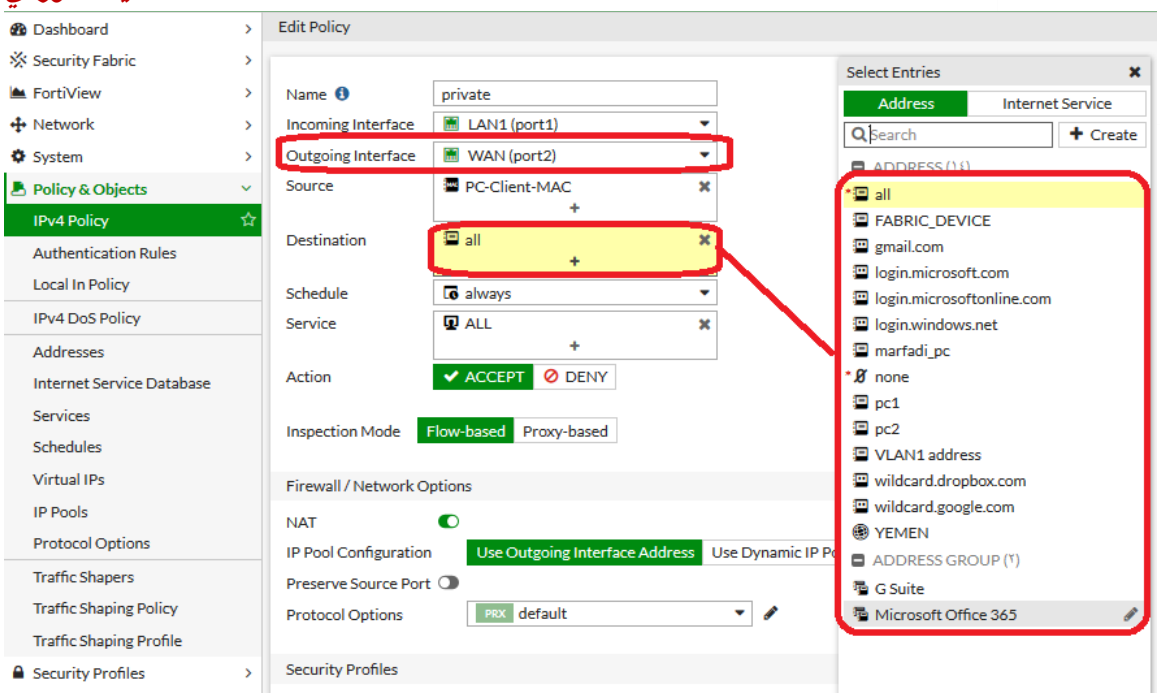


لاحظ بالصورة أعلاه بأن العنوان PC-Client-MAC معمول له visible ومرتبط مع ال LAN1(port1) interface فهذا يعني بأن هذا العنوان لن يظهر الا لو كان الـ interface نوع LAN1 ماعدا ذلك فانه لن يظهر كما بالصور ادناه:



حيث ظهر العنوان PC-Client-MAC في خانه الـ source لان incoming interface =lan1

اما العنوان PC-Client-MAC في خانه الـ destination فانه لا يظهر وذلك لأن outgoing interface=WAN(port2) لأننا قمنا بربط العنوان PC-Client-MAC مع الـ interface lan1 فقط..



نلاحظ بالصورة أعلاه بأن PC-Client-MAC لم يظهر في Destination لأن الـ Outgoing interface =wan

لذا لن يظهر الPC-Client-MAC الا ان كان outgoing interface =lan1 لأني في الأساس رابط العنوان PC-Client-MACمع الـ interface =lan1

الخلاصة:

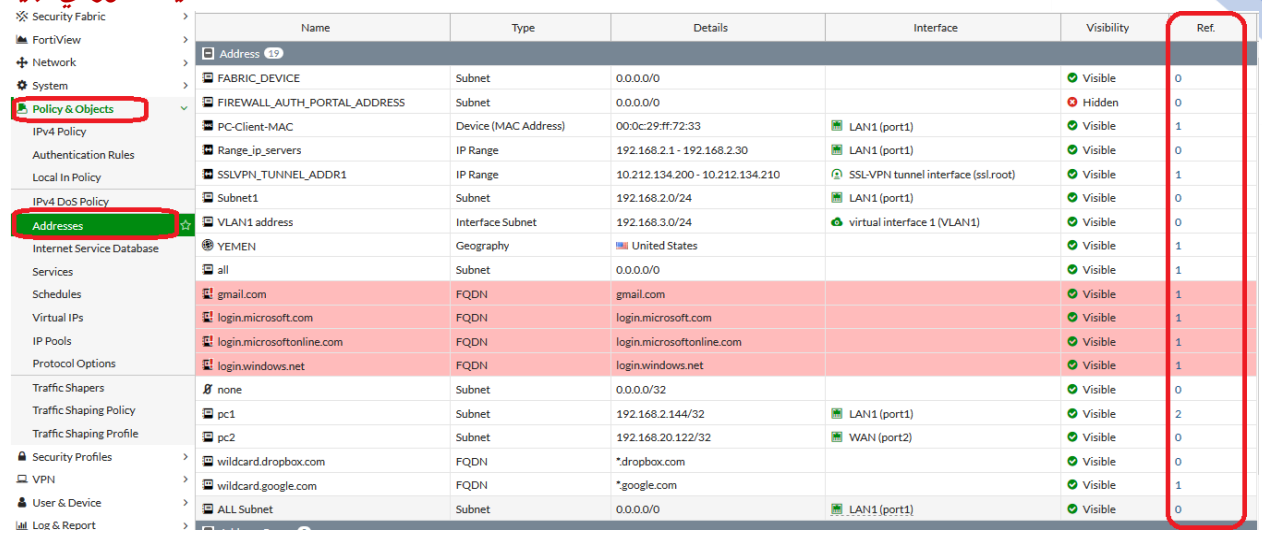
العنوان لو تم ربطه بالـ interface نوعه any فهذا يعني بان هذا العنوان سيظهر في كل الـ interfaces

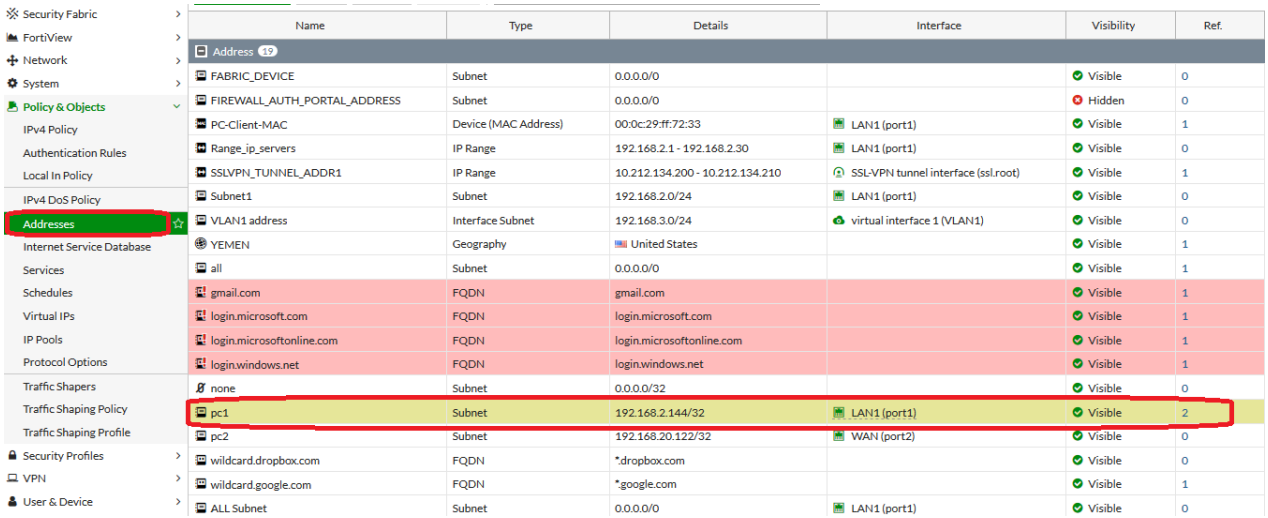
اما لو تم ربط العنوان بالـ interface مثلا LAN1 فهذا يعني بأن هذا العنوان لن يظهر الا مع الـ interface Lan1 فلو تم اختيار الـ interface =lan2 مثلا فأن هذا العنوان لن يظهر..

Incoming interface= source

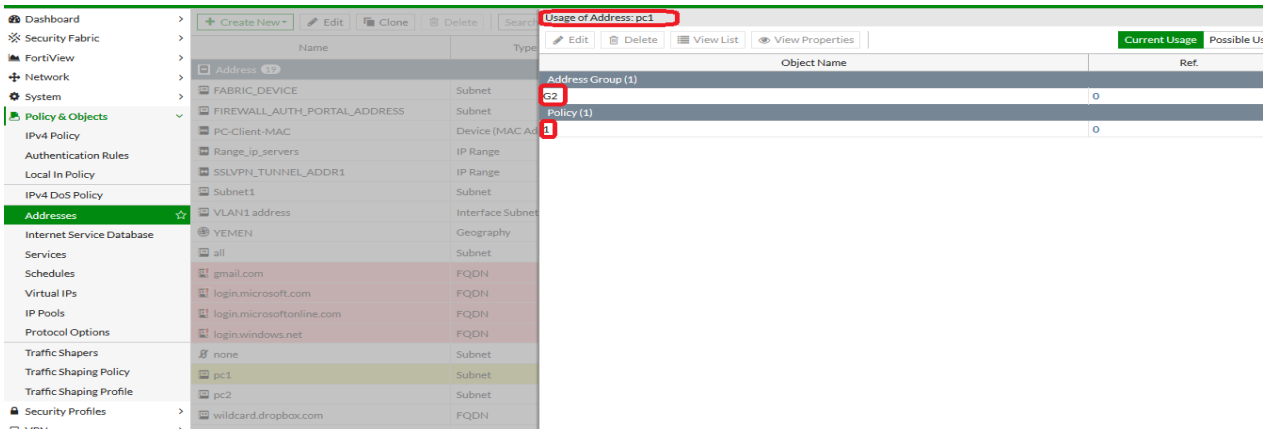
Outgoing interface=Destination

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





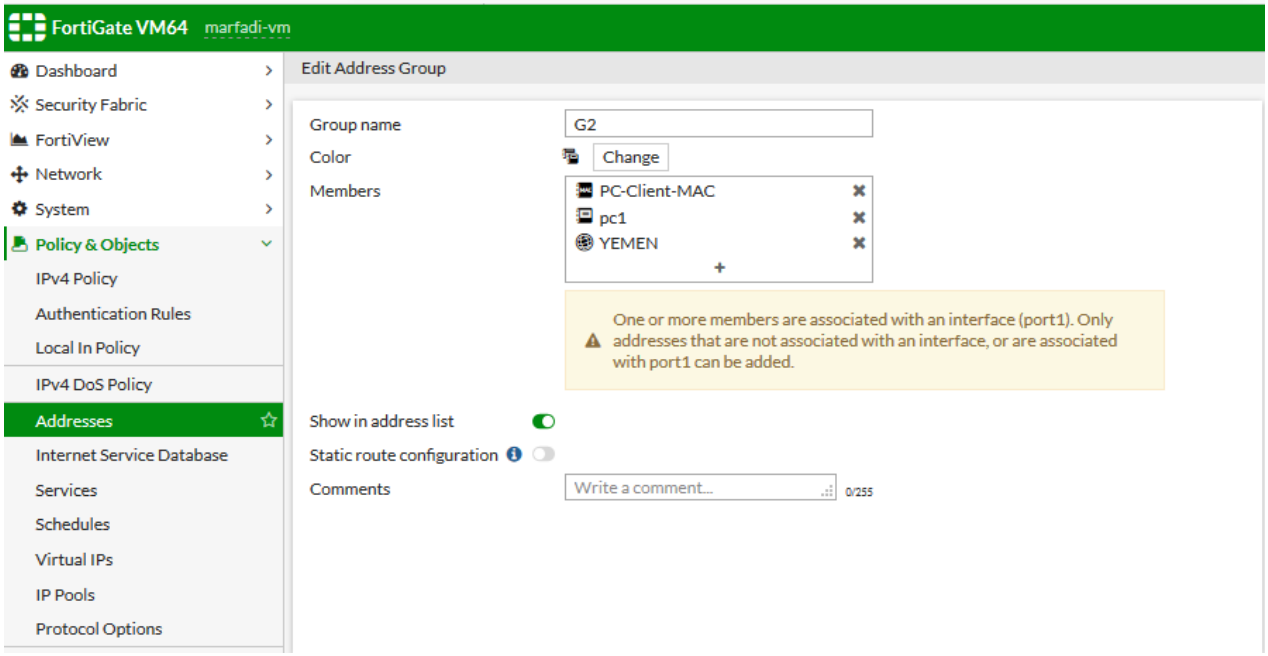
لاحظ بأن العنوان pc1 الـref=2 وهذا يدل بأن العنوان مرتبط مع 2 أشياء فبمجرد النقر على العدد 2 يقتح لك مكان الربط

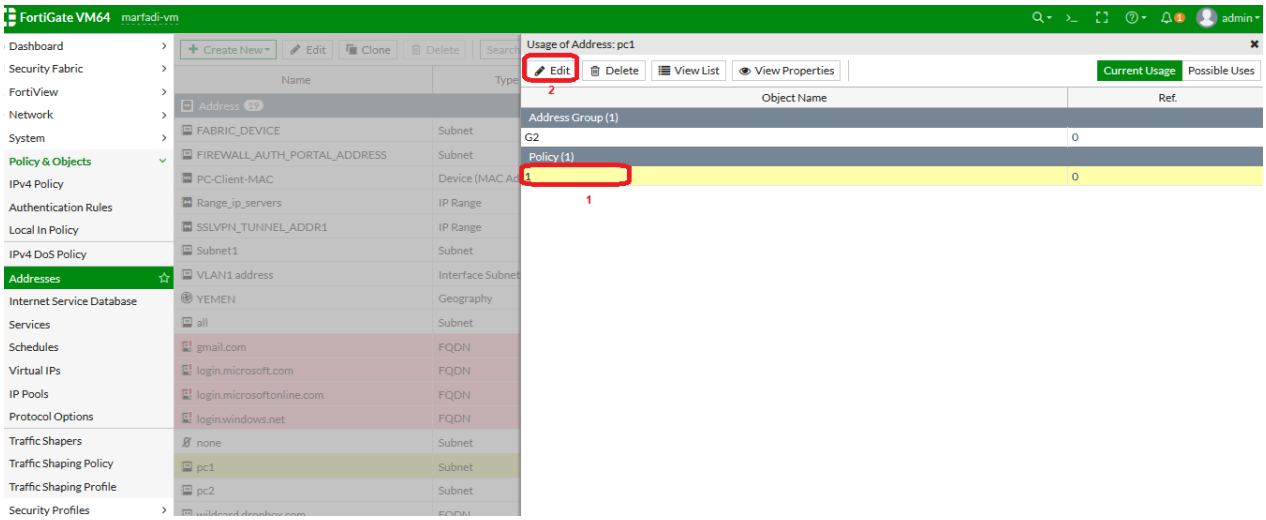


كما بالصورة أعلاه فأن العنوان مرتبط مع address group=G2 ..

والـ1 = policy ...

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 الـ policy(1) ثم Edit سوف يظهر شاشه الـ policy كما بالصورة التالية:

Services

عباره عن بروتوكولات وبورتات حيث أي نظام تشغيل يحتوي على بورتات يستخدمها لكي يقوم بعمليه الارسال والاستقبال للبيانات مع جهاز اخر.

حيث كل بروتوكل يسخدم بورت معين حيث من 1-1024 هذا ارقام بورتات محجوزة للأعمال القياسية

ومن1025- 65535

يمكن استخدامه لأي تطبيق..

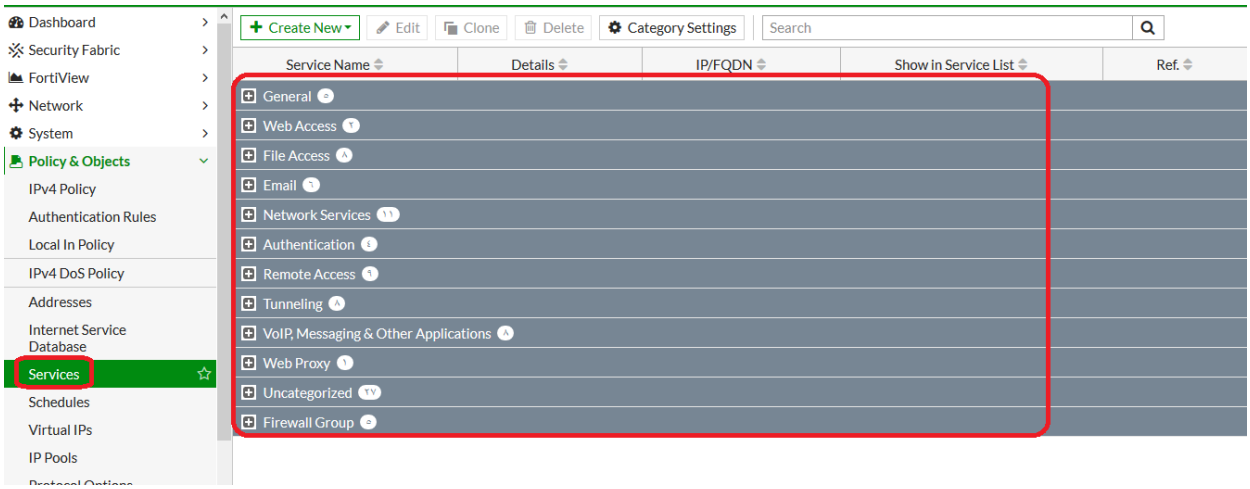
لو قدرت تتحكم في البروتوكولات والبورتات فأنك تستطيع التحكم بالتطبيقات التي يستخدمها المستخدم..

الفورتي جيت يستخدم السيرفس لتحديدرقم البورت لعمل

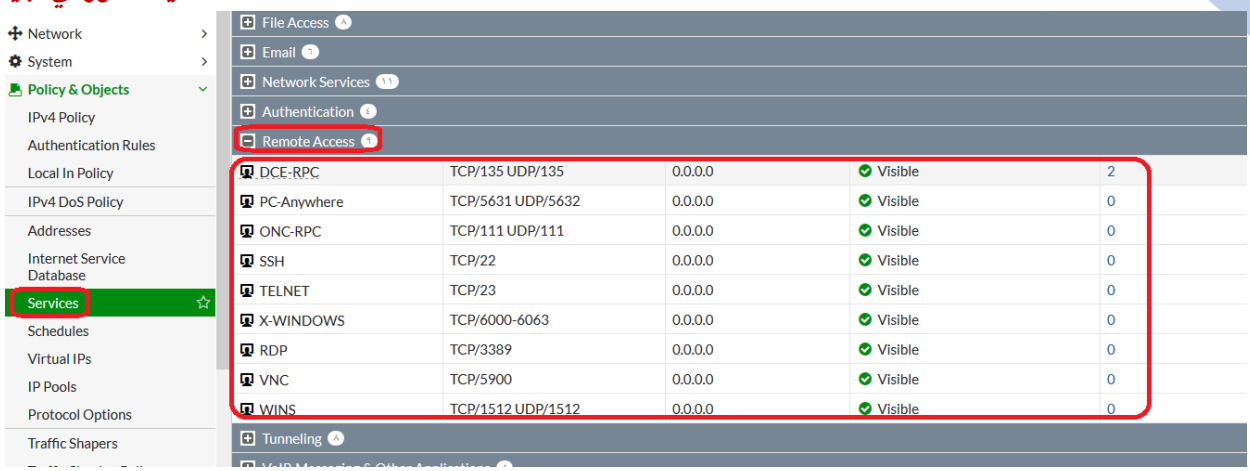
Accept or deny للترافيك

All معناها كل البورتات ..

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



حيث توضح التصنيف مثلا ويب اكسس او ايميلات اوريموت اكسس.. الخ وماهي البروتوكولات المدرجه تحته وكم ارقامها



الصوره أعلاه توضح التصنيف الخاص بالوصول عن بعد وماهي البروتوكولات وأرقام البورتات المتسخدمة في هذا التصنيف.

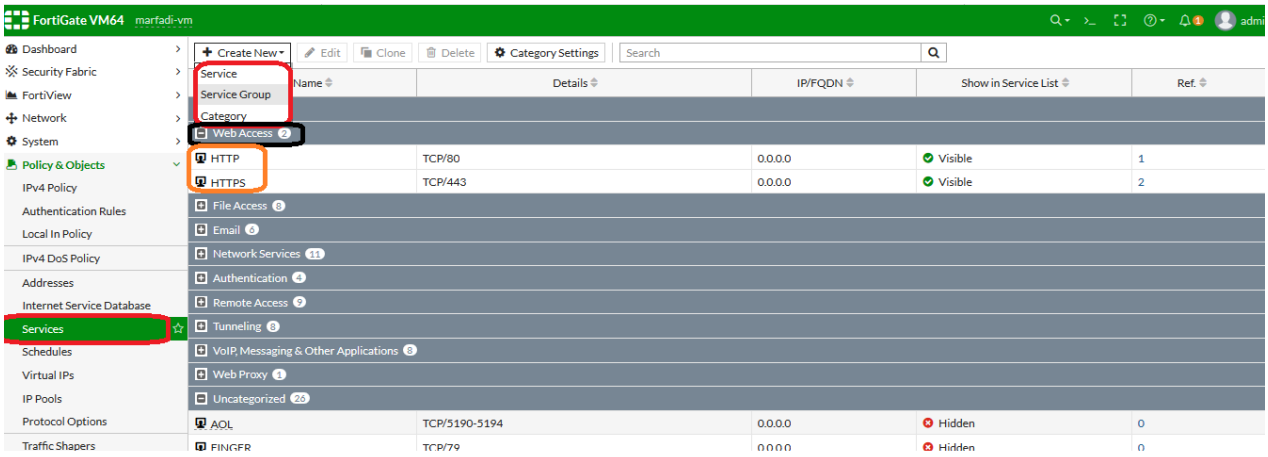
ماهي أنواع الـــservices ؟

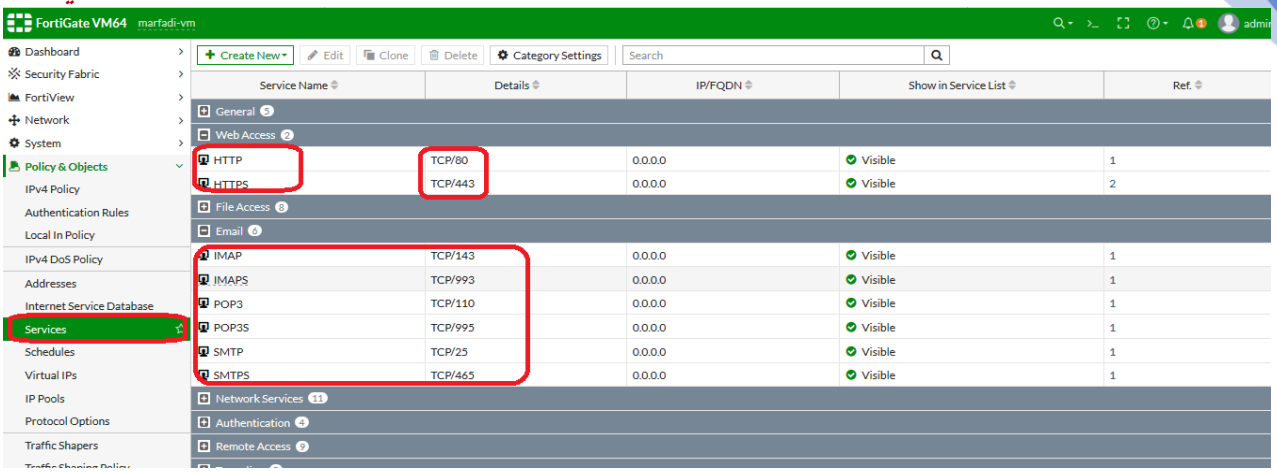
1- Services

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

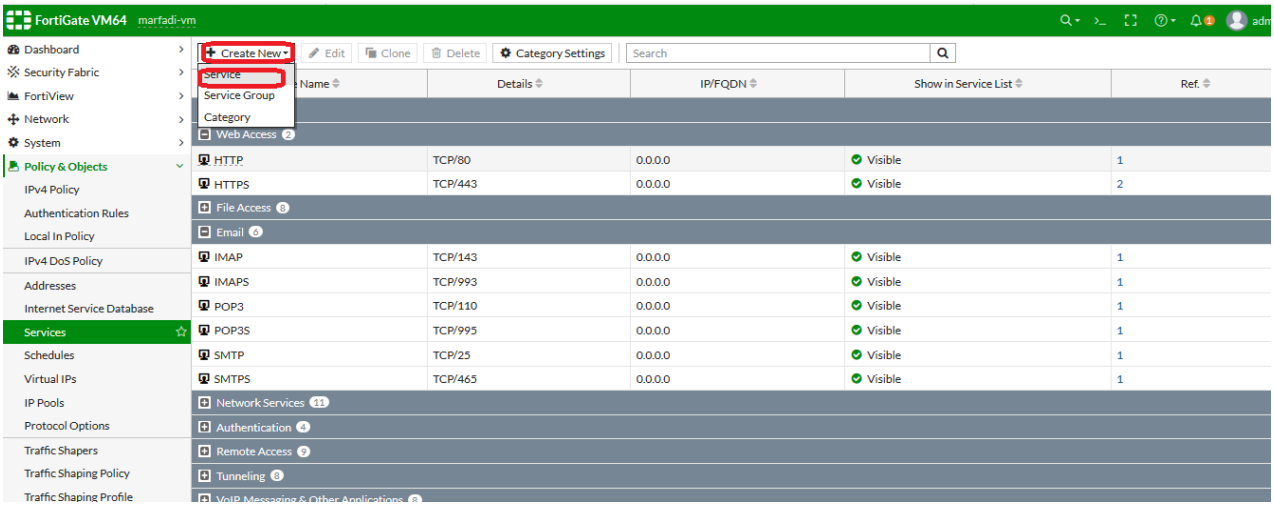
3- Category: مجموعة من الـ services تتشابه في نفس الخصائص مثل category خاصه بـ web access الخاصة بتصفح الانترنت حيث تحتوي على http و https او الخاصة باستقبال وارسال الايميل

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





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



Show in Service List لكي تظهر معك بالبوليسي .

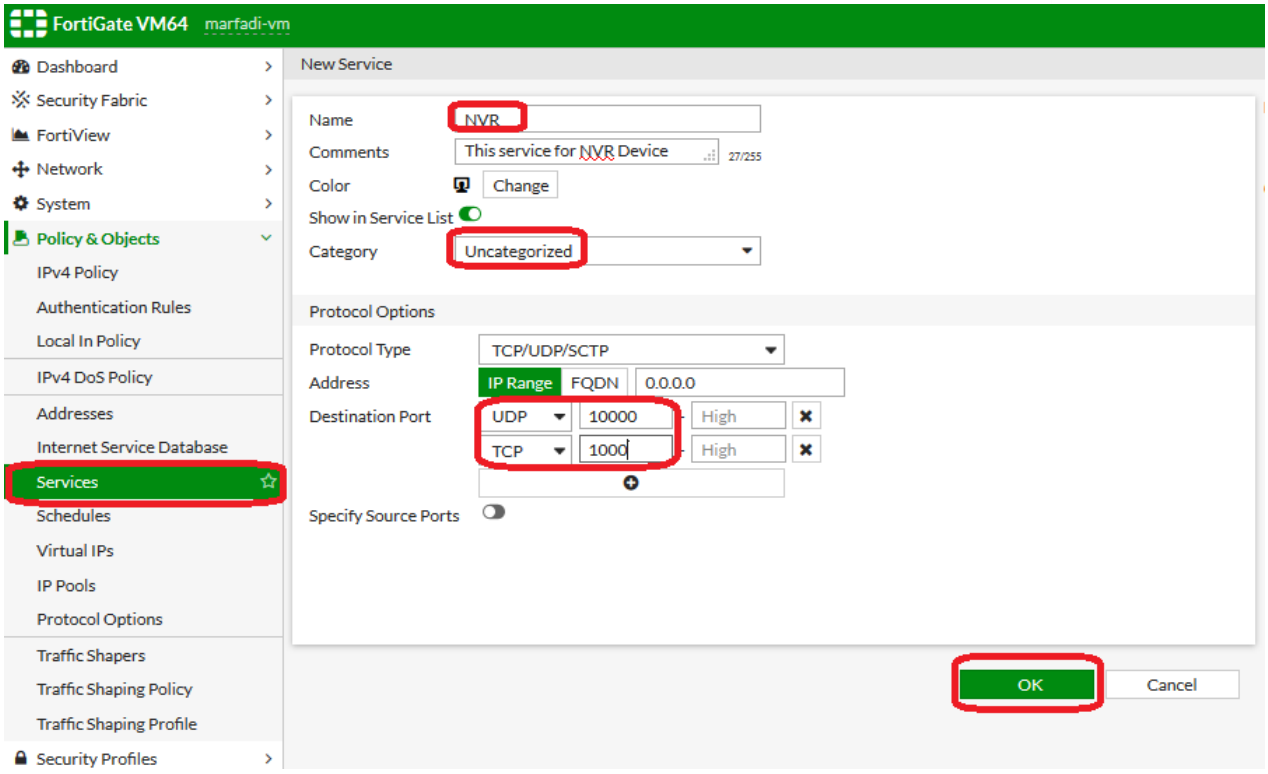
TCP : Protocol يكون اكثر موثوقية ولكن بطئ مقارنه بالبروتوكول **UDP** الذي يعتبر اقل موثوقية واكثر سرعه ..

البروتوكولات التي من نوع **TCP** هي **HTTP** و**HTTPS** ...الخ

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

حيث تختار نوع البروتوكول هل TCP او UDP حسب السيرفيس المستخدمة

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

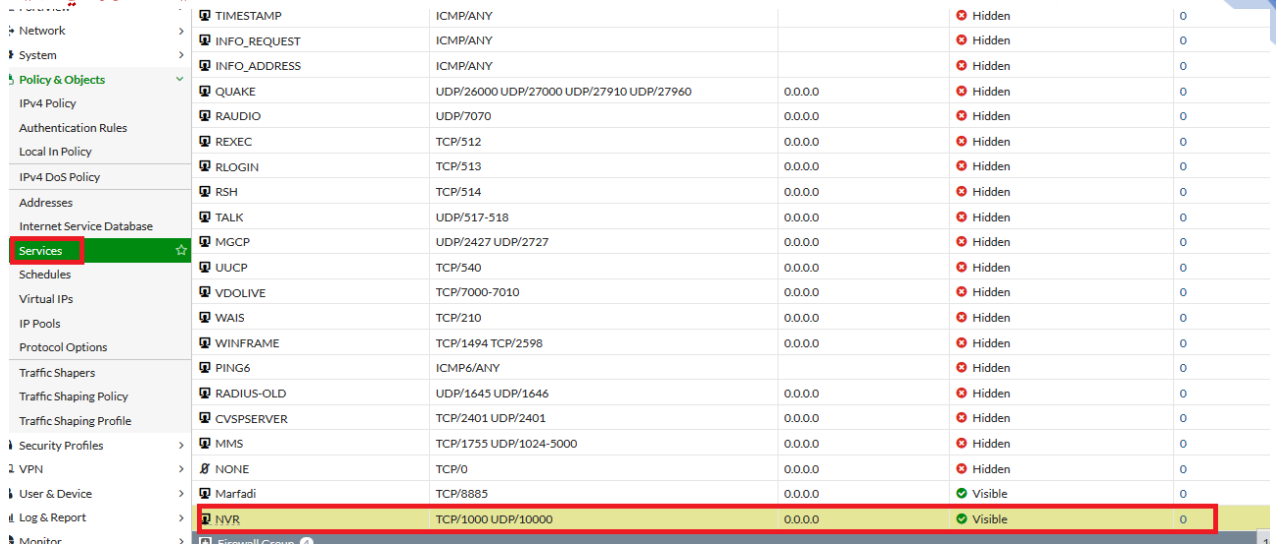


كما بالصورة أعلاه تم انشاء service باسم NVR وسوف تندرج تحت التصنيف Uncategorized ونوع البروتوكول سوف يكون UDP والبورت الافتراضي لأغلب اجهزه الـNVR تكون 10000 حيث اخترنا نوع البروتوكول UDP لأننا سوف ننقل بيانات من نوع streaming أي فيديو وصوت ..الخ

وايضا اجهزه الـNVR تستخدم الـip وهذا يحتاج الى البروتوكول TCP والبورت أيضا 10000 ..

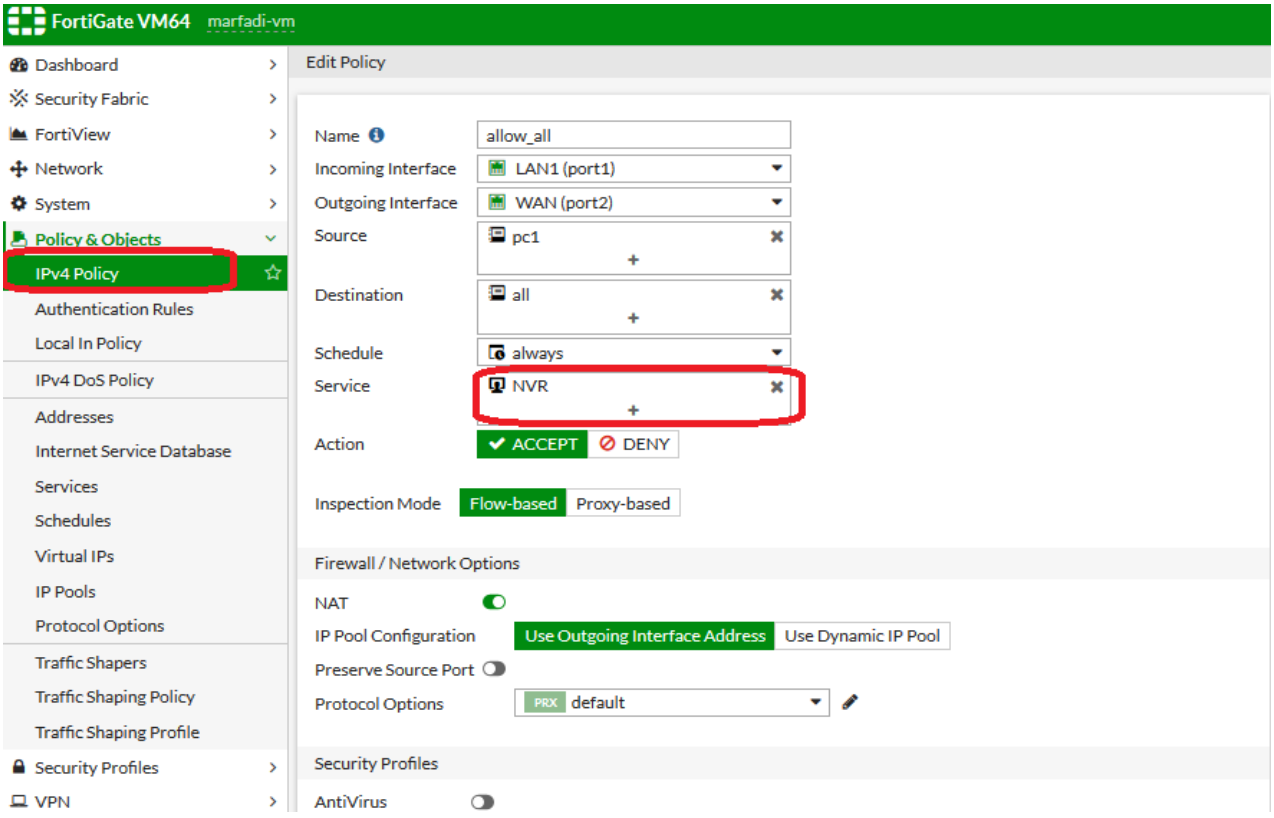
حيث قمنا بتحديد بأن الـnvr سوف يكون هدف(Destination Port) وليس مصدر أي اننا لو اردنا الوصول الى جهاز الـnvr سوف يكون على البورت 10000

اما لو اردنا ان نقوم بتحديد اكثرونريد ان نقوم بإخراج جهاز الـnvr من بورت معين فأننا سوف بتفعيل الخيار Specify Source Ports ..

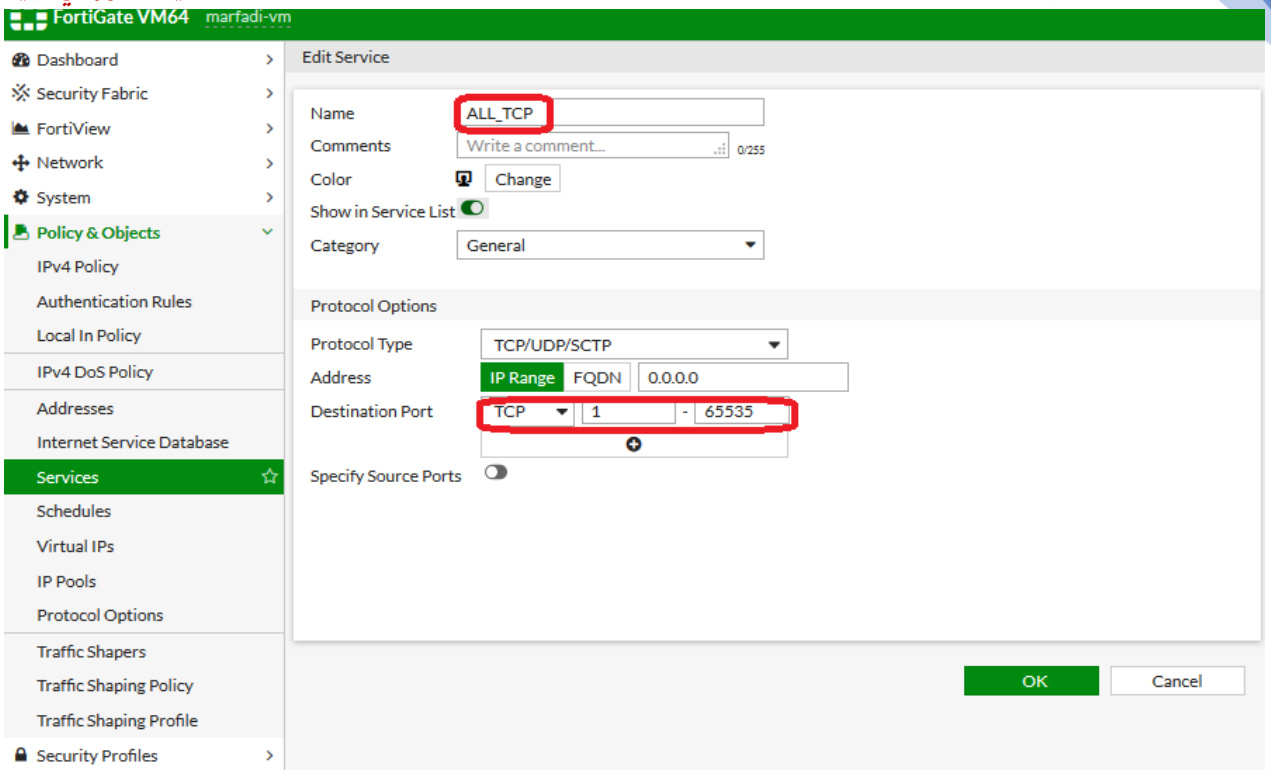


تمت الاضافة بنجاح للservice المسماة NVR ..

حيث يمكن استخدامها في البوليسي كما بالصورة ادناه

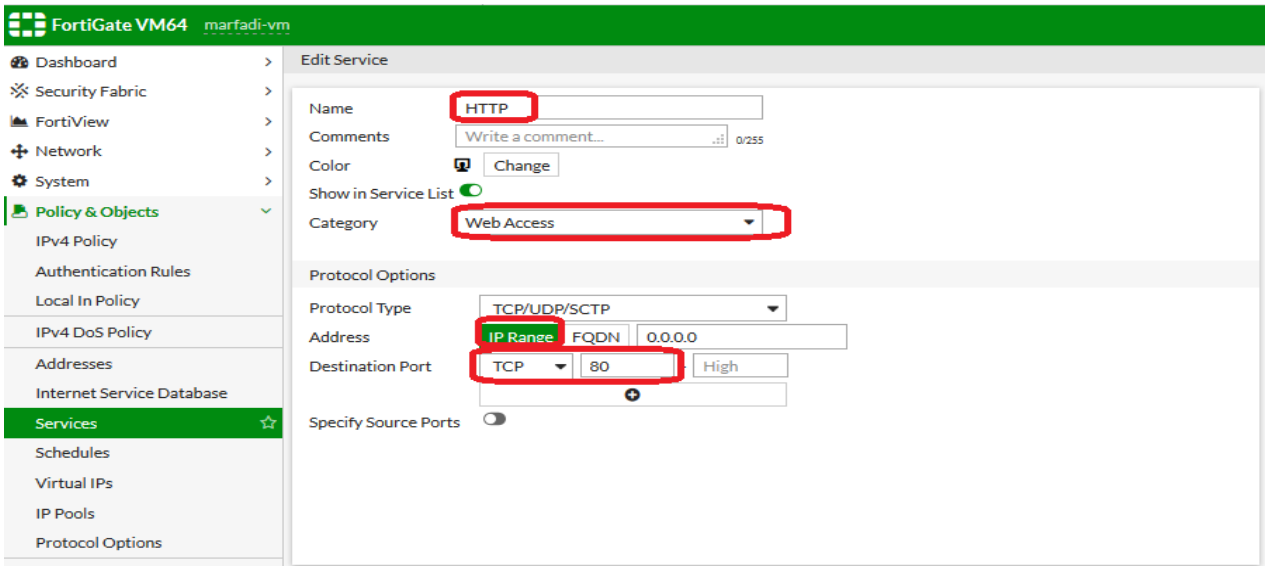


فمن الـ services الافتراضية التي منشاه أصلا هي all_tcp كما موضح بالصوره

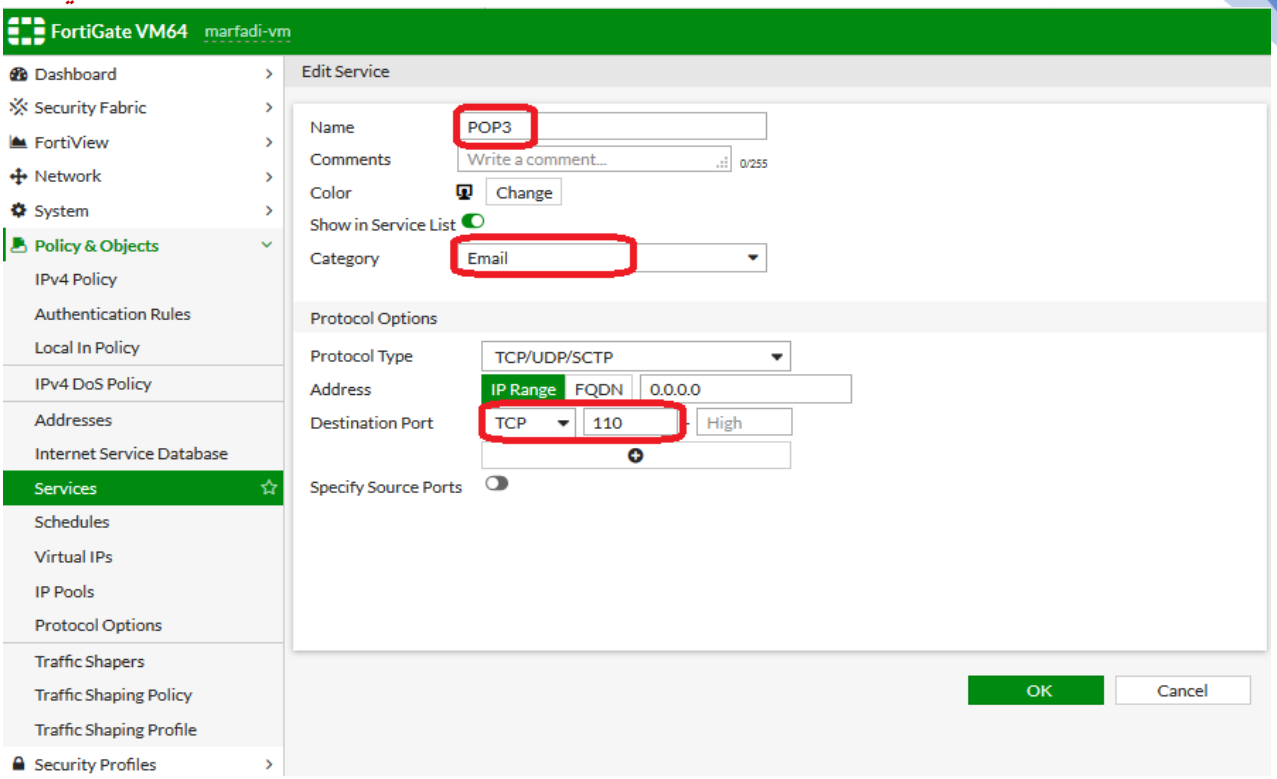


نوع الـTcp=Destination port البورت من 1-65535 .

وأيضا الـ service الخاصة بـ http كما بالصورة ادناه

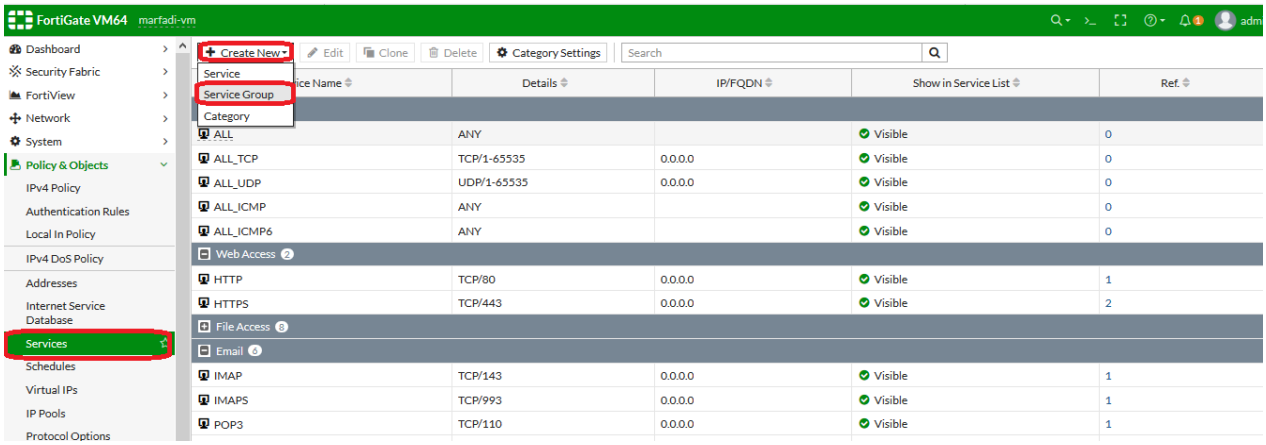


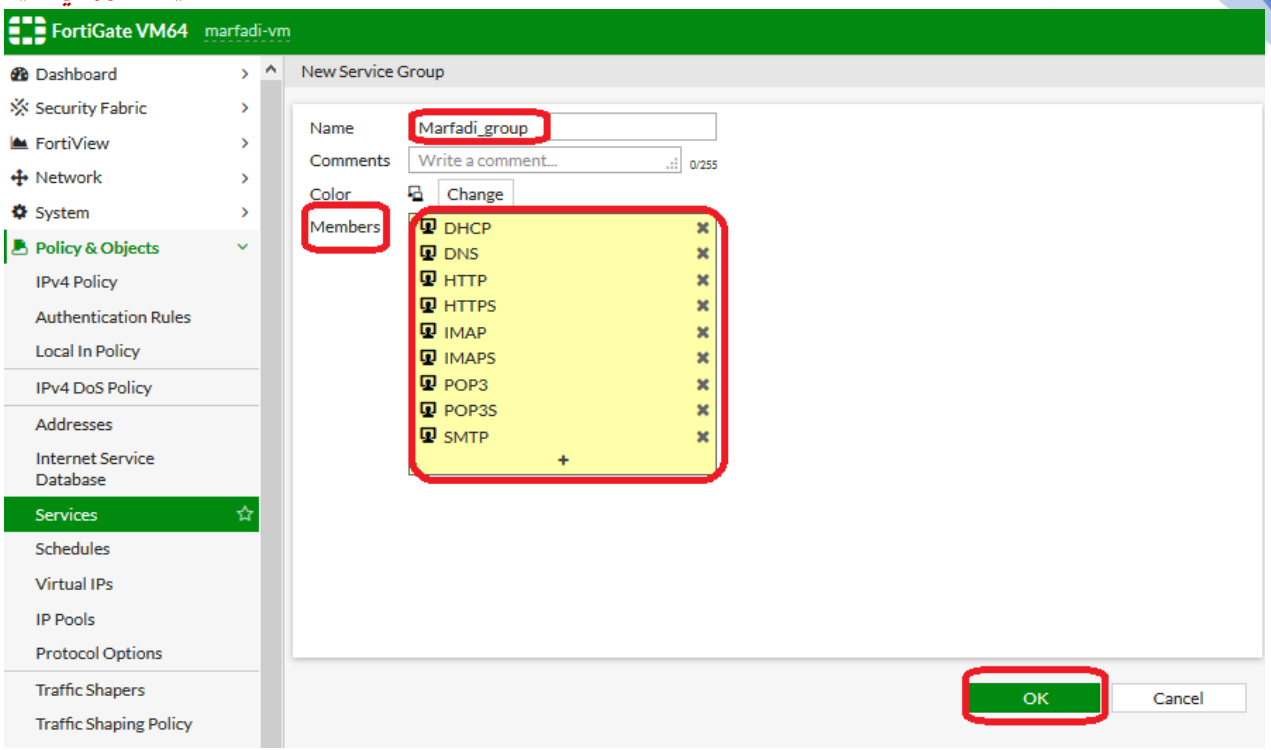
وأيضا لـ pop كما بالصورة ادناه ...



ما هو الـ service group :

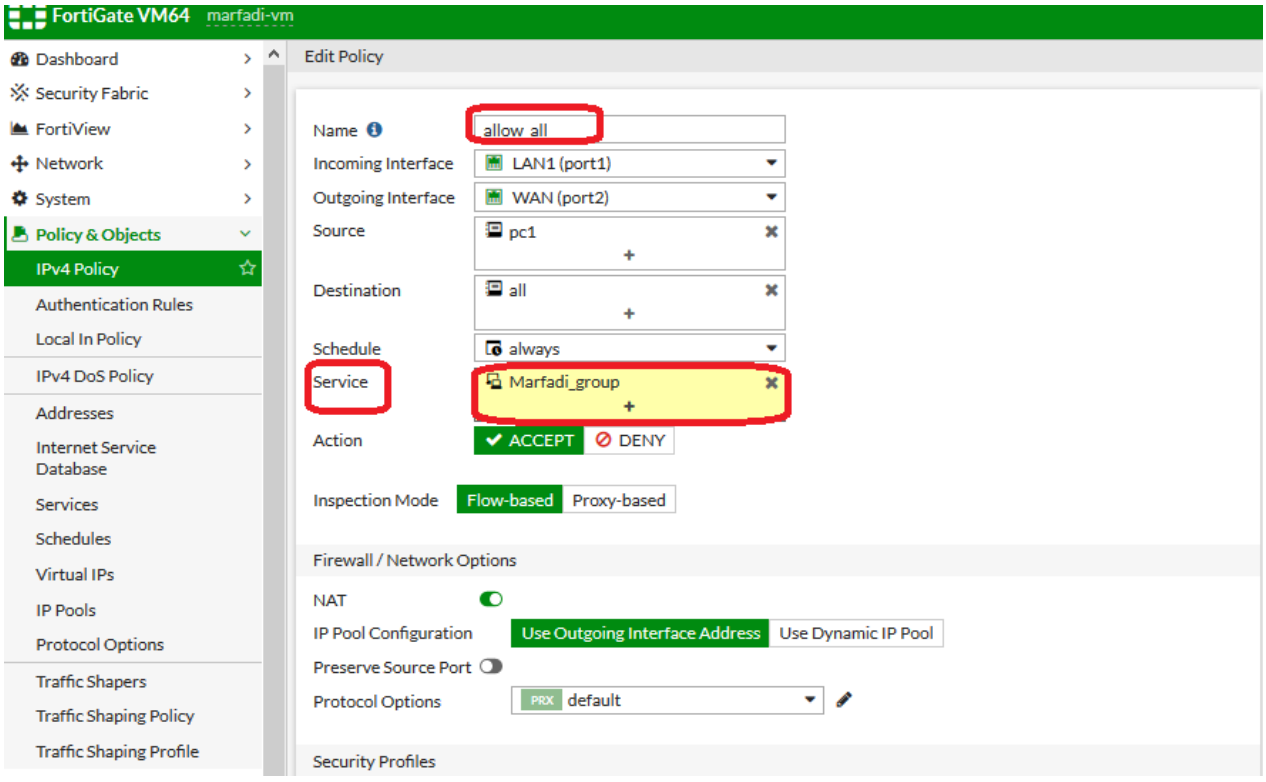
هي عمليه انشاء group تتكون من مجموعة من الـ service التي أنشأناها مسبقا .





وبهذا قمنا بإنشاء مجموعة اسمها Marfadi_group تحتوي على مجموعة من الـ service كما باالصوره أعلاه ..

فبهذا لو اردنا تطبيق البوليسي ونختار الـMarfadi_group التي انشاناها مؤخرا ..



Schedule:

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

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

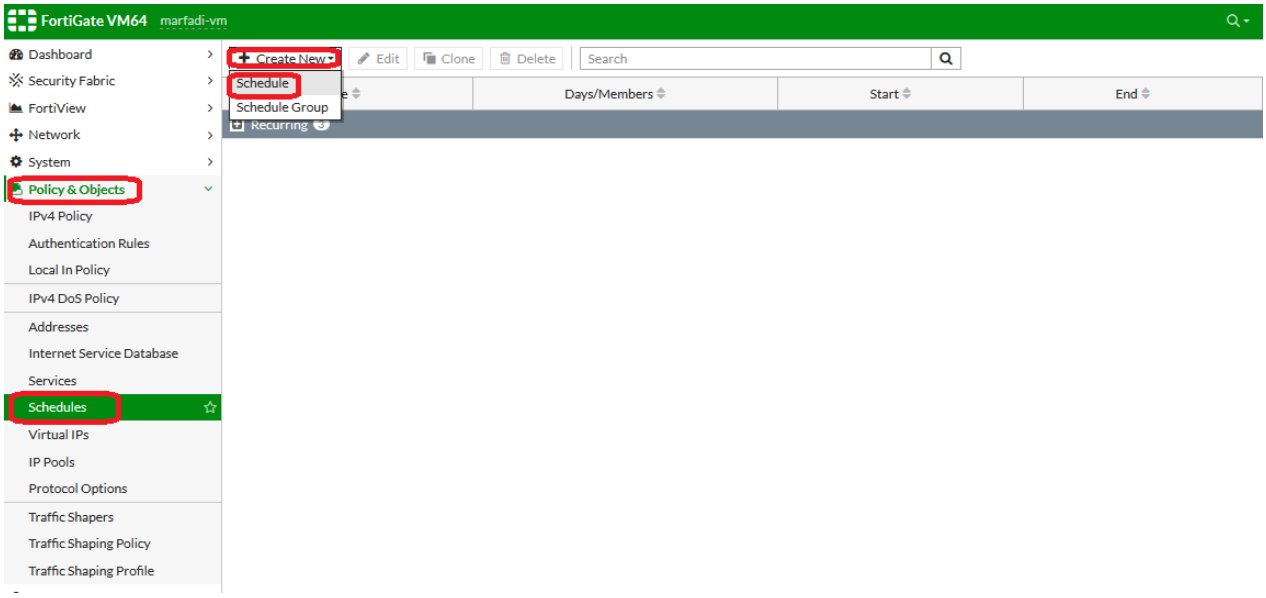
لأن بعض الأحيان اريد ان أقوم بتطبيق البوليسي في وقت معين او حدث معين .حيث لا يمكنك ان تنشى بوليسي بدون تحديد الـ schedule حيث القيمة الافتراضية له هي always يعني ان هذا البوليسي سوف تطبق بشكل دائم.

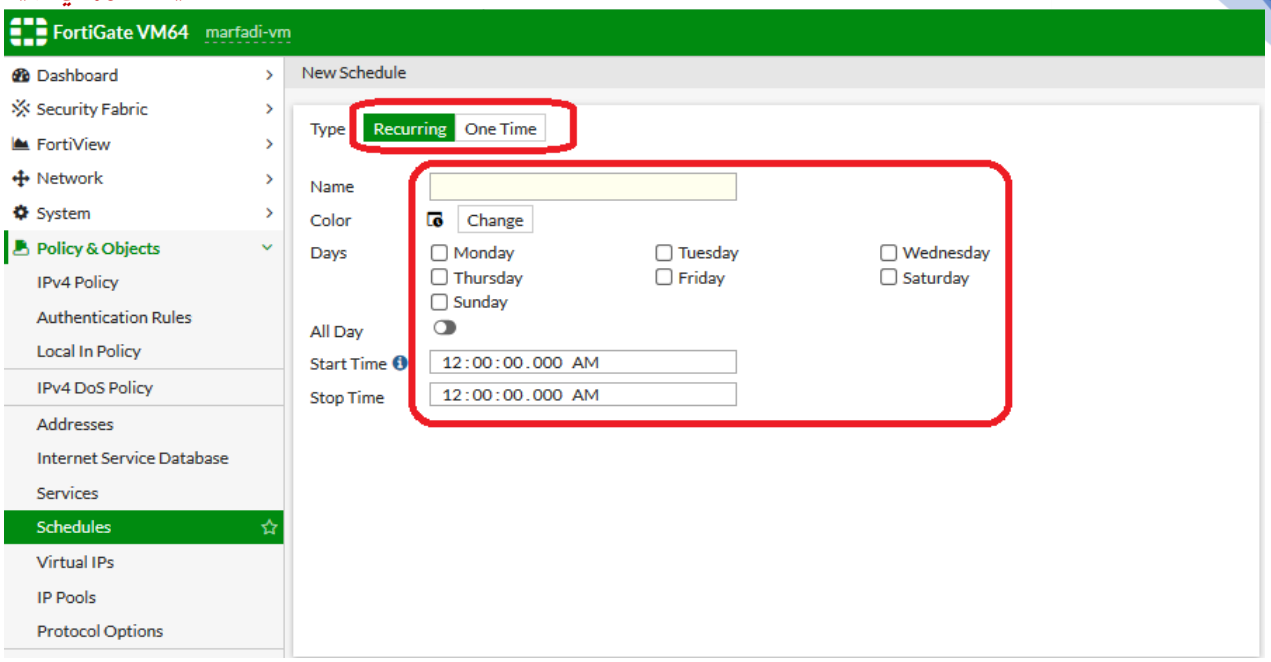
الـ schedule مقسم الى نوعين :

١- Recurring :بوليسي سوف تطبق بشكل متكرر مثلا اريد تطبيقها كل أسبوع اوكل يوم اوكل يوم معين او مرتين بالأسبوع ..الخ أي ان العملية متكرره .

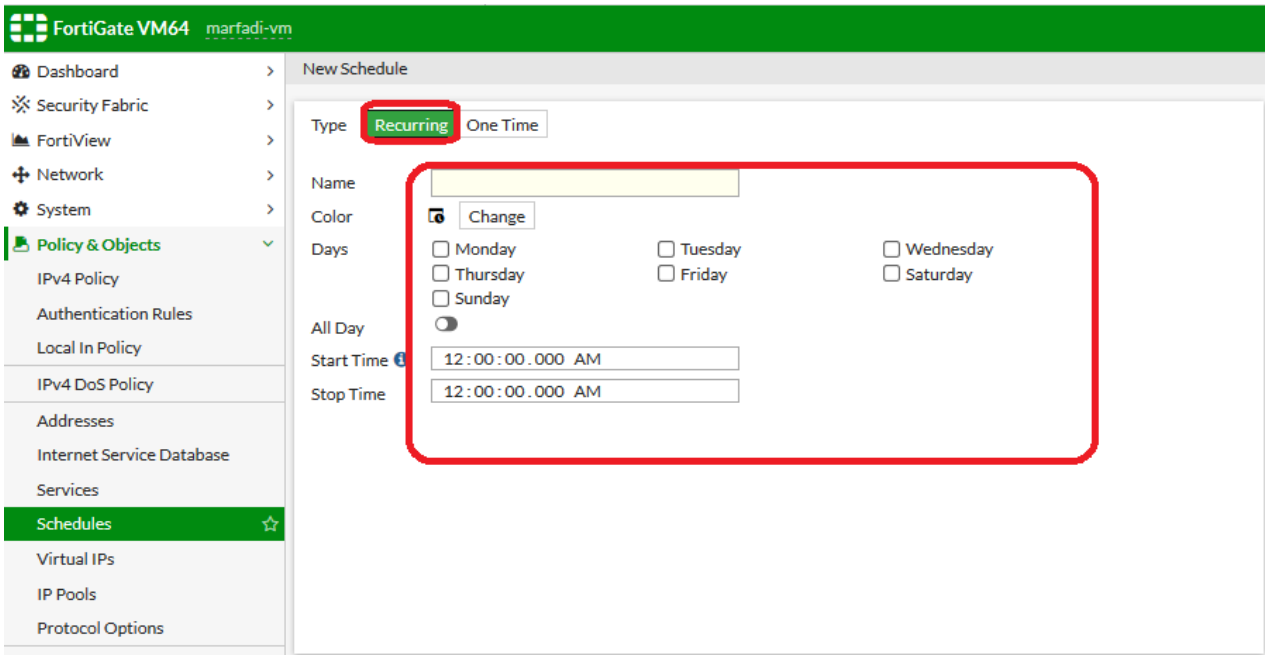
٢- One-time : بوليسي سوف تطبق مره واحده و في وقت محدد فقط .

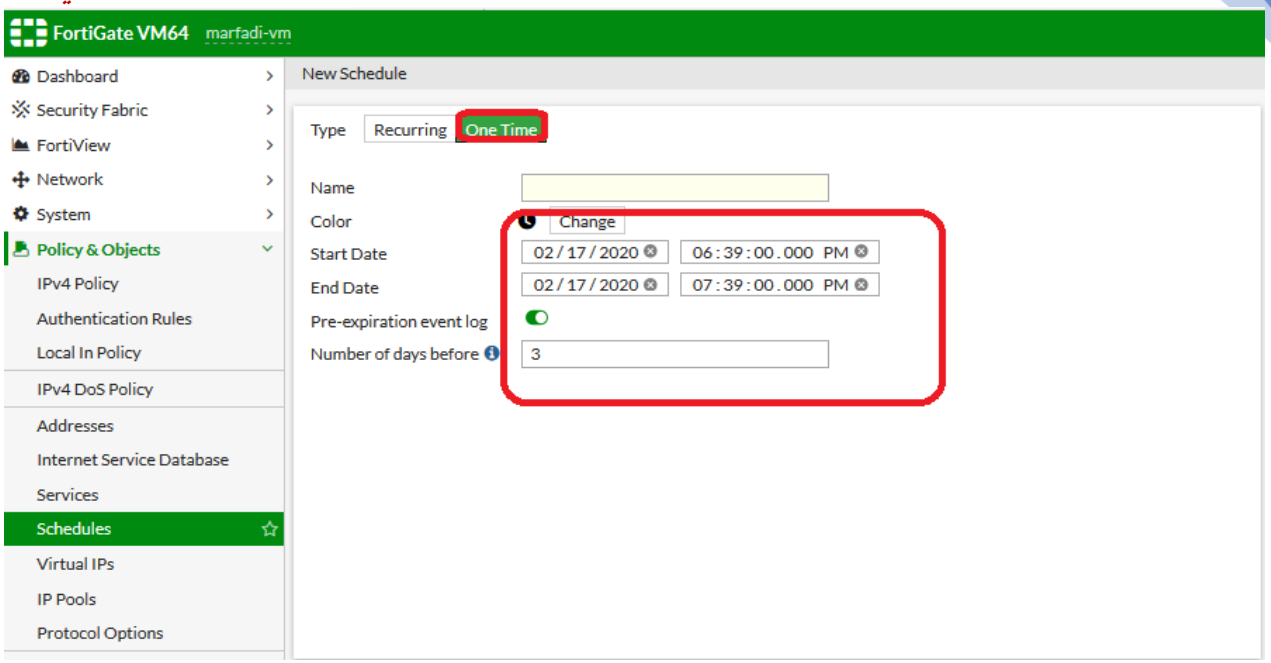
➢ طريقة انشاء schedule جديد :



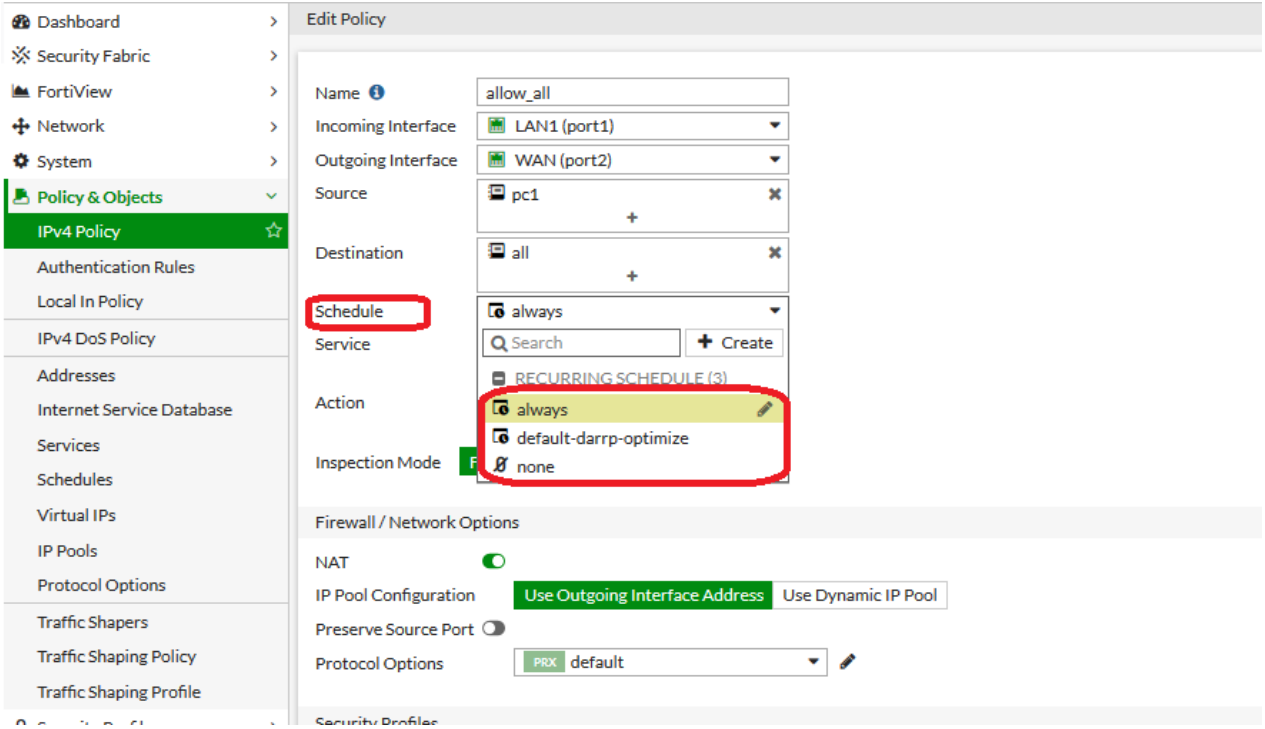


ثم نحدد النوع كما شرحناه سابقا ..



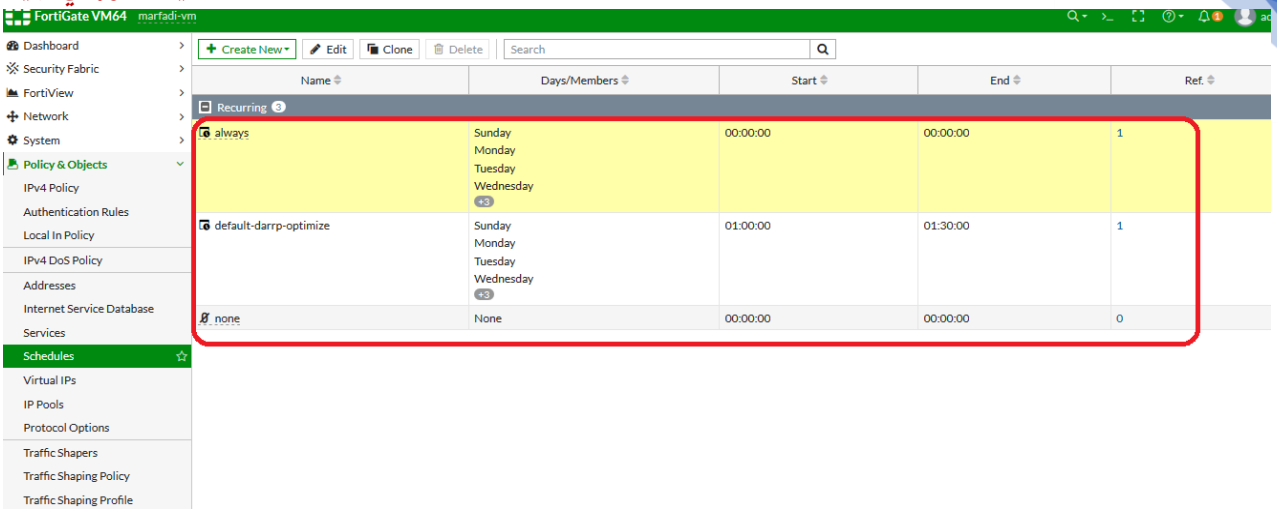


حيث نلاحظ بأنه يوجد لدينا 3 قيم افتراضيه من الـ schedule كما بالصورة ادناه



حيث الاختيار always معناها طبق البوليسي بشكل دائم .

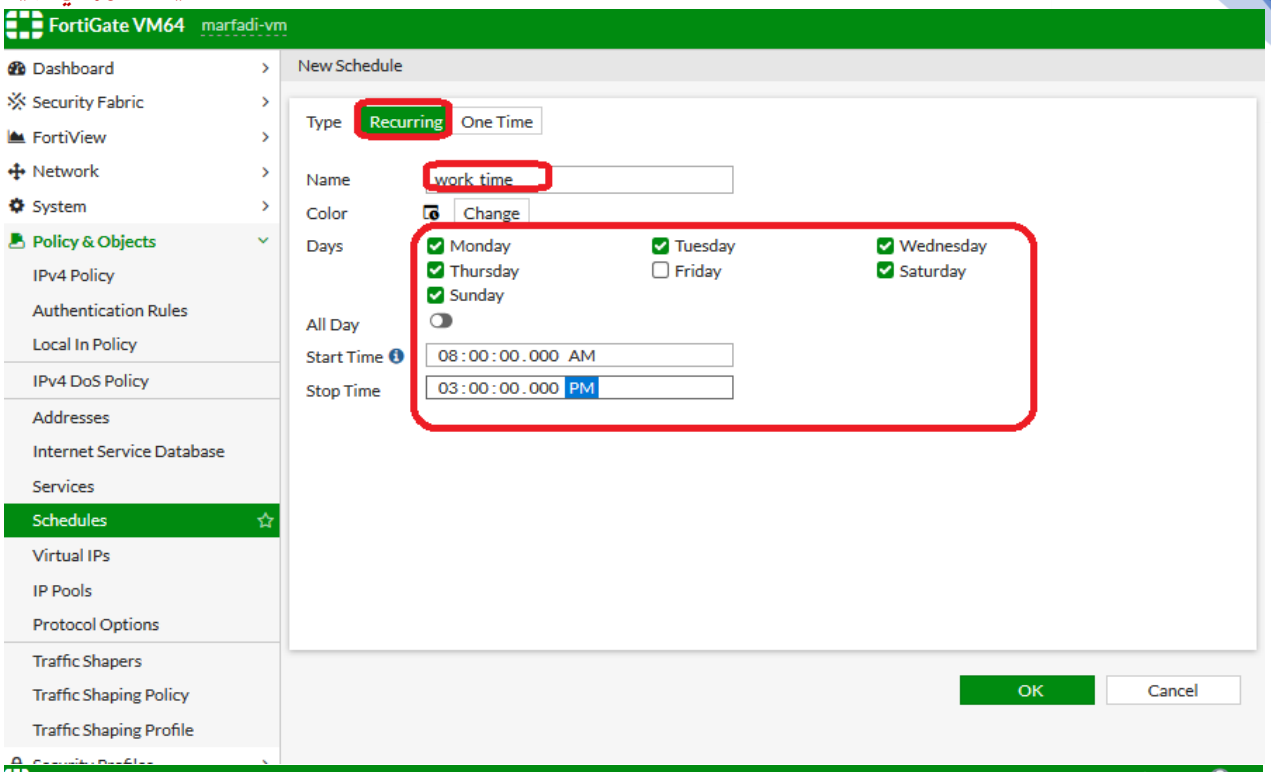
اما الخيار none وهذا معناها بان لا تقوم بتطبيق البوليسي وكأنك عملت في الـaction=deny أي لا احد سوف يتم تطبيق هذه البوليسي عليه ..

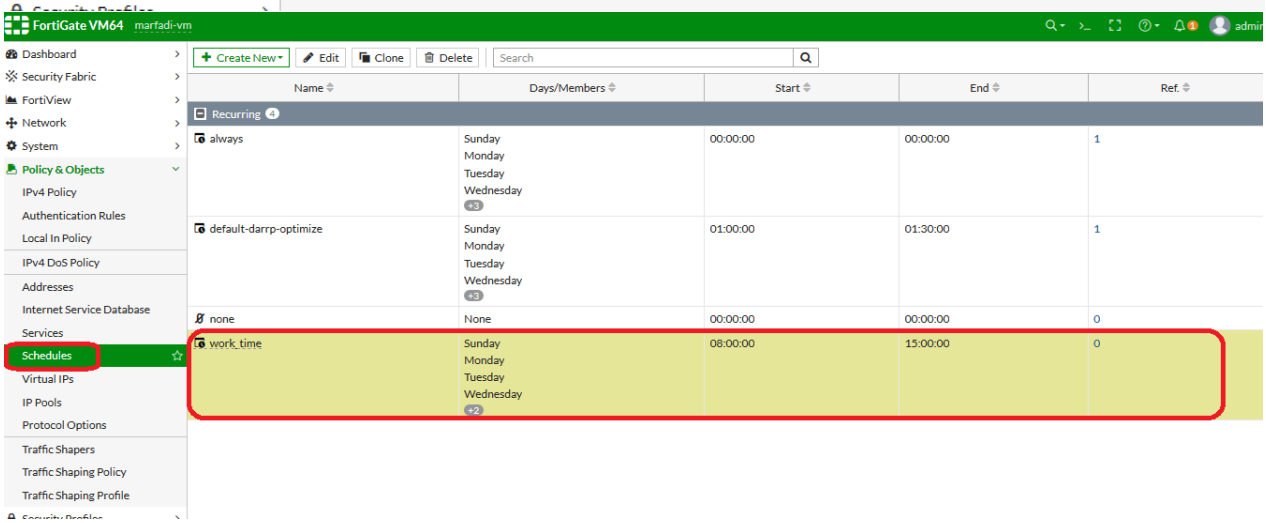


كما بالصورة أعلاه يوضح بأن الخيار always سيتم تطبيقه في كل الأيام وفي كل الأوقات من 00:00:00 الى 00:00:00

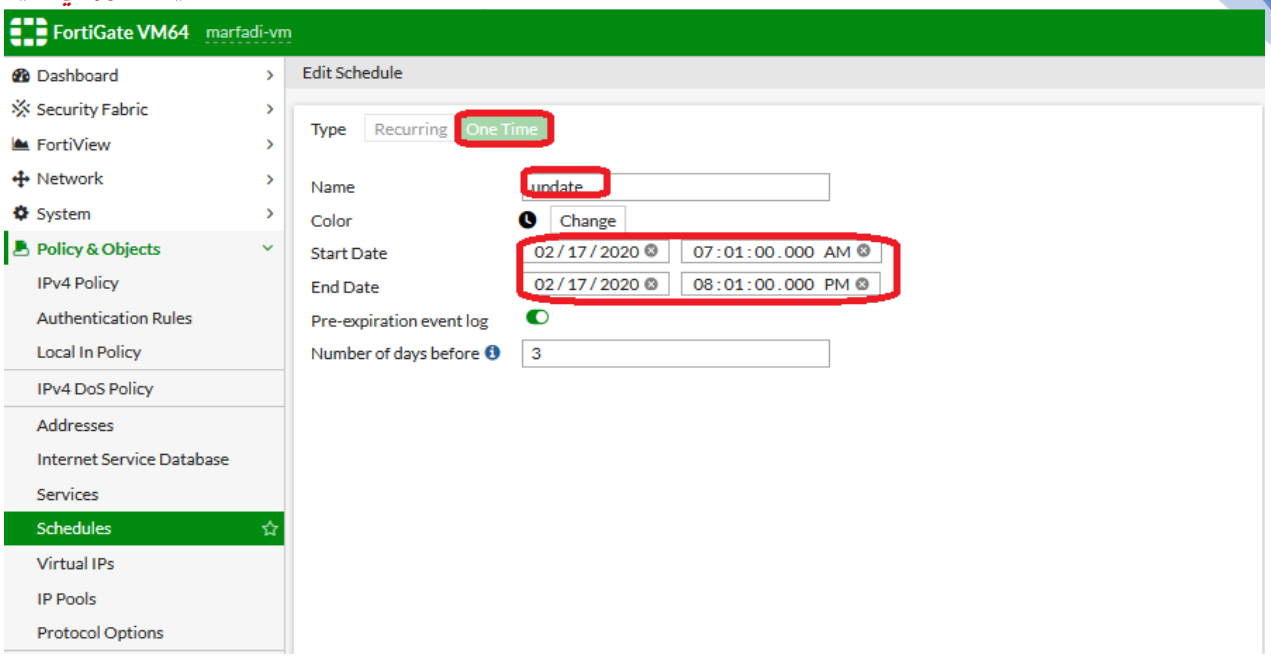
اما الخيار none فهذا يعني بأنه لن يتطبق بأي يوم ولا في أي وقت .

مثلا سوف أقوم بإنشاء schedule باسم work_time أي أوقات العمل بالشركة :



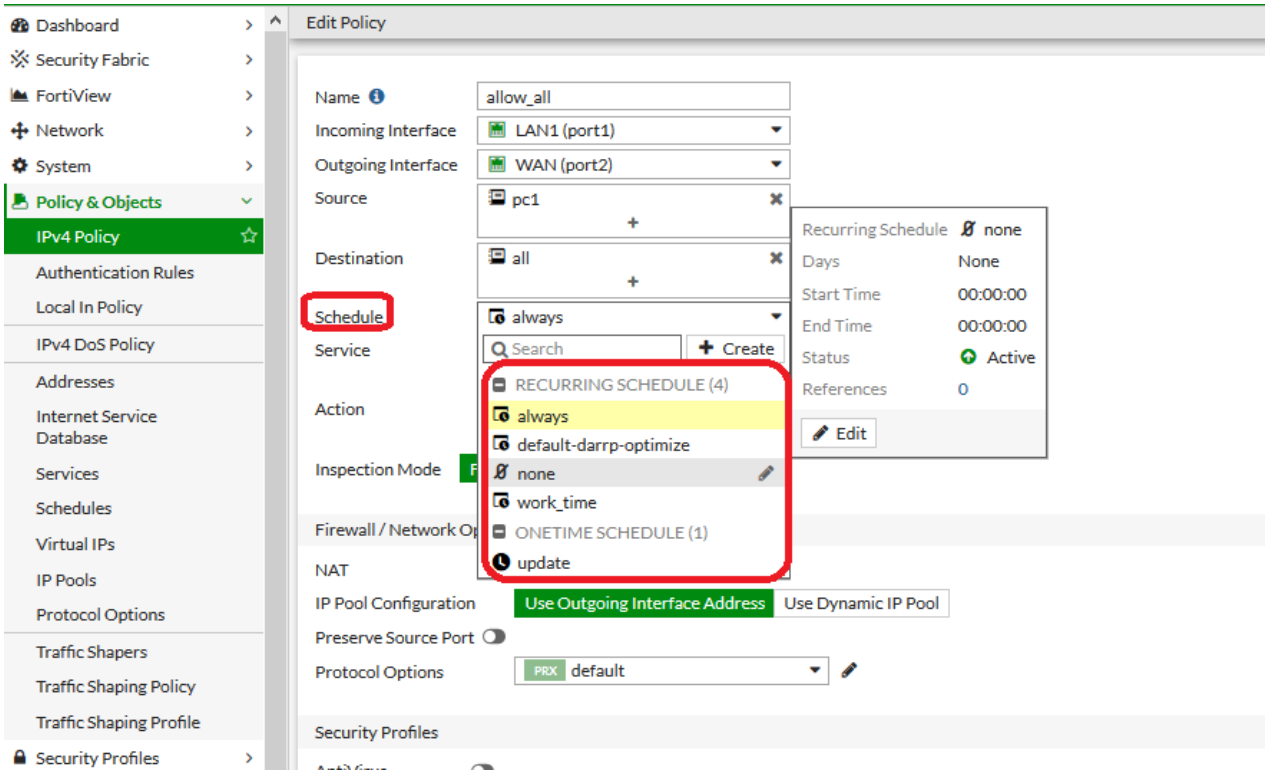


الان سوف نقوم بإنشاء schedule باسم update حيث لن تعمل الا مره واحده وبتاريخ معين ووقت معين



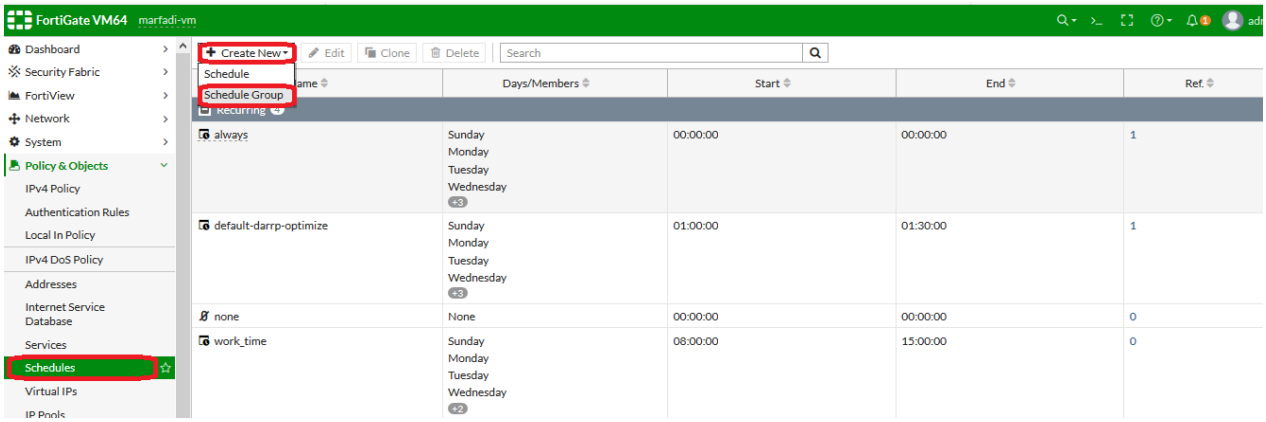
النوع One-time يستخدم في حالة كان لديك في الشركة اجتماع في تاريخ معين مره واحده ويحتاجوا يفتحوا مثلا موقع معين وليكن اليوتيوب فأننا سوف أنشئ هذه ال schedule واختارها في البوليسي حيث هذه البوليسي سوف يتم تطبيقها مره واحده وبيوم واحد فقط ولن تتكرر ..

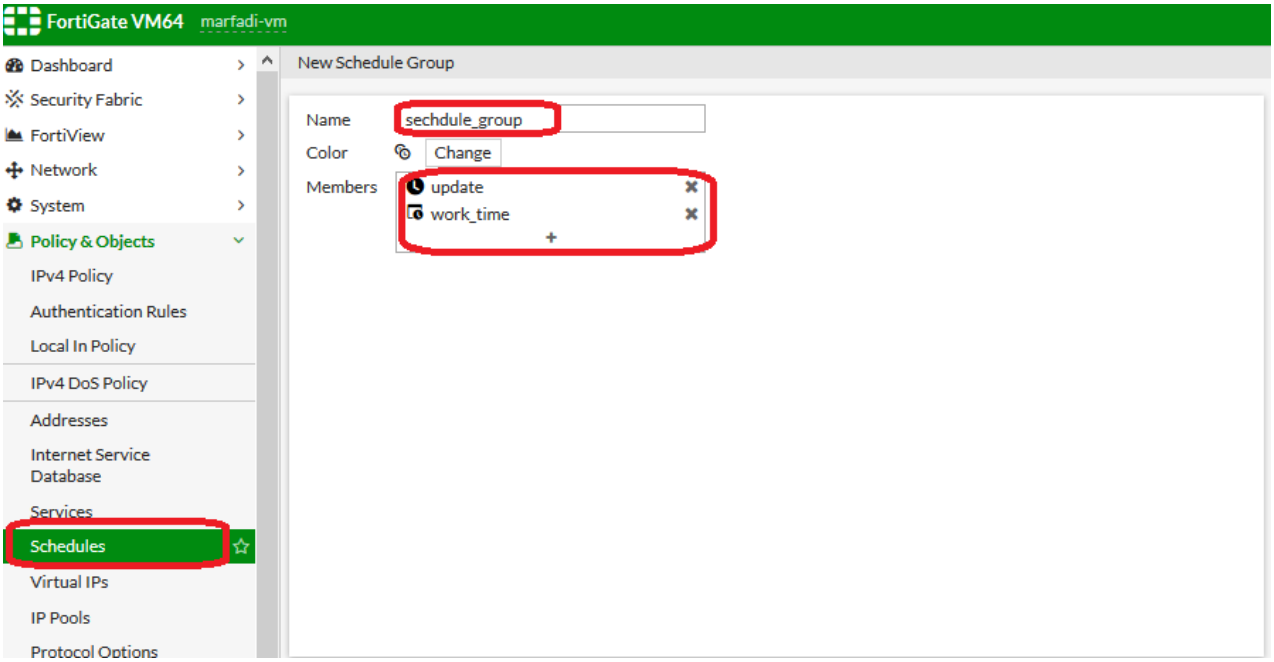
الان بعد انشاء الـ schedule سوف نختارها عند انشاء البوليسي ما نريده هل always,none,work_time,update :

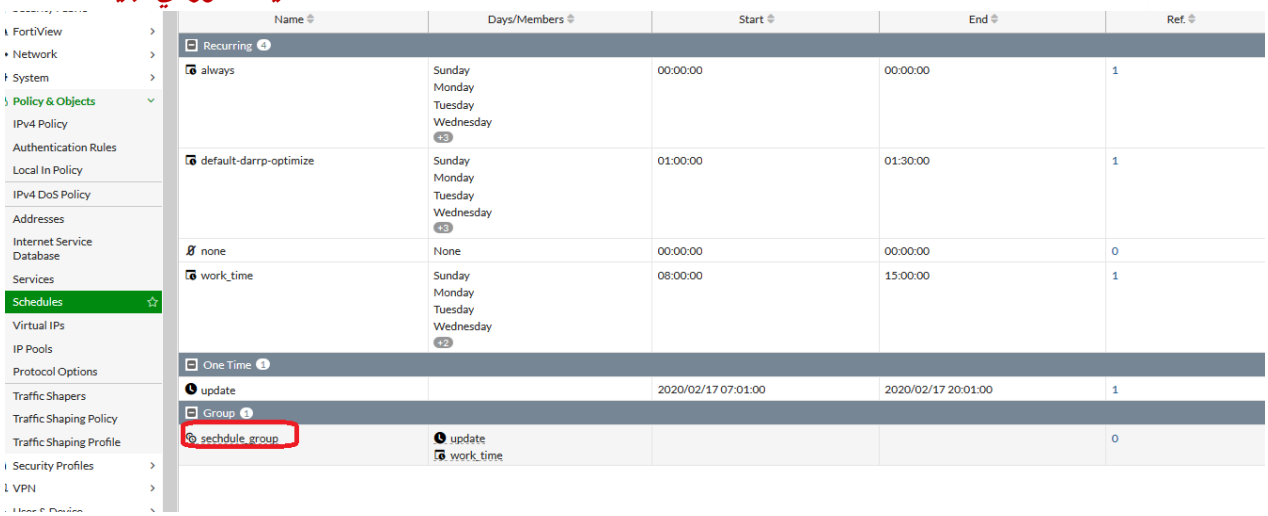


➢ طريقة انشاء schedule group :

يتم استخدامها لإنشاء مجموعة مكونه من اكثر من schedule بغض النظر عن نوعها هل one-time او recurring ..







➢ نفترض بأن لدينا شركه مواعيد العمل فيها من 8 ص الى 3 عصرا كل يوم ماعدا الجمعه ..

يعني نريد الانترنت على اجهزه الكلاينت يكون فيها متاح خلال دوام العمل فقط ..

اما في السيرفرات يكون الانترنت طوال الوقت .

الحل :

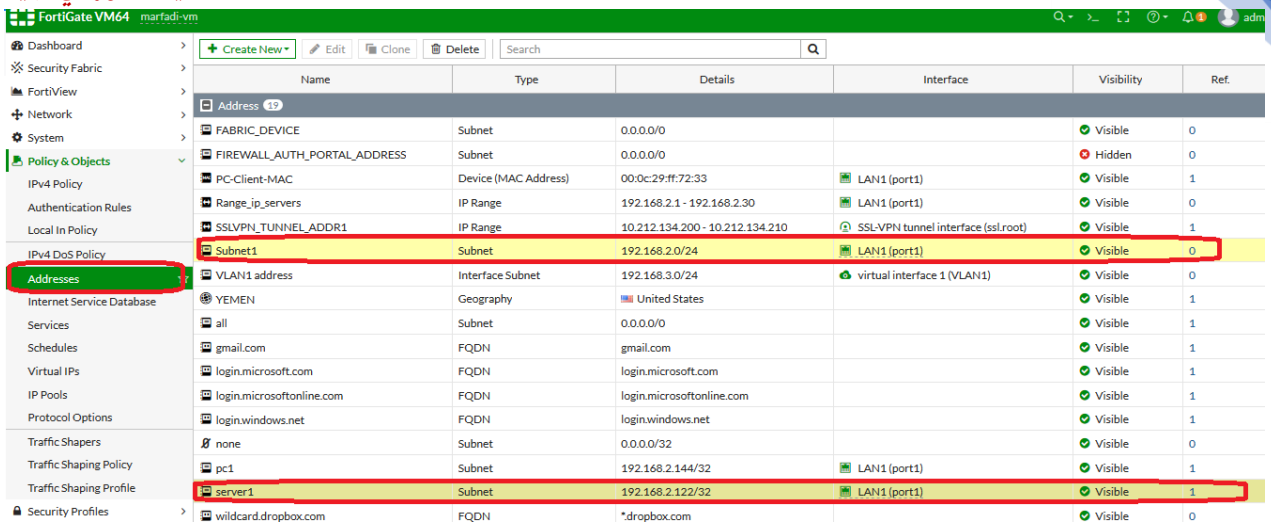
1 – انشاء عنوان باسم subnet1 تحتوي على رينج الشكبه الداخليه كامله (255.255.255.0/192.168.2.0)

2 – السيرفرات سوف نقوم بعمل ايبيهات استاتيك حيث سيتم انشاء عنوان باسم server1 بايبي 192.168.2.122 .

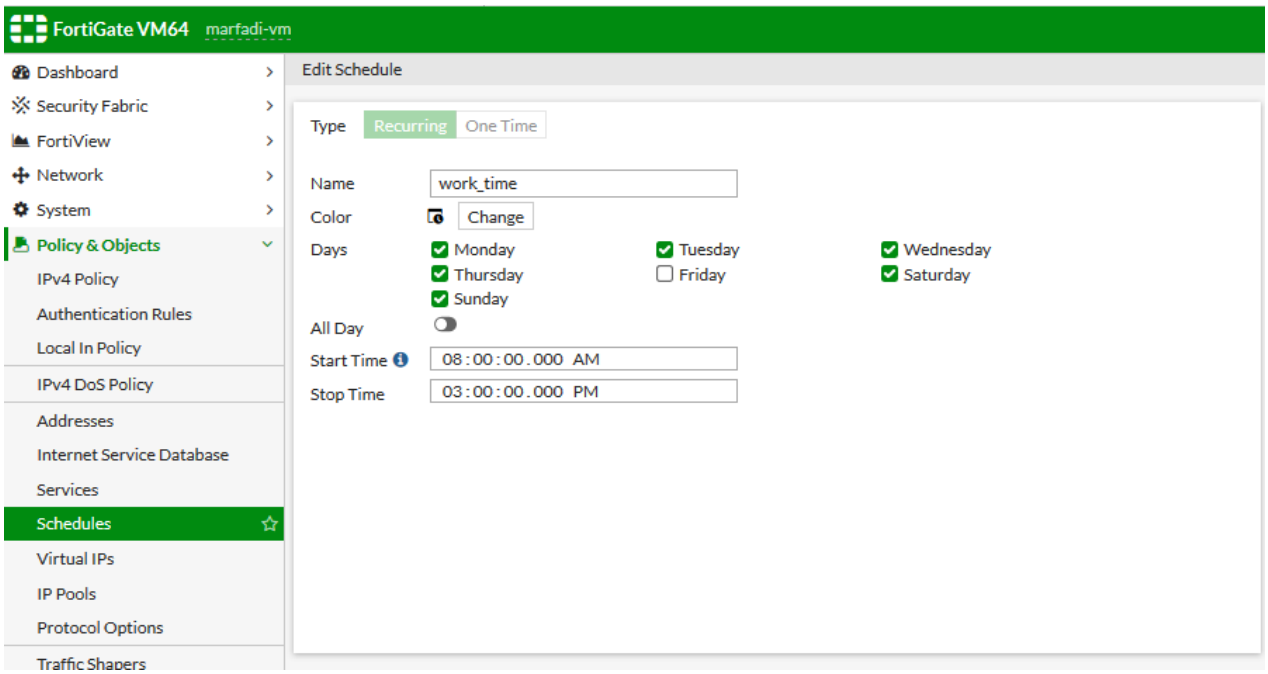
3 – انشاء schedule باسم work_time حيكون أوقات العمل .

4 – انشاء 2 بوليسي التي سوف تنفذ مانريده أعلاه ...

الحل :

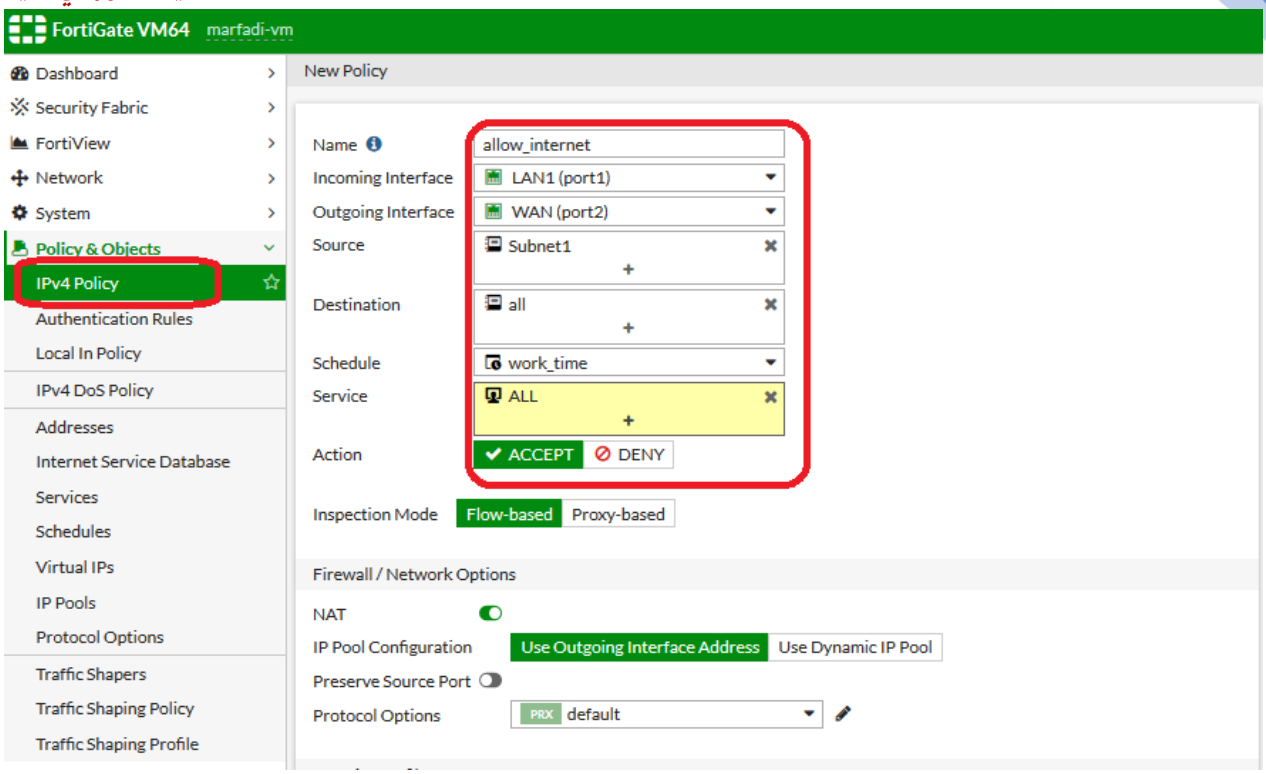


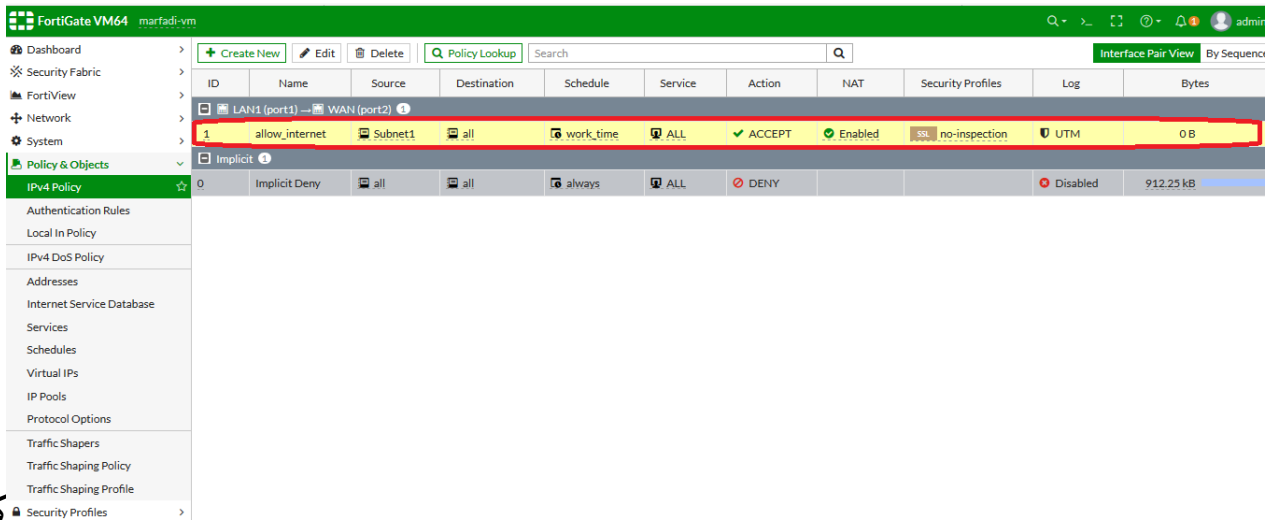
كما بالصورة أعلاه تم انشاء العناوين للكلاينت من الـsubnet1 وهي من الرينج (32/192.168.2.0)و أيضا للسيرفر تم تحديد العنوان server1 وتم تحديد الايبي 192.168.2.122 .



تم انشاء schedule باسم work_time مسموح فيها من 8 صباحا الى 3 عصرا لكل أيام الاسبوع ماعد الجمعه ..

الآن سوف نقوم بإنشاء البوليسي باسم allow_internet

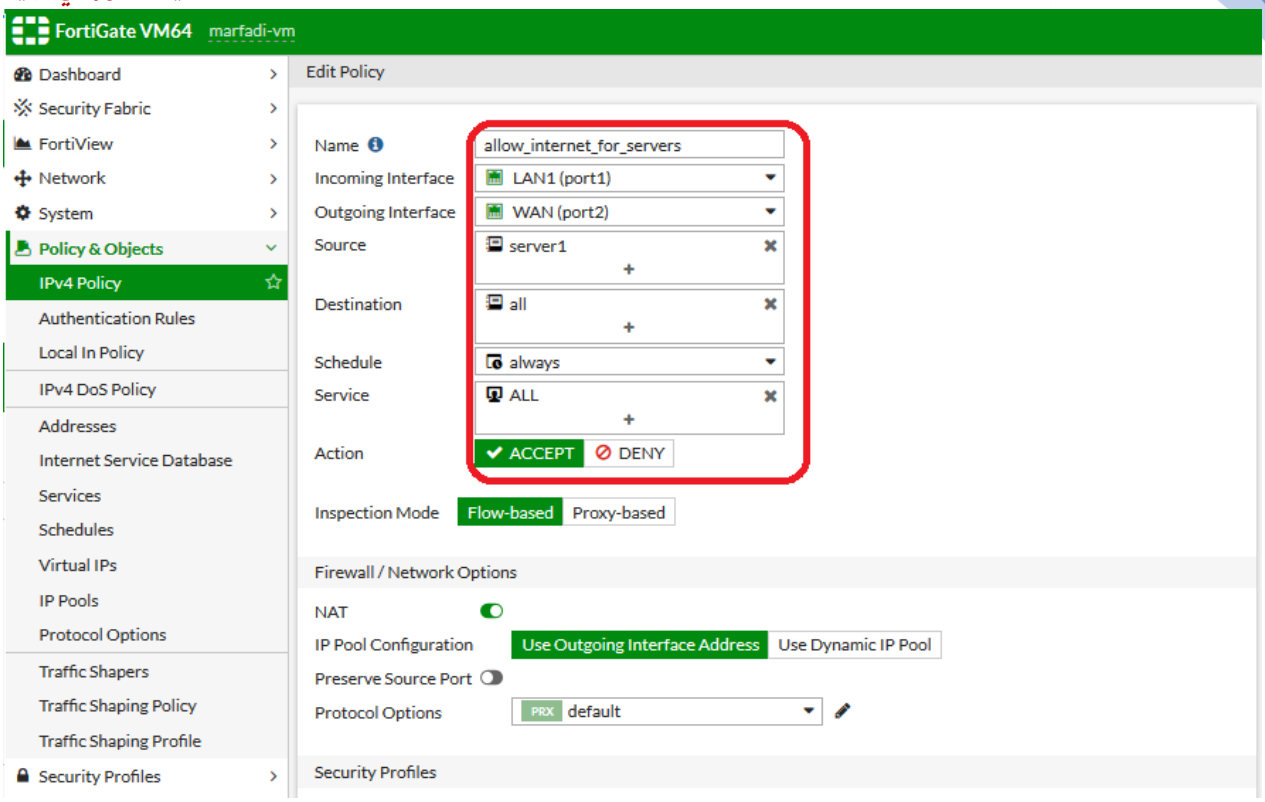




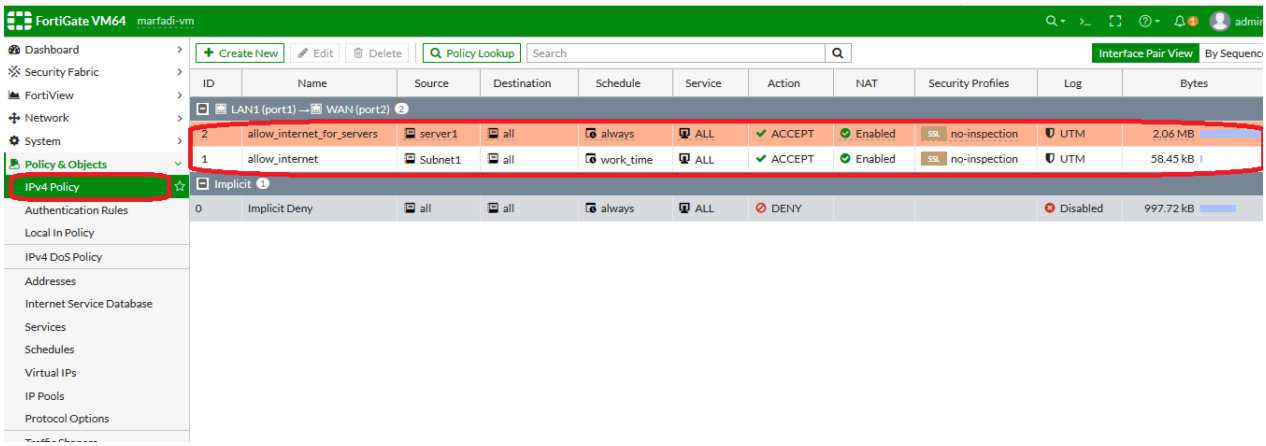
كما

بالصورة أعلاه توضح البوليسي allow_internet بانه 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 الـ schedule =always .



❖ Policy order

عباره عن ترتيب البوليسي ..

حيث أحيانا بيحصل تداخل في البوليسي(overlap) حيث بمجرد انشاء البوليسي فأن الفورتي جيت بيعطيها رقم يسمى policy id ..

حيث البوليسي يتم تطبيقها أولا بحسب الـ policy id (من فوق الى تحت).

حيث اول بوليسي يكون رقمها 1 ثم 2 ثم 3 ....الخ ولتفادي تداخل البوليسي يتم ترتيب البوليسي يدويا وذلك بسحب البوليسي الخاصة للأعلى ..الخ.

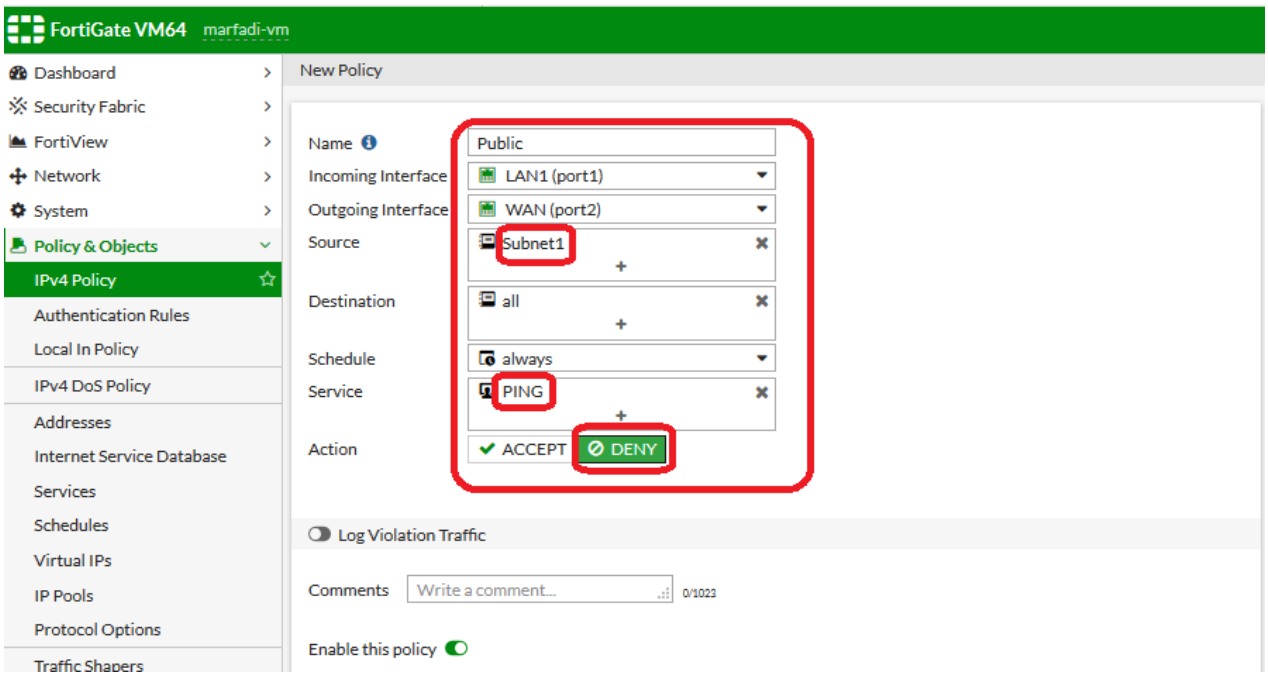
دائما تقوم بترتيب البوليسي بحيث تكون البوليسي الخاصة بالاعلى والبوليسي العامه تحت وهكذا ..

مثال :

سوف نقوم بإنشاء 2 بوليسي واحده خاصه(الأكثر تعقيدا) وواحده عامه

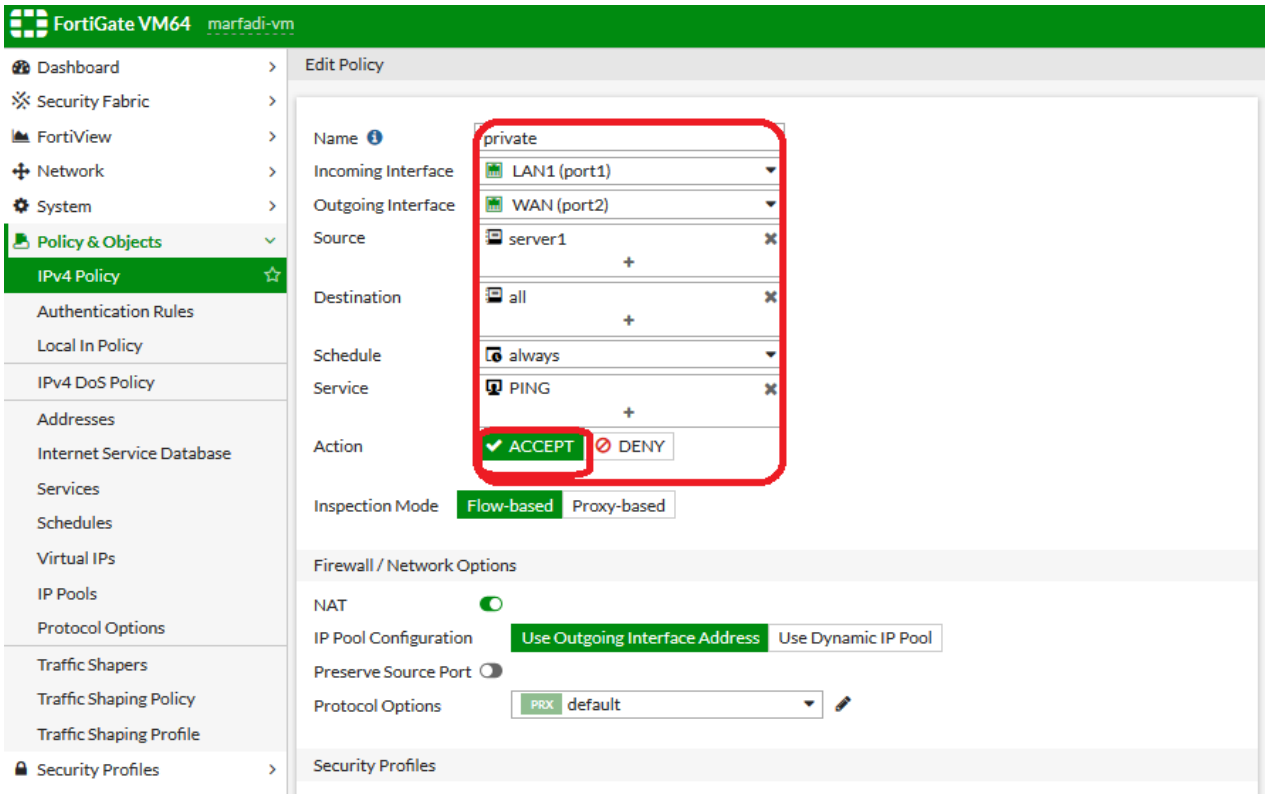
العامه :نمنع عمليه الـ ping لكل الـ subnet (الشبكة الداخليه)

الخاصة:اسمح لجهاز server1 ان يعمل الـping .

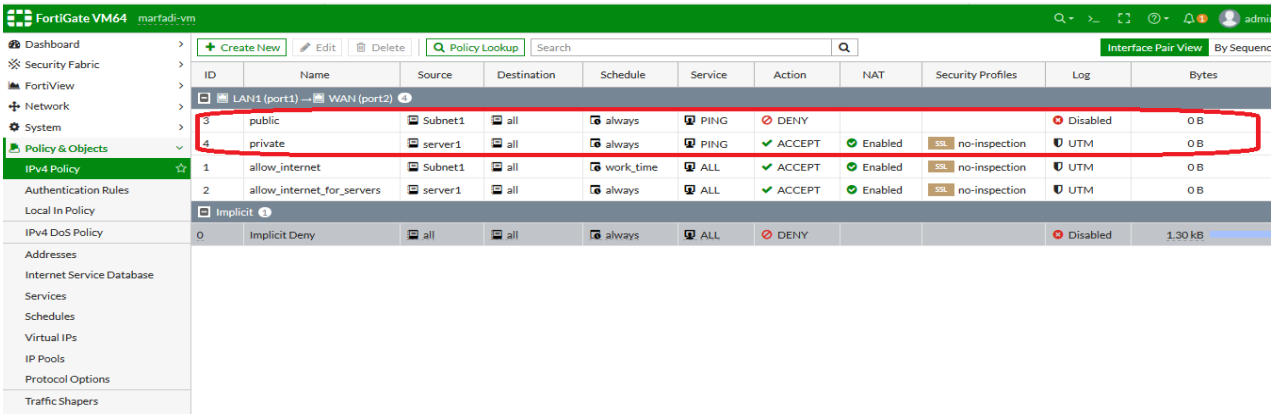


كما بالصورة أعلاه تم انشاء بوليسي عامه باسم public بتمنع الـping على كل الـsubnet1 .

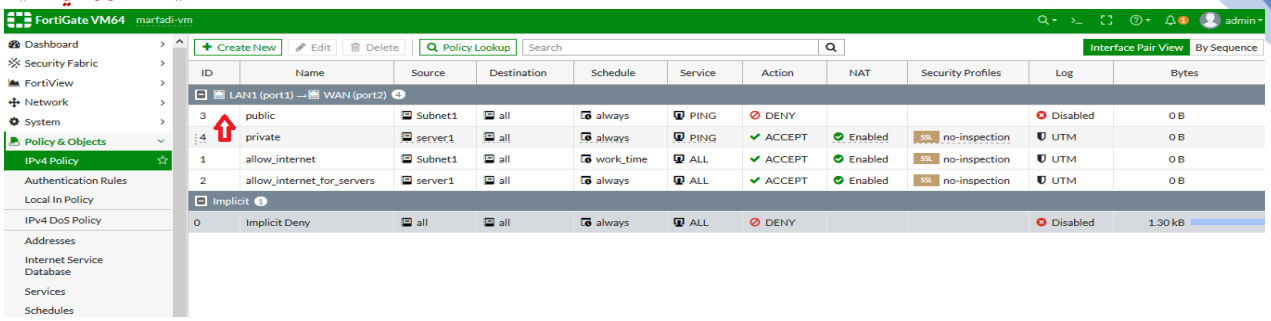
ثم سنقوم بإنشاء بوليسي خاصه باسم private حيث نسمح للجهاز server1 بأن يعمل ping ..



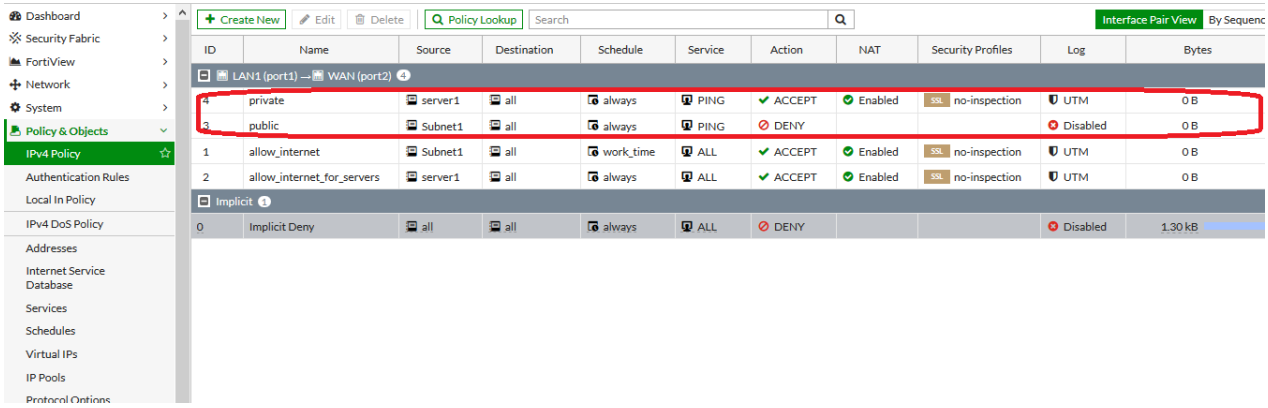
ثم نلاحظ كيف اصبح ترتيب البوليسي ..



الان أي جهاز من الشبكة الداخليه(192.168.2.0/32(subnet1 سوف يحاول يعمل ping لأي موقع مثلا 8.8.8.8 –t ping فانه لن يستطيع حتى وان كان الجهاز هو server1 وذلك لأن ترتيب البوليسي بيطبق من اعلى الى اسفل..لكننا لو قمنا بإعادةترتيب البوليسي وذلك بالسحب والافلات كما بالصورة ادناه



وتصبح البوليسي بهذا الترتيب :



بحيث تصبح البوليسي الأكثر(تعقيدا)(الخاصة)هي التي في الأعلى والبوليسي العامه في الأسفل ..

حيث الآن الجهاز server1 لو حاول يعمل ping 8.8.8.8 –t سوف تنجح العملية ..

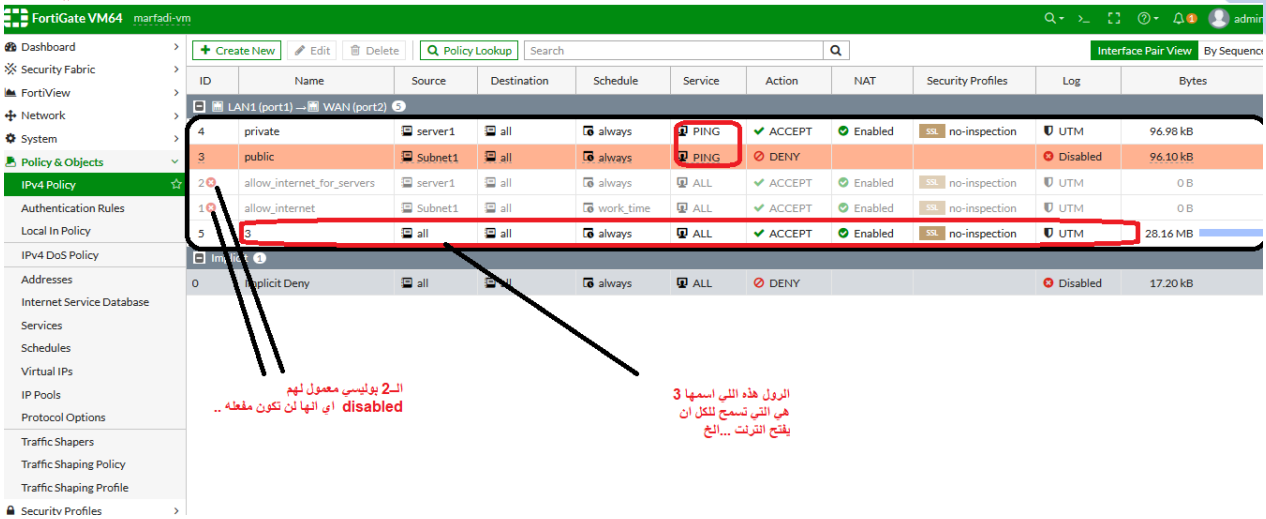
اما باقي الاجهزه في الـsubnet1 سوف لن يقدروا ..

مثال اخر :

لو قمنا 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 ابدا لأن البوليسي المسماة public تمنع أي سيرفيس (all).



نلاحظ اول رول (بوليسي) اسمها private وبتقول بأن الجهاز اللي 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 فأنك سيتمكن من فتحه بالرغم من اني حددت فقط بأن ping هو اللي مسموح !!

الجواب هو:

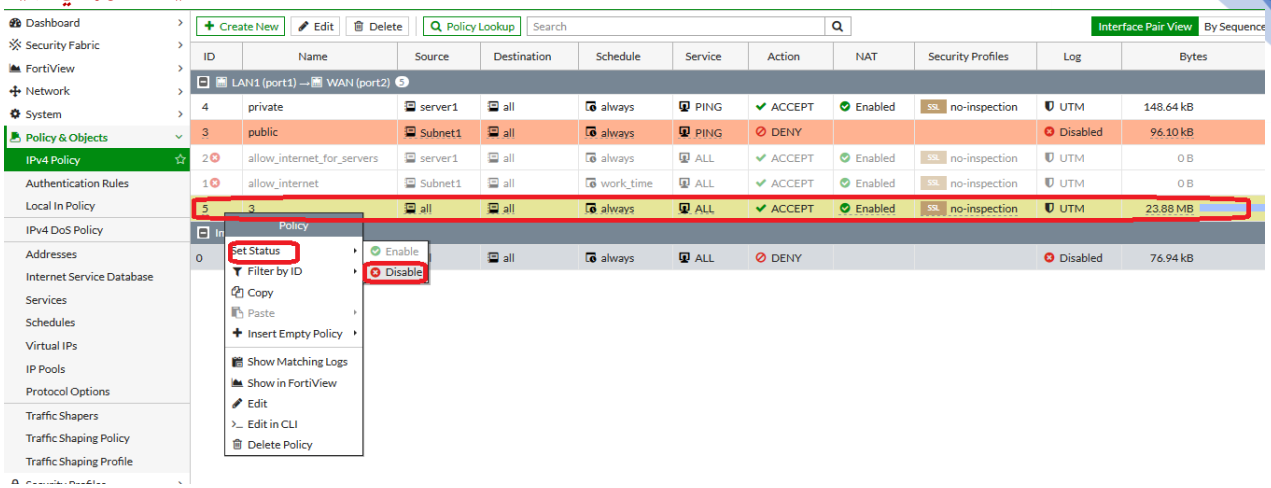
اول رول سمحت فقط له بعمل ping فقط ومن ثم سوف ينزل الى الرول الثانية التي اسمها public والتي تقول بأن الـsubnet1 كلها لا يمكنها الوصول الى الـping ولم تقل له بأنك تمنع أي شيء (all)بل حددت بأنك تمنع فقط الـping .

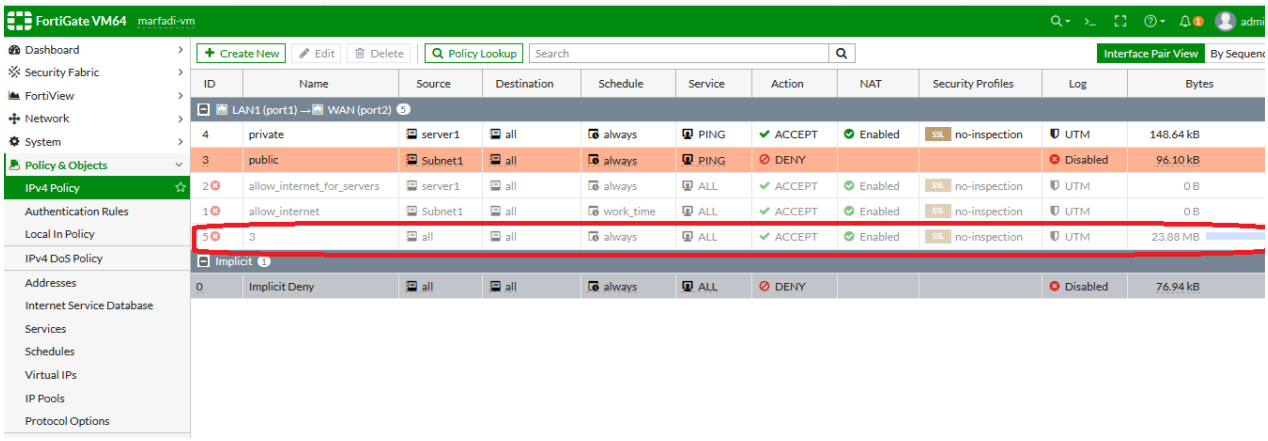
طيب لماذا لازال الجهاز server1 قادر على فتح جميع المواقع !!

الاجابةهي بسبب الرول المسماة 3 والتي مضلله باللون الأحمر كما بالصورة أعلاه والتي بتسمح بكل السيرفس (all) وهذه فكره ترتيب البوليسي ..

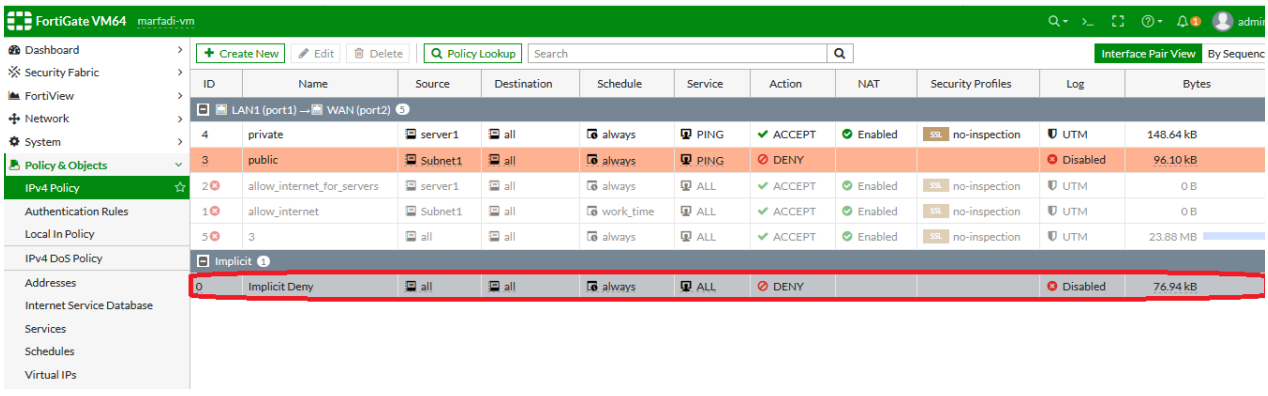
طيب السيناروا الأخير:

ماذا لو قمت بعمل تعطيل (disabled)للبوليسي التي باسم 3 !! كما بالصورة ادناه



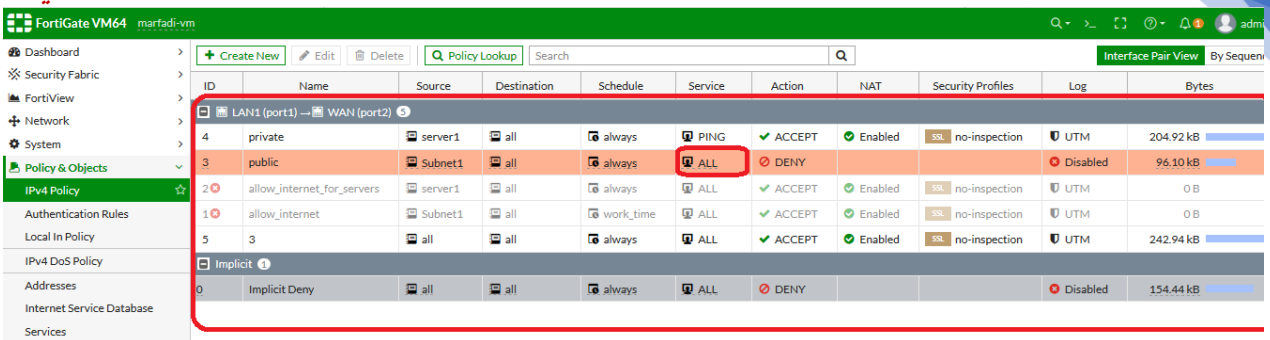


فأن الجهاز server1 يستطيع فقط ان بقوم بعمل ping لأي موقع ولكنه لن يتمكن من فتح أي موقع لأن لا توجد رول بتسمح له بذلك بالإضافة ان اخر بوليسي(الافتراضي)(Implicit policy) بتمنع أي ترافيك بحسب الصوره ادناه ..



اخر مثال :

لو قمت بإنشاء بوليسي كما بالصورة ادناه



هل

يستمكن الجهاز server1 من ان يعمل ping ؟ لماذا؟؟

هل سيتمكن الجهاز server1 من ان يفتح أي موقع ؟؟لماذا؟؟

الاجابةعلى السؤال الأول هي نعم لأن البوليسي الأولى بتسمح الـping .

الاجابةعن السؤال الثاني هي لا ..

لن يتمكن الجهاز server1 ان يفتح أي موقع وهذا بسبب الرول رقم 2 المسماة public وذلك لأني عملت deny= all services فمجرد ان الـdeny حصل فأن الفورتي جيت لا ينظر الى البوليسي اللي تحته ..

بالرغم ان البوليسي الأخيرة التي بالاسم 3 مفعله وتتيح لكل الاجهزه ان تصل الى الانترنت ولأي موقع ..

❖ Managing devices

يقصد بها اداره الأجهزة..

الـfortiOS (نظام التشغيل التابع للفورتي جيت)يستطيع اداره 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 الموصله بالشبكة سواء كانت تلك الاجهزه وايرلس(مرتبطة بـaccess point) او واير (موصله بالسويتش).

❖ كيف يقوم فورتي جيت بإدارة الأجهزة ؟

يعمل بأحدى الطرق :

1 – Agent based:يكون هنالك وكيل (برنامج الفورتي كلاينت)يتم تنزيله على تلك الاجهزه .

2 – Agentless :بدون وكيل على تلك الاجهزه .

الان سنتعامل مع طريقة Agentless :

يتم توصيل تلك الاجهزه بالشبكة بالفورتي نت سواء بالسويتش او بالاكسس بوينت حيث مثلا اعطى الباسورد لأي احد مثلا يريد الوصول الى شبكة الوايرلس وبهذا انا قمت بتجميع المعلومات للأجهزة بالشبكة سواء وايرا اووايرلس حيث بعد ذلك يتم التحكم بتلك الاجهزه عبر الماك ادرس (mac address)حيث ستتمكن من السماح او منع تلك الاجهزه بحسب الماك ادرس .

بعد ذلك سوف استخدم البوليسي للتحكم بهذه الاجهزه مثلا اريد امنع كل الاجهزه من نوع الجلاكسي اومن نوع ابل ...الخ من الوصول الى الانترنت والسماح للانواع الأخرى مثل بلاك بيري او الوندوز ..الخ أي ان جهاز الفورتي جيت اصبح بيتحكم بالأجهزة بحسب نظام التشغيل لتلك الاجهزه .

او مثلا عمل بوليسي 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 الـ category او بحسب الماك ادرس او اسم الجهاز او بالايبي للجهاز.

أي ان الفورتي جيت يعمل على جلب المعلومات التالية بعد توصيلها بالشبكة لكي استطيع التحكم بها بعد ذلك عبر البوليسي :

الماك ادرس

الايبي للجهاز

نظام التشغيل للأجهزة

اسم الجهاز

اسم اليوزر(في حالة كان الجهازضمن الدومين)

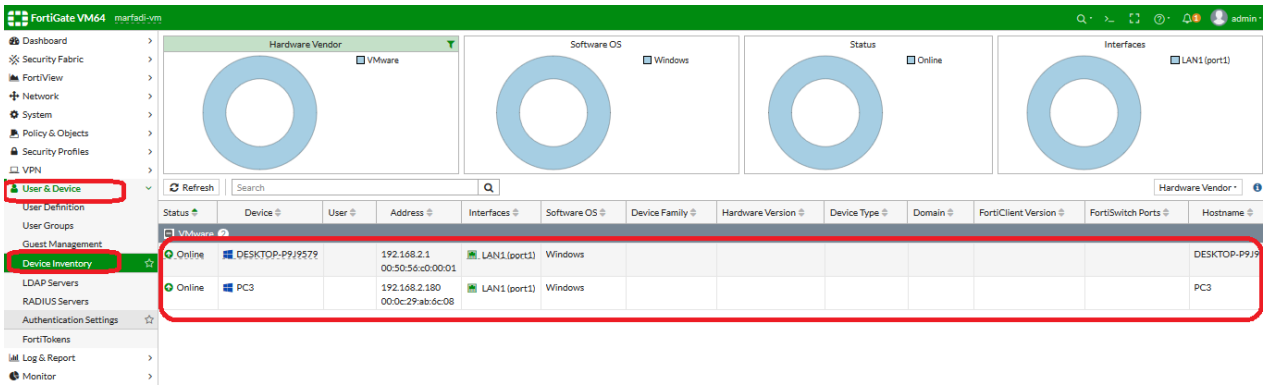
اظهارمتى اخرظهور للجهازوعلى أي من interface موصل هذا الجهاز(lan1،lan2 ....الخ)

ملاحظة :

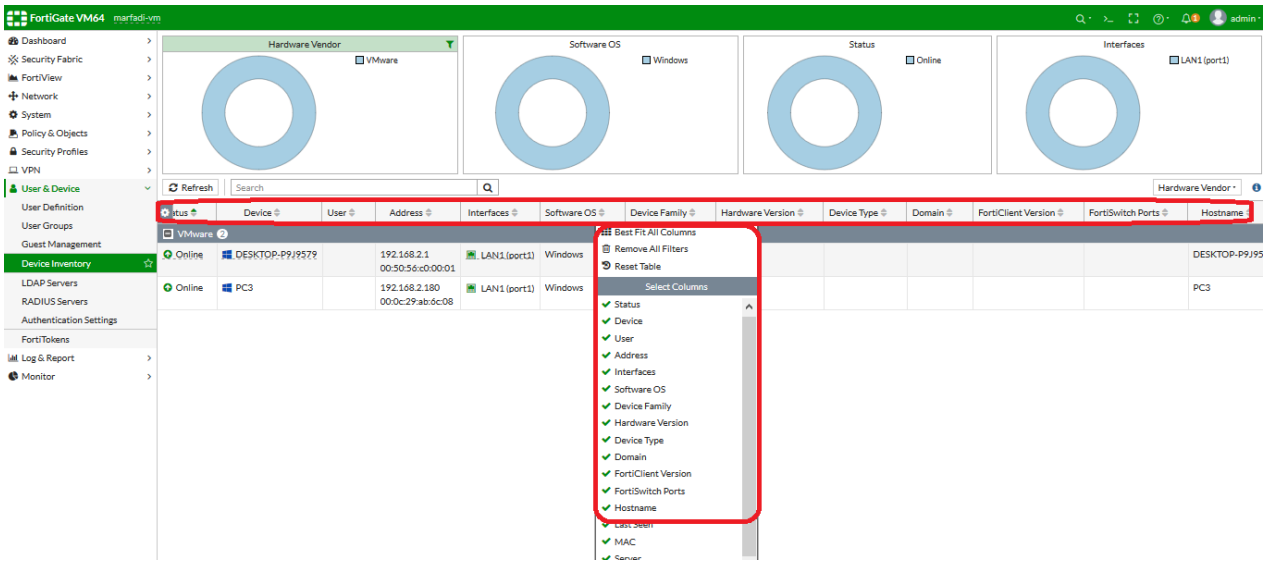
الفورتي جيت بيتحكم بالمستخدمين وبالأجهزة ..

نقوم بفتح الفورتي جيت ونتأكد بأن الفورتي جيت بيشوف الاجهزه عبرأي من interface حيث كل الاجهزه بتسجل نفسها بشكل اوتوماتيكي في المكان التالي :

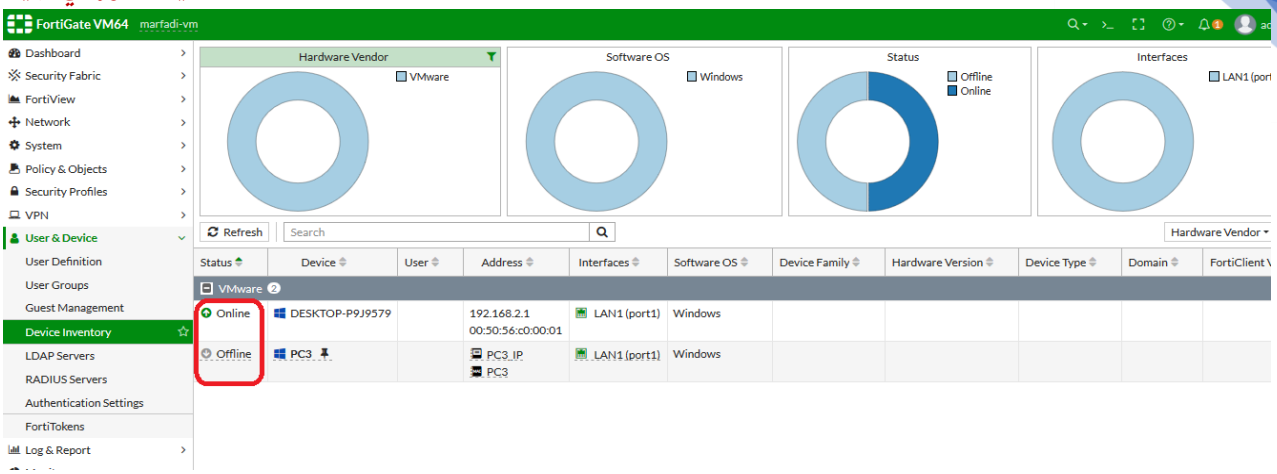
User&Device>Device Inventory >



حيث يمكنك اظهارالمعلومات(الأعمدة)وذلك بالنقربالزر الأيمن على الشريط المظلل بالأحمرومن ثم نختارالخيارات المراد اظهارها ثم apply كما بالصورة ادناه



حيث سوف يظهرلك حالة الاجهزه المتعرف عليها (online , offline)أي الجهازشغال حاليا ام طافي !!



وأيضا يظهر لك اسم الجهاز(Device host name) ،

اسم اليوزر(يقوم بإظهار اسم اليوزر لو كان اليوزر ضمن الدومين)

العنوان (الايبي)

والـinterface المتوصل عليه الجهاز

ونوع نظام التشغيل للجهاز هل 7 او 8.1 او 10

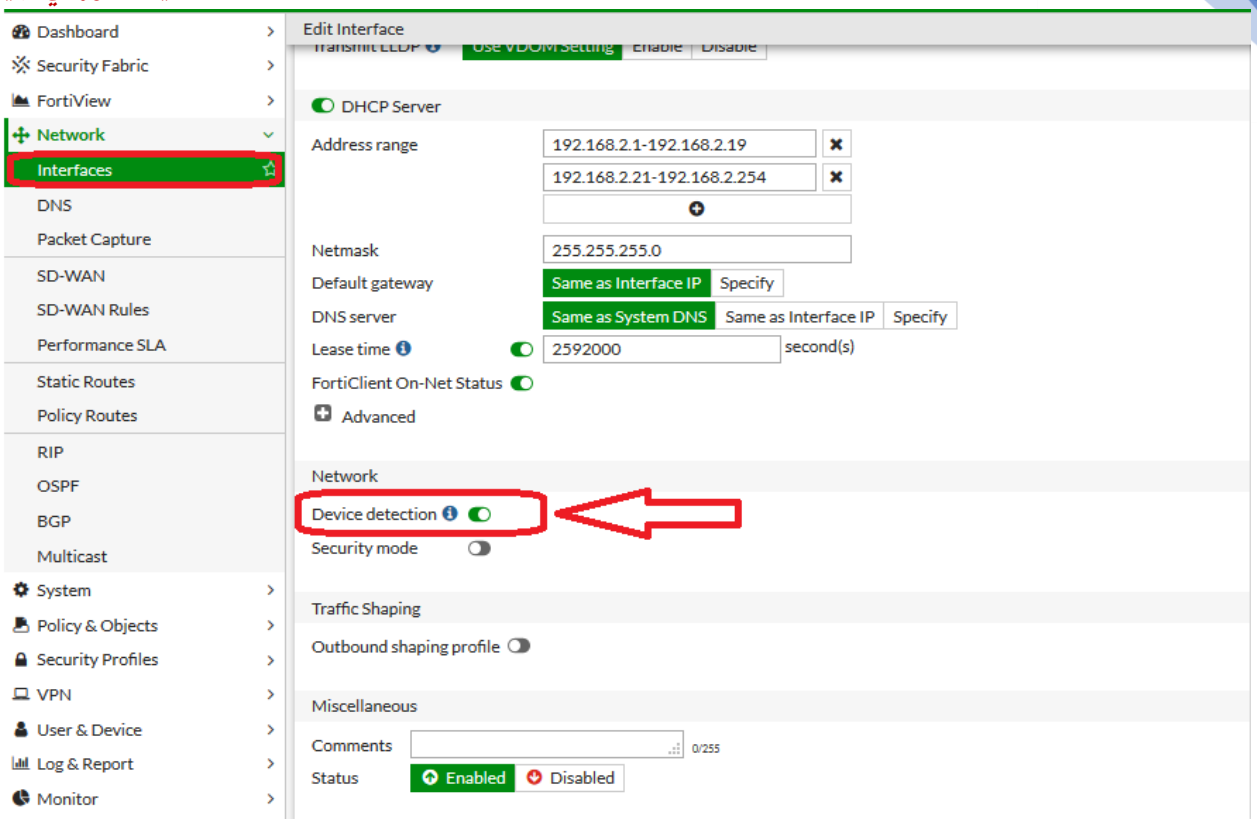
وايضا هل يحتوي على فورتي كلاينت وماهو إصداره

ومتى اخر ظهور للجهاز

الماك ادرس للأجهزة

حيث الفورتي لكي يقوم بعمل كشف وجلب للمعلومات أعلاه يجب ان تقوم بتفعيل خيار معين على الـ interface سواء كانت هذه الاجهزه اخذت ايبي من dhcp server on FG او dhcp server مستقل او الاجهزه لم تأخذ ايبيهات أصلا او اخذت static ip ..

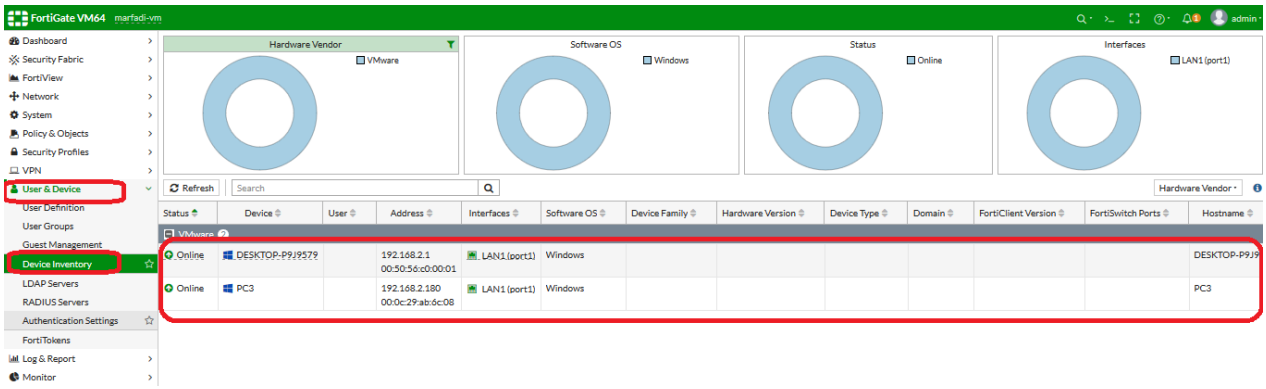
مثلا لو اريد ان اجلب المعلومات أعلاه للأجهزة المتوصله عبر الـinterface مثلا lan1 أي الاجهزه المتوصله بالشبكة الداخليه يجب ان أقوم بتفعيل الخيار التالي على الـ interface lan 1 ..



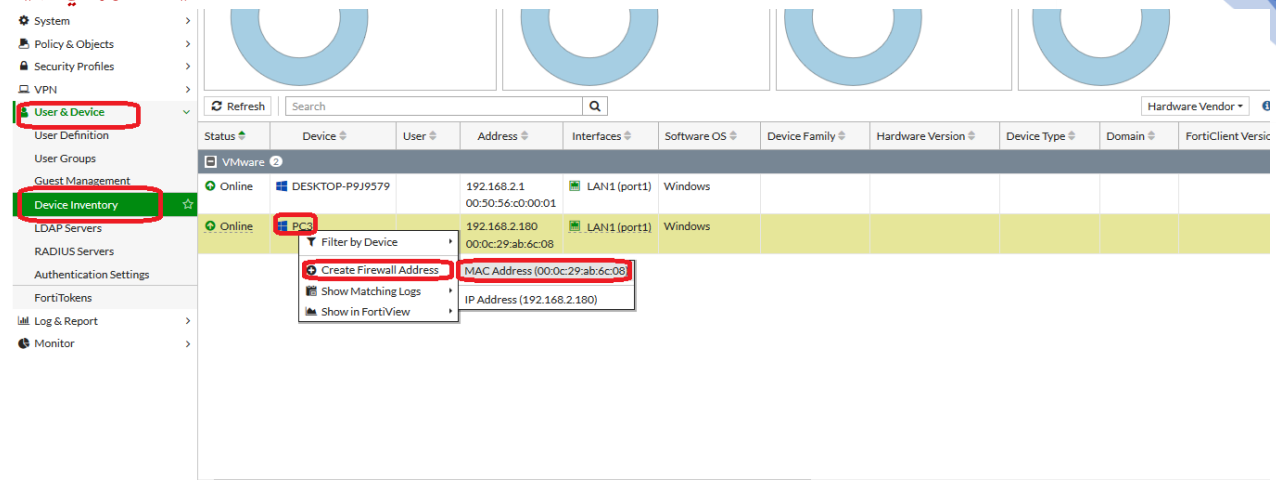
حيث الخيار Device detection لا يكون مفعل بشكل افتراضي ويجب تفعيله

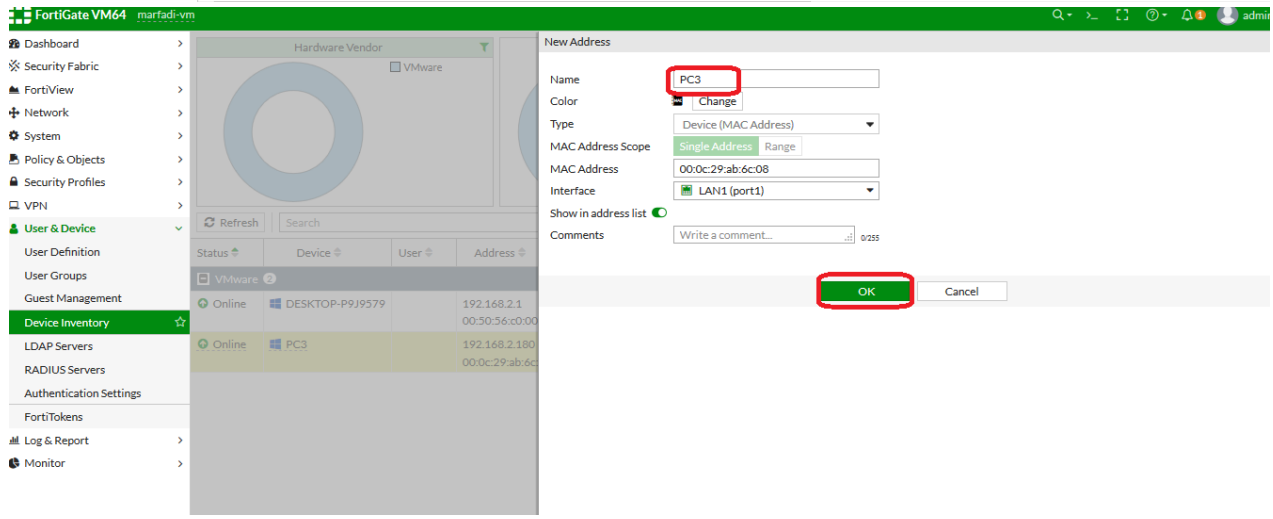
لو اردت تكتشف وتتعرف(detect) على جميع المعلومات المذكورة سابقا لتلك الاجهزه والموصله على المنفذ lan1 مثلا ..

فمجرد الحصول على جميع المعلومات لتلك الاجهزه كما بالصورة ادناه

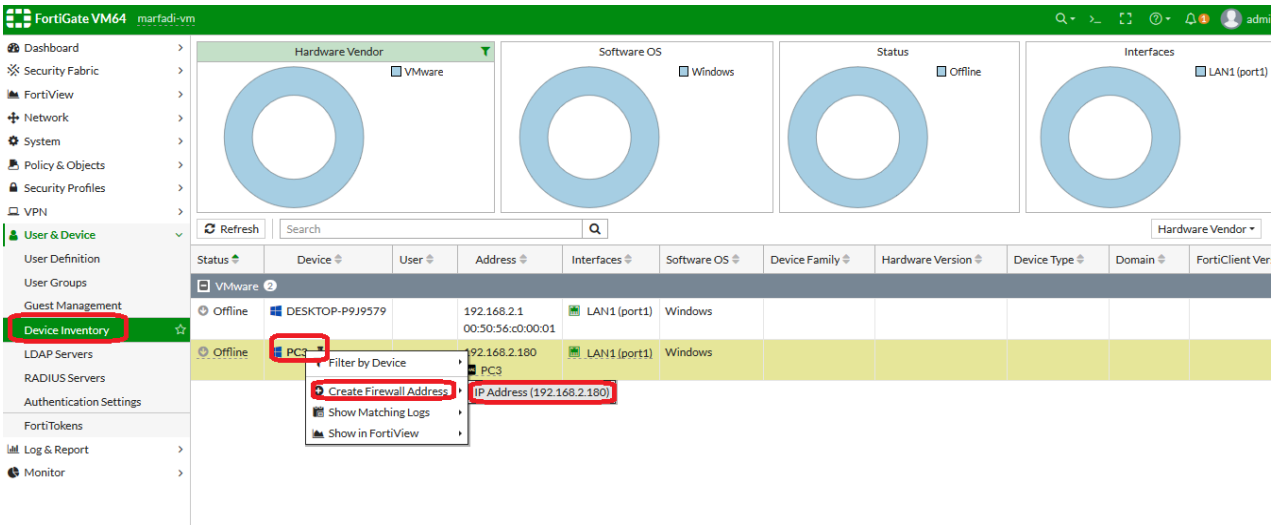


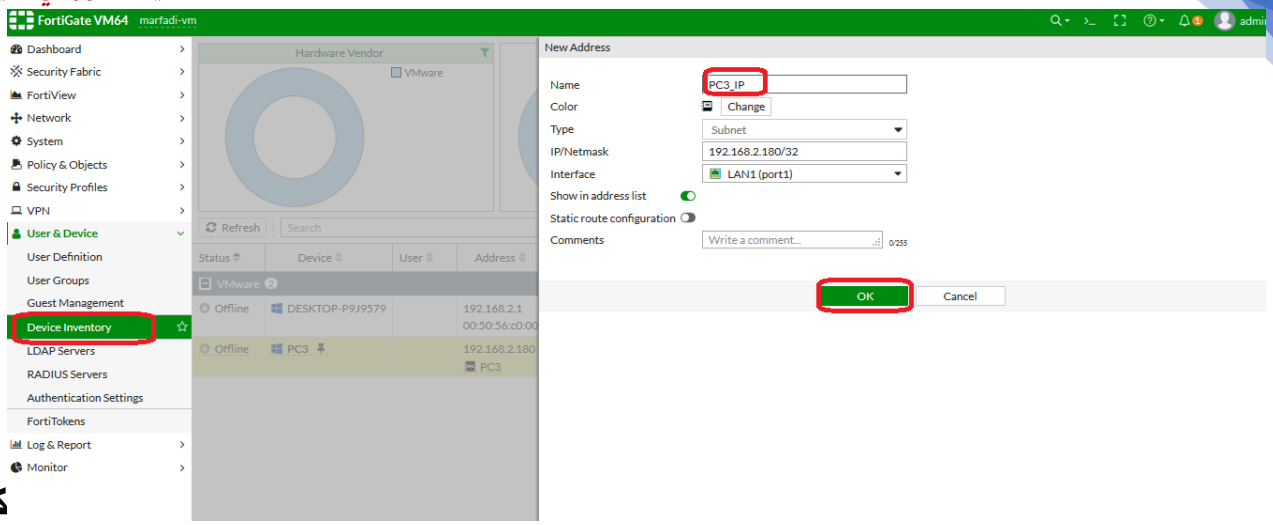
فنقوم بتسميه تلك الاجهزه بحسب الماك وذلك بالنقر بالزر الأيمن على اسم الجهاز(pc3)





اونقوم بأضافه هذا الجهازبالايبي



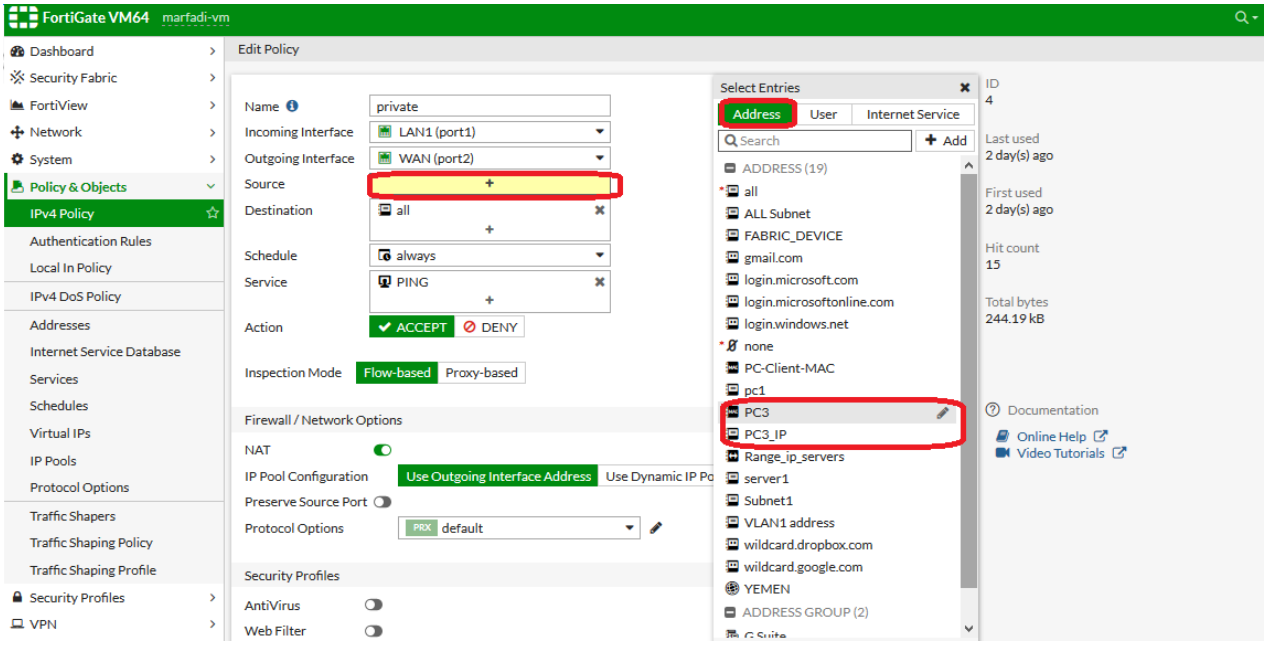


كما

بالصورة ادناه قمت بإنشاء عنوان باسم PC3_IP بحسب الايبي ..

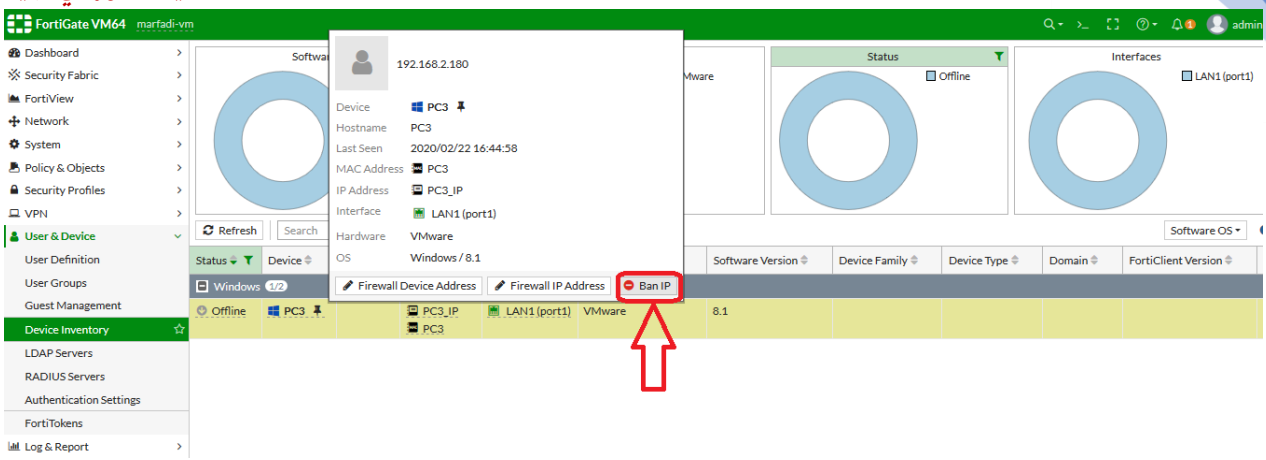
فلذلك لو قمت بإنشاء بوليسي فيمكنني ان اتحكم بهذا الجهاز سواء بالماك او بالايبي كما بالصورة ادناه

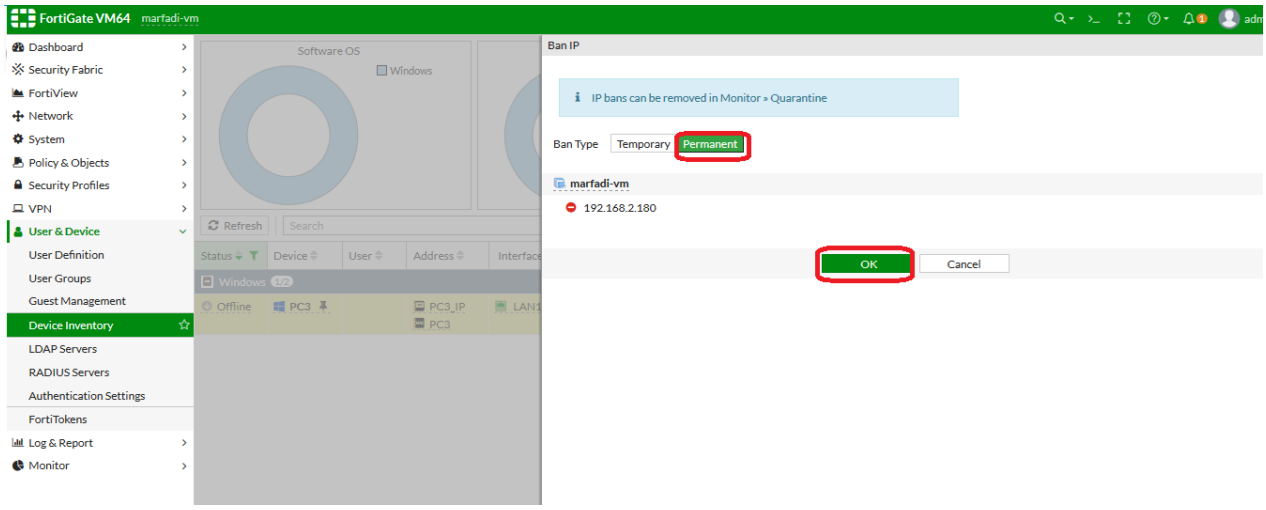
..

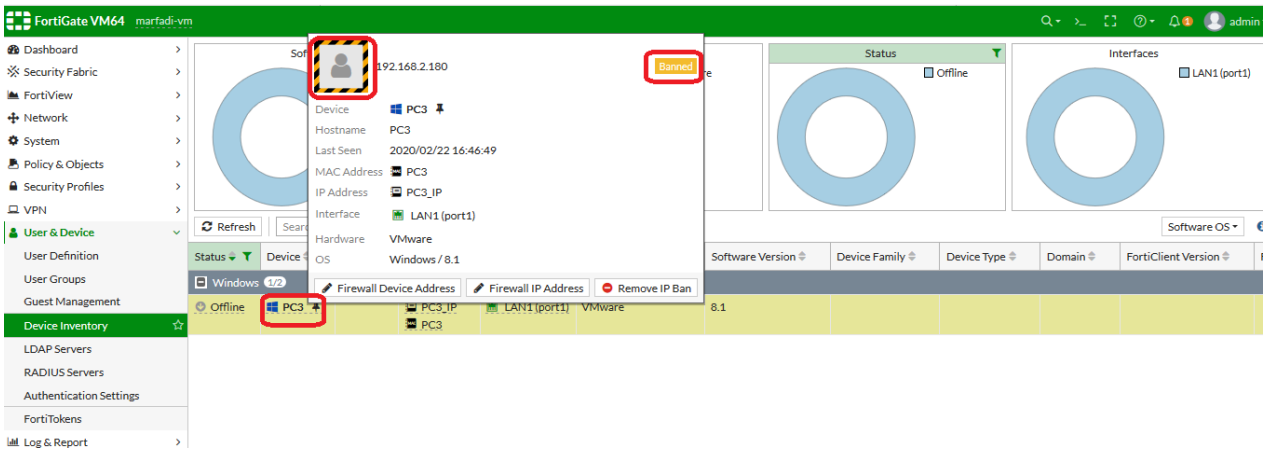


وبهذا استطعت ان اتحكم بالجهاز عبر الماك ادرس لهذا الجهاز او عبر الايبي .

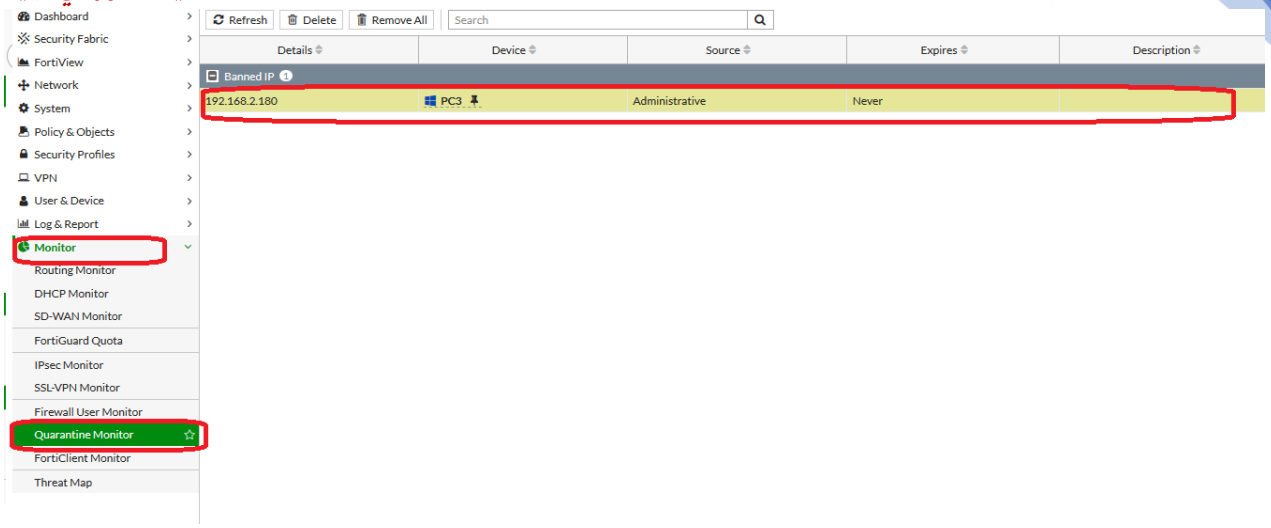
وتكرر نفس العملية لكل الاجهزه التي تظهر لك والتي تم اكتشافها ..



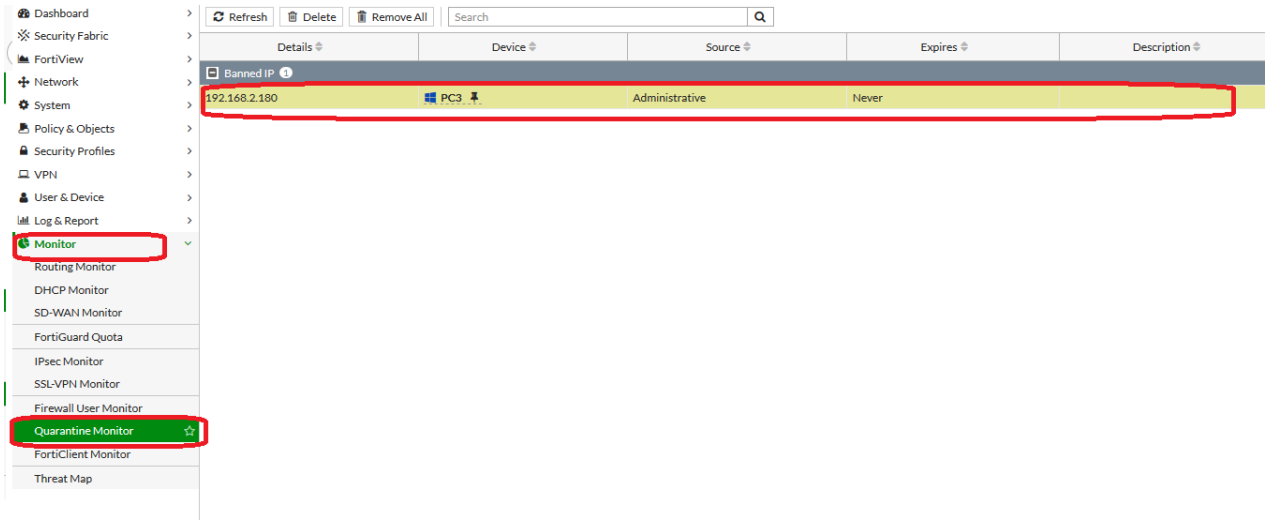




قمت بعمل permanent (أي تم عمل حضر للجهاز 192.168.2.180 بشكل دائم) لذا سوف يتم عمل له بلوك من كل شيء بشكل دائم في الخيار التالي :



حيث تم وضعه بمنطقة الحجر(Quarantine)حيث جهاز الفورتي جيت بيعمل حظر(ban) للأجهزة التي يكتشف بوجود بها اختراق او فايروسات ويمكنك فك الحظر بالذهاب الى



ونحذف الجهاز المحظور لكي يتم رفع الحظر(remove ban)

Access control list (ACL) :

عباره 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 ايبي بعد (أي ان الجهاز مثلا يأخذ ايبي 0.0.0.0 او ايبي من الipipa 169.254.x.x)فجهاز الفورتي جيت بيسجل الماك ادرس لهذا الجهاز في قائمه Devices inventory حتى وان لم يحصل على ايبي بعد .

ولتفعيل خاصيه ACL يجب ان تقوم بتفعيل DHCP server على جهاز الفورتي جيت نفسه وليس كسرفر مستقل وبهذه يقوم بالفورتي جيت بتوزيع الايبيهات لكل الاجهزه الموجودة في الشبكة الداخليه ..

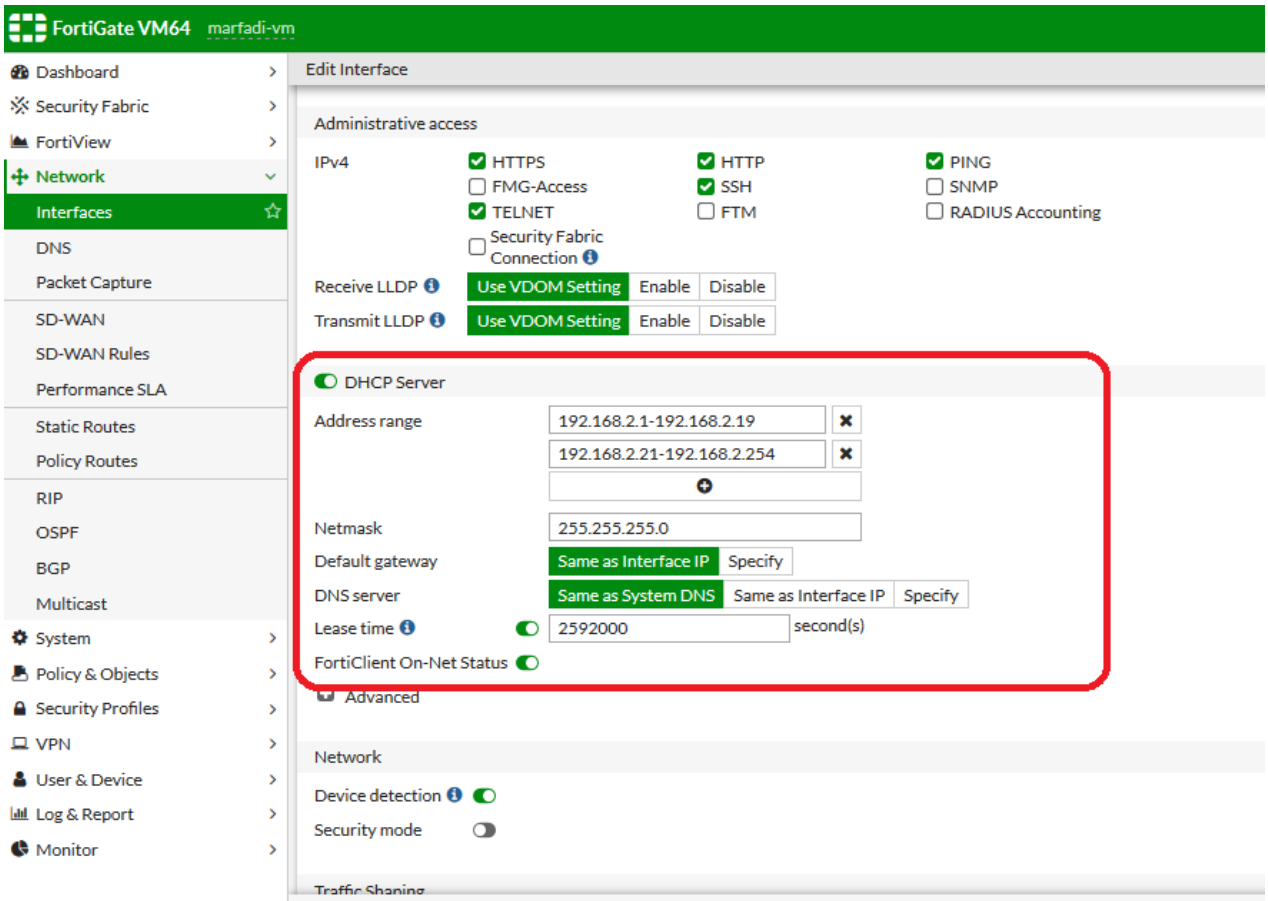
والمفترض بأن ليس أي جهازيتوصل بالشبكة لدي يحصل على ايبي بل فقط الاجهزه التي اثق فيها بالماك ادرس ،،وبهذا اصبحنا نتحكم بالقائمة (lists) بالأجهزة التي لدي بالفورتي جيت من خلال الماك ادرس عبر ACL .

ما هو Mac reservation :

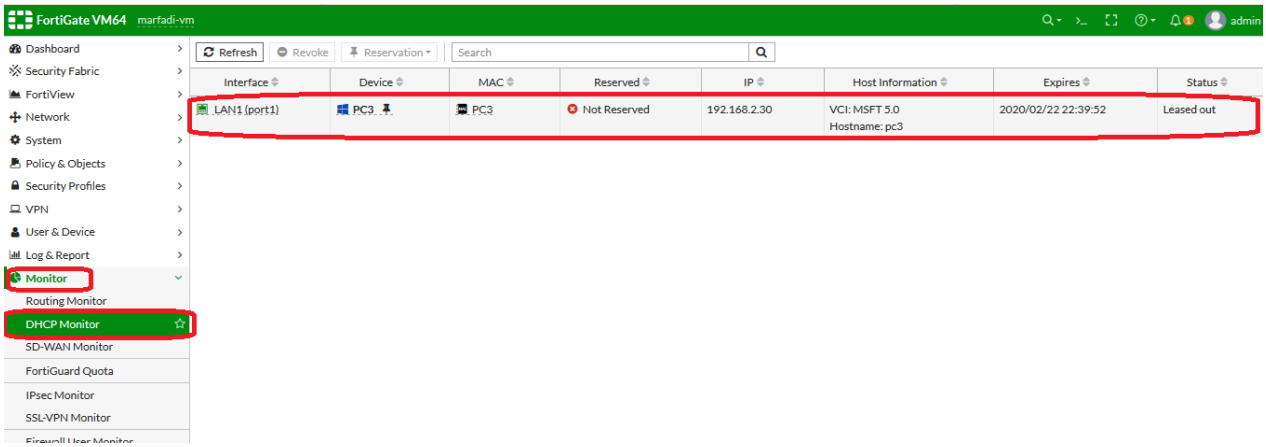
نربط بين الايبي وبين الماك للأجهزة

أي كل مره يأتي الجهاز صاحب الماك الفلاني فأن dhcp server يعطيه الايبي الفلاني في كل مره ..

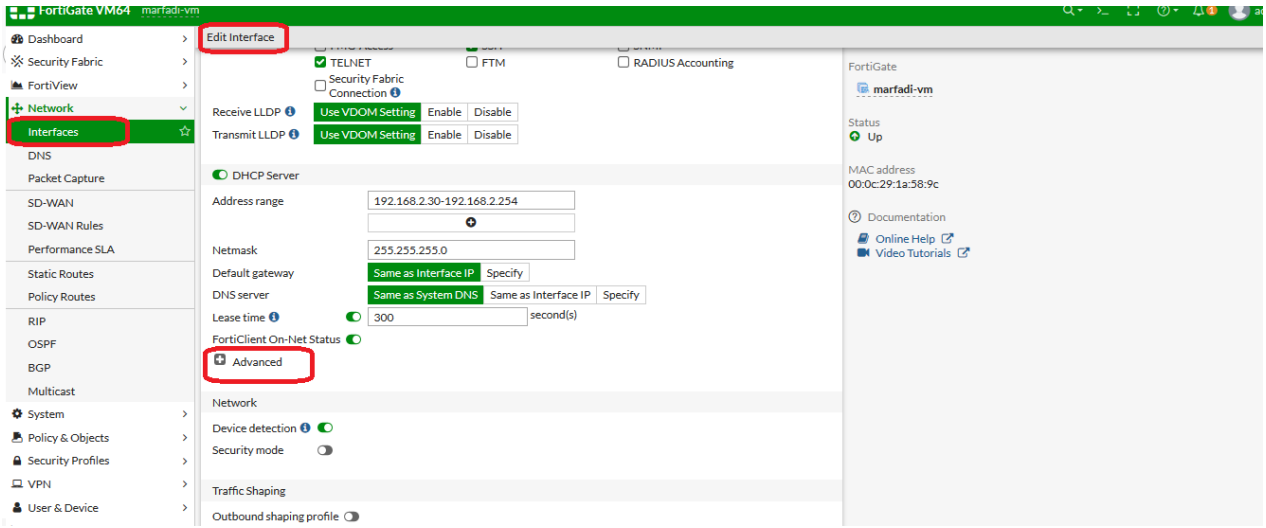
فلو قمنا بتفعيل ال dhcp server على البورت LAN1 كما بالصورة ادناه



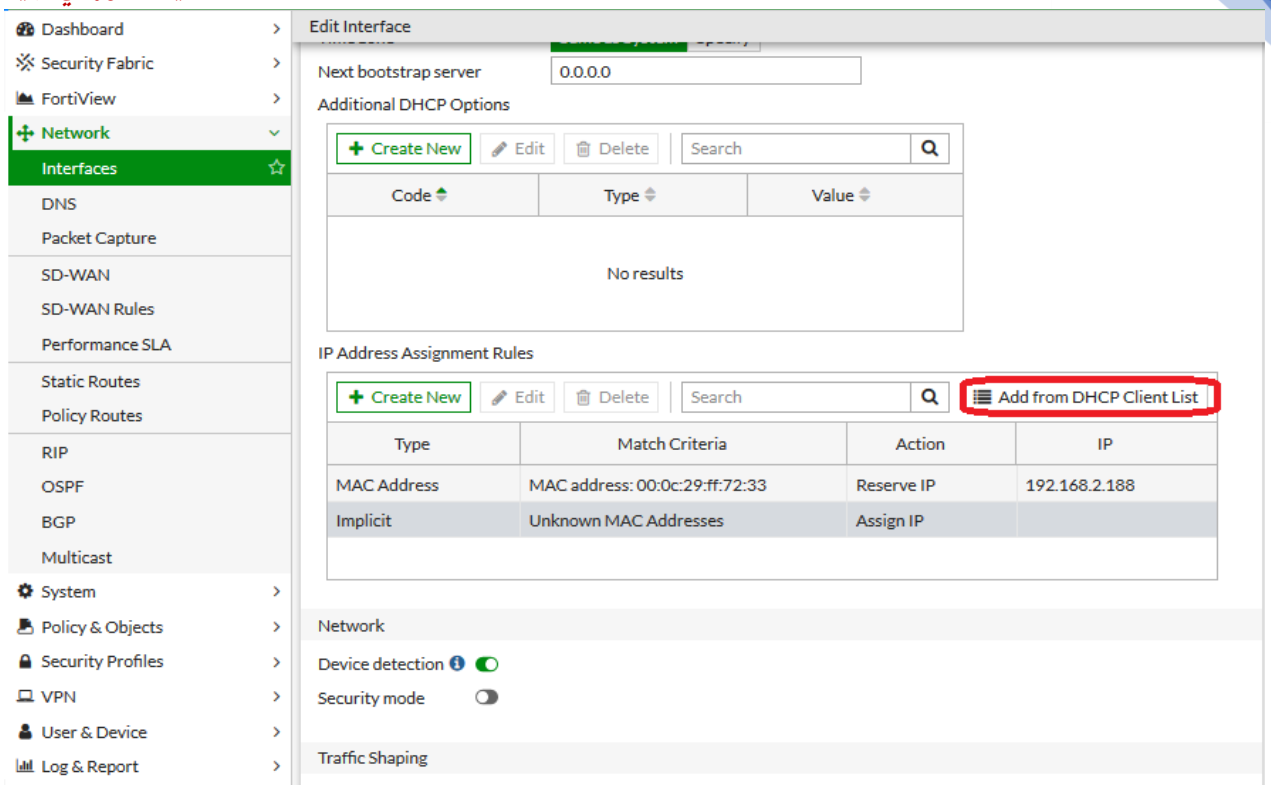
فنذهب الى اجهزه الكلاينت والتي هي على الشبكة الداخليه ونعمل لكروت الشبكة disabled و enabled لتتمكن من الحصول على ايبي من الـdhcp server .



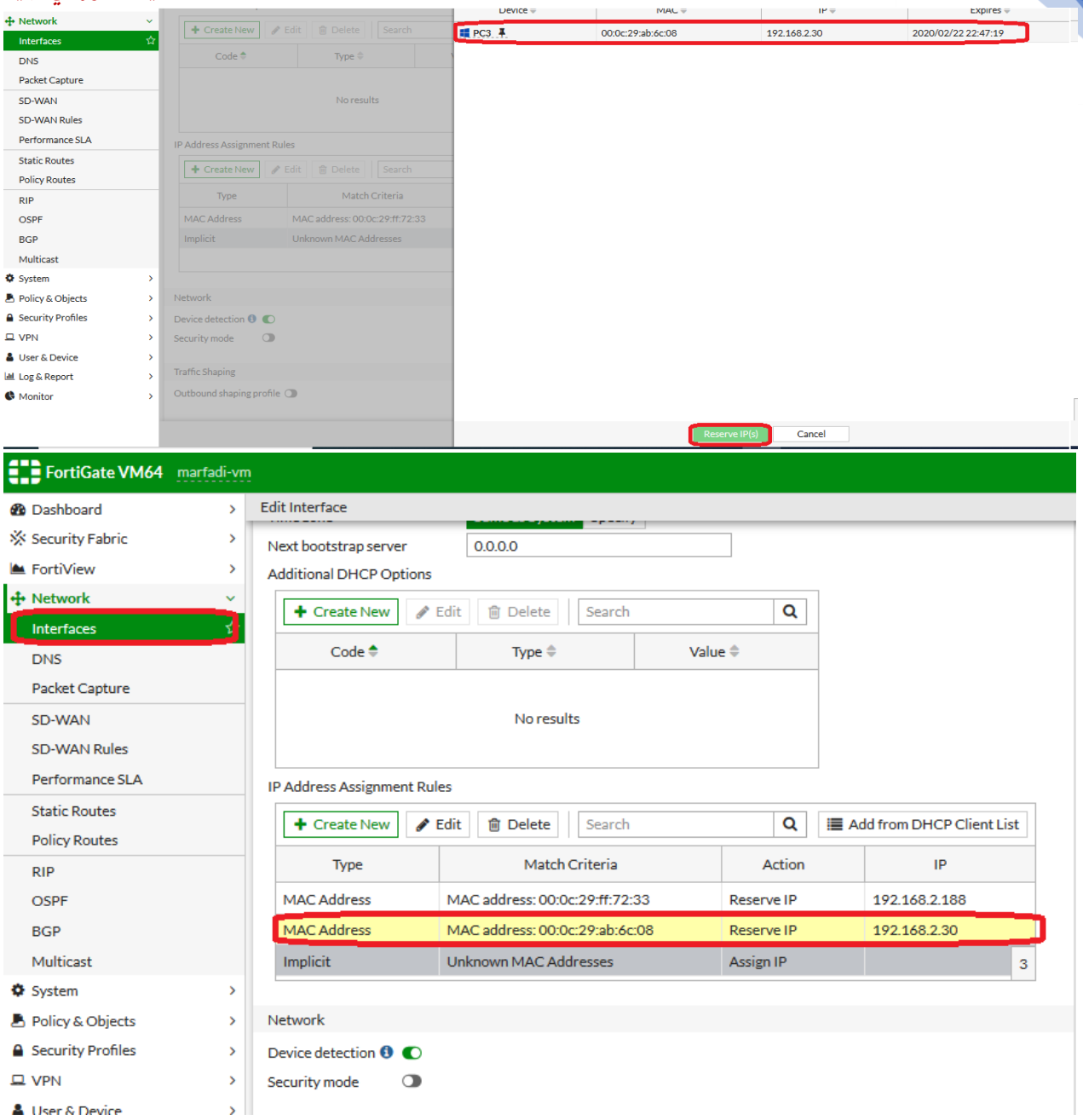
نلاحظ بأن الجهاز pc3 حصل على ايبي 192.168.2.30 من dhcp server



ندخل على كرت LAN1 ثم نختار الخيار Advanced

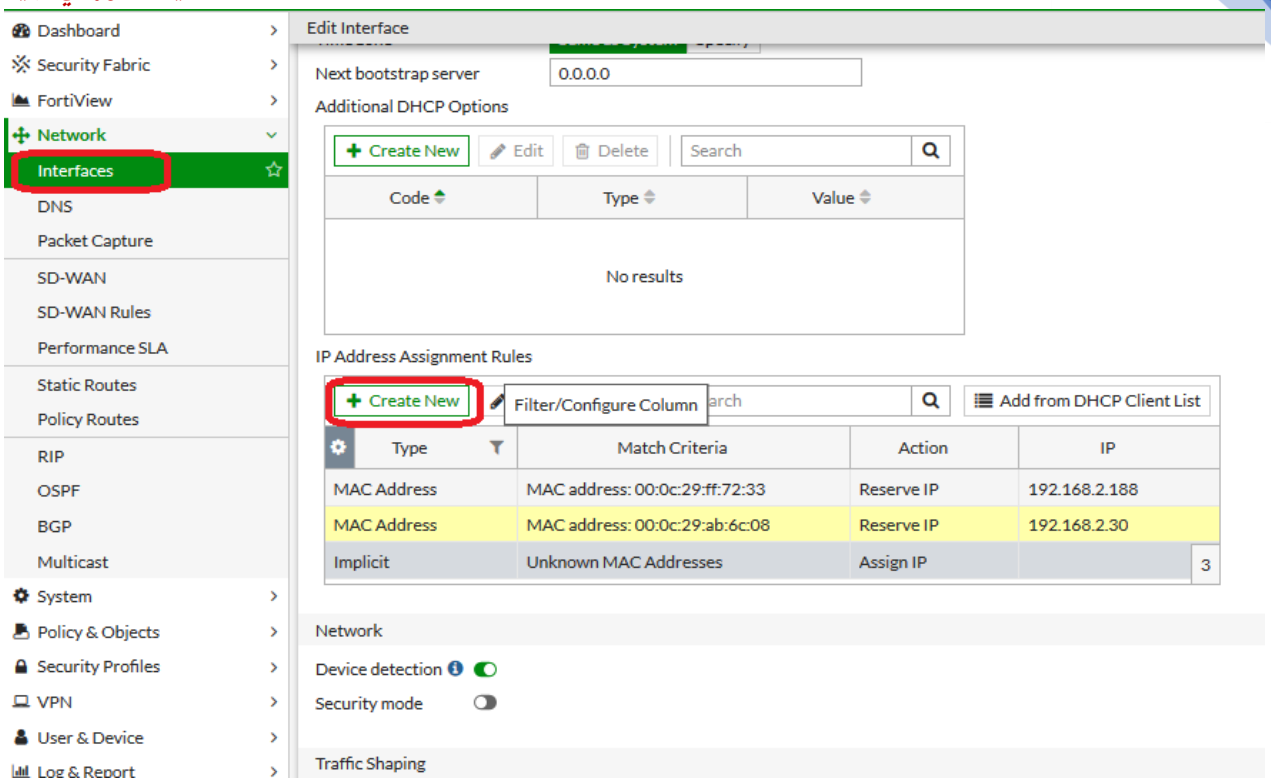


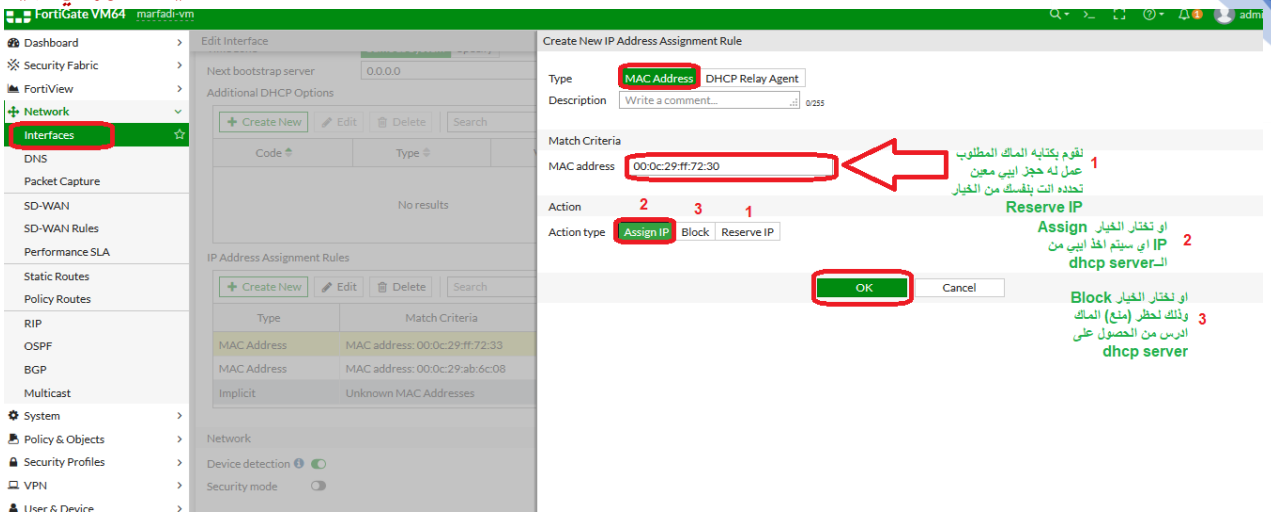
من الخيار Add from DHCP client List سوف يظهر لك كل الاجهزه التي اخذت ايبي من الـdhcp server ومن ثم يمكنك اختيار الماك والايبي لعمل reserved (حجز) بحيث هذا الجهاز صاحب الماك الفلاني دائما اعطيه الايبي الفلاني...

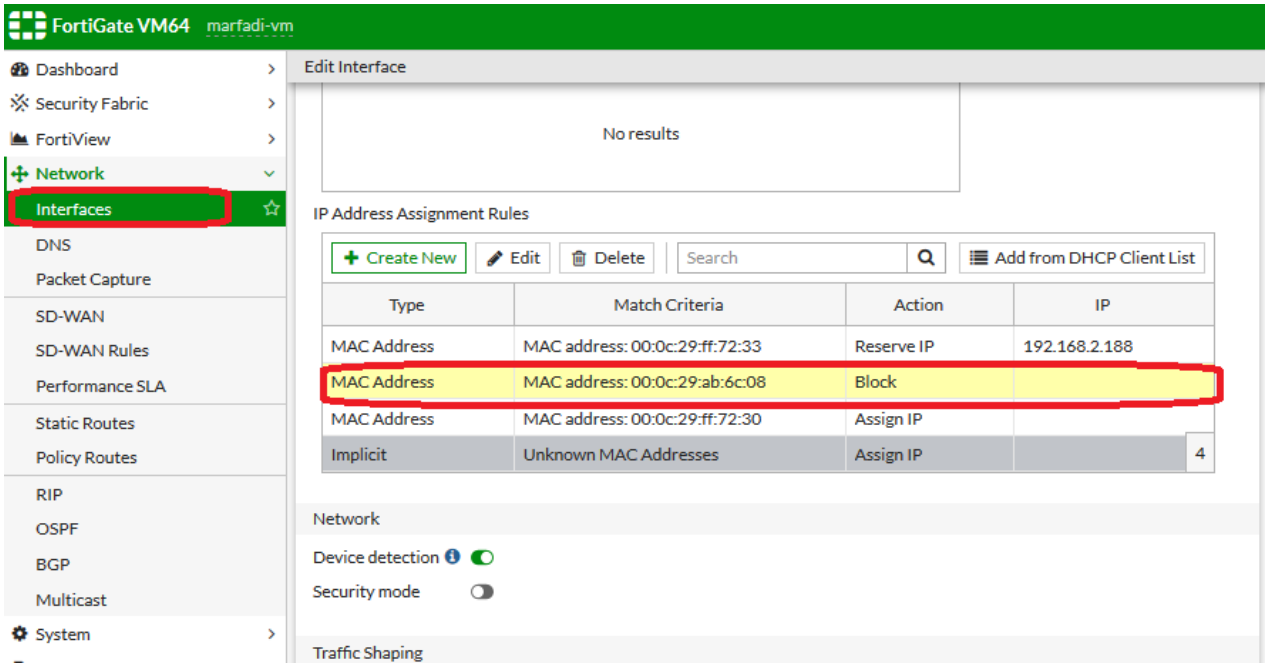


نلاحظ بأنه تم حجز (reserved)الايبي 192.168.2.30 للماك ادرس المشارله بالاحمر..

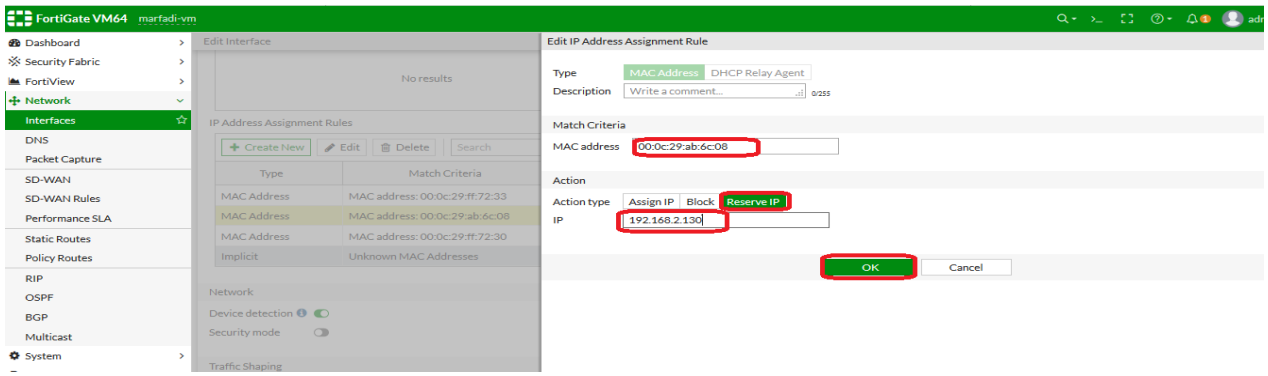
فأذا اردت انشاء reserve ip مانوال


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
Code
Type
Value
No results
IP Address Assignment Rules
Create New
Filter/Configure Column
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

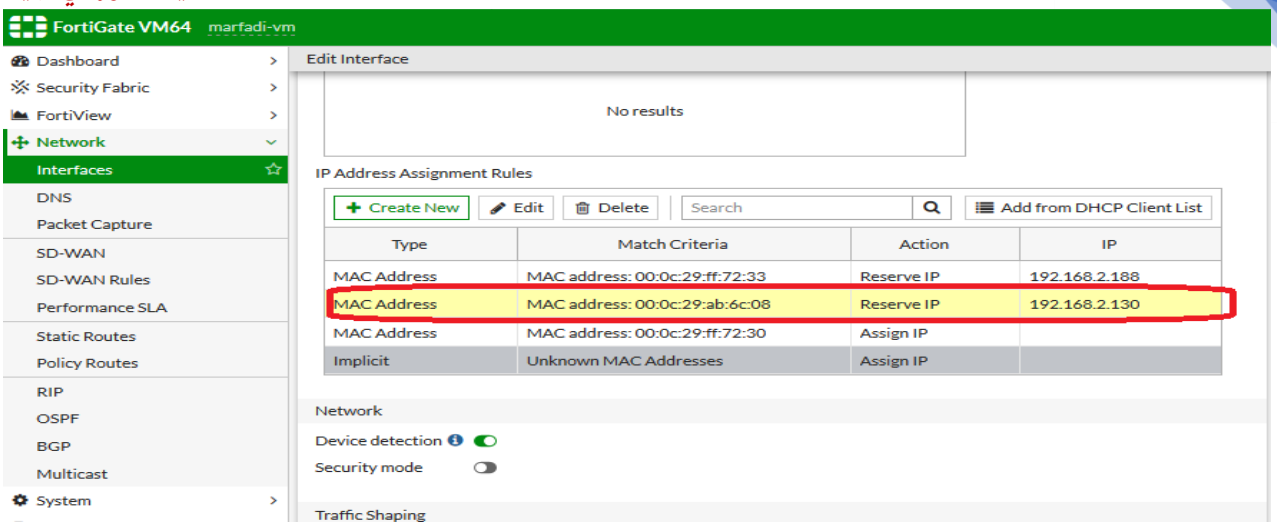




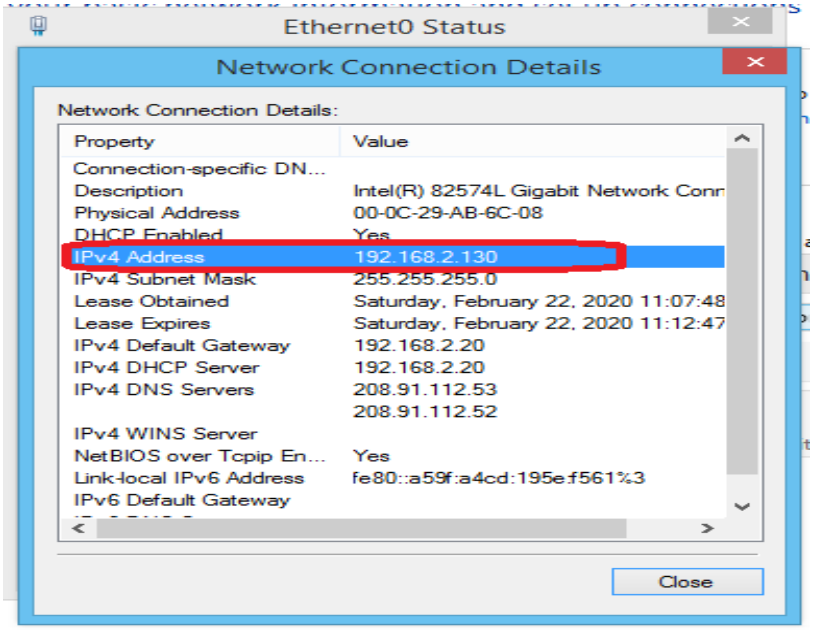
كما بالصورة أعلاه تم حظر الماك ادرس بأن يحصل على ايبي عن طريق dhcp server فعند عمل disabled و enabled لجهاز الكلاينت الذي له هذا الماك ادرس فأنه لن يجد ايبي مهما حصل ...



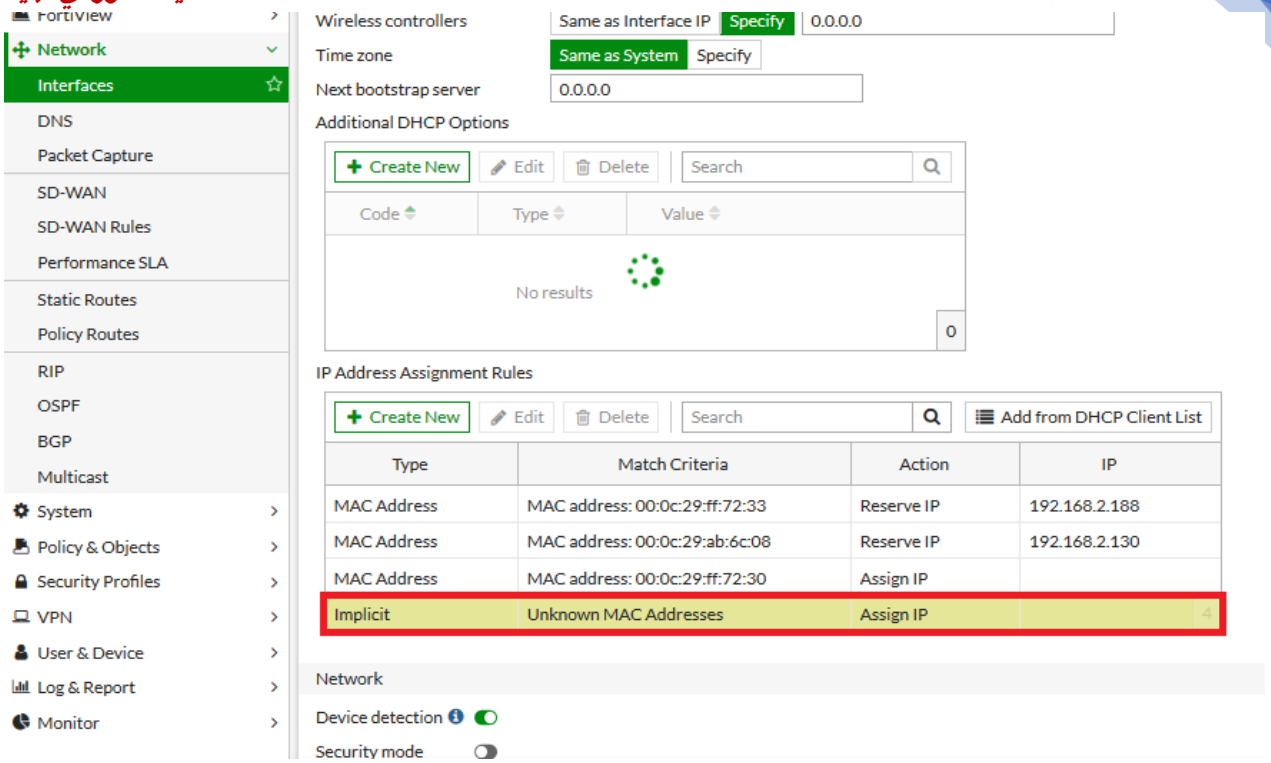
اما الصوره أعلاه تم كتابه الماك ادرس للجهاز الذي تريد حجز له الايبي 192.168.2.130



فندخل على جهاز الكلاينت ونعمل disabled ومن ثم enabled لكرت الشبكة ونلاحظ بأنه حصل على الايبي 192.168.2.130 كما بالصورة ادناه



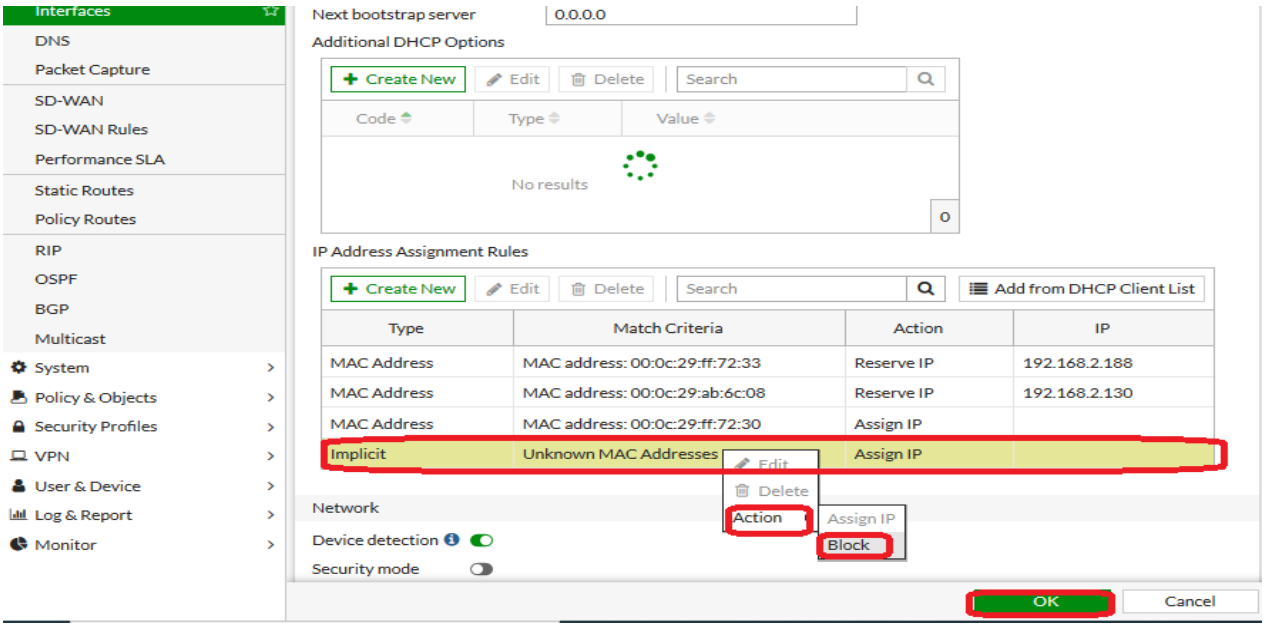
ملاحظة هامه :

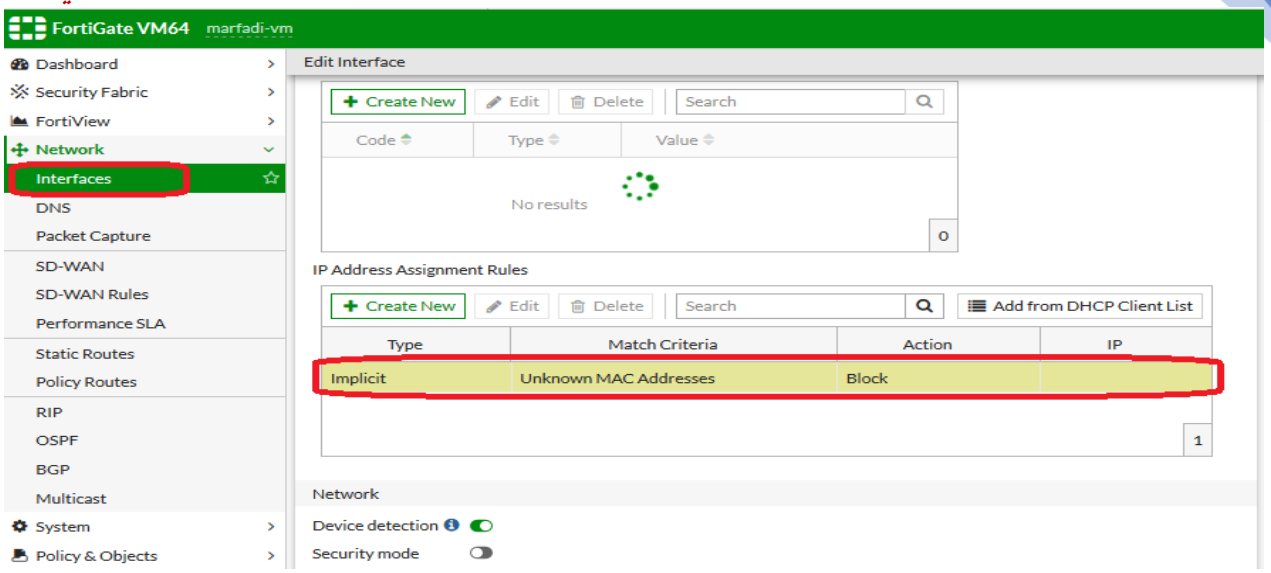


المالك ادرس الغير معروف قم بتخصيص له ايبي من dhcp server وهذا بشكل افتراضي كما بالصورة أعلاه.

حيث ان الـDHCP server يقوم بتخصيص ايبي لكل جهاز بالشكبه ..

حيث لو قمنا بتغيير الخاصية الى Block= unknown mac address فأن أي جهاز لن يحصل على ايبي من dhcp server الا لو كان معروف ..

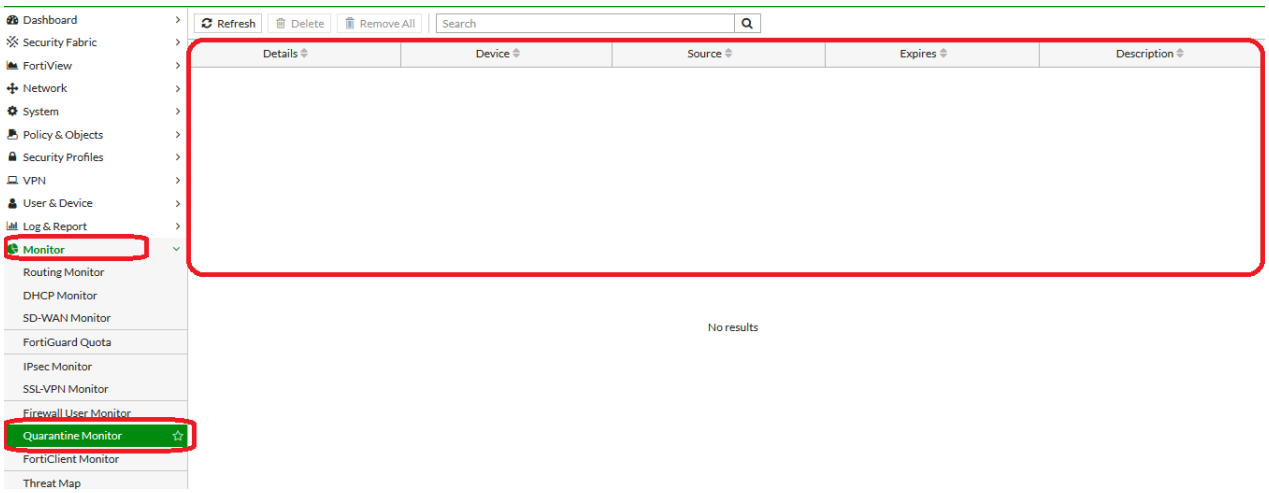




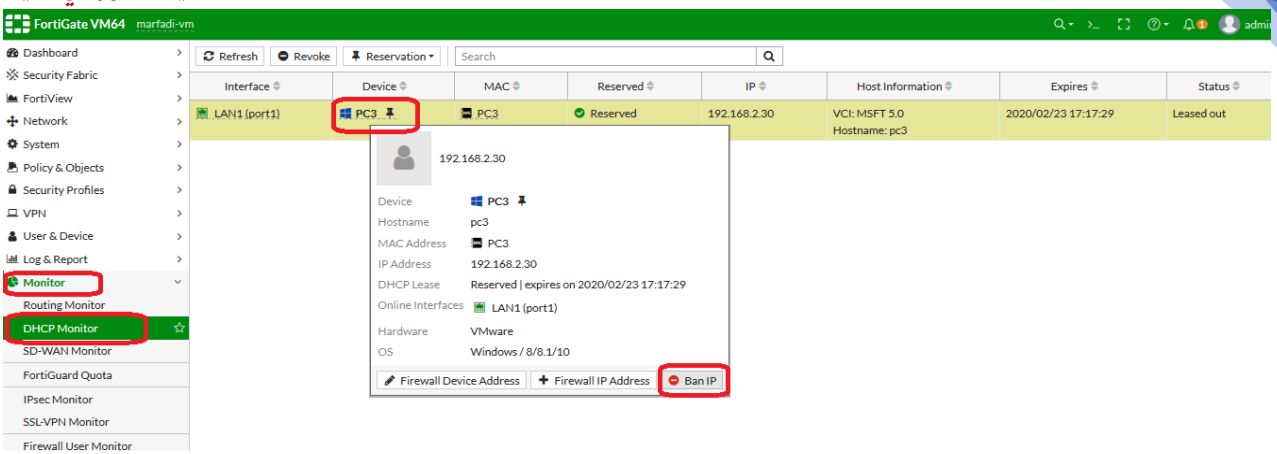
حيث بالخيار أعلاه لن يتمكن أي جهاز من الحصول على ايبي من DHCP SERVER .

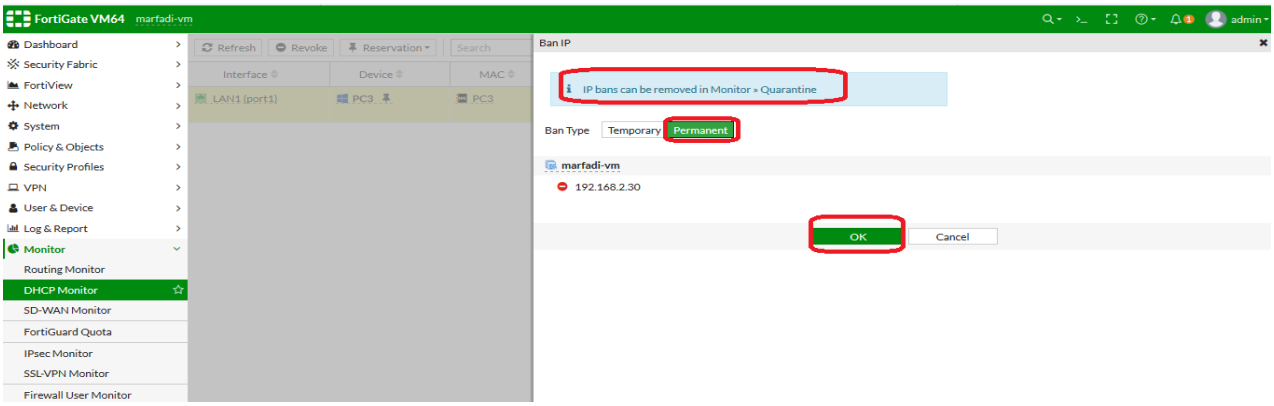
كيفيه حظر ايبي معين من الحصول على الانترنت :

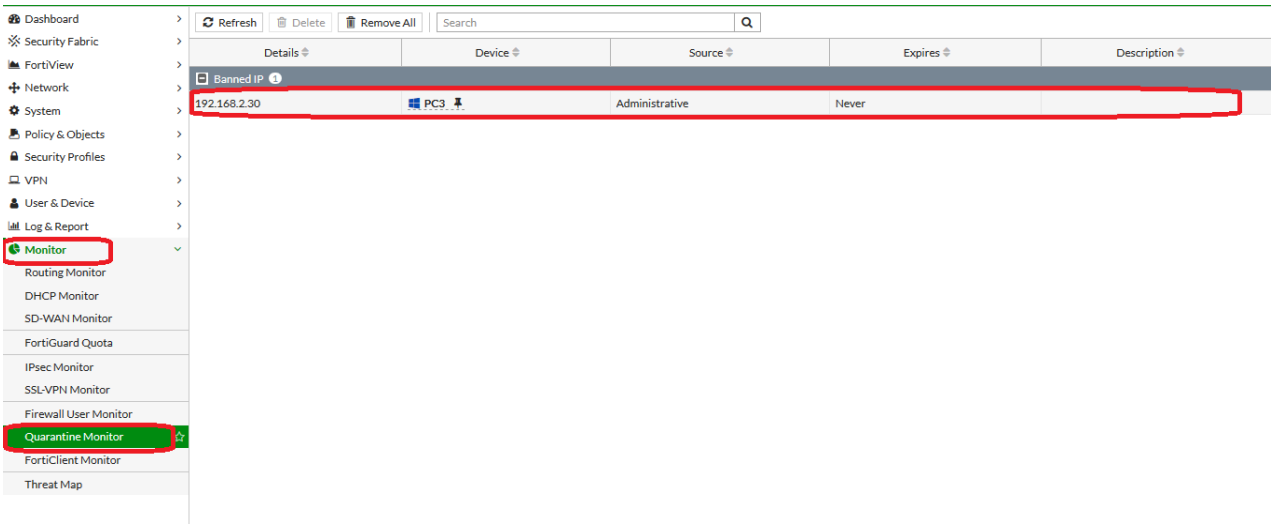
نلاحظ بأن منطقه الحجر الى الآن فارغ



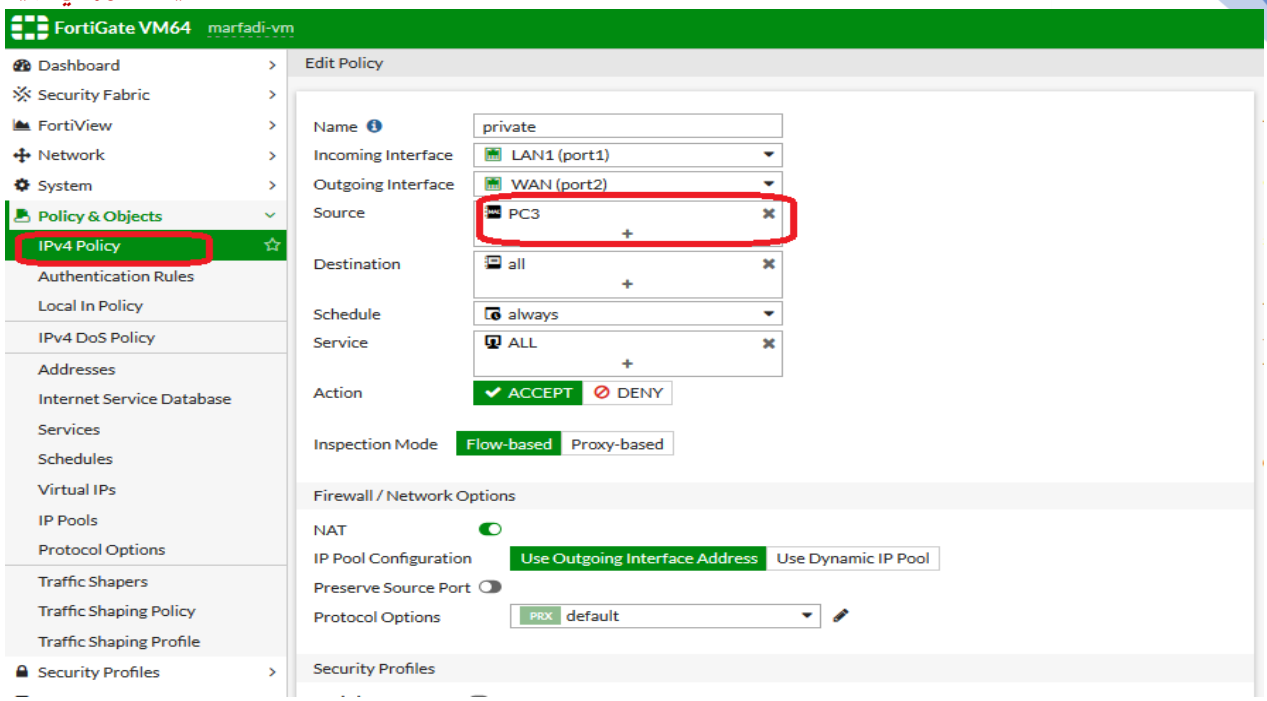
الآن سوف نقوم بعمل حجر للايبي 192.168.2.30 ..







نلاحظ بأن الجهاز PC3 معمول له حظر ولن يحصل على الانترنت مهما حصل الا لو قمت بحذف الايبي من الـ 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 تقنيه اداره 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 الLAN او موجودة على شبكة الWAN (على الانترنت)حيث سيقوم فورتي جيت فايروول بتوفير الحمايه للأجهزة التي بعيده عن الشبكة الداخليه وذلك عبر برنامج الفورتي كلاينت .

➢ حيث الفورتي 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 الفورتي كلاينت مجاني على أي الاجهزه .

حيث يوجد اصدارين من الفورتي 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 FortiGate[1]				
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 لوكان لديك فورتي جيت فأن النوع Basic سوف يتيح لك كل المزايا المحدده أعلاه بحسب الجدول أعلاه .

ولكن لولم يكن لديك فورتي جيت فايروول فيمكن الاستفاده من الفورتي كلاينت ك web filtering و Antivirus فقط .

اما النوع Registered with fortiGate فأن اهم ميزه يوفرها لي الفورتي كلاينت هي Centralized management أي اداره مركزيه أي سيتم التحكم بشكل مركزي بكل الفورتي كلاينت عن طريق الفورتي جيت فايروول.

يجب عليك قبل ماتقوم بشراء الفورتي كلاينت فأنك تبحث عن جهاز الفورتي جيت الى حد كم بيدعم forticlients .

مثل FG 30-90 بيدعم فقط الى 200 forticlients .

فاذا كان لديك عدد اجهزه تريد تنزل عليها فورتي كلاينت اكثر من 200 جهاز فيجب عليك ان تقوم بشراء جهاز فايروول فورتي جيت بحيث يدعم عدد اكبر من الفورتي كلاينت ..

حيث النسخ (الفورتي 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 8,000 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 الصوره توضح موديل الجهاز الفورتي جيت وعدد الاجهزه التي يدعمها الفورتي كلاينت .

ملاحظة :اشتراك الفورتي جارد يختلف عن اشتراك الفورتي كلاينت ..

❖ طريقة تنزيل الفورتي كلاينت على الاجهزه :

١- تنزيل الفورتي كلاينت على اجهزه المستخدمين في حالة عدم وجود دومين :

يتم تنزيل الفورتي كلاينت بعد تنزيله من الموقع forticlient.com (مجانا) او من Dashboard ثم Forticlient تقوم بتنزيل ملف بالكيلوبايت ومن ثم تقوم بتنزيله على كل اجهزه الموظفين حيث اثناء التثبيت يجب ان تكون الاجهزه متاح عليها الانترنت لكي يعمل اتصال مع الـ FDN لكي ينزل منه التحديث .

او من السوق بلاي (google play)لأجهزه الاندرويد .

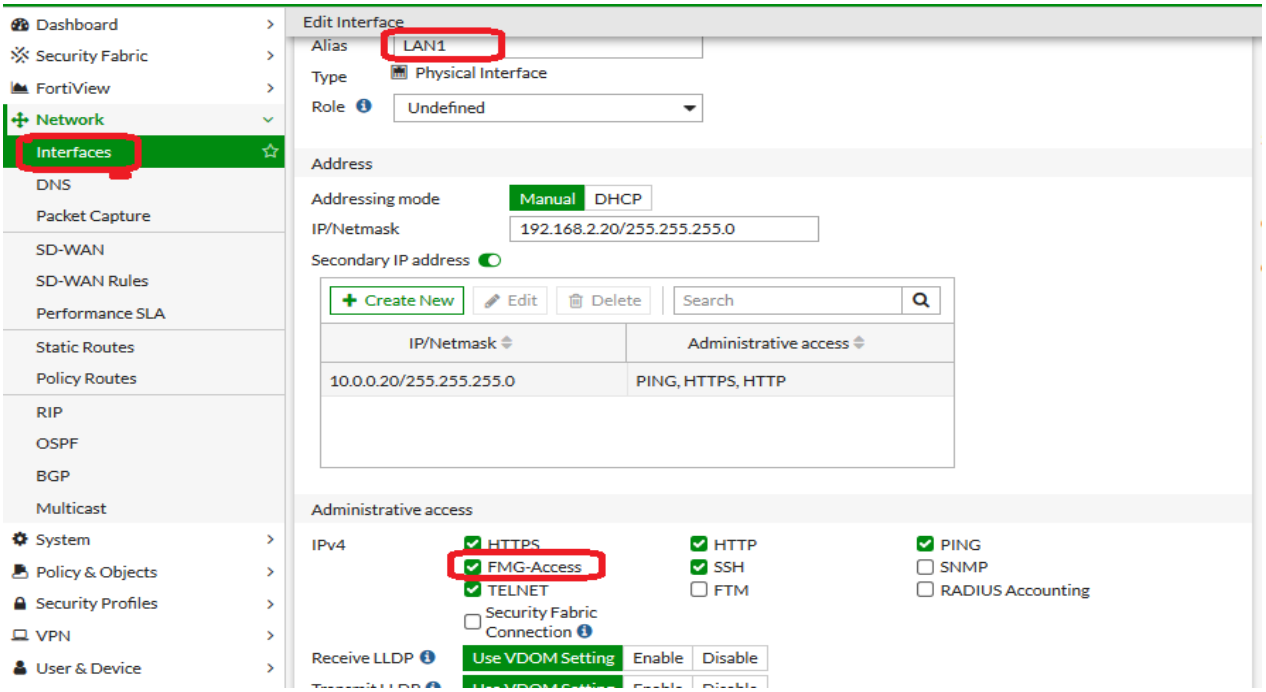
أحيانا تكون هنالك اجهزه مفيرسه ولا يمكن تنزيل عليها برنامج الفورتي كلاينت من الوضع الطبيعي بل يحتاج الدخول الى الوضع الآمن مع الشبكة (safe mode with networking)ومن ثم نقوم بتنزيل برنامج الفورتي كلاينت حيث ستظهر لك رساله خطا تجاهلها واعمل اعاده تشغيل للويندوز ومن ثم ادخل على الوضع الطبيعي ستلاحظ بأن التطبيق يعمل تنزيل بشكل طبيعي ..

2 - نشر الفورتي كلاينت عبر الجروب بوليسي من سيرفر الدومين (Deploy)على الاجهزه في الشبكة، حيث يجب ان يكون الفورتي كلاينت امتداده MSI وليس exe (يتم تحويله عبر برنامج third party).

طريقة عمل integration بين الفورتي كلاينت و الفورتي جيت لكي نتمكن من عمل تحكم مركزي بكل الفورتي كلاينت عبر الفورتي جيت (تحديث من الفورتي جيت للأجهزة وجميع البيانات لتلك الاجهزه متواجدة في الفورتي جيت ...الخ)

- شروط عمل integrate بين الفورتي جيت و الفورتي كلاينت :

١- تفعيل خاصيه FortiClient access على الـ interface مثلا LAN1 وبذلك انت تسمح للأجهزة التي مثبت عليها الفورتي كلاينت من الوصول الى الفورتي جيت .



Authentication :

يتم استخدام الـ authentication في امن الشبكات .

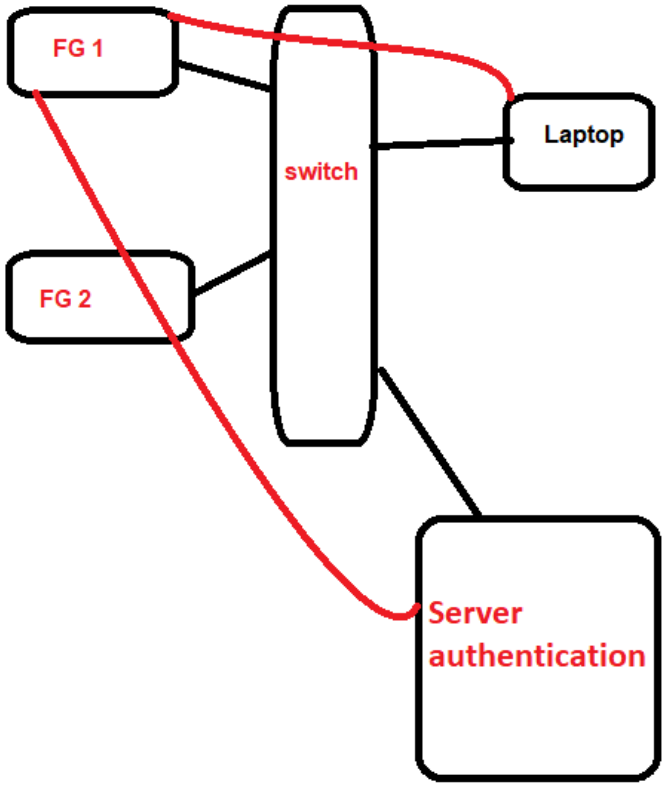
ماذا يقصد بعمليه الـ authentication ؟

يقصد بها المصادقة ويتم استخدام اليوزرنيم وكلمه السر للتأكد(التحقق) من هويه المستخدمين .. أي عمليه التأكد بأن الشخص الذي يستخدم اليوزرنيم والباسورد هو الشخص الحقيقي وذلك عبر الـ authentication .

❖ ماهي طرق الـ authentication (التحقق من الهوية) في الفورتي جيت :

➢ Local authentication :اليوزرنيم والباسورد المعتمد عليهم في عمليه المصادقة تكون مخزنه على جهاز الفورتي جيت نفسه

1- Server authentication :



في الشركات الكبيرة بتحتوي على اكثر من جهاز فورتي جيت فايروول بالشبكة فلو قام المستخدم بإدخال اليوزرنيم والباسورد فأن الفورتي جيت يقوم بارسال الطلب الى server authentication سواء كان هذا السيرفر (pop3,LDAP,RADIUS,TACACS+,) للتحقق من اليوزرنيم والباسورد الذي ادخله المستخدم .

1- Certificate authentication : يقوم جهاز الفورتي جيت بإصدار شهاده (RSAx 509)لجهاز الكمبيوتر التابع للكلاينت ياخذها الجهاز ويتحقق منها كلما يطلب مصدر من مصادر الشبكة

حيث الذي يقوم بإصدار الشهادة يسمى CA حيث CA ممكن يكون جهازكمبيوتر او جهاز الفورتي جيت وممكن تكون شركه خارجيه ..

: Two factor authentication -2

يحتوي على عامل إضافي بجانب الي وزنيم والباسورد حيث تعتبر مستوى اعلى من التحقق ..

هذا العامل اسمه الـ token لرفع مستوى الحمايه .

الـtoken معناها رمز..

حيث الفورتي جيت بيستخدم طريقة الـ token بانه بيقوم بتوليد OTP(one time password) وهي عباره عن باسورد إضافية يجب ان أقوم بإدخالها بعد ادخال اليوزرنيم والباسورد الأولى .

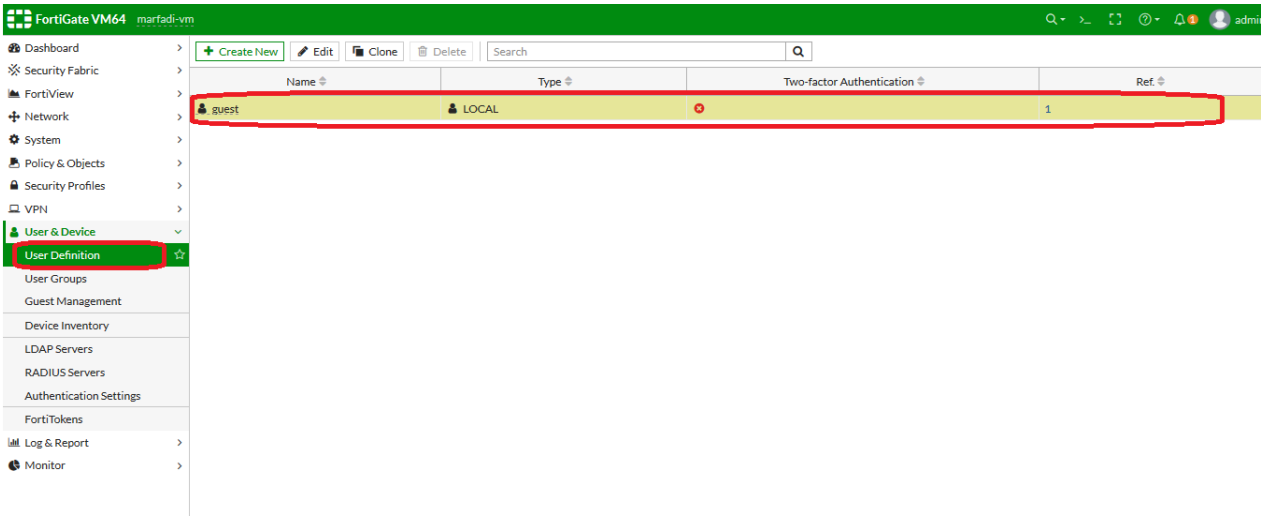
حيث الباسورد الثانية سيقوم جهاز الفورتي جيت بتوليدها كل 60 ثانية ويرسلها على جهاز اخر مثلا SMS او ايميل حيث بعد ادخال اليوزرنيم والباسورد وبالباسورد الثانية المرسله عبر SMS او غيرها سيتم عمل تحقق وتأكد من عمليه الـ authentication وبعدها سيسمح لك بالوصول الى مصادر الشبكة لو كانت العملية تمت بنجاح ..

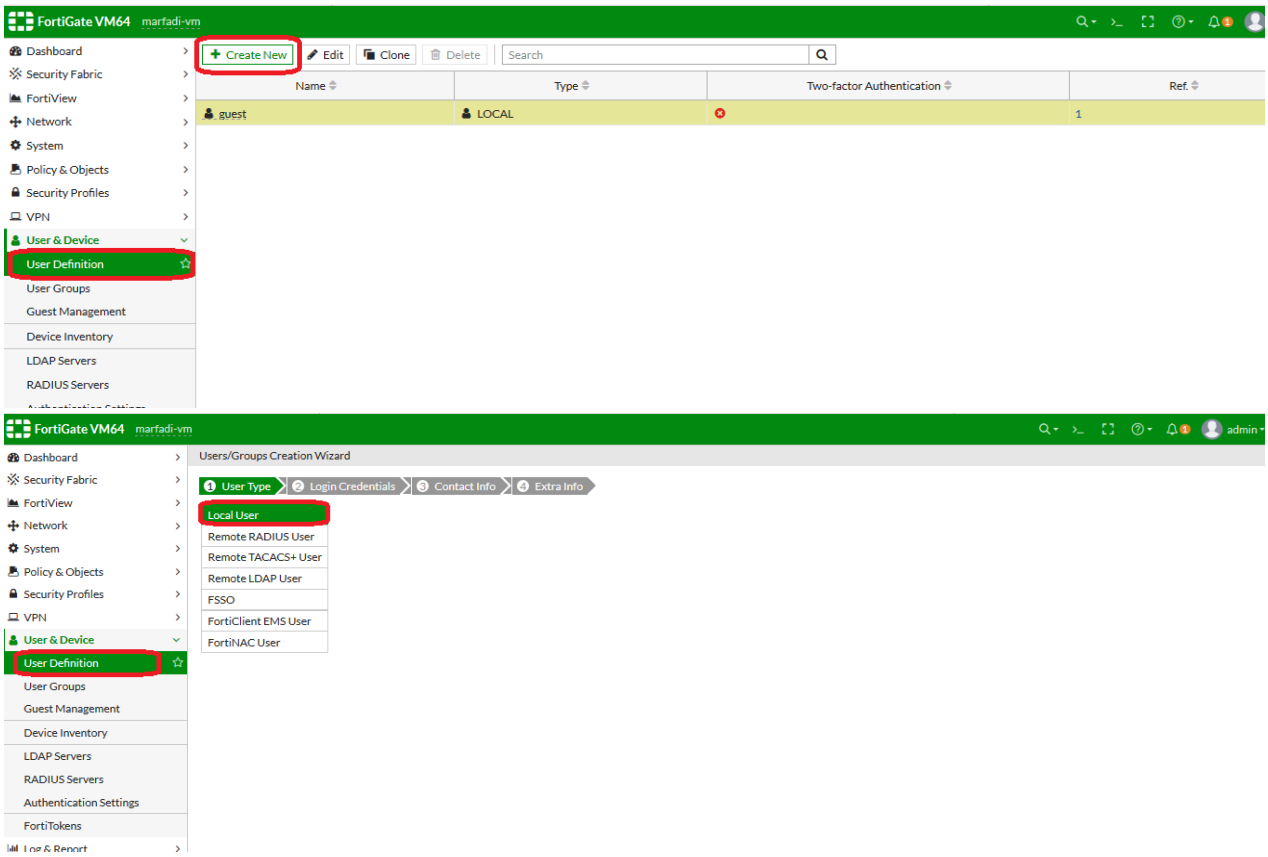
حيث أصبحت العملية معقده على الهاكر على الاختراق ..

Local authentication

طريقة عمل local authentication على الفايروول .

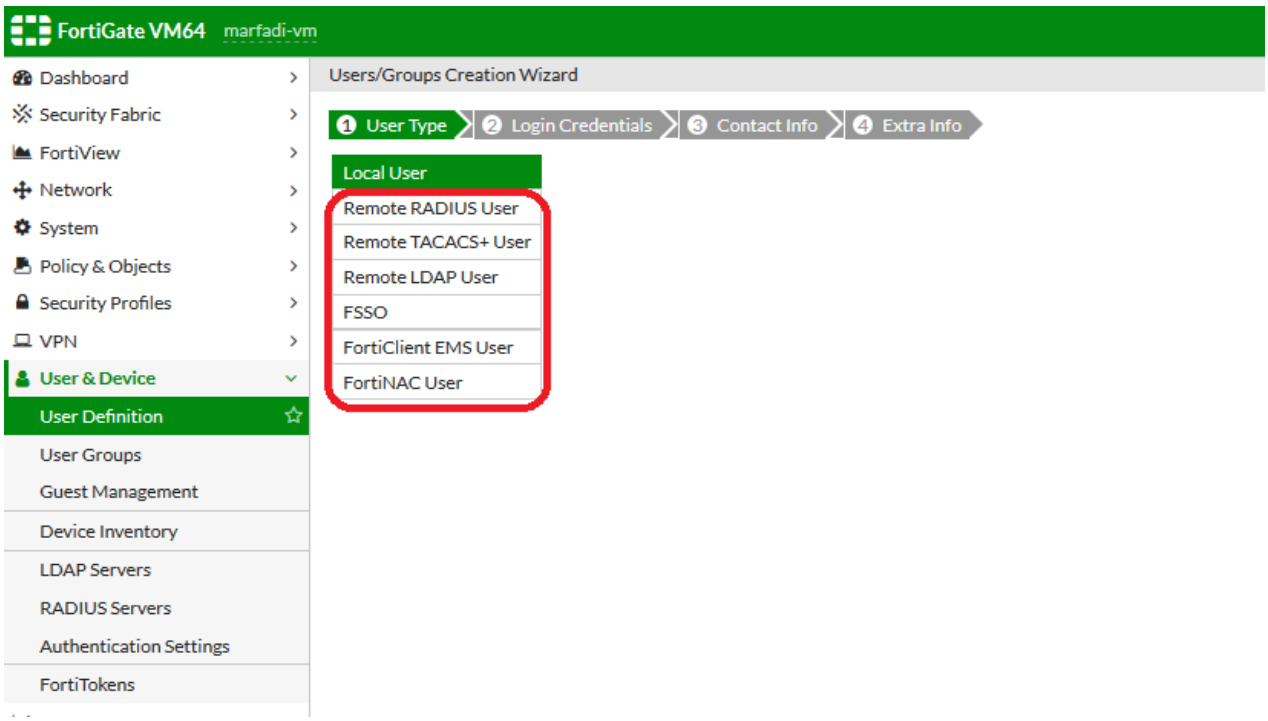
أولا سنقوم بإنشاء حسابات محليه (يوزرنيم وباسورد)على الفورتي جيت حيث بشكل افتراضي يكون لدينا يوزرباسم Guest ونوعه local كما بالصورة ادناه





حيث سنختار نوع اليوزر الذي نريد انشاءه هو local user (أي ان اليوزر نيم والباسورد موجودين على الفورتي جيت نفسه)

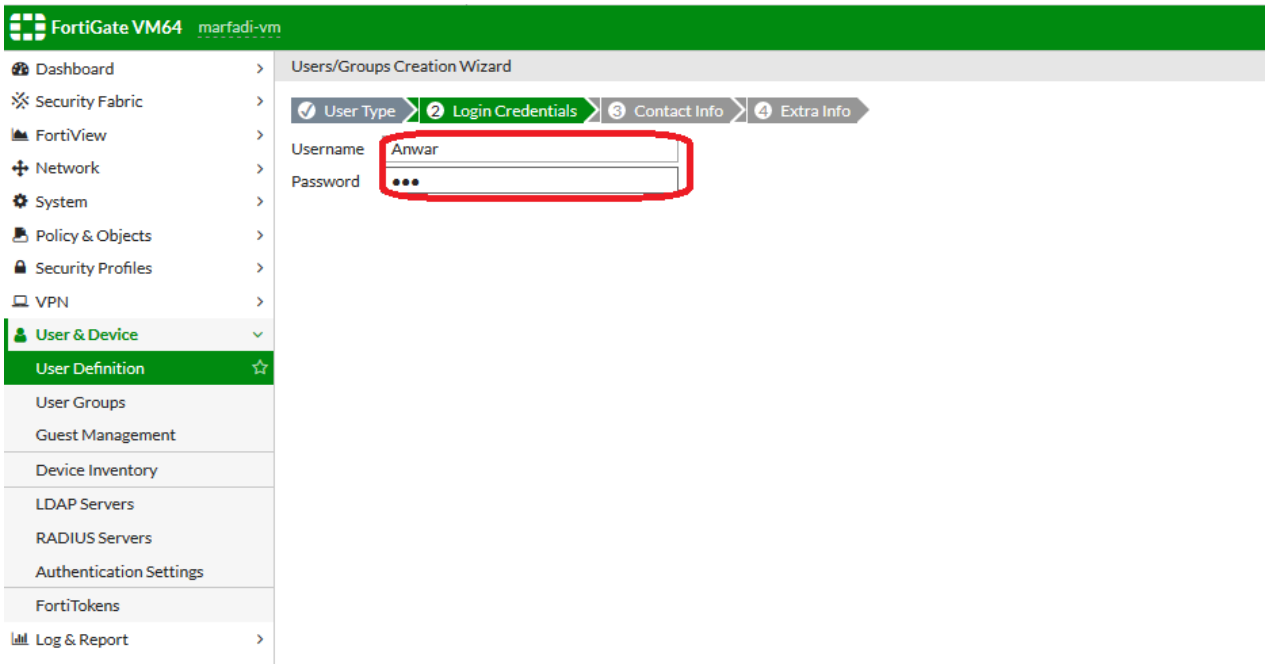
او تريد انشاءه باي أنواع أخرى :



حيث كل يوزر من الأنواع أعلاه سوف تكون له اعدادات معينه ..

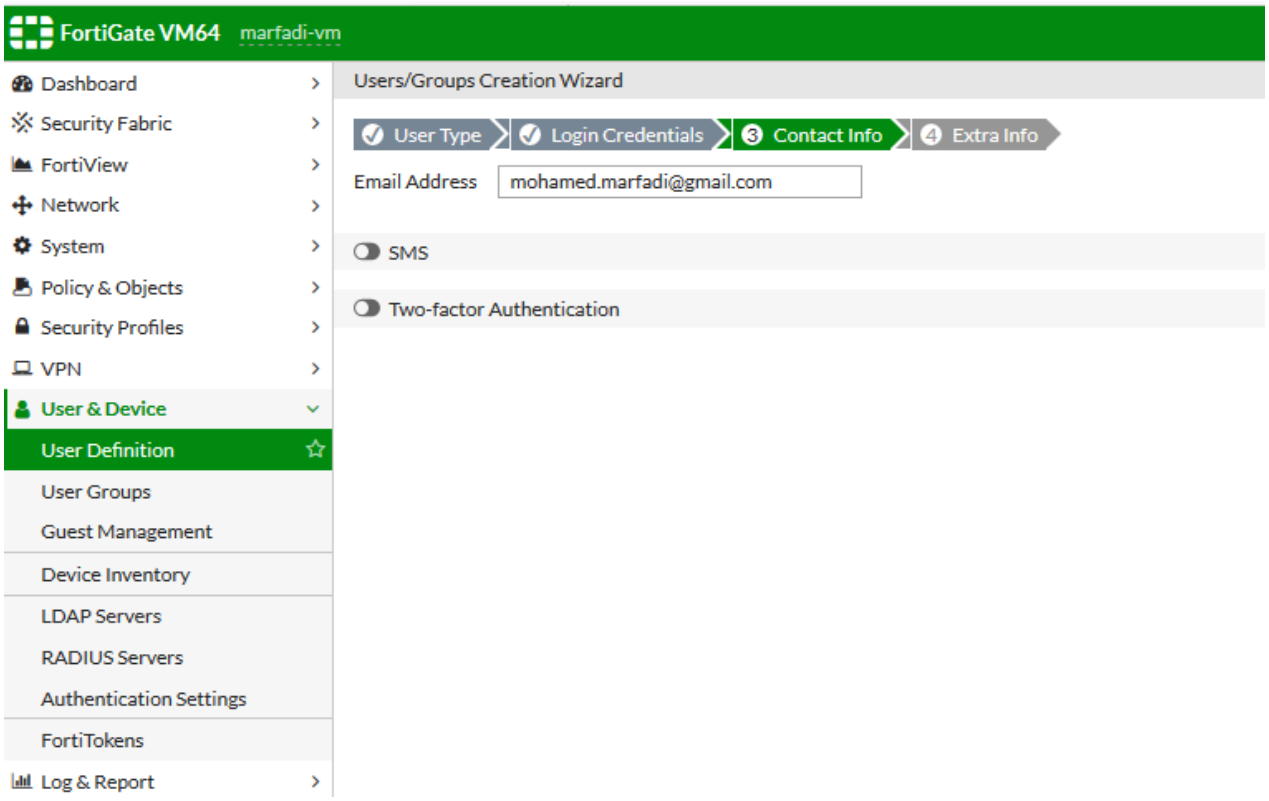
نحن الان سنختار النوع الأول Local User .

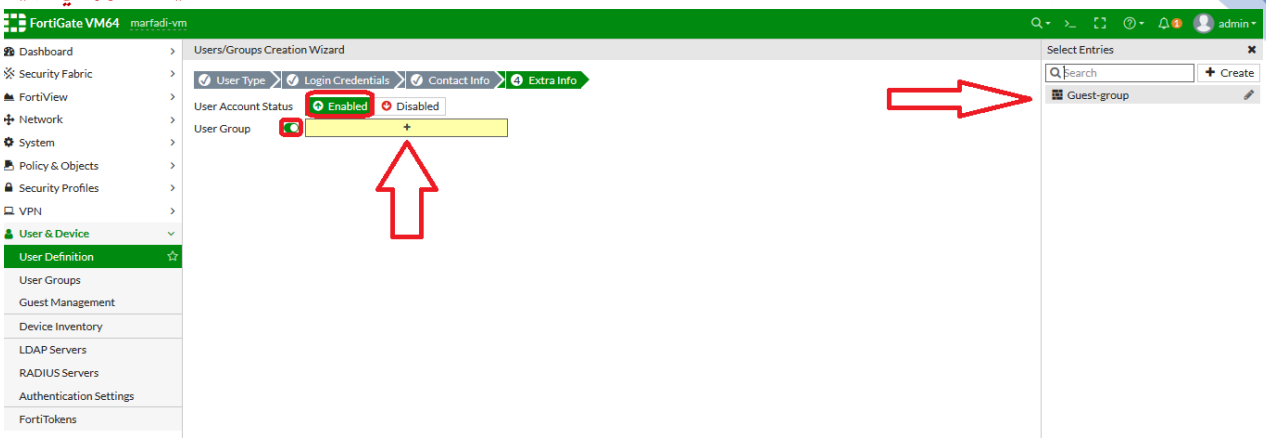
حيث بعد ذلك سنكتب اليوزرنيم والباسورد التي سنعتمد عليهم في عمليه المصادقة بعد ذلك ..



ثم لو تريد تحديد ايميل لهذا اليوزر حيث لو لديك اشتراك من فورتي جارد لـ Messaging services

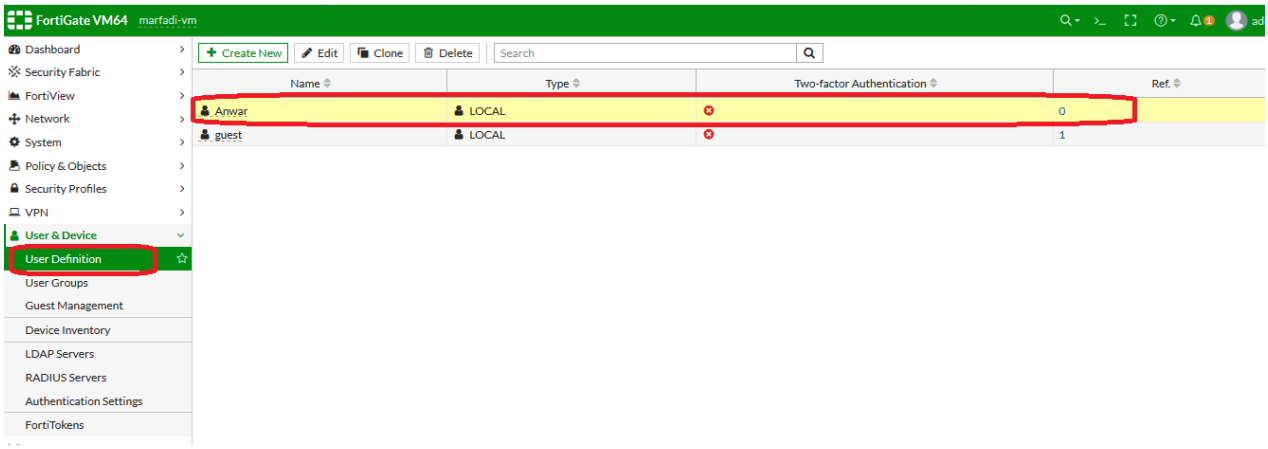
فيمكنك استخدام خاصيه الـsms ويمكنك تخطي خطوه الايميل والـ sms .



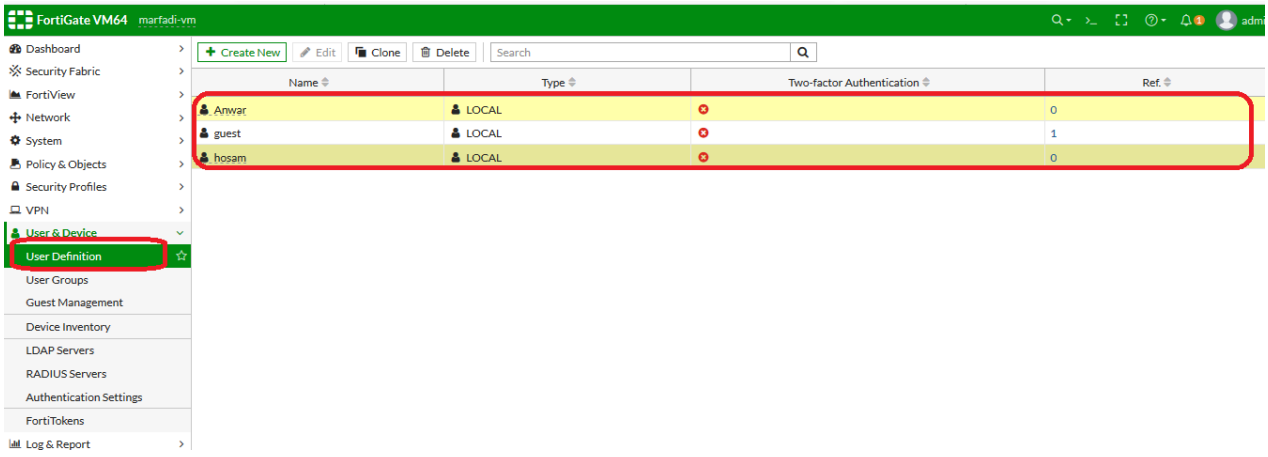


كما بالصورة أعلاه نعمل Enable لهذا اليوزرولو تحب نضع هذا اليوزرلأي مجموعة منشأه مسبقا (User group).

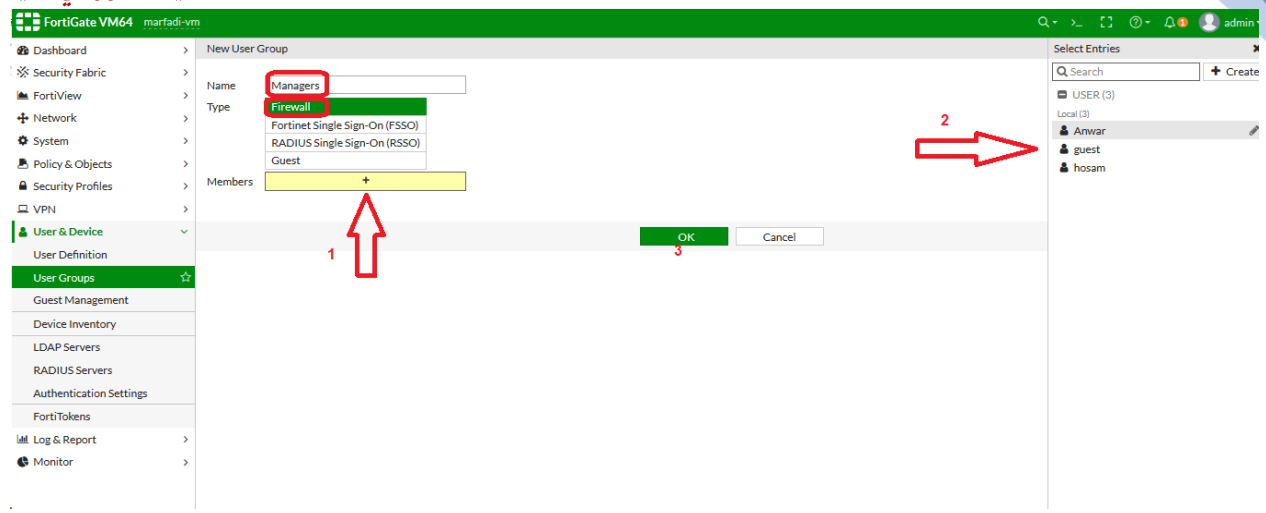
ثم ننقرعلى الزر Submit لأتمام عمليه الانشاء ..

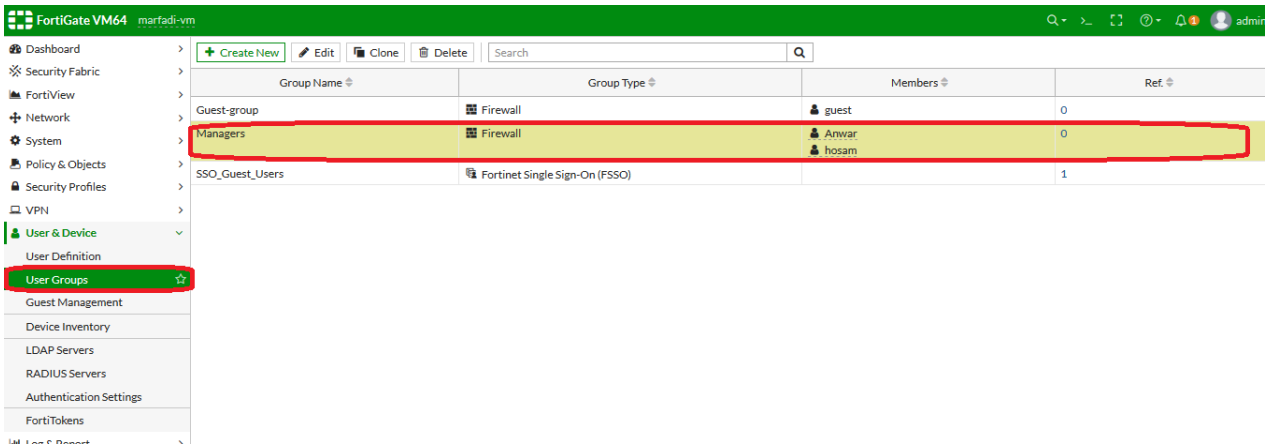


تم الانشاء اليوزرAnwar وبنفس الطريقة تم انشاء يوزرباسم hosam كما بالصورة ادناه



طريقة انشاء user group باسم Managers ونوعها Firewall واضافة اليوزرات السابقة الى هذه الجروب .





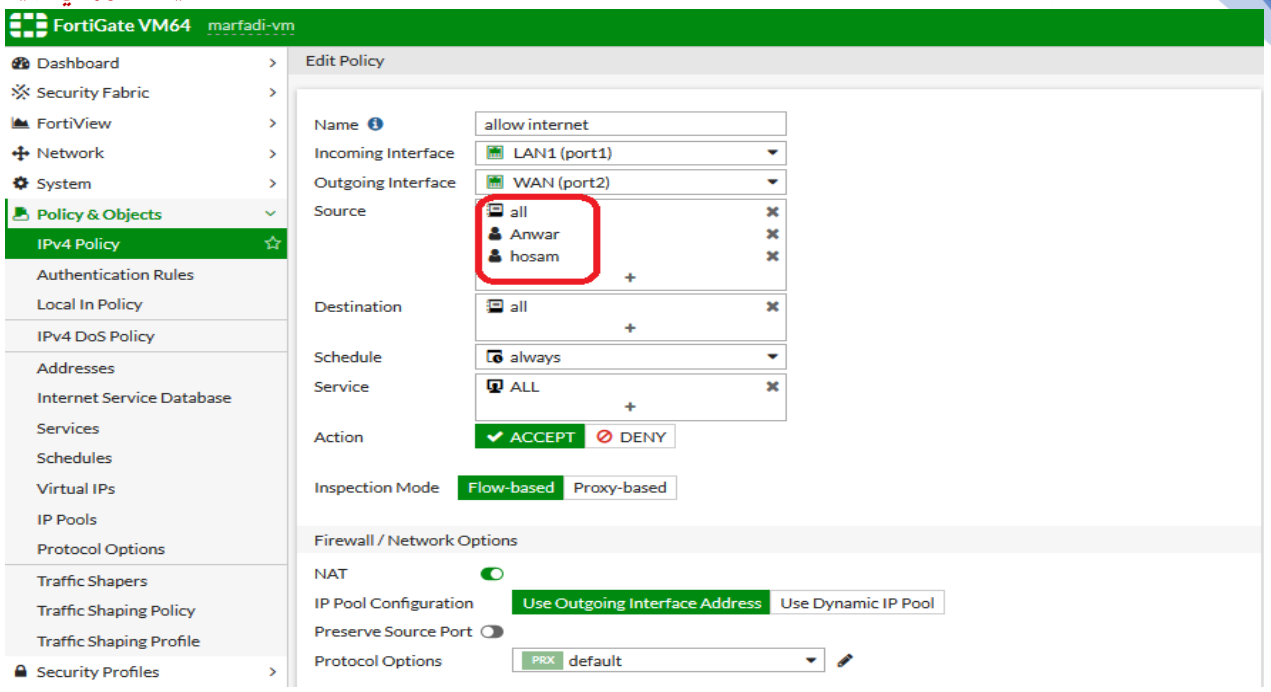
حيث ممكن للموظفين بالشركة استخدام اليوزرات أعلاه بدلا عن الايبي ..

حيث عند تطبيق البوليسي حنختار اليوزروسوف استخدمها في عمليه الـ authentication .

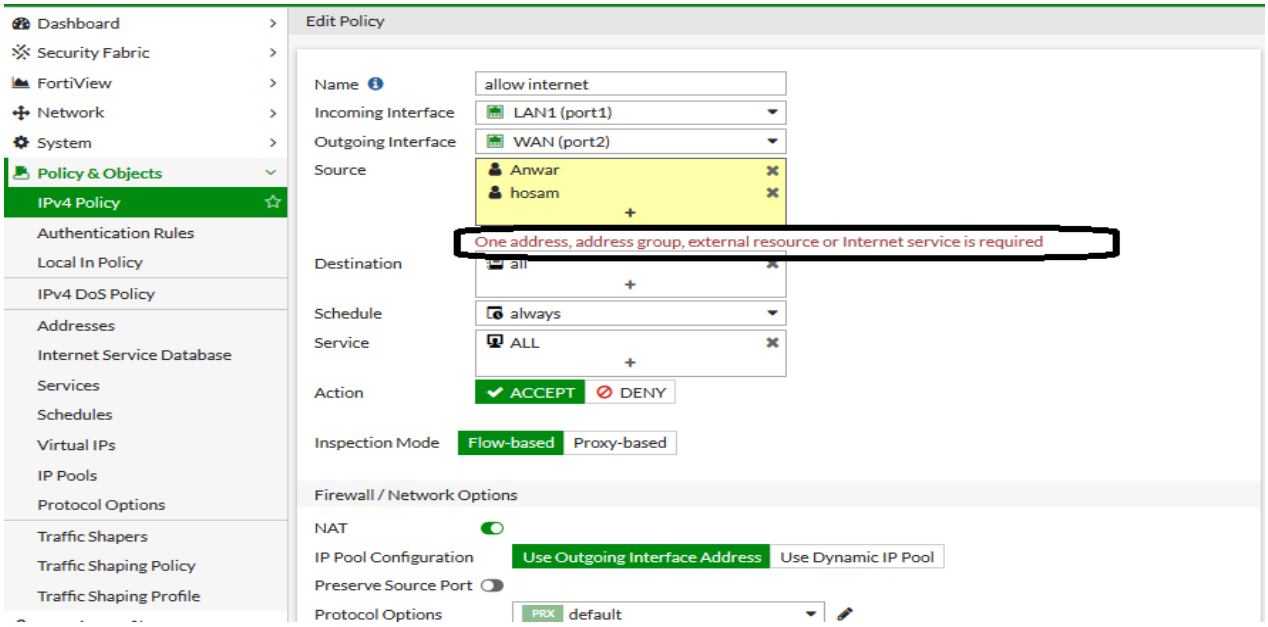
أي اني اريد المستخدمين يطلعوا على الانترنت عن طريق اليوزرنيم والباسورد وليس عن طريق الايبي ..

حيث لن يحصل الجهاز على الانترنت مالم يقوم بفتح متصفح الانترنت ويظهر لك واجهه (portal) ويكتب اليوزرنيم والباسورد .

الآن سوف نقوم بإنشاء بوليسي بيسمح للموظفين بالحصول على الانترنت بشرط يكون لديهم local users فقط وليس عن طريق الايبي ..

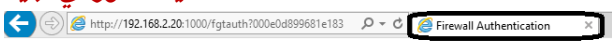


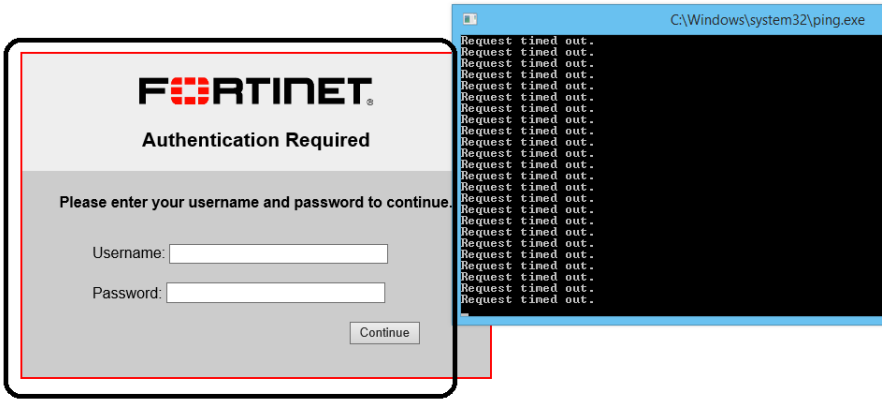
ملاحظة:تم أضافه العنوان all وبهذا يصبح (Anwar+hosam/all) طبق البوليسي ليوزرات معينه من ال all وهو ضروري لكي يتم قبول البوليسي لأنه يجب على الأقل وجود عنوان (address) والأ سوف يظهر لك رساله الخطأ التالية :



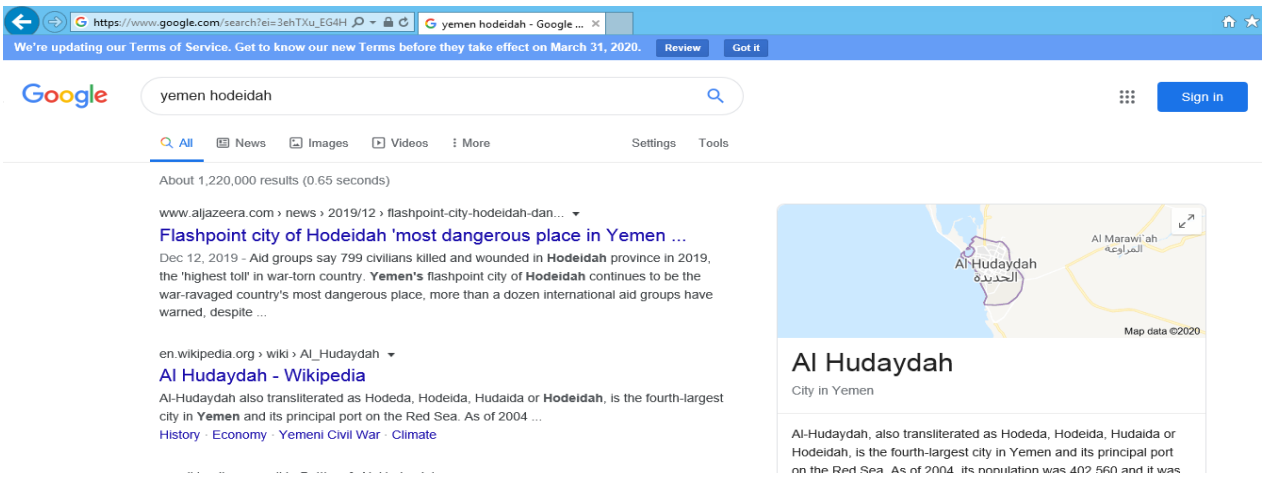
وأيضا ممكن اختيار الجروب المسماة Managers والتي تحتوي على اليوزرات (hosam+Anwar)بدلا من اختيار اليوزرات واحد واحد

الآن نقوم بالدخول الى احدى اجهزه الشبكة الداخليه فنلاحظ بأن الانترنت ليس موجود حاليا على الجهاز

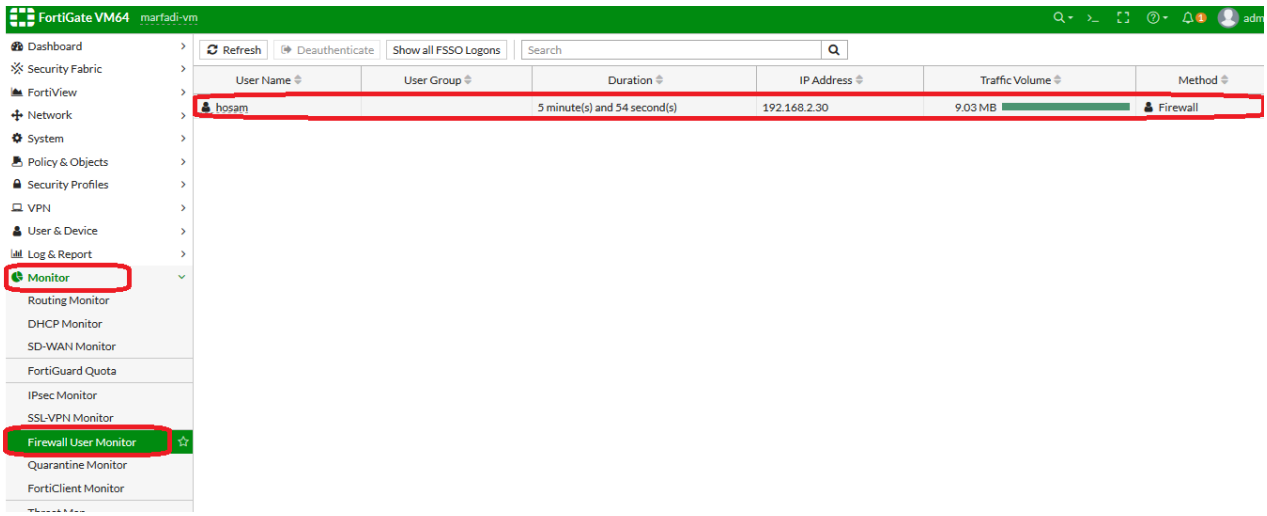




وبمجرد فتح متصفح الانترنت نلاحظ ظهور واجهه فسنقوم بإدخال يوزرنيم وباسورد hosam والباسورد 123 والذي قمنا بإدخاله سابقا وبعد ذلك يصبح الجهاز قادر على الوصول الى الانترنت حتى بعد اعاده تشغيل الجهاز..

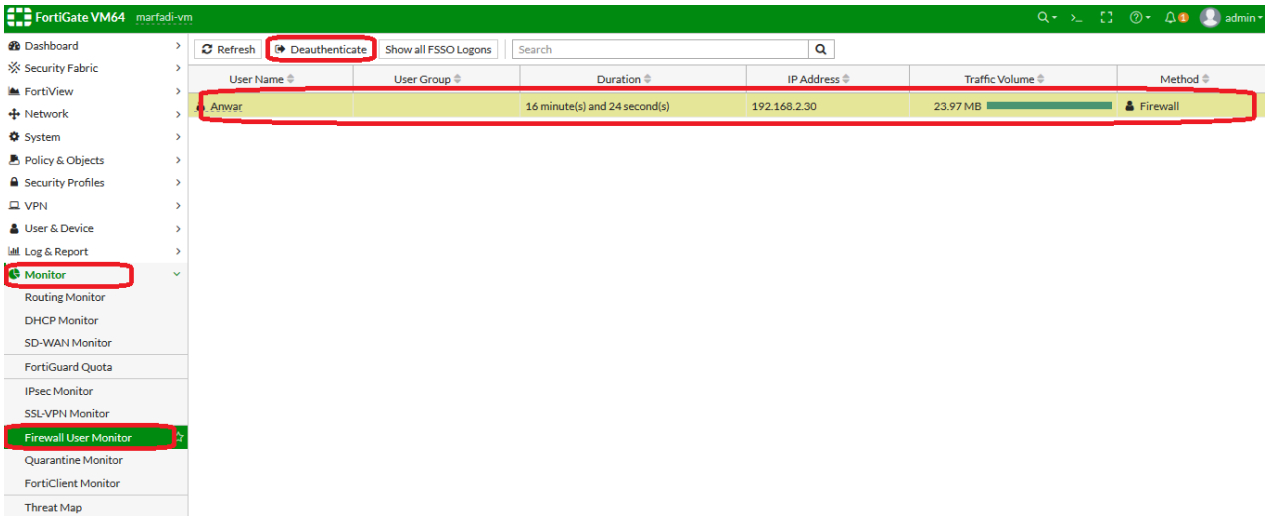


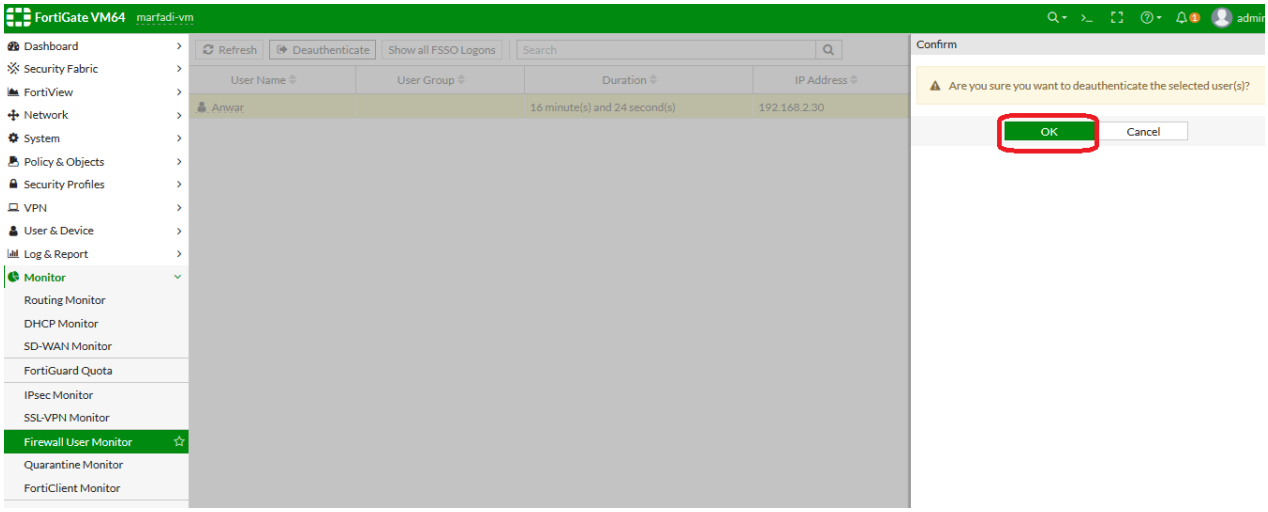
ولمعرفة اليوزرات التي تمكنت من الوصول الى الانترنت من نوع local users

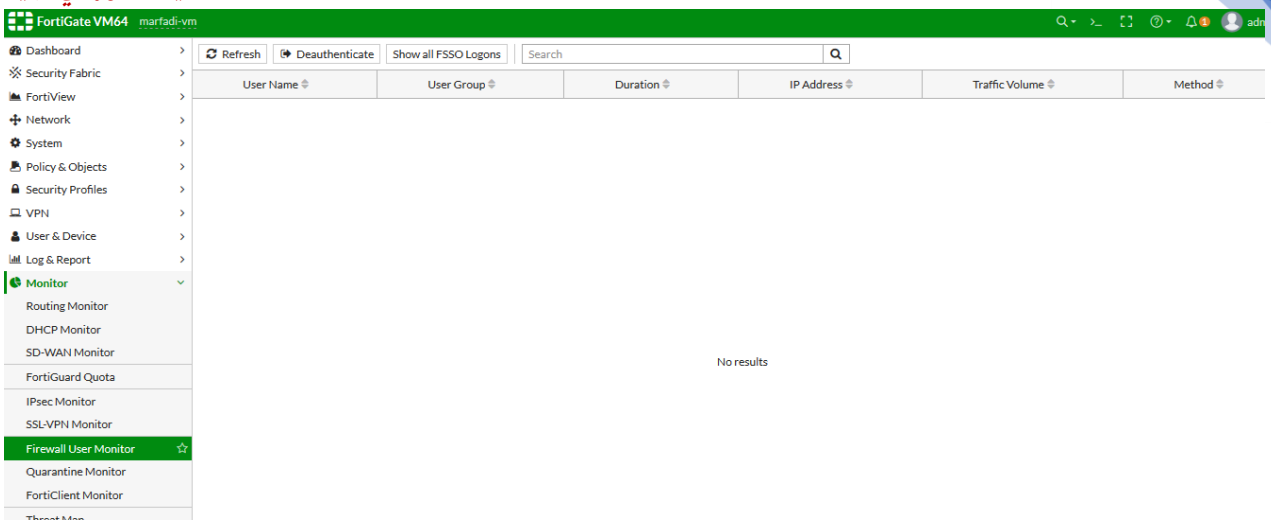


نلاحظ تم دخول اليوزر hosam والايبي الخاص به هو 192.168.2.30 وتم استخدام 9 ميجا من الترافيك ونوعه firewall .

طريقة الغاء المصادقة (authentication)ليوزر معين من يوزرات الـ local user وبذلك لن يستطيع الجهاز الوصول الى الانترنت مالم يقوم بعمل المصادقة وإدخال اليوزرنيم والباسورد مره أخرى على متصفح الانترنت ..

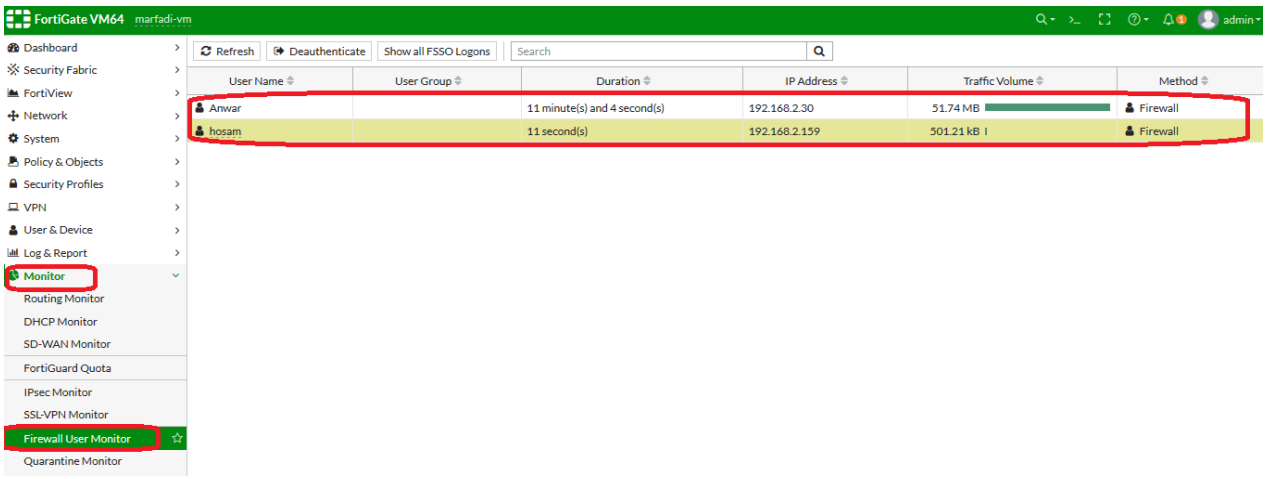






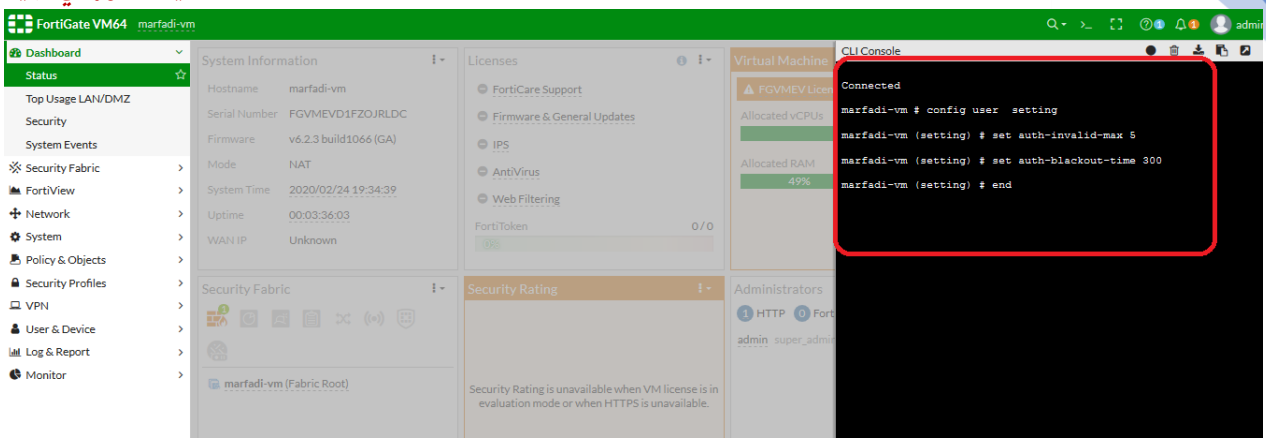
اصبح الان لا يوجد أي يوزر من نوع (local user) firewall ..

بمجرد ادخال اليوزر نيم والباسورد على الجهاز من قبل المستخدم يتم أضافته على القائمة firewall User Monitor كما بالصورة التالية :



Max invalid authentication

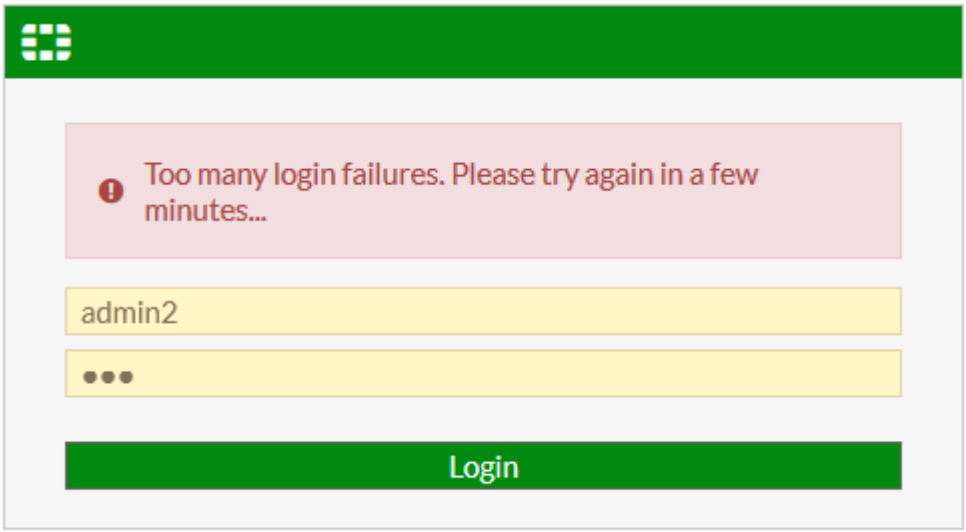
يجب تطبيق سياسه للحد من عدد المحاولات الخاطئة(يوزر نيم او باسورد خطأ) المسموح فيها بعد ذلك نقوم بتطبيق عقوبه بأنه سوف يكون غير مسموح لهذا اليوزر لوقت معين من ادخال اليوزر نيم والباسورد .



مثلا بعد 5 محاولات ادخال خاطئه فأننا نقوم بإغلاق الحساب

لمده 300 ثانية(5 دقائق) .

اي ان اليوزرلن يتمكن من المصادقة لأن البورتال (نافذه اليوزرنيم والباسورد لن تظهر خلال 5 دقائق)

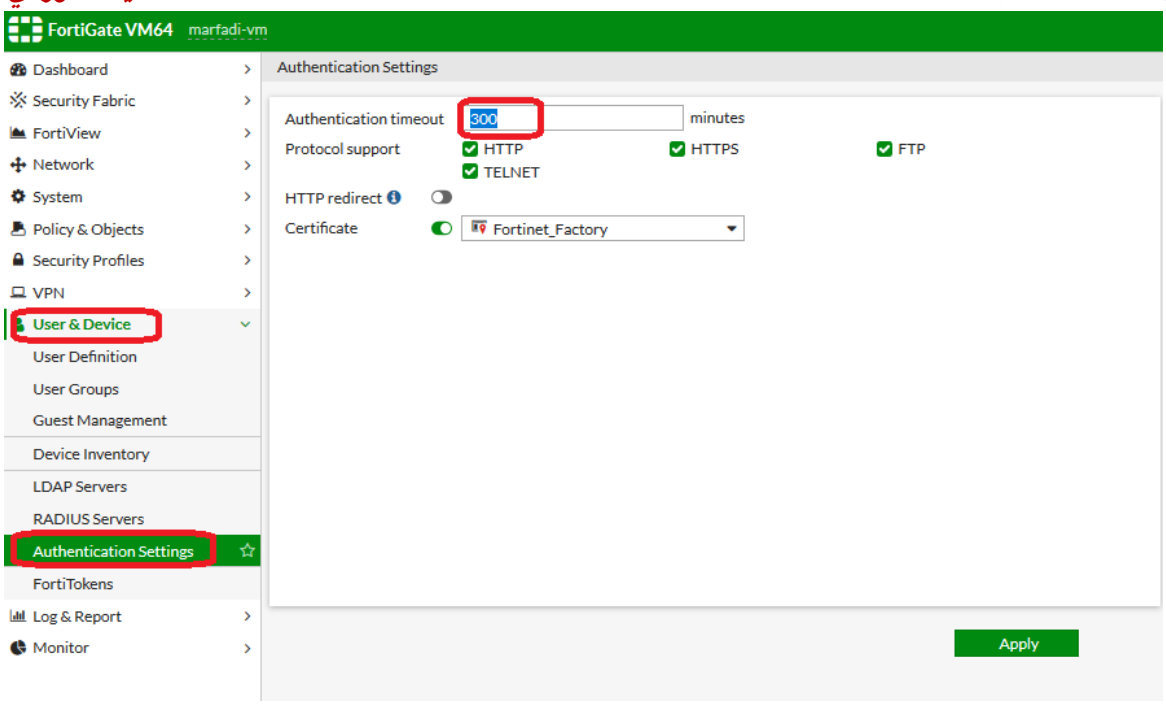


Authentication timeout

السياسة الأخرى التي يتم تطبيقها على local users اسمها Authentication timeout بأن لو لم يستخدم الانترنت خلال فتره معينه فأنه يجب ان يعمل

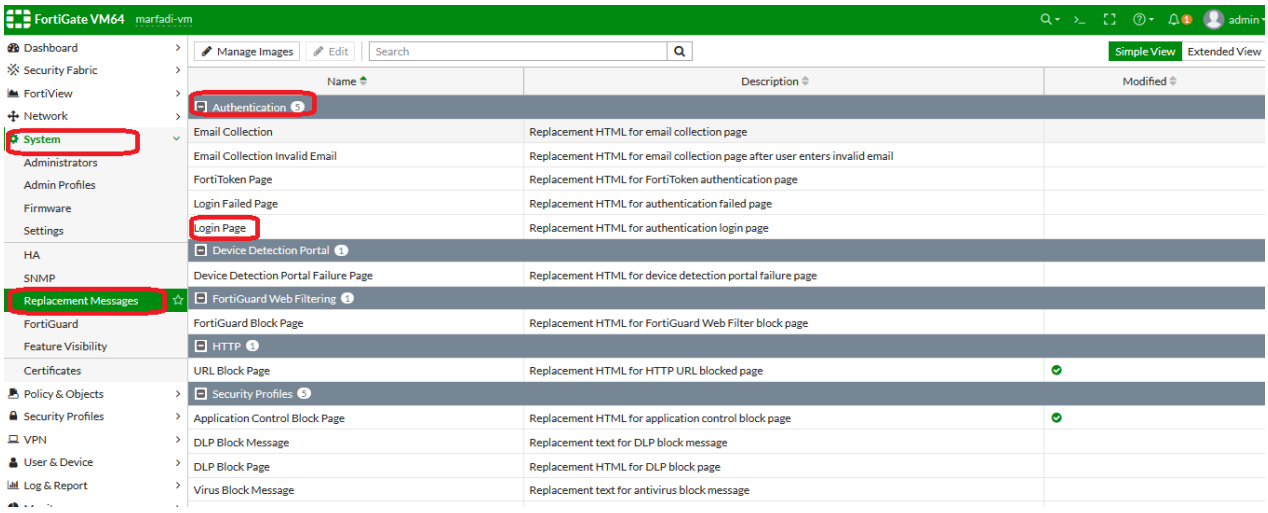
re-authentication مره أخرى .

حيث الافتراضي بعد 300 دقيقه بدون ان يقوم اليوزرباستخدام الانترنت فيجب عليه ادخال اليوزرنيم والباسورد مره أخرى ..

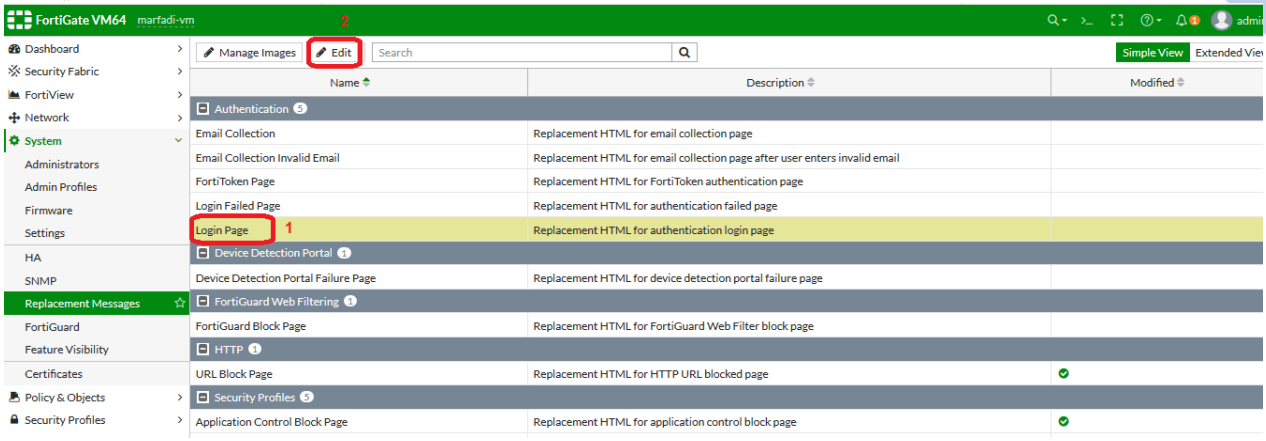


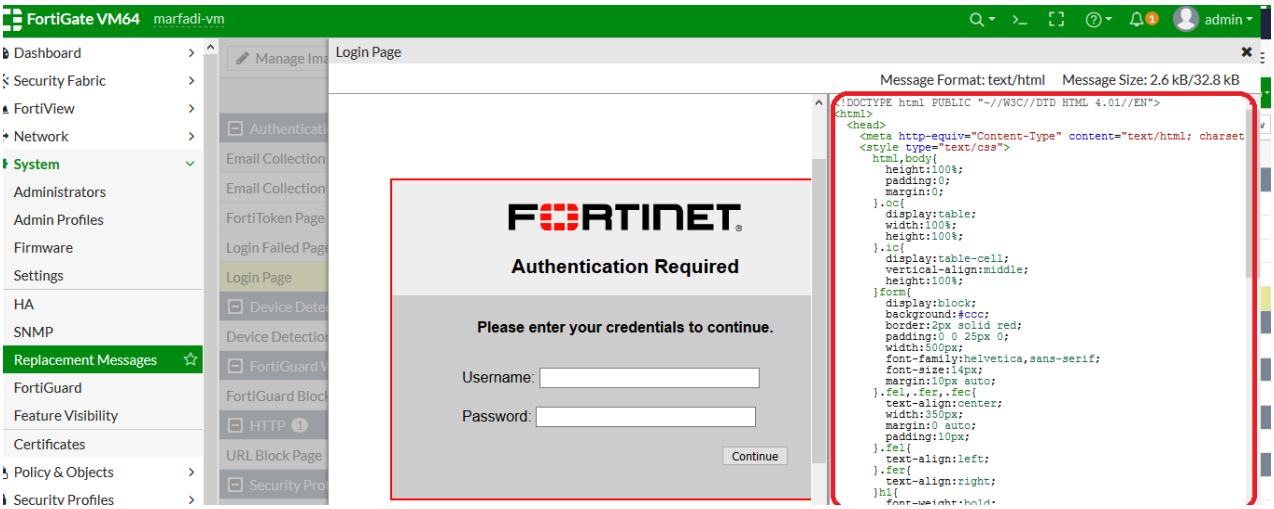
طريقة تعديل الـ replacement message حيث أي رساله تظهر بالفورتي جيت يمكنك تعديلها ،

الآن سنقوم بتعديل الرساله التابعه لـ authentication وتحديدا الشاشة Login Page وأيضا شاشه Login failed Page في حالة انك أدخلت يوزرنيم او باسورد خطأ .



نحدد الشاشة المراد تغيرها ثم edit

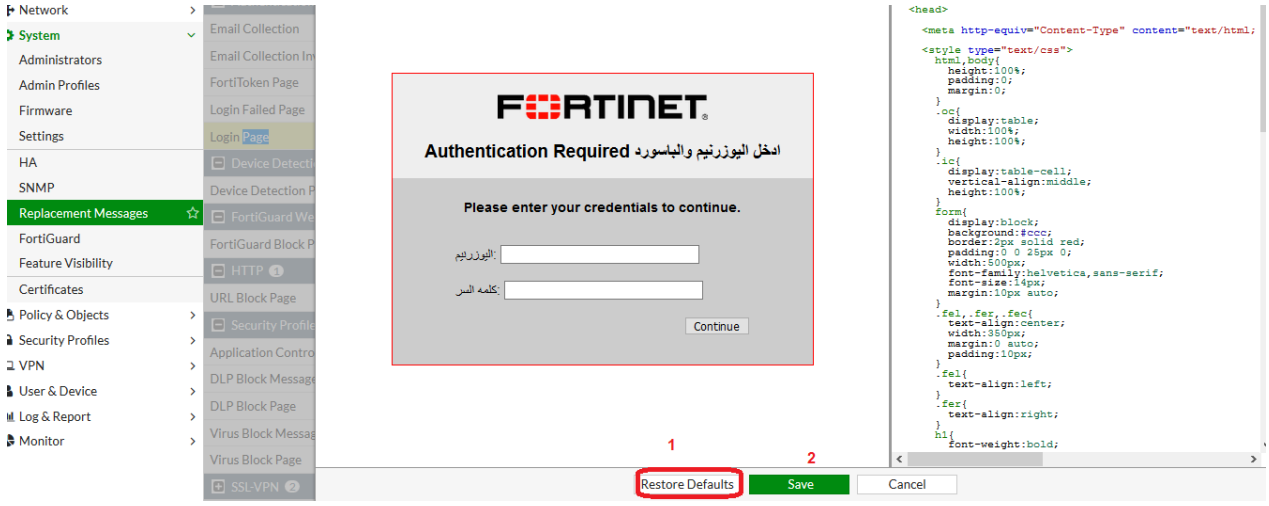




ثم نقوم بتعديل ما نريده بكل سهوله ..

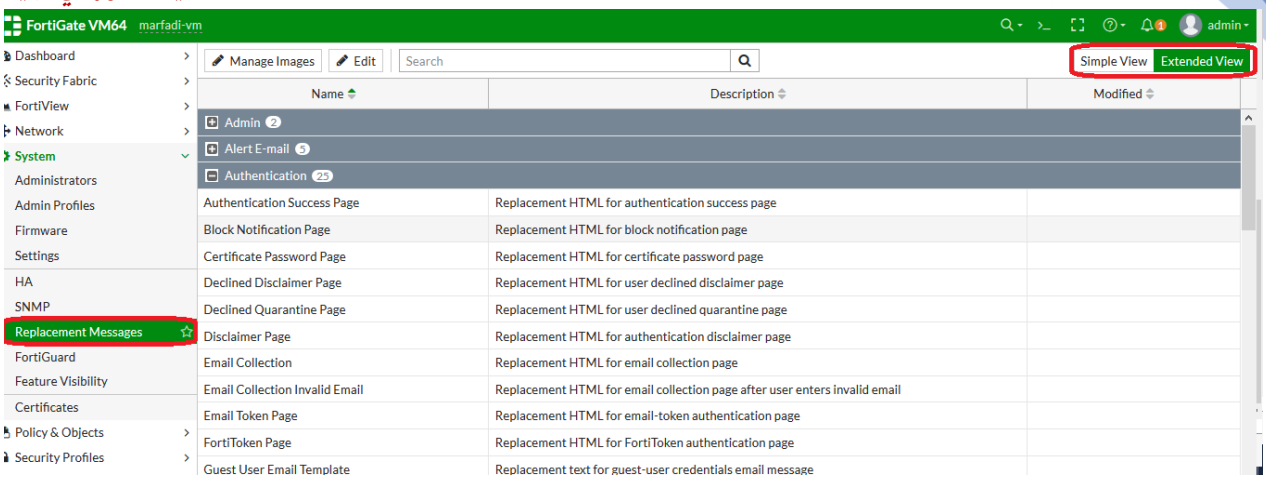
ونلاحظ الشاشة بعد التعديل

ولو تريد ارجاع الشاشة كما كانت فنقوم بعمل restore defaults ثم save



ملاحظة :

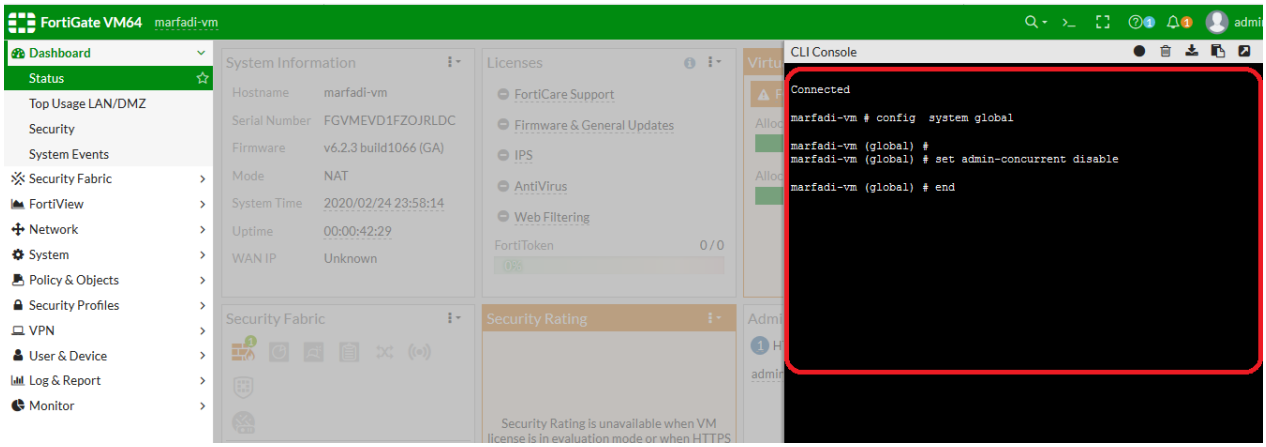
يوجد خيارين لآظهار الرسائل بالفورتي جيت هما extend view والأخر Simple View حيث الخيار Extend view بيظهر كل الرسائل على مستوى الفورتي جيت اما simple View فيظهر لك الرسائل الأساسية فقط..



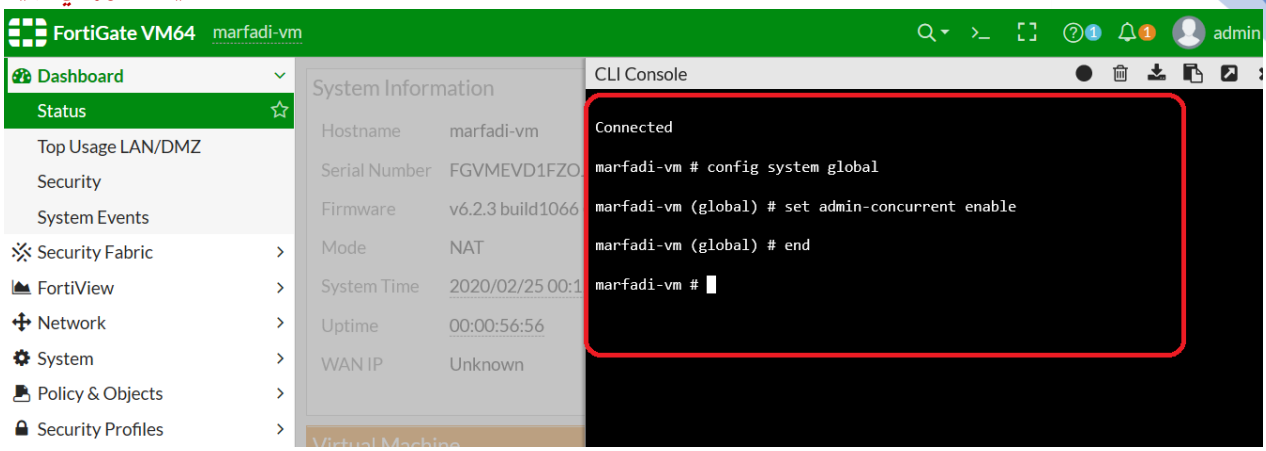
Restricting number of concurrent user logons

كم عدد الـ sessions الذي مسموح الـ administrator يقدروا يعملوا login على الفورتي جيت او session واحده فقط عبر الويب ،حيث الوضع الطبيعي بأنه مسموح لعدد session غير محدود ..

لتقييد الدخول الى الفورتي جيت لأكثر من administrator (تحدد session واحده فقط)كنوع من الـ security وذلك عبر الاوامر التالية :



ولو اردت اعادتها كما كانت كما بالصورة ادناه..



Managing guests

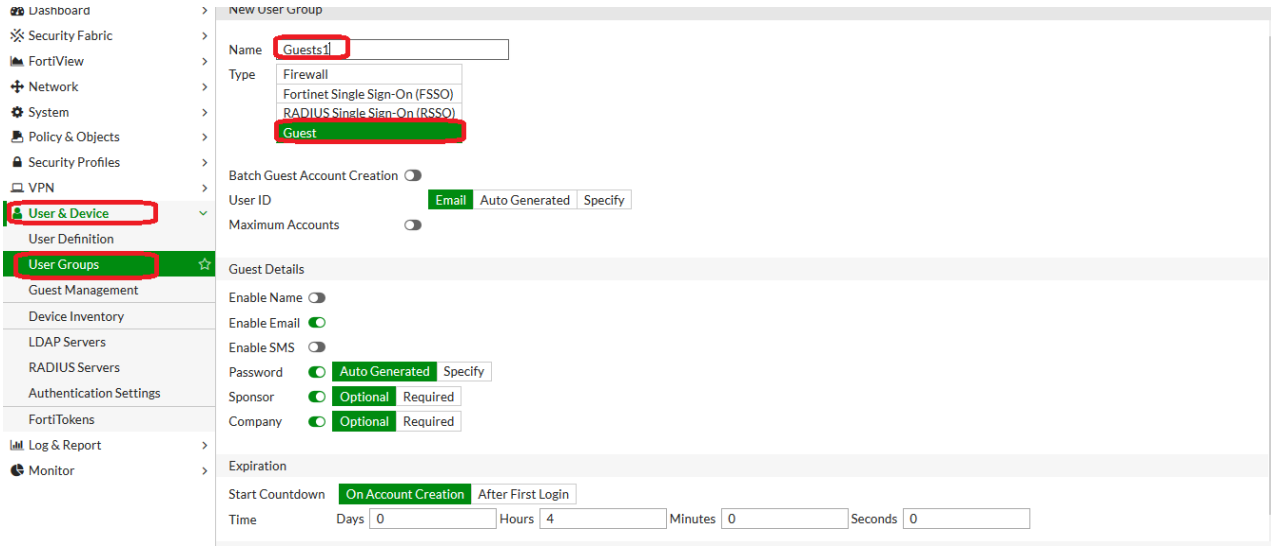
هي عباره عن اداره الزوار القادمين للشركه حيث يكونوا لفتره مؤقته فقط حيث يمكن لجهاز الفورتي جيت ان يعطيك حسابات مؤقته تنتهي بعد فتره معينه .

حيث سيتم انشاء حسابات لهؤلاء الزوار بشكل عشوائي عبر الفورتي جيت نفسه او بنفس الايميلات الشخصيه لكل زائر او نقوم بتخصيص حسابات بشكل يدوي .

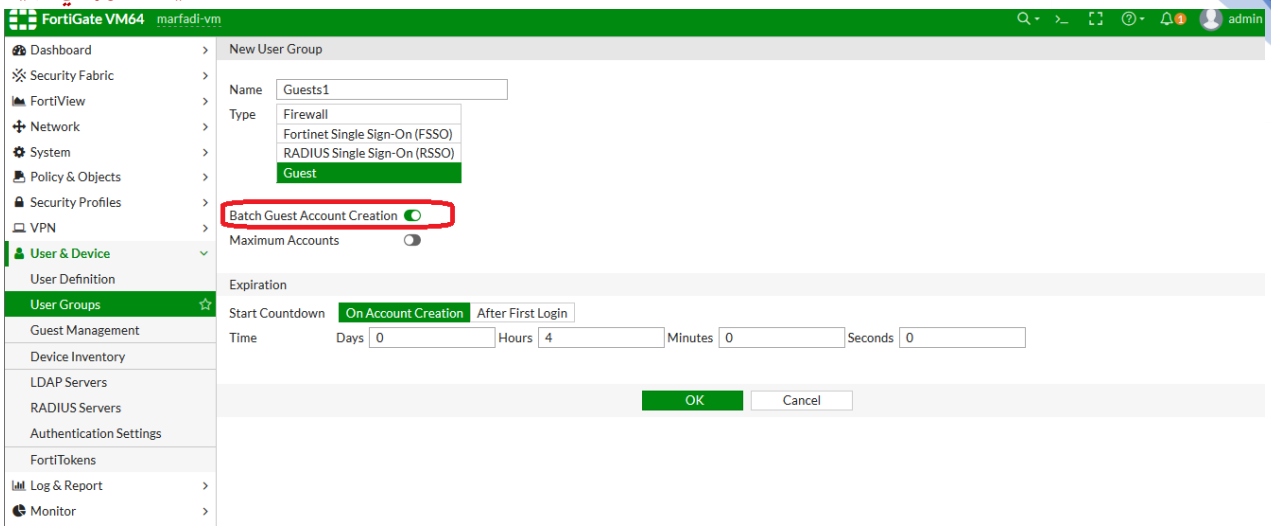
وسيتم تسليم الزائر لحساباتهم اما عن طريق طباعه الحسابات او ارساله بالايميل او عبر SMS .

لكي أقوم بعمل هذا الشي يجب تخصيص جروب للزوار (Guests group) تحتوي على عدد من الحسابات .

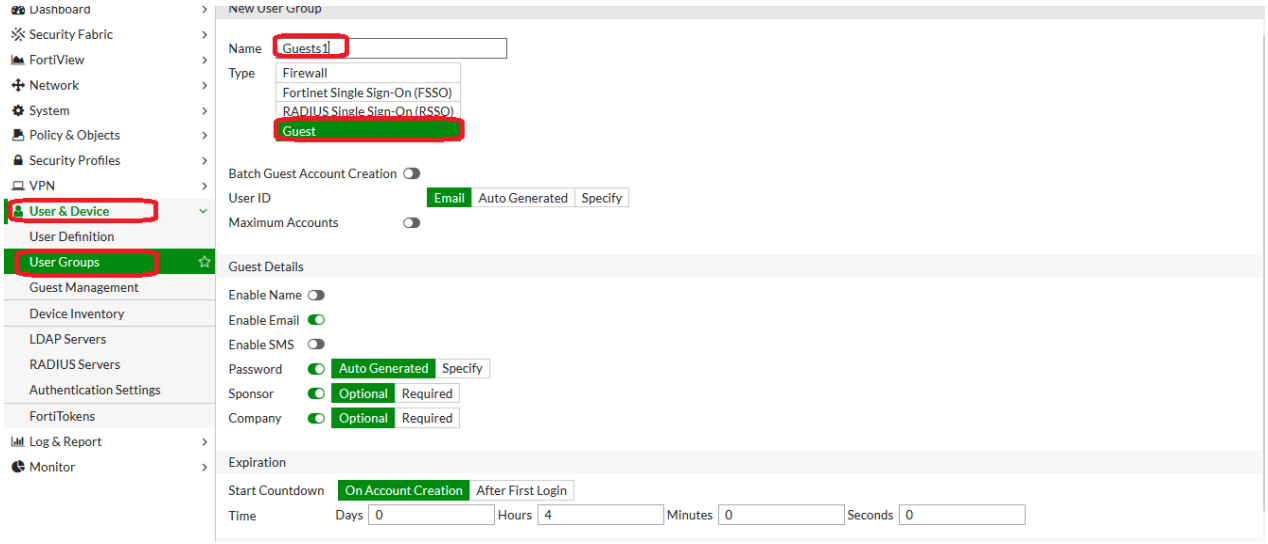
نقوم الان بإنشاء جروب باسم Guest1 ونوعه guest



حيث لو كان عددهم كبير جدا فانك سوف تقوم بتفعيل الخيار Batch Guest Account Creation



الان سوف نقوم بإنشاء الحسابات بشكل منفرد وليس مره واحده لذا لن نقوم بتفعيل هذا الخيار



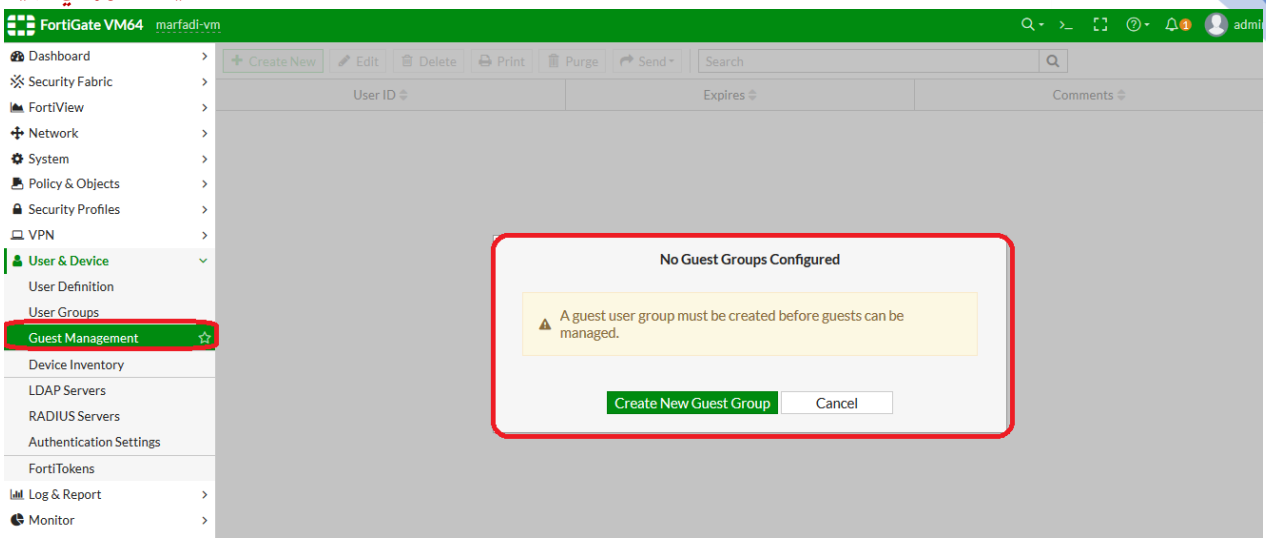
لذا سوف تقوم باختيار نوع الـUser ID بحسب الخيارات التالية:

Email :حيث يكون اسم حساب الزائر هو نفسه ايميل الزائر.

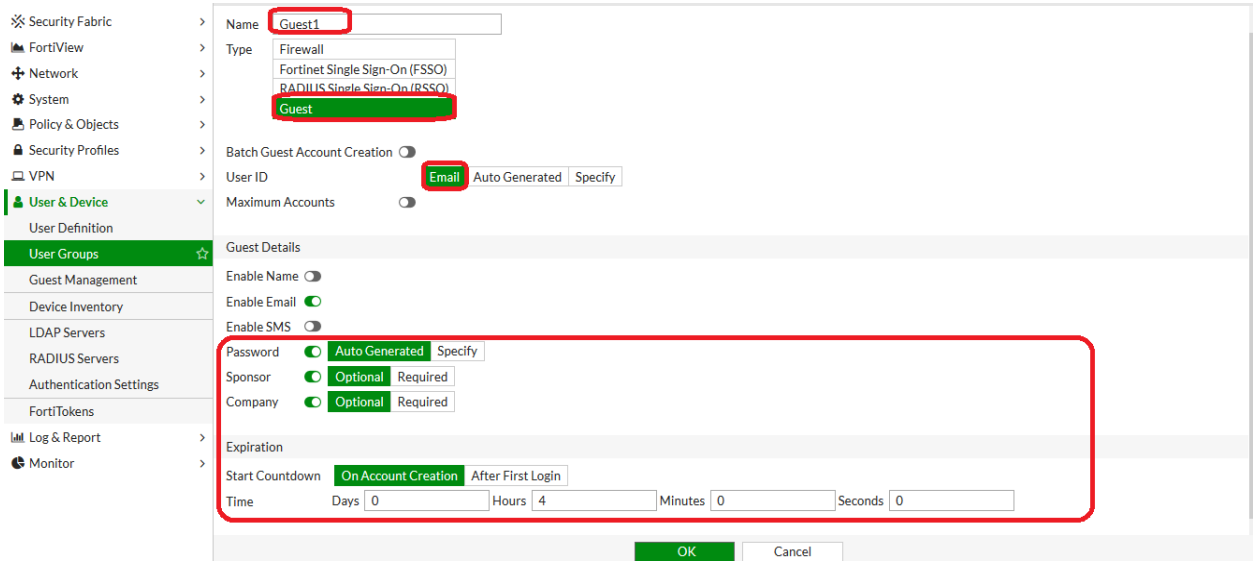
Auto generated :أي ان الفورتي هو الذي سوف يقوم بإنشاء أسماء الحسابات(اليوزرات)بشكل اوتوماتكي .

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 أولا لذا لو حاولت الدخول الى Guest management قبل انشاء الجروب سوف تظهر لك رساله تحذيريه كما بالصورة التالية :



لذا أولا قم بإنشاء الـGuest group بالنوع الي تريده مثلا email او auto generated او specify مثلا سوف نختار النوع Email

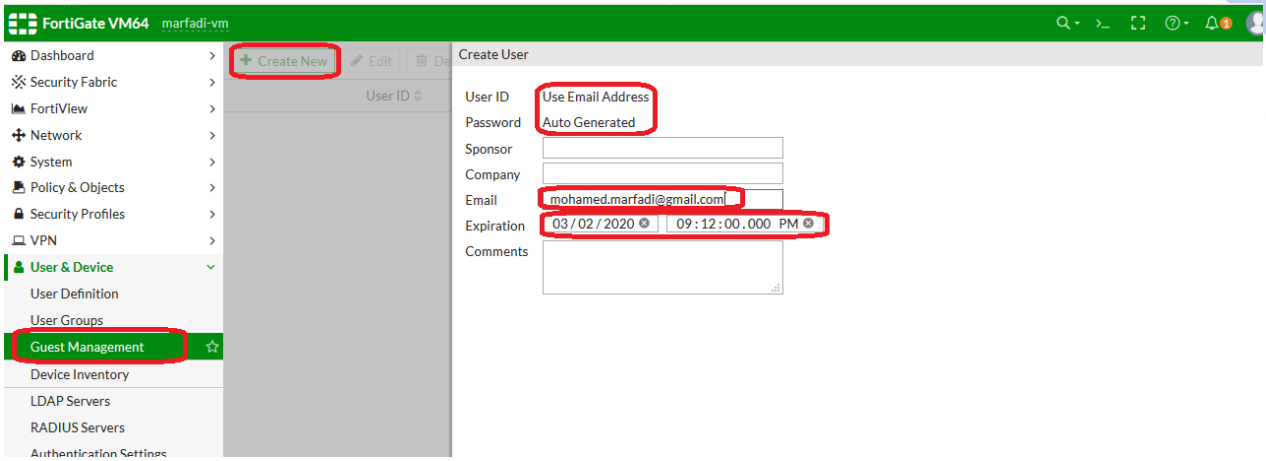


نلاحظ كما بالصورة أعلاه بأننا اخترنا بان الباسورد سوف يتم توليده بشكل اوتوماتيكي عبر الفورتي جيت(Auto Generated)وبأنه سوف تكون نهاية الحساب بعد 4 ساعات من وقت انشاء الحساب ..

لذا عند انشاء الحساب سوف يكون الid هو نفسه الايميل الخاص بالزائر

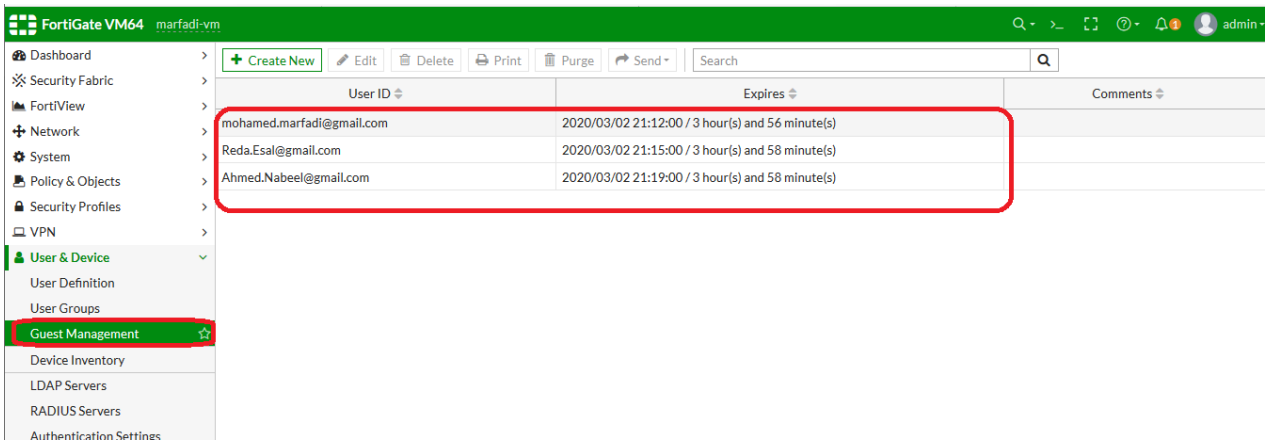
ملاحظة:

لو قمت بجعل Password=disabled فان عند انشاء اليوزر لن يطالبك بالباسورد ابدا ..

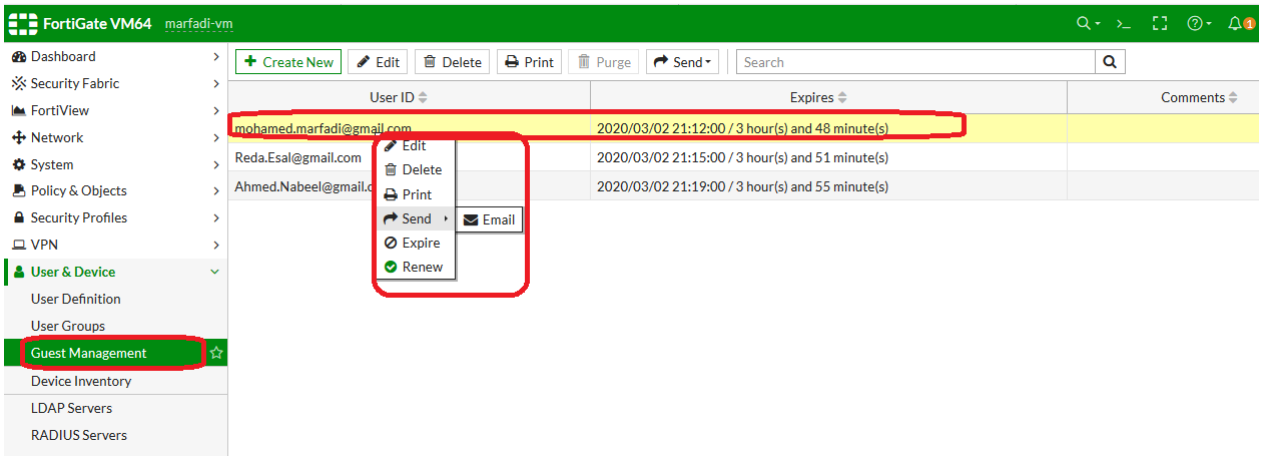


كما بالصورة أعلاه يتبين بأن الـUser Id هو عباره عن ايميل الزائر ويجب ان تقوم بكتابته مثلا Mohamed.marfadi@gmail.com في الخانه Email والا لن تتم عمليه الانشاء لهذا الحساب ويتبين بأن مده انتهاء الحساب بعد 4 ساعات .

حيث سيتم ارسال الحساب على ايميل الزائر المحدد أعلاه بشرط انك تكون قد فعلت بأن الفورتي جيت يمكنه الارسال عبر الايميل..



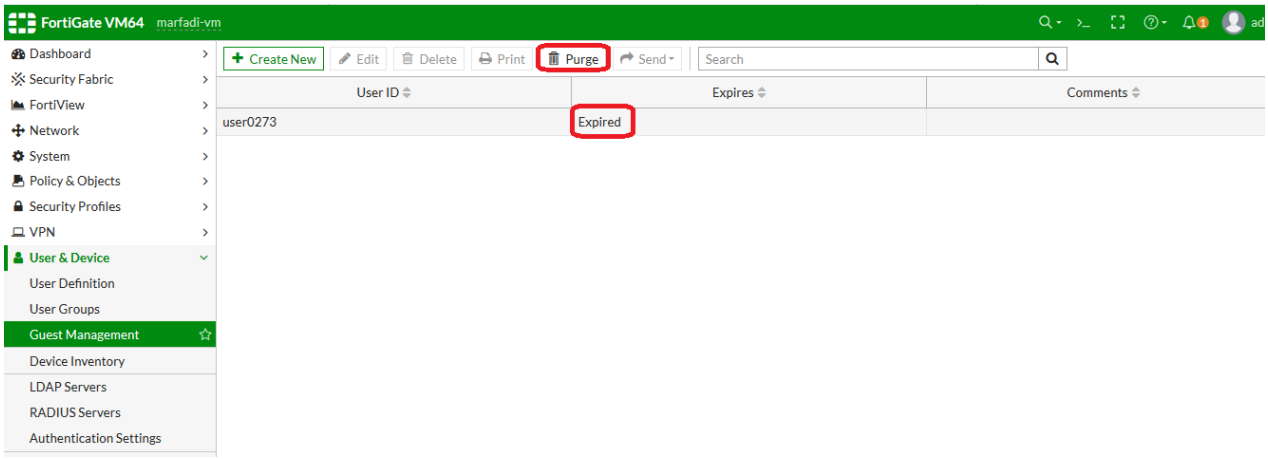
حيث قمت بإنشاء الحسابات بحسب الايميل كما بالصورة اعلاه ..



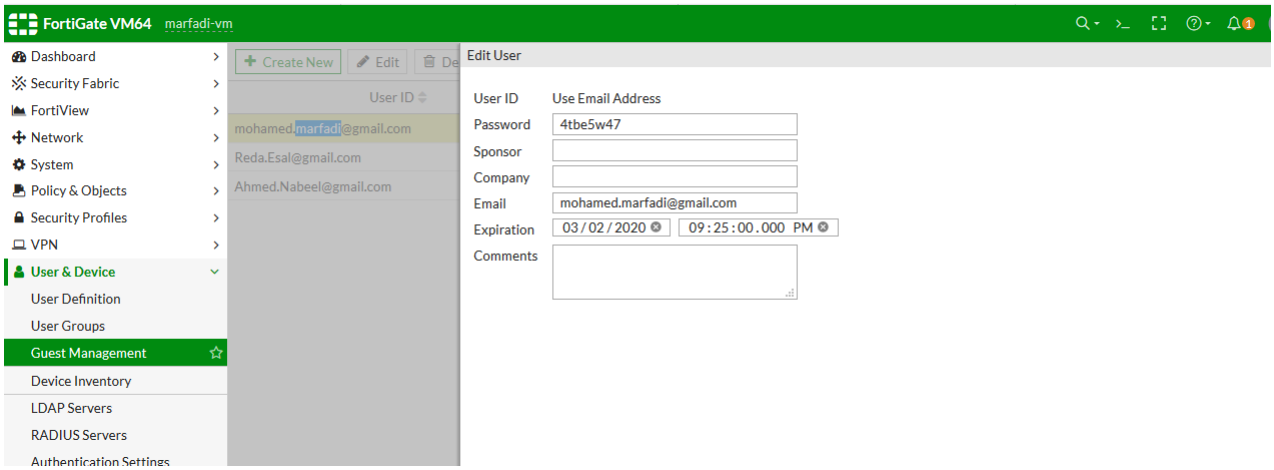
يمكنك التحكم بالحساب من حيث ارسال الباسورد الى ايميل الموظف او مده انتهاء الحساب فورا او حذف الحساب او التعديل عليه او تجديد مده الحساب ...

وهناك خيار اسمه purge حيث عند النقر عليه يقوم بحذف كل الحسابات التي انتهت مدتها ويتبقى لك الحسابات التي لازالت valid .

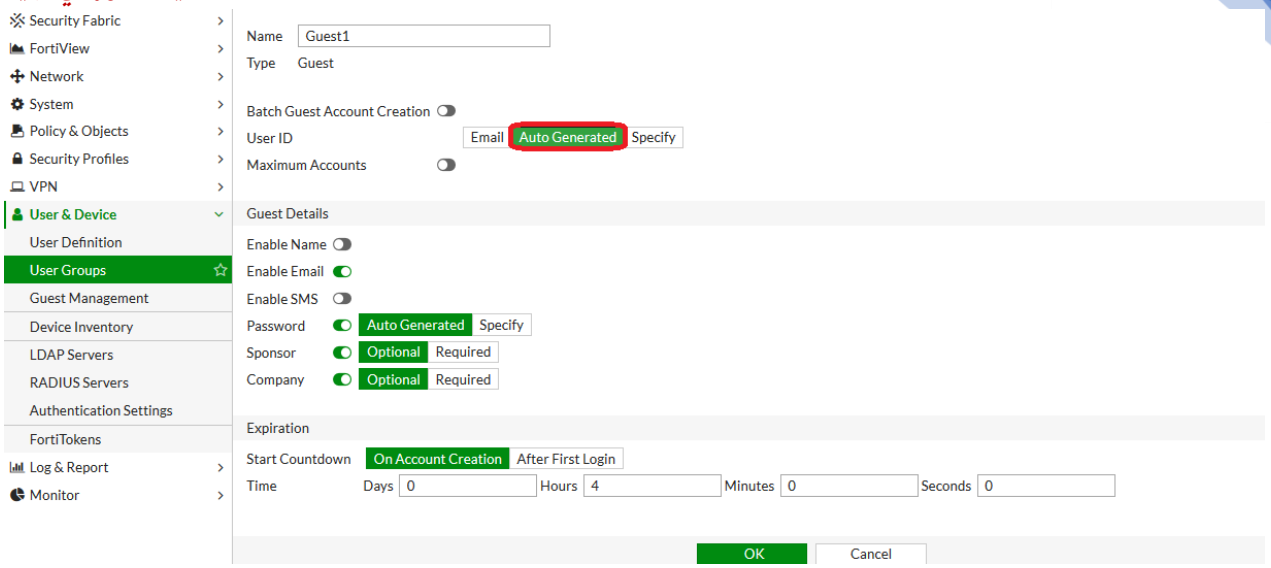
حيث نلاحظ بأن الخيار Purge لا يفعل الا لو كان هناك حسابات منتهيه كما بالصورة ادناه



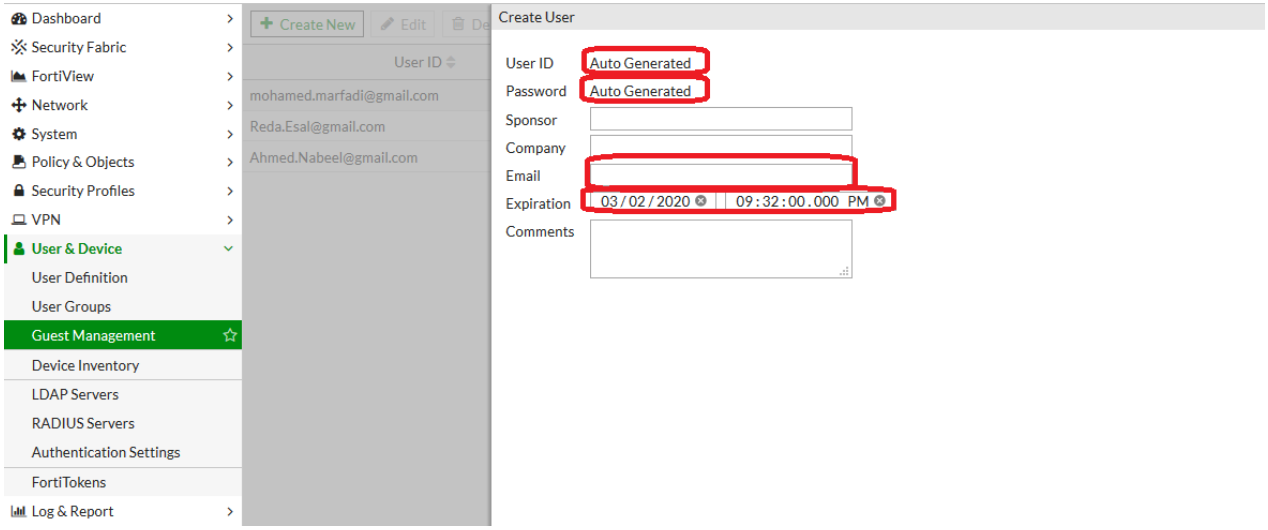
ولمعرفة الباسورد الذي قام الفورتي جيت بتوليده بشكل اوتوماتيكي نقوم بالنقر على الحساب نقرتين بزر الفاره الايسر وسوف يظهر لك كما بالصورة ادناه



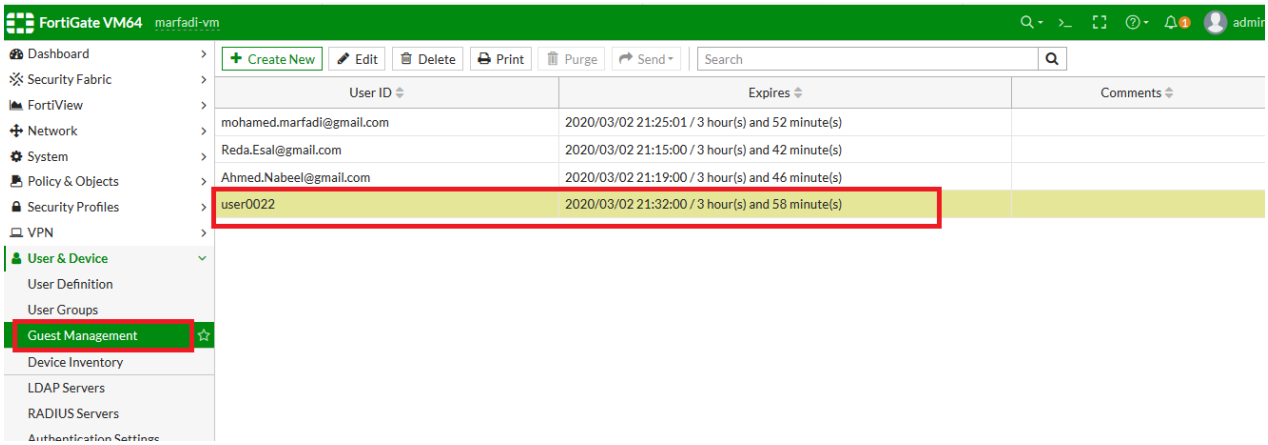
الان سوف أقوم بتغيير نوع الجروب Guest1 الى Auto Generated



لذا عن انشاء اليوزرفي هذا النوع فانك لن تقوم بكتابه اليوزرنيم ولا الباسورد

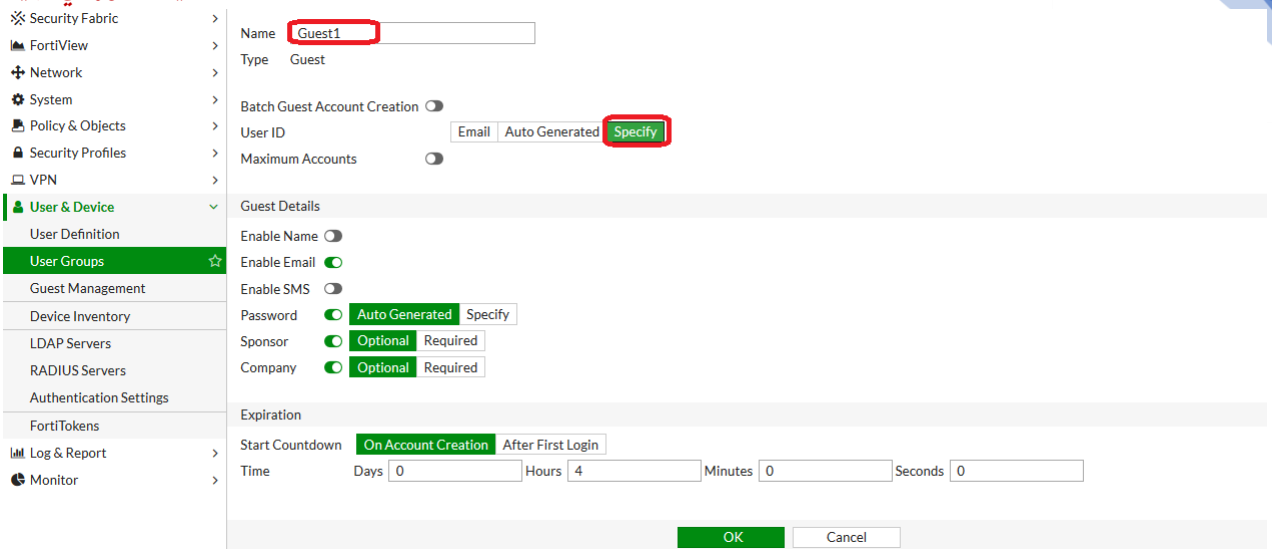


حتى الemail يمكنك تركه فارغا ...



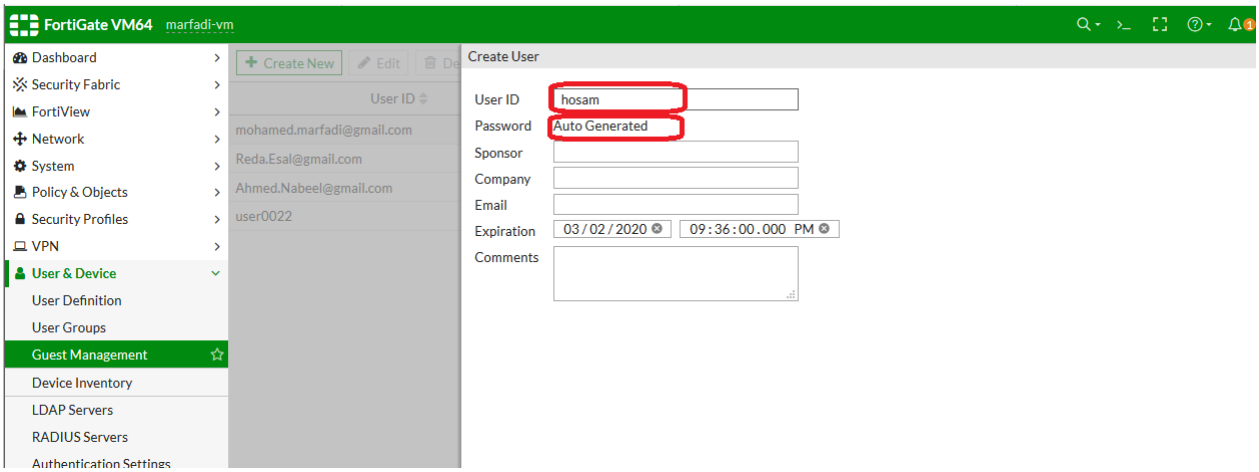
تم انشاء الحساب اوتوماتيكيا باسم user0022

النوع الأخيرمن Guest group هو specify أي انك سوف تقوم بإنشاء اسم اليوزربشكل يدوي .



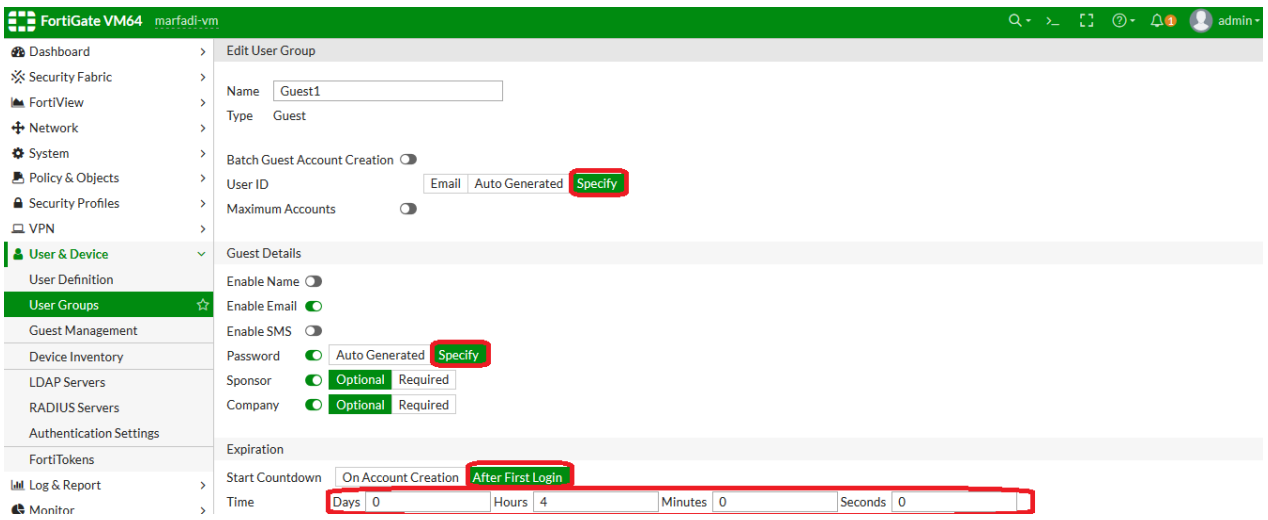
كما نلاحظ بأن خيار انشاء الباسورد هو Auto Generated أي بأن الفورتي جيت هو الذي يقوم بإنشاء

ه لكل حساب ..



كما الصوره أعلاه قمنا بكتابه اسم الحساب hosam بشكل مانوال ..

الخلاصة :



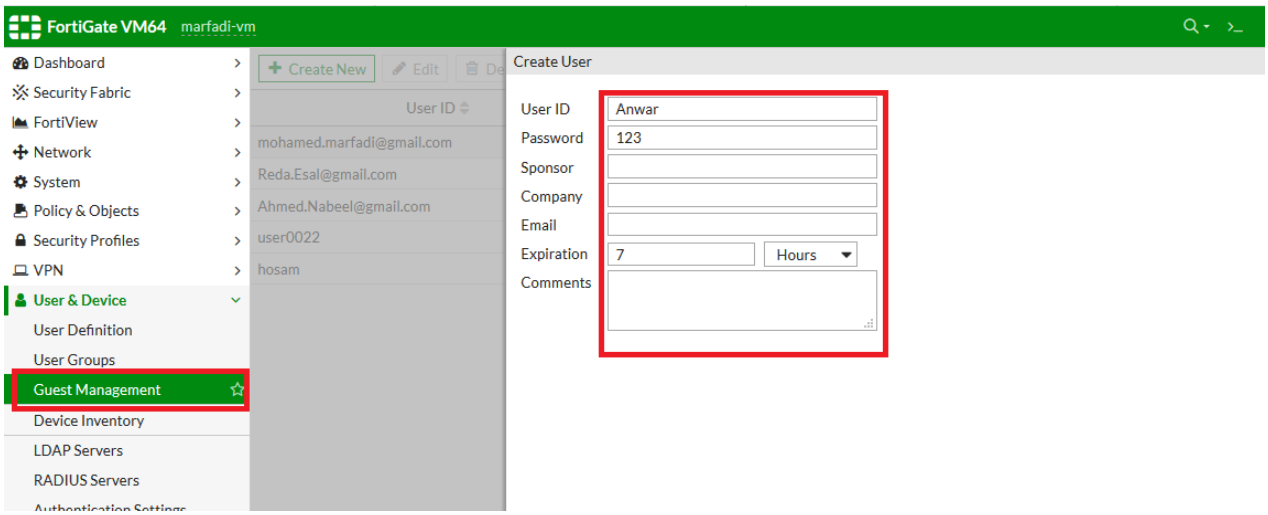
الخيار Expiration (متى سينتهي الحساب) هناك خيارين

Start countdown :

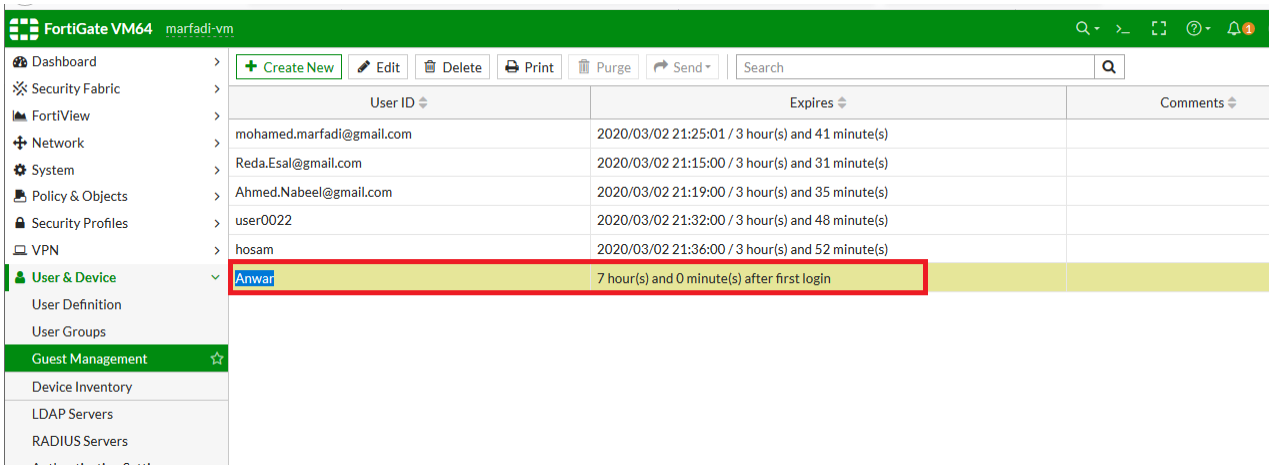
On Account creation :أي سيتم احتساب فتره الانتهاء(4 ساعات مثلا)منذ انشاء الحساب ..

After First Login : سيتم احتساب فتره انتهاء الحساب من بعد اول دخول للحساب من قبل الزائر..

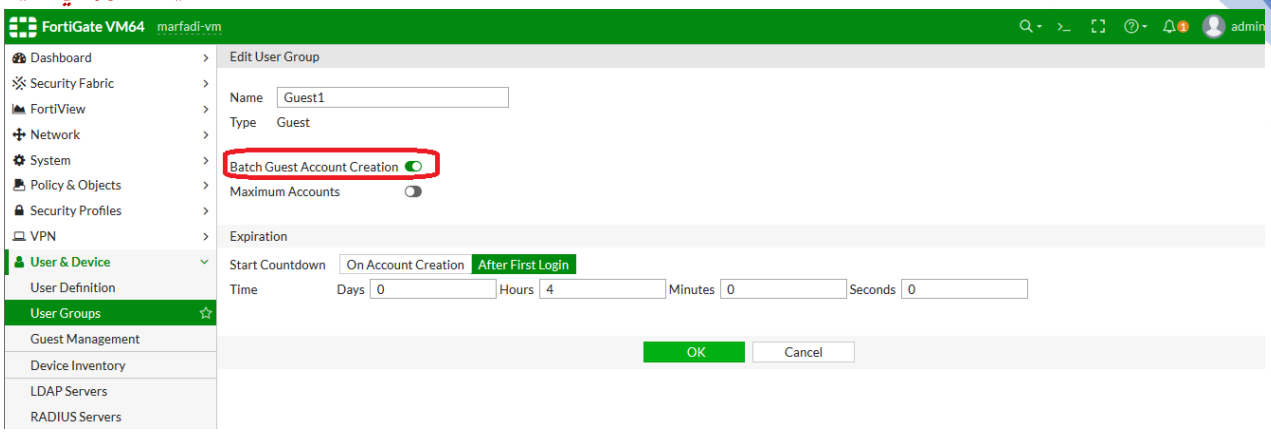
نلاحظ عند انشاء الحساب

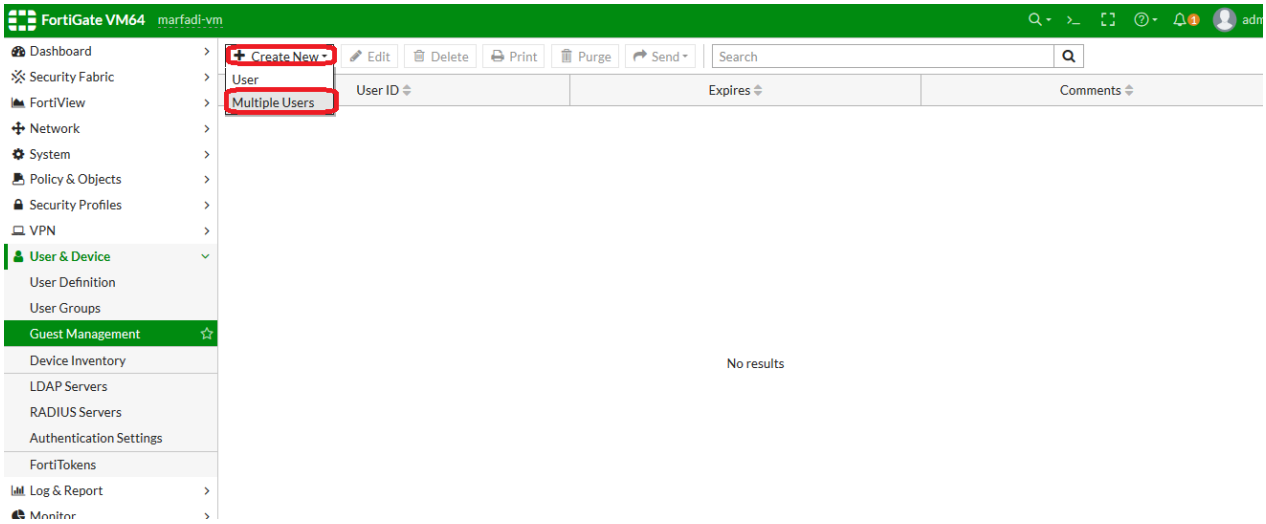


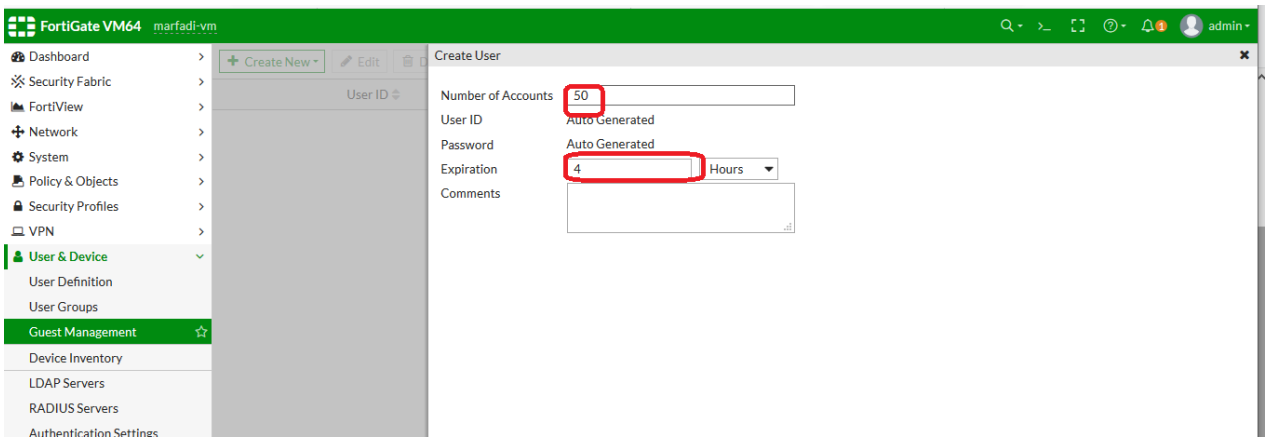
باننا قمنا بكتابه اسم اليوزروالباسورد بشكل مانول ...

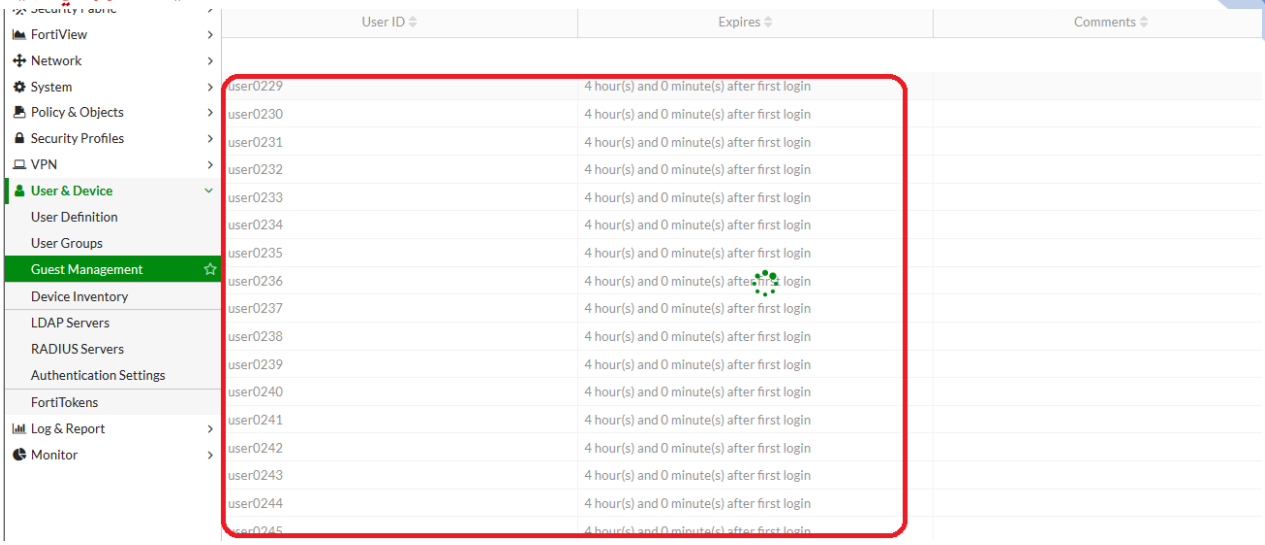


لو اردت انشاء حسابات بشكل اوتوماتيكي لعدد مثلا 50 يوزر.


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
Edit User Group
Name Guest1
Type Guest
Batch Guest Account Creation
Maximum Accounts
Expiration
Start Countdown On Account Creation After First Login
Time Days 0 Hours 4 Minutes 0 Seconds 0
OK
Cancel


FortiGate VM64 marfadi-vm
Create New
Edit
Delete
Print
Purge
Send
Search
User
Multiple Users
User ID
Expires
Comments
No results
Authentication Settings
FortiTokens
Log & Report

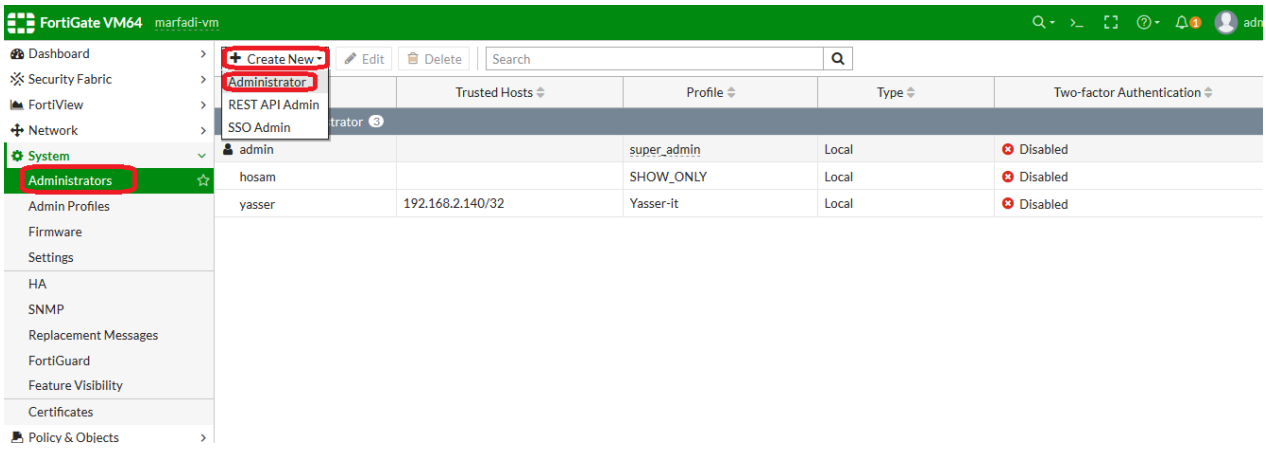

FortiGate VM64 marfadi-vm
Create New
Edit
User ID
Create User
Number of Accounts 50
User ID Auto Generated
Password Auto Generated
Expiration 4 Hours
Comments

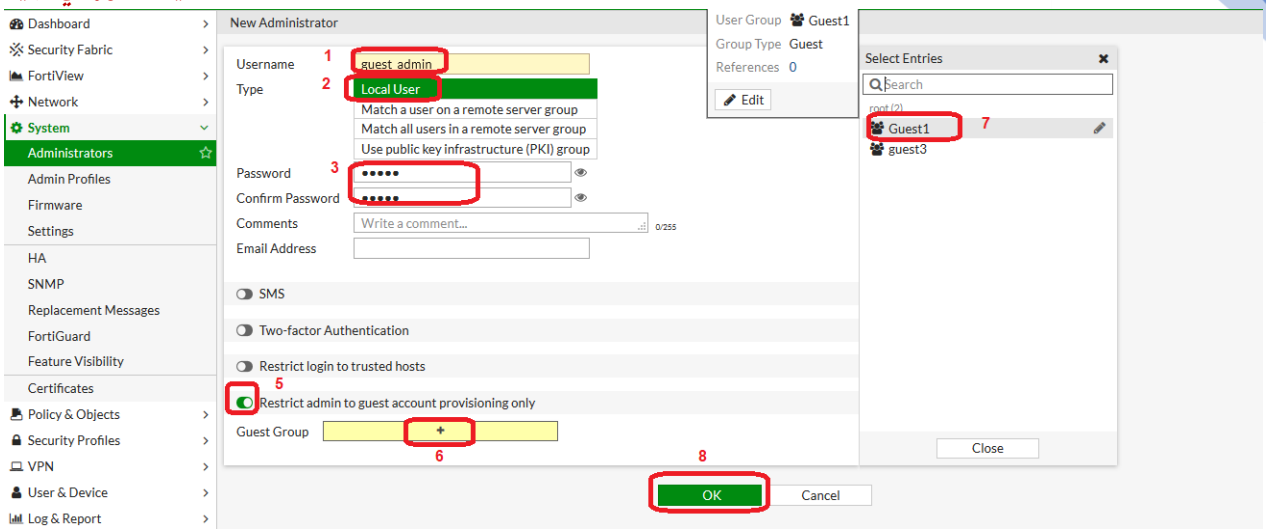


تم انشاء 50 حساب بشكل اوتوماتيكي فيمكنك طباعتها او ارسالها للزوار باي طريقة ..

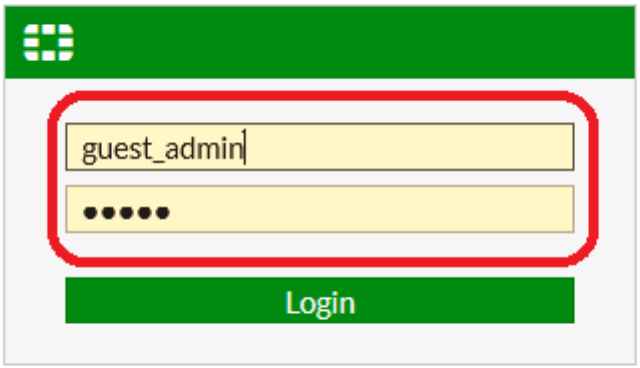
- ثم بعد ذلك سنقوم بإنشاء بوليسي ونحدد بها الجروب المسماة (Guest1) في الSource.

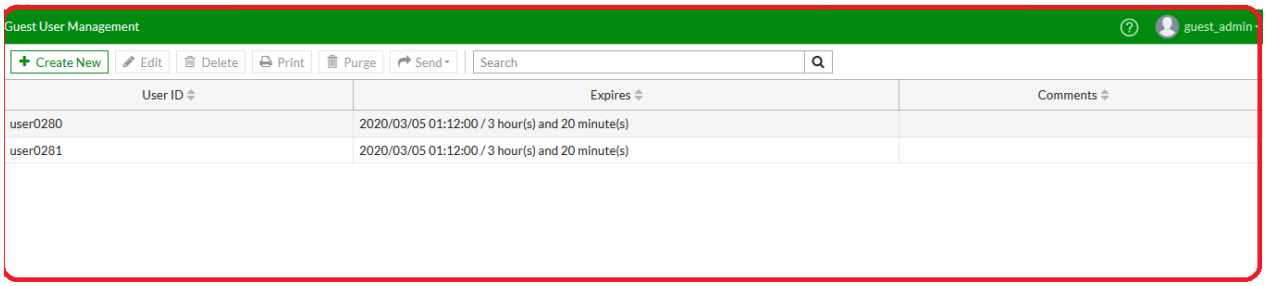
لو تريد مثلا احدى موظفي الايتي عندك لا تريد ان تعطيه صلاحيه كامله على الفورتي جيت وتريد فقط ان يدير حسابات الزوار(Guest users) نقوم بالخطوات التالية :





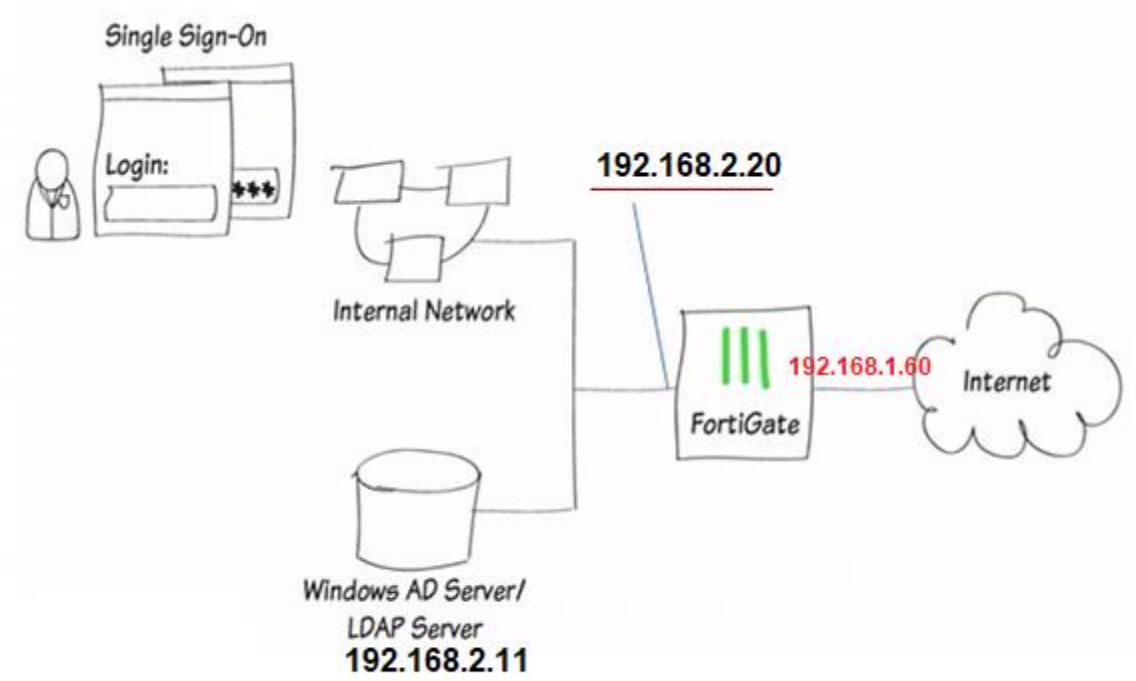
كما بالصورة أعلاه تم انشاء يوزرباسم guest_admin يقوم بإدارة الجروب المسماة Guest1 .





الان اليوزرguest_admin يمكنه اداره الجروب المسماة Guest1 من انشاء يوزروالتعديل عليه وحذف اليوزرات التابعه للجروب Guest1 وأيضا عمل Purge وطباعه اليوزرات ..الخ ..

FSSO(fortinet single sign on)



نحن في الدروس السابقة لكي نصل الى الانترنت عبر الفورتي يجب ان يكون لدينا يوزر في الفورتي جيت لذا لكي افتح الانترنت على أي جهاز يوجد لدينا خطوتين

١- ادخال اليوزر نيم والباسورد للويندوز(للجهاز اول مره)أي login to computer
٢- ادخال اليوزر نيم والباسورد(local account) الموجود بالفورتي جيت

وبهذا استطيع الوصول الى الانترنت

اذا لدينا خطوتين لكي يتمكن الجهاز من الوصول الى الانترنت ...

ولتخفيض العملتين السابقتين الى عمليه واحده فقط

أي الاعتماد على اليوزر نيم والباسورد الموجودين في الـAD فقط .

وذلك لتعريف كل اليوزرات و الجروبات الموجودة في AD على الفورتي جيت .

وبذلك يمكنني التحكم بكل اليوزرات و الجروبات عبر الفورتي جيت كأنهم local users وذلك عبر عمل integration الـAD مع fortigate .

ملاحظة :

LDAP server ممكن يكون AD server in windows

او لينكس او نوفل ...الخ .

Ldap هي DB الخاصة بالحسابات

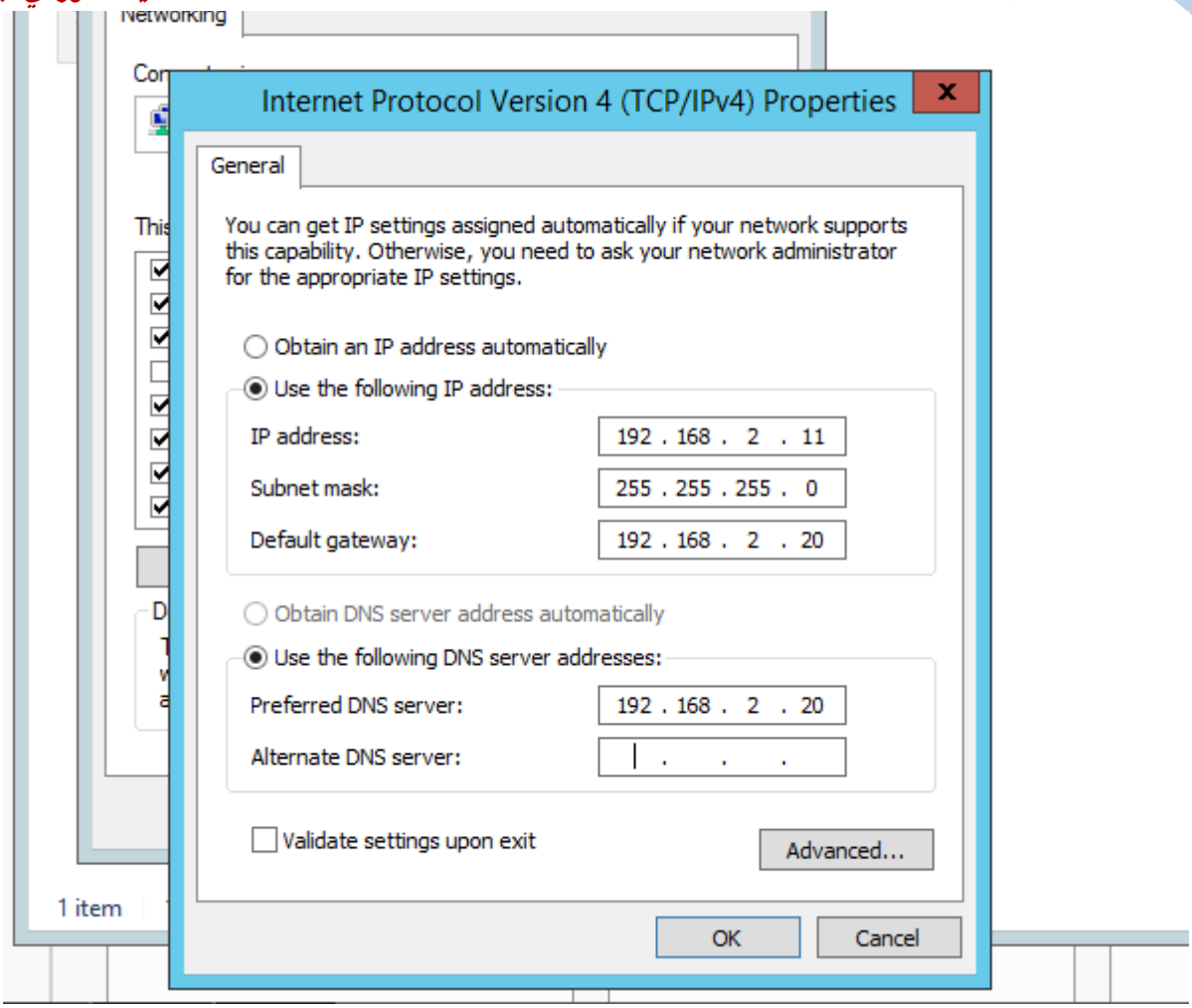
نحن سوف نتعامل مع ldap server in Microsoft وهو AD server

ولكي نقوم بعمل integrate للفورتي جيت مع الAD يجب ان تقوم بالخطوات التالية :

١- تحديد الLdap server للفورتي جيت أي من هو الAD server
٢- عمل اعدادات للLdap server لكي يعمل single sing on أي يجب تفعل خاصيه single sign on على الفورتي جيت .
٣- سنقوم بإنشاء FSSO group تحتوي بداخلها على اليوزرات او الجروبات الموجودة على الAD
٤- انشاء بوليسي ونختار الجروب التي قمنا بأنشائها 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 الفورتي جيت لأنك في البوليسي قمت بتخصيص FSSO group الا لو انت سمحت بذلك .

الان سنقوم بعمل AD server بالايبي 192.168.2.11 ونقوم بإنشاء يوزرات على الAD

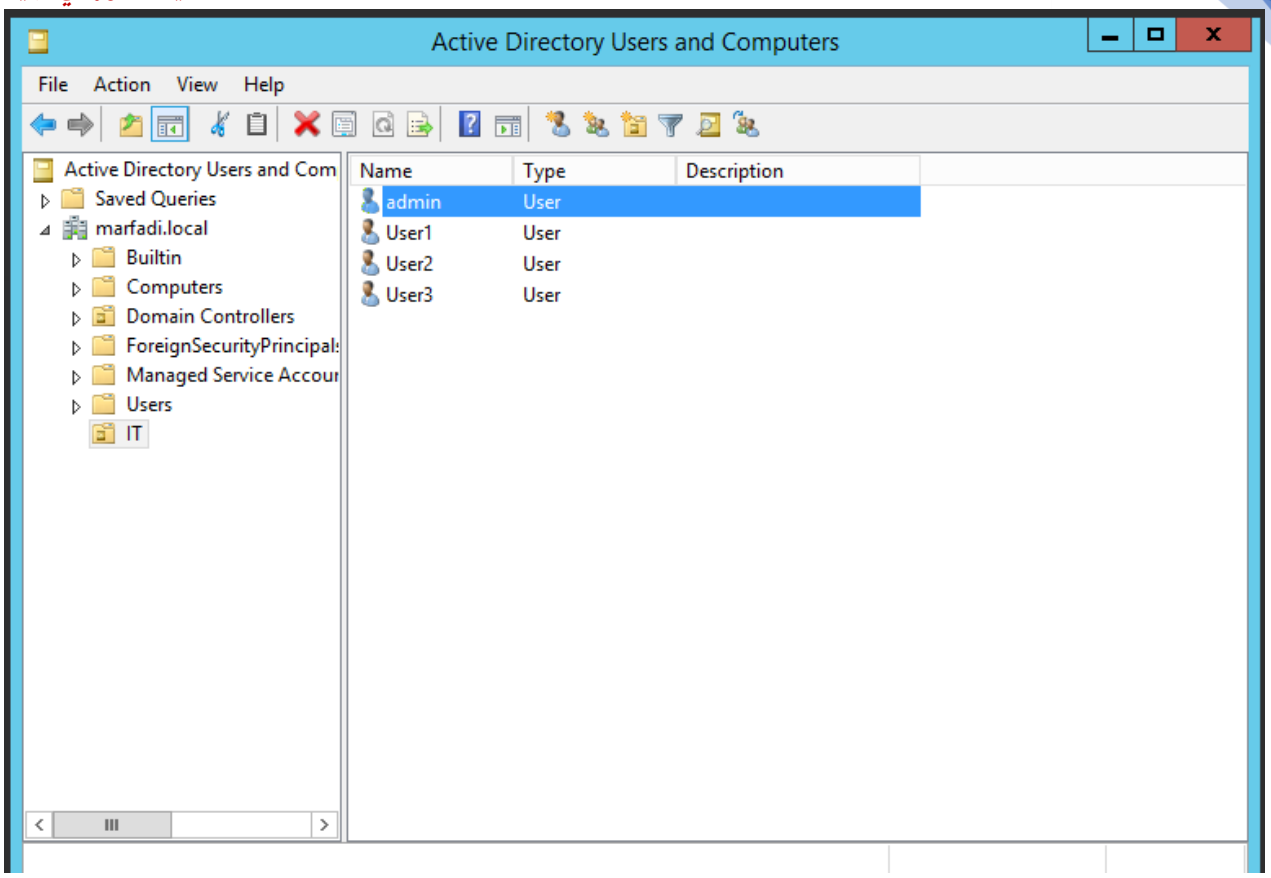


ملاحظة:قم باغلاق الفايروول للويندوز سيرفر 2012 (Active directory)

نقوم بإنشاء يوزرات على الAD كالتالي :

Admin ونوعه domain admins

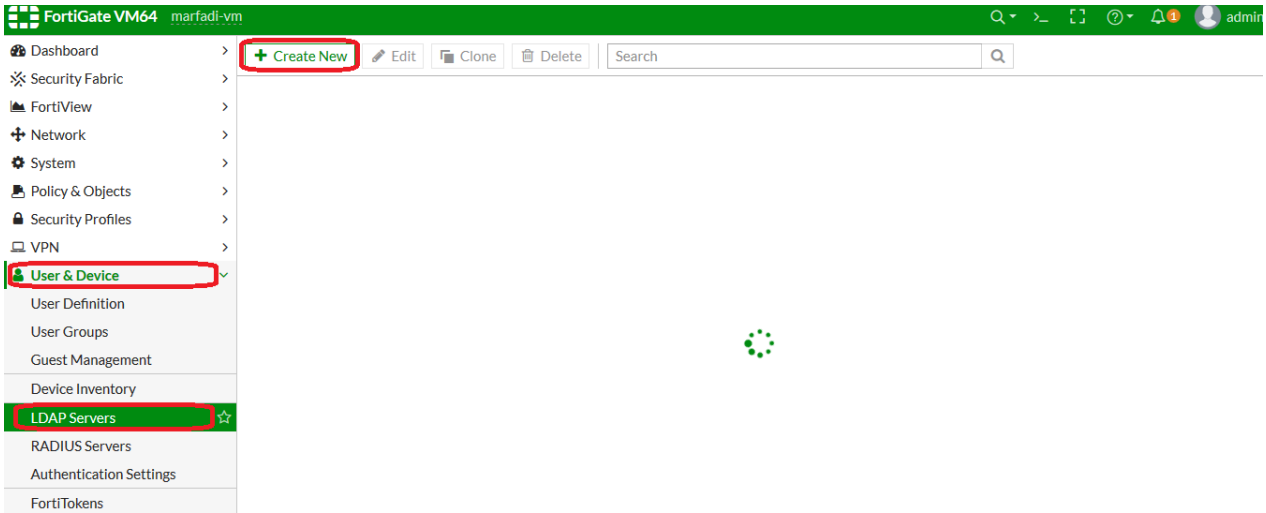
User1،User2،User3 ونوعه domain users

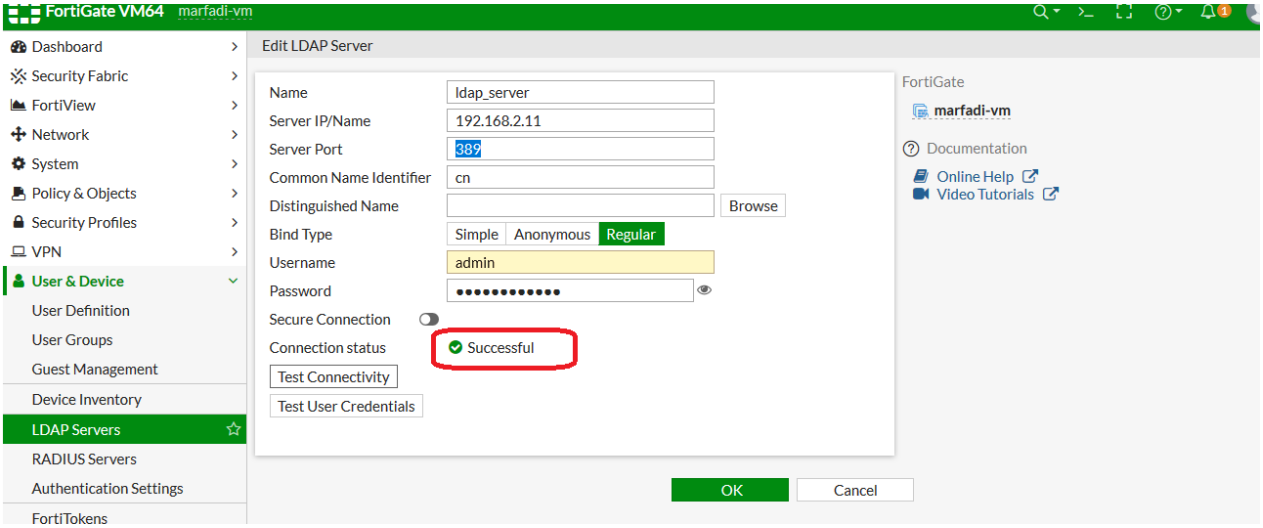


نتاكد من جهاز الكلاينت(Win 8.1)معمول له Joined للدومين وان السيرفر AD

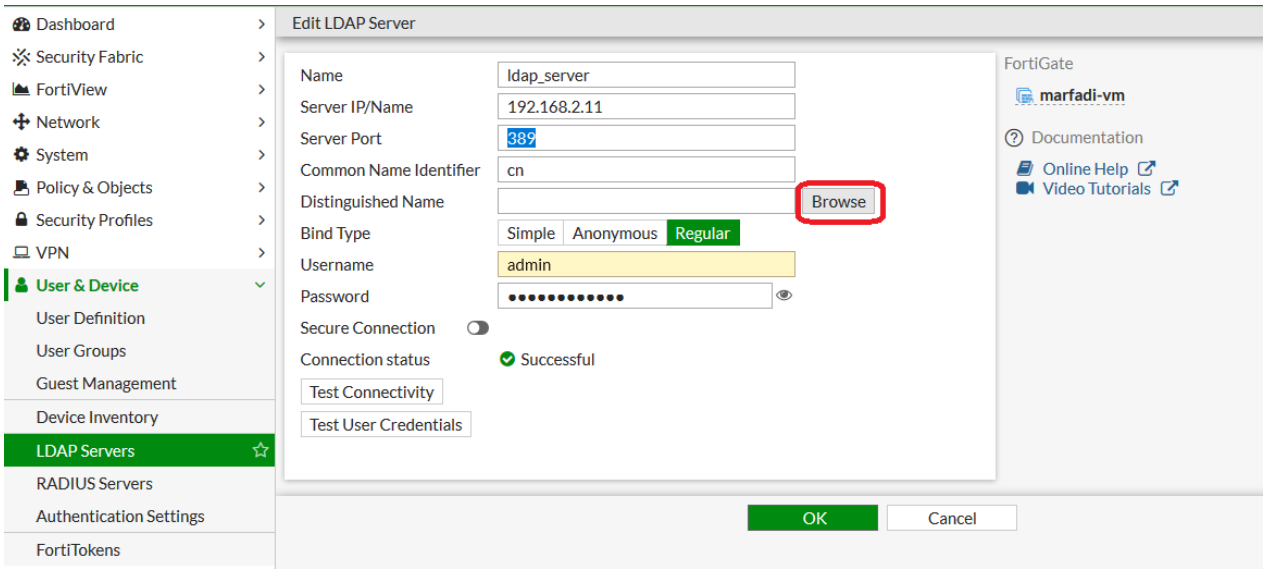
بيقدروا يوصلوا لبعض (موصلين على سويتش واحد Vnet1)وبيقدروا يعملوا ping بينهم البعض ..

الان سنقوم بأضافه الـ ldap server الذي هو AD (192.168.2.11)الى الفورتي جيت

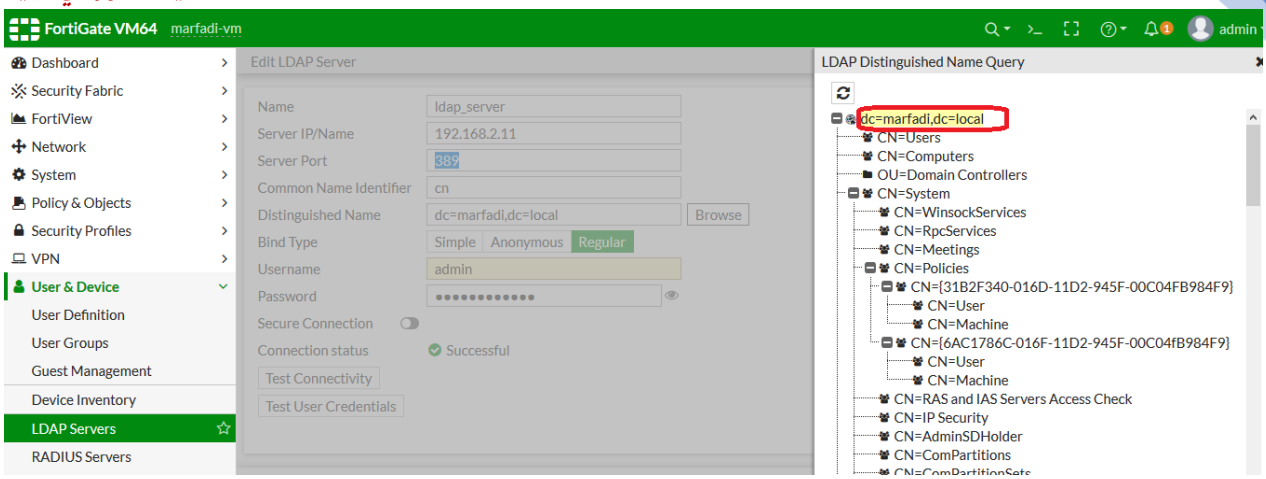


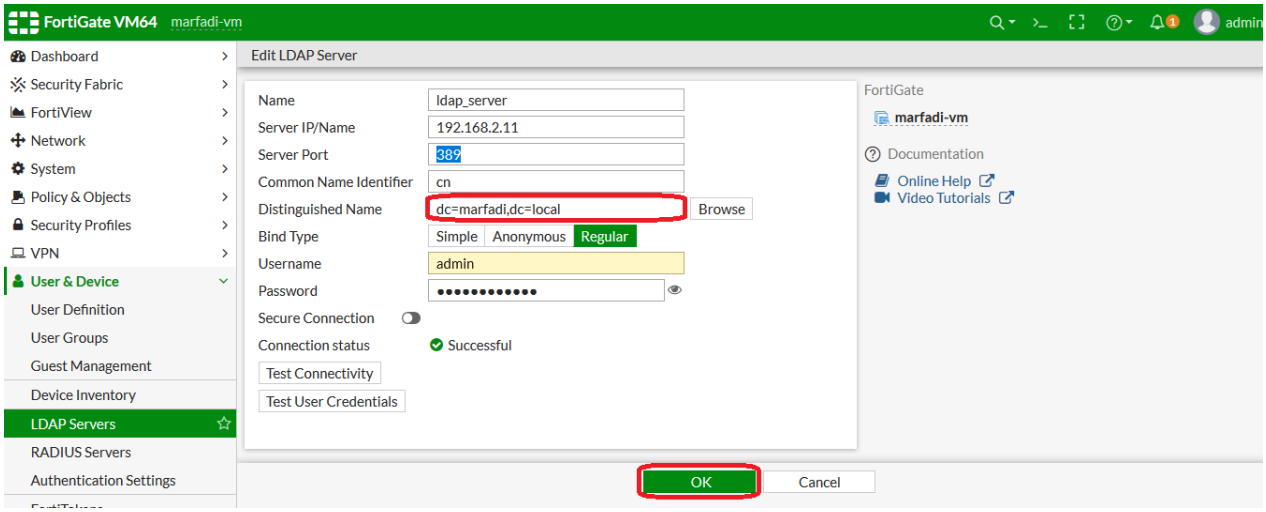


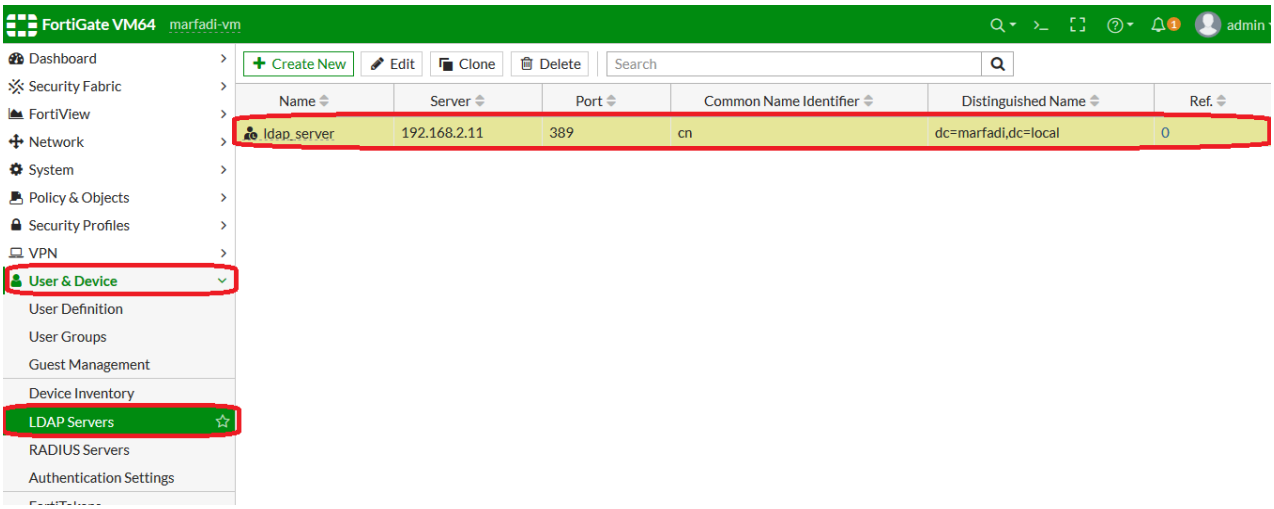
كما بالصورة أعلاه تبين بأن الاتصال بسيرفر الـ ldap سليم ..



بعد النقر على الزر browse نقوم باختيار الدومين كما بالصورة ادناه



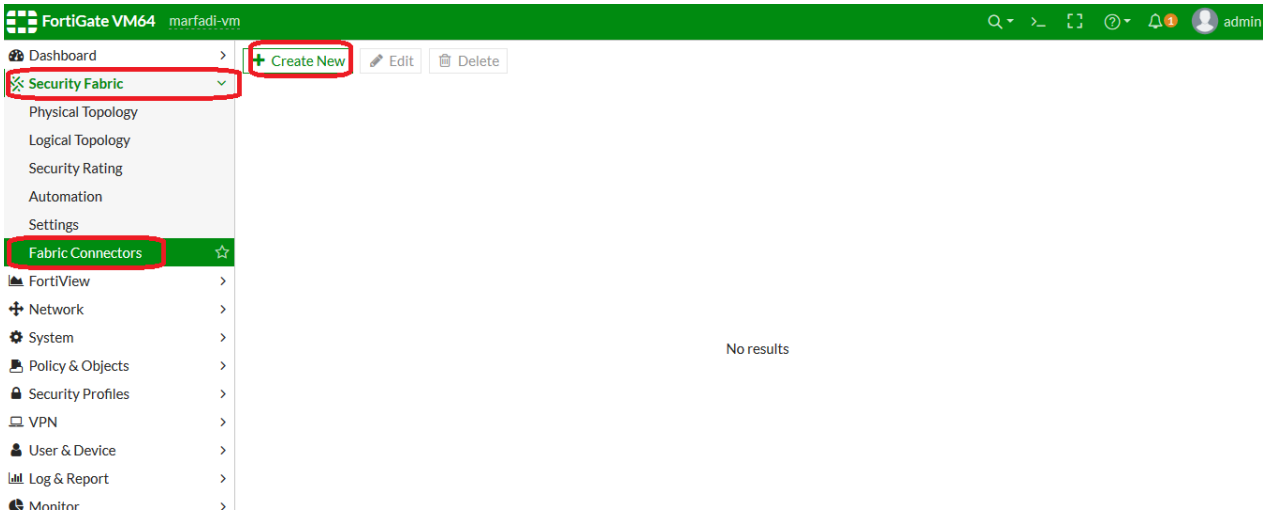




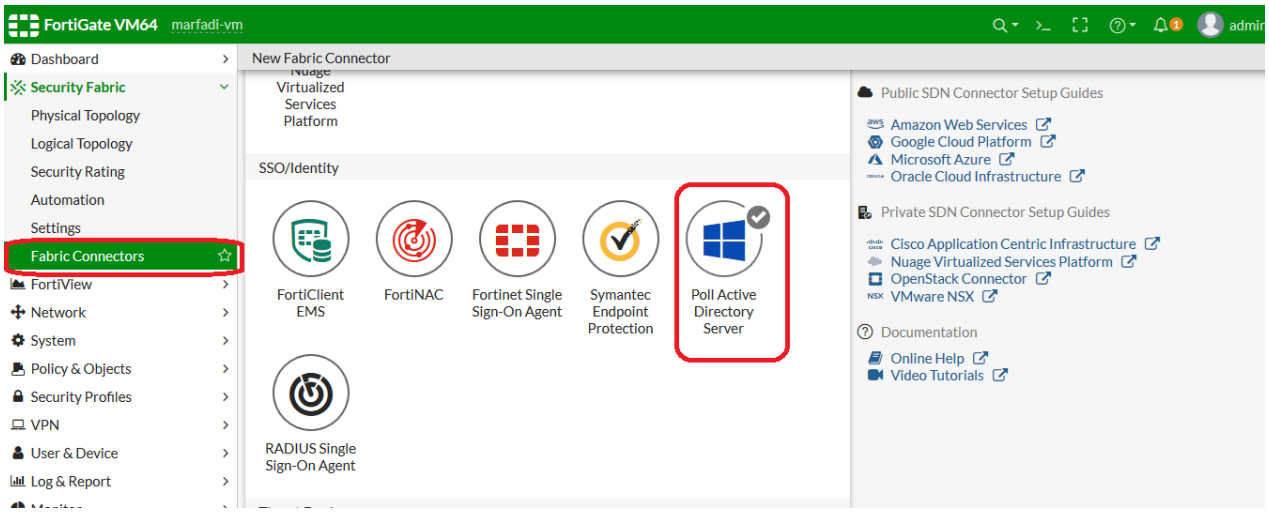
كما بالصورة أعلاه تم أضافه الـ ldap server بنجاح ...

الخطوة الثانية :

نقوم بضبط الاعدادت لتفعيل خاصيه FSSO



هناك طريقتين لعمل ذلك وهما

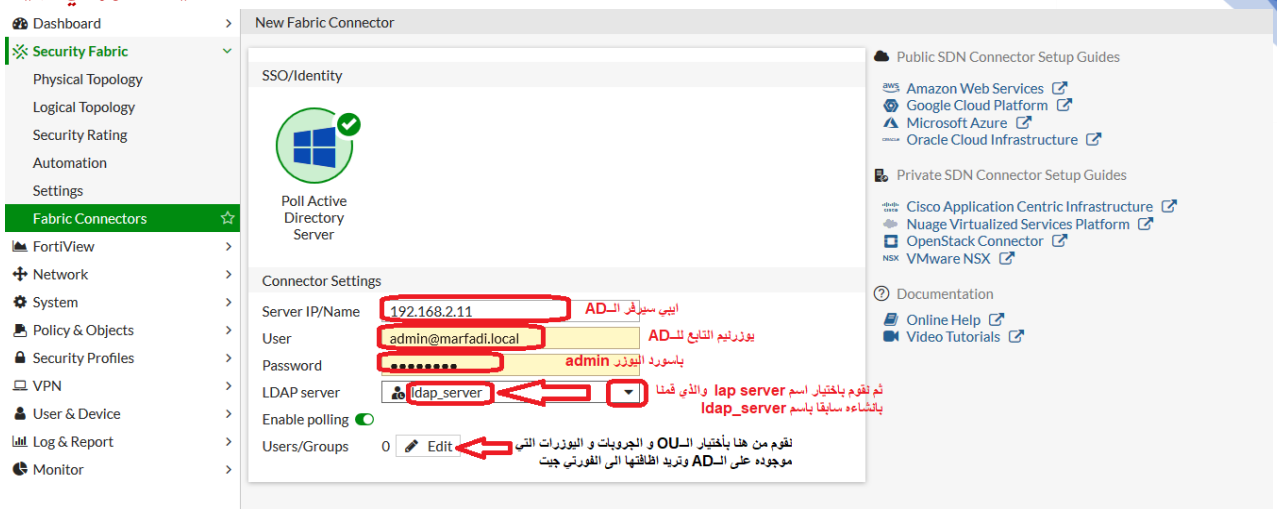


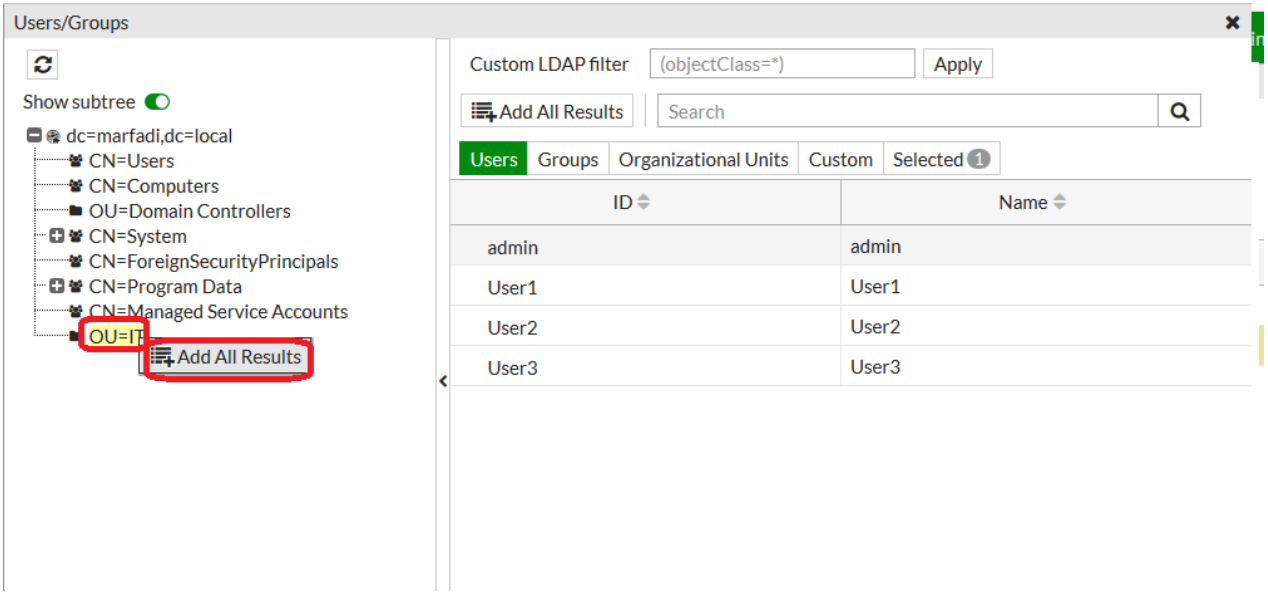
الطريقة الأولى Poll Active Directory server

وهي الطريقة التي سنعمل عليها الآن

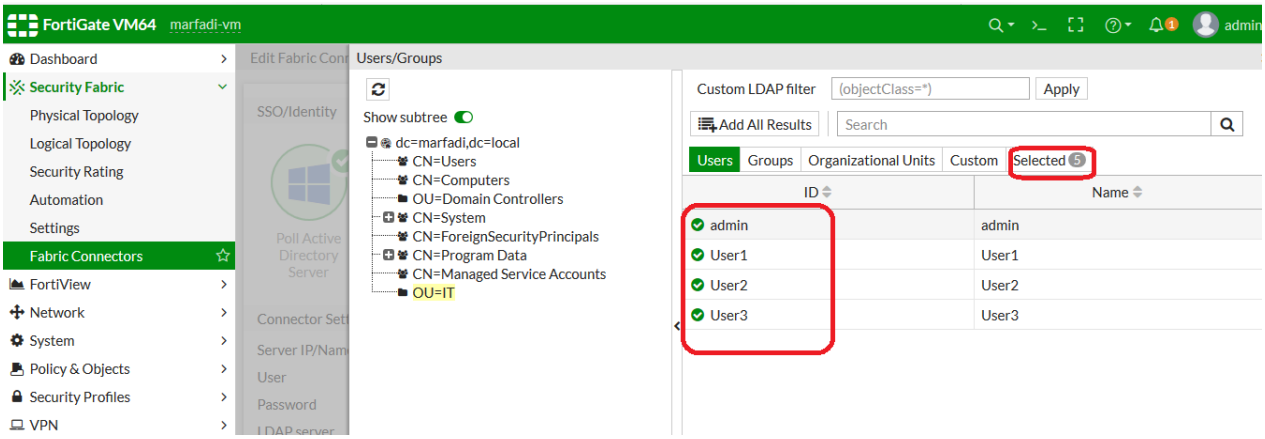
و الطريقة الأخرى هي Fortinet Single Sign-on Agent

وسوف يتم شرحها لآحقا ..



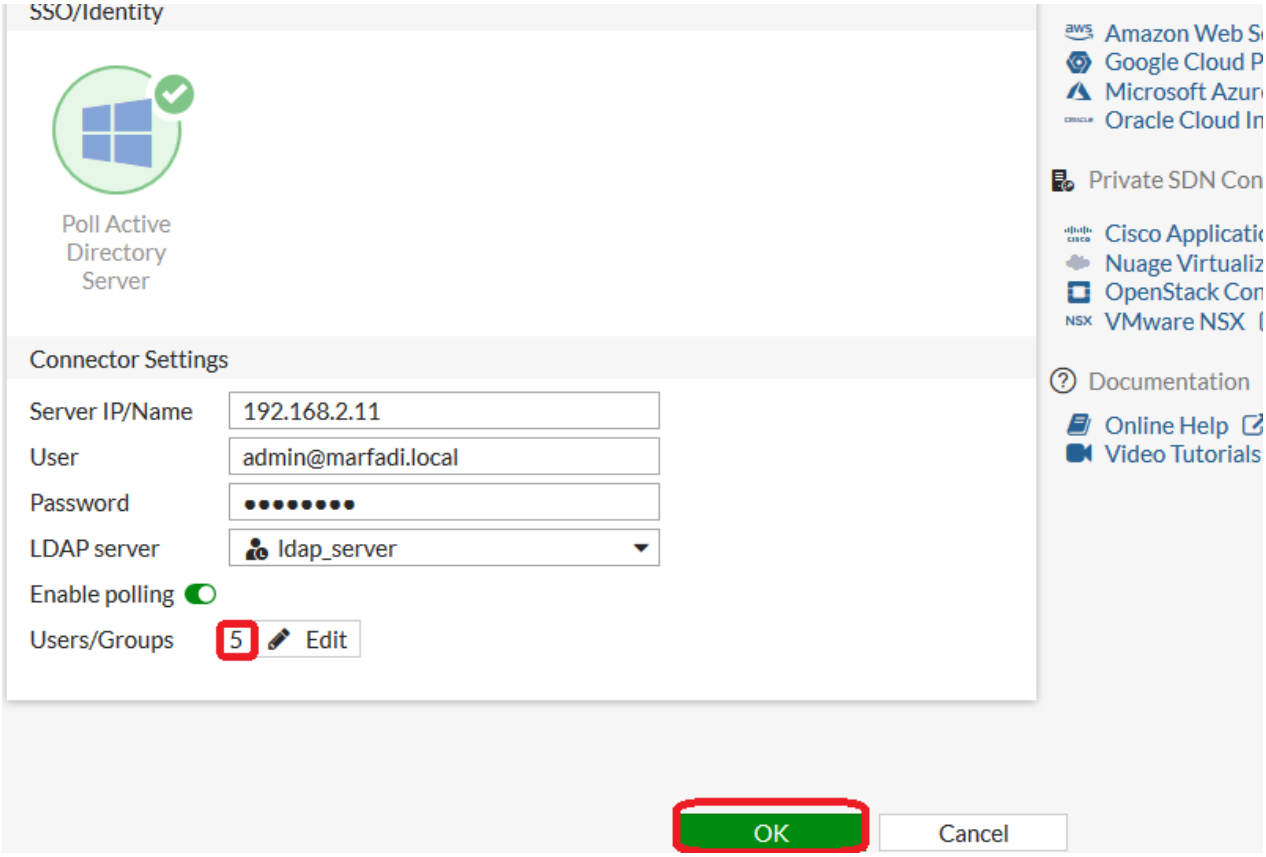


قمنا باختيار الوحده التنظيميه (OU) المسماة IT والتي تحتوي على اليوزرات User3،User2،User1 من قائمه اليوزرات التي موجودة في الـAD لكي أتمكن من رؤيتها على الفورتي جيت حيث بعد التحديد ننقر بالزر الأيمن ثم Add Selected ..

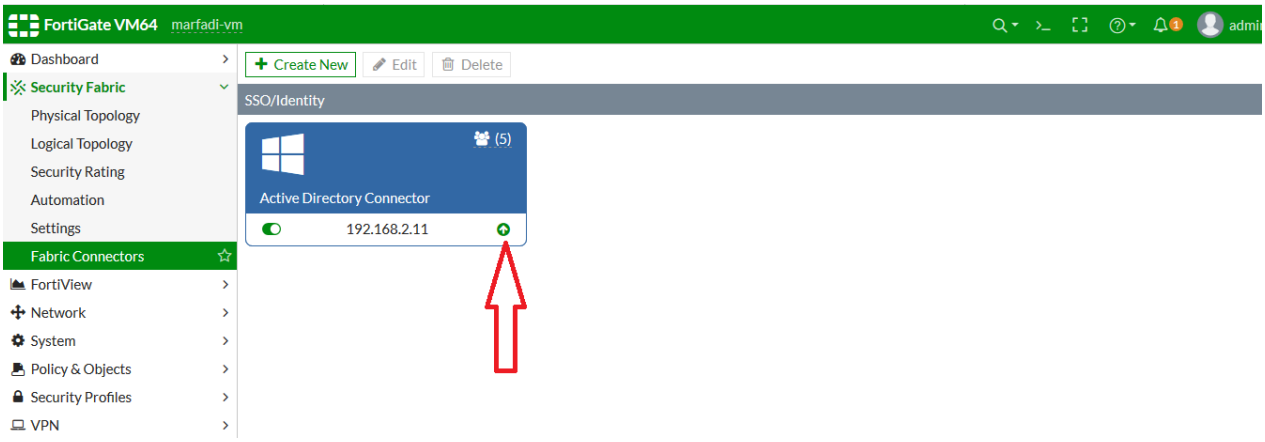


تم أضافه الـOU من الـAD الى الفورتي جيت لكي أتمكن من ان اتحكم فيها لاحقا عبر الفورتي جيت

تم أضافه الOU المسماة IT ..



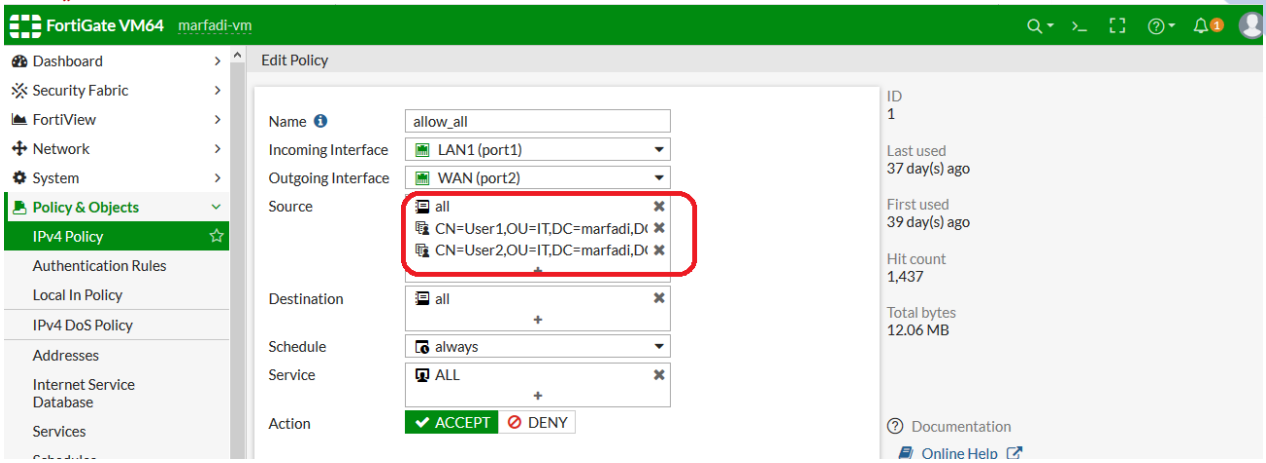
تمت بنجاح كما بالصور ادناه توجد علامه صح خضراء

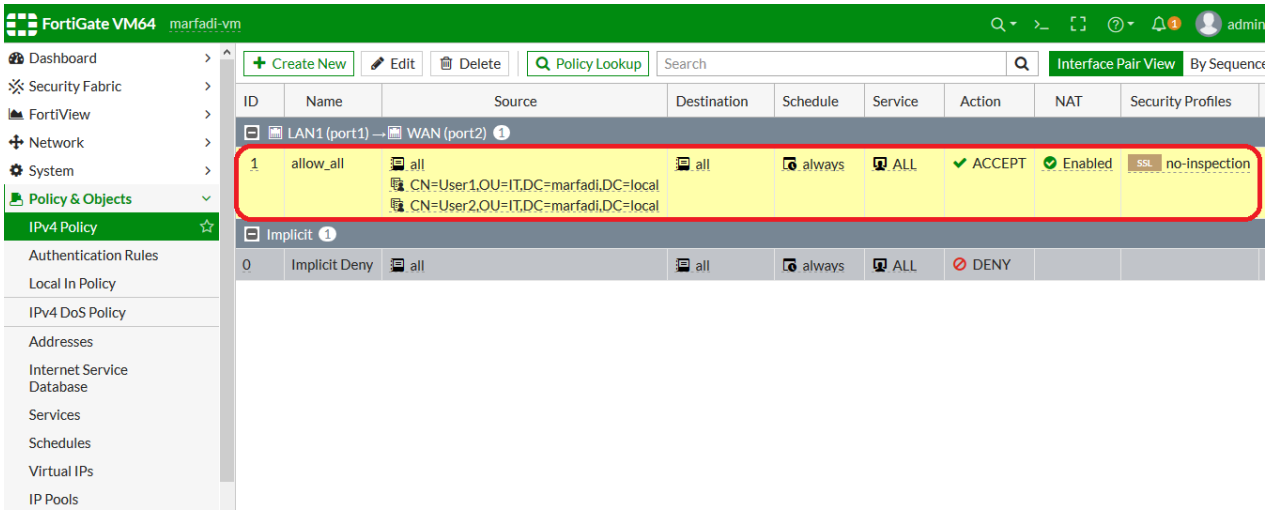


لوكانت العملية لم تتم بنجاح فيكون السهم باللون الأحمر ليدل على فشل العملية ..

الآن سنقوم بإنشاء يوليسي ونختار منها اليوزرات مثلا User1 و User2 فقط ..

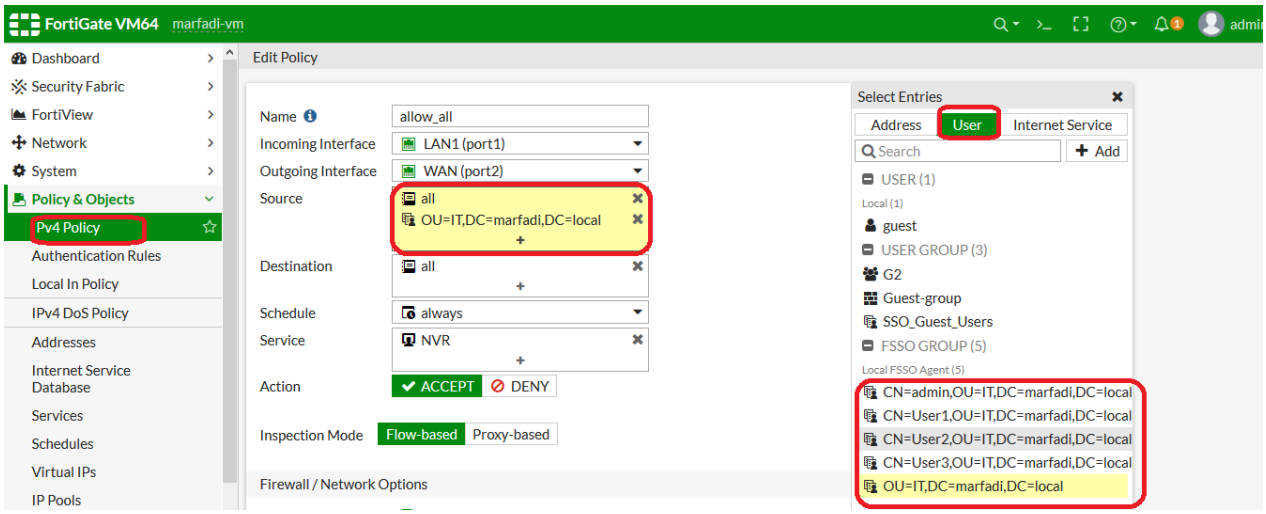
حيث هما فقط لهما الحق بالوصول الى الانترنت ..

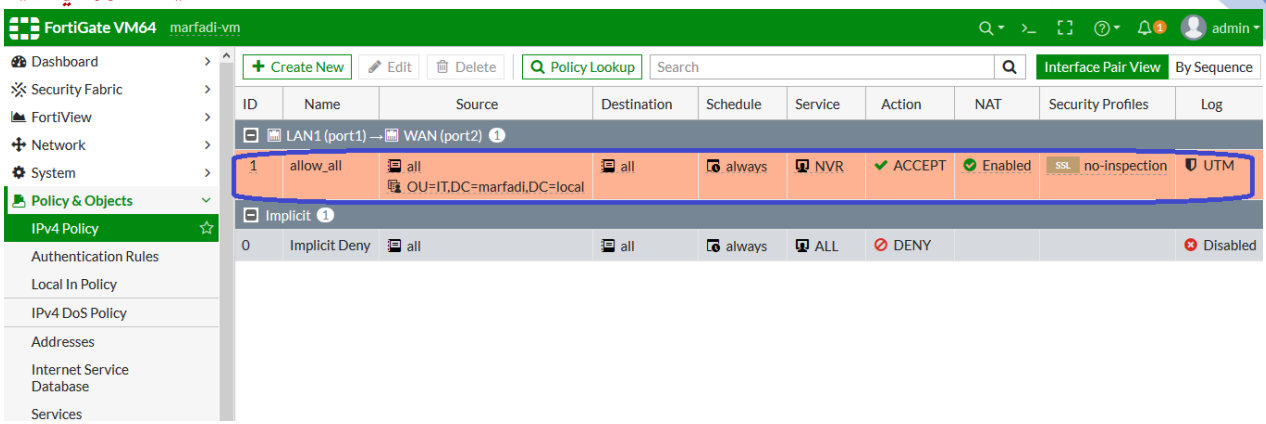




ملاحظة :

لو قمنا باختيار الOU كامله كما بالصورة ادناه فأن اليوزرات التي بداخل تلك الOU لن تستطيع الوصول الى الانترنت وكأن الفورتي جيت لا يتعرف على الـOU ..



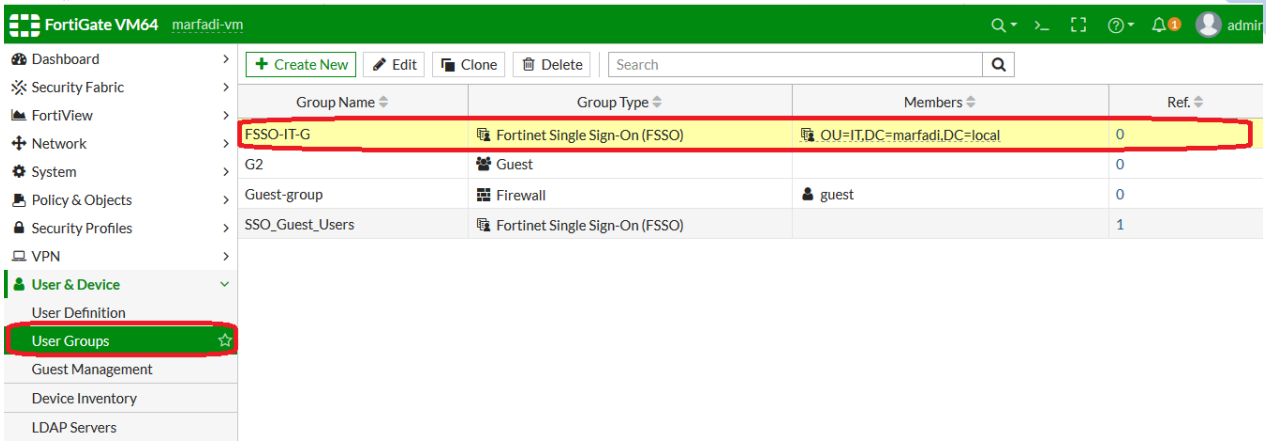


البوليسي أعلاه لن تجعل اليوزرات التي بداخل الOu المسماة IT يحصلوا على الانترنت ..

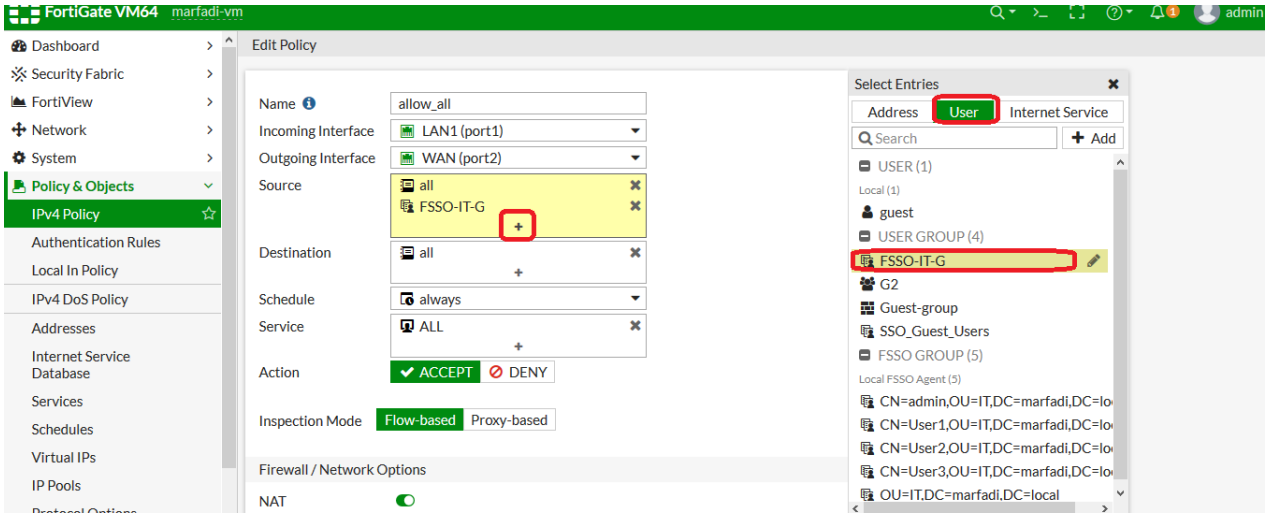
الخطوة الثالثه :

لذا من الأفضل انشاء جروبات من نوع FSSO لكي نتمكن من استخدامها في البوليسي 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 .



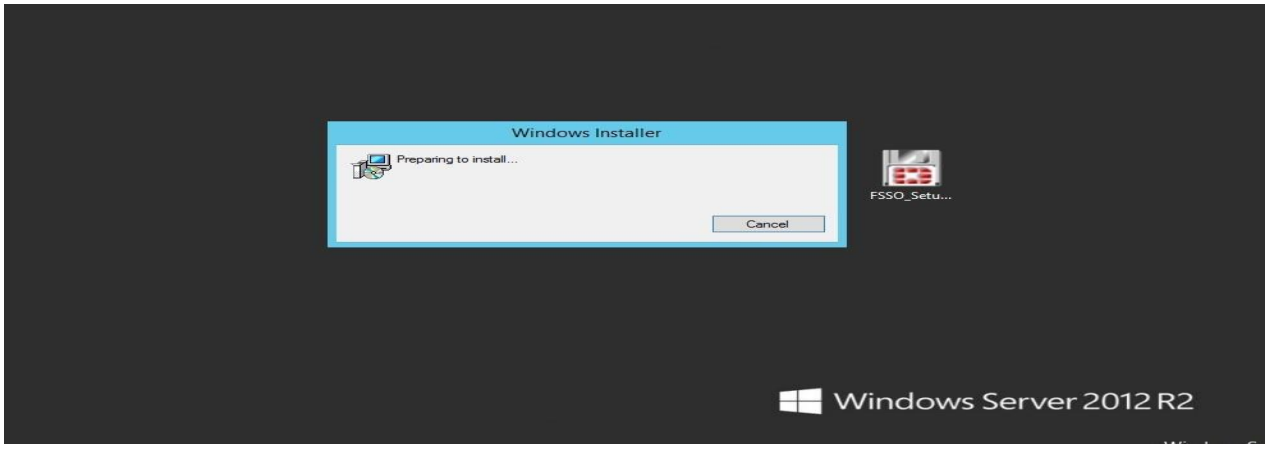
الآن سنقوم بالتعديل على البوليسي السابقة لنقوم باختيار الجروب المسماة FSSO-IT-G كما بالصورة ادناه



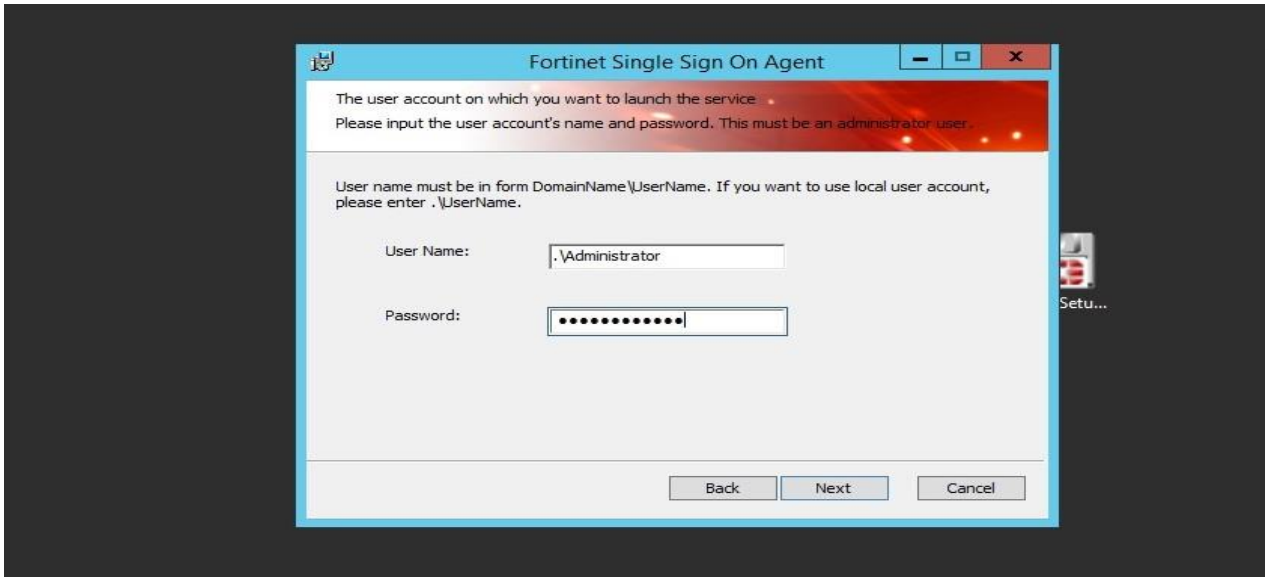
❖ الطريقة الثانية لعمل الـ integeration بين الفورتي جيت والـAD تسمى

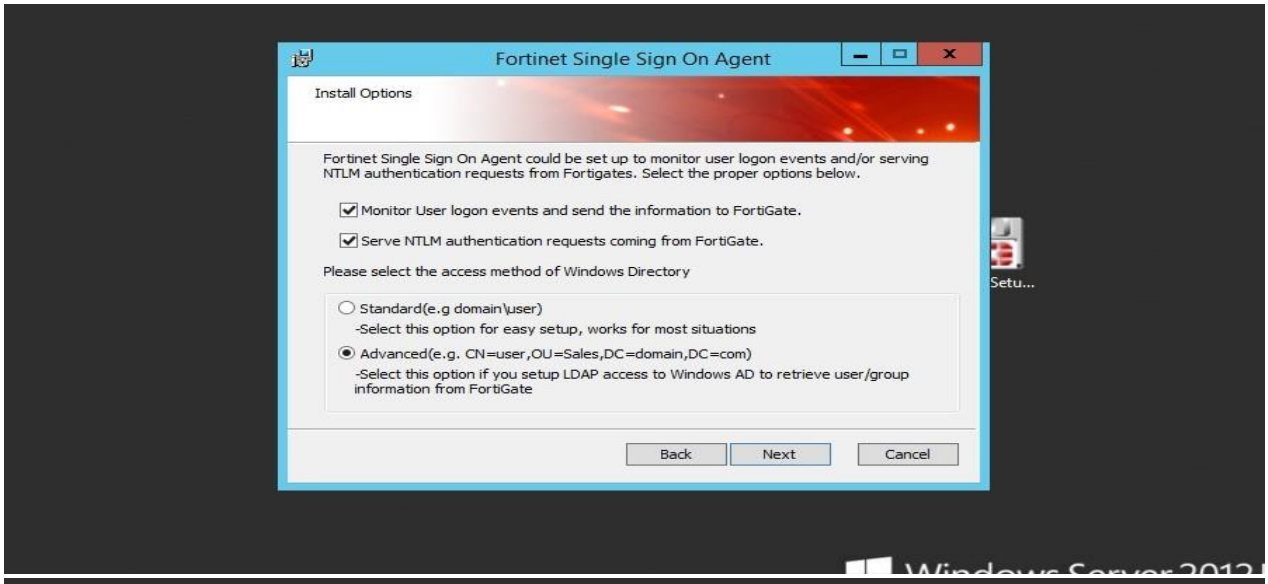
Fortinet Single Sign-on Agent

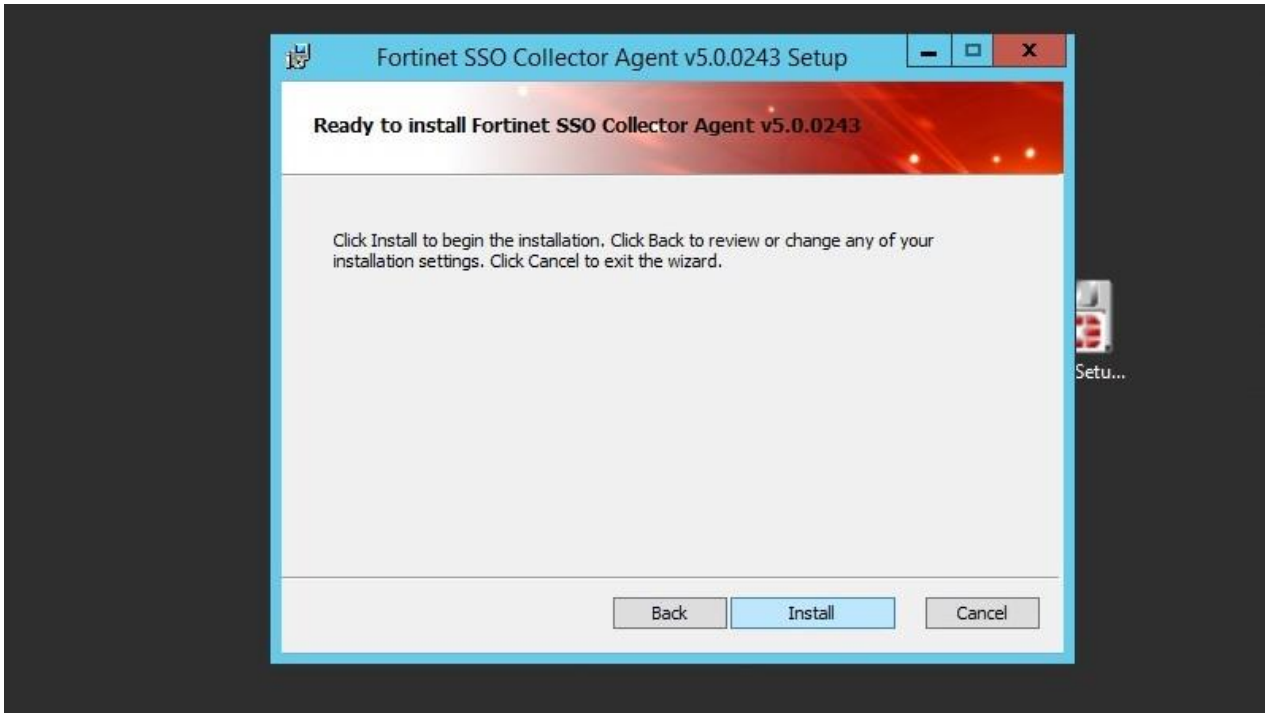
يتم تنزيل برنامج اسمه FSSO على سيرفر الدومين(AD)

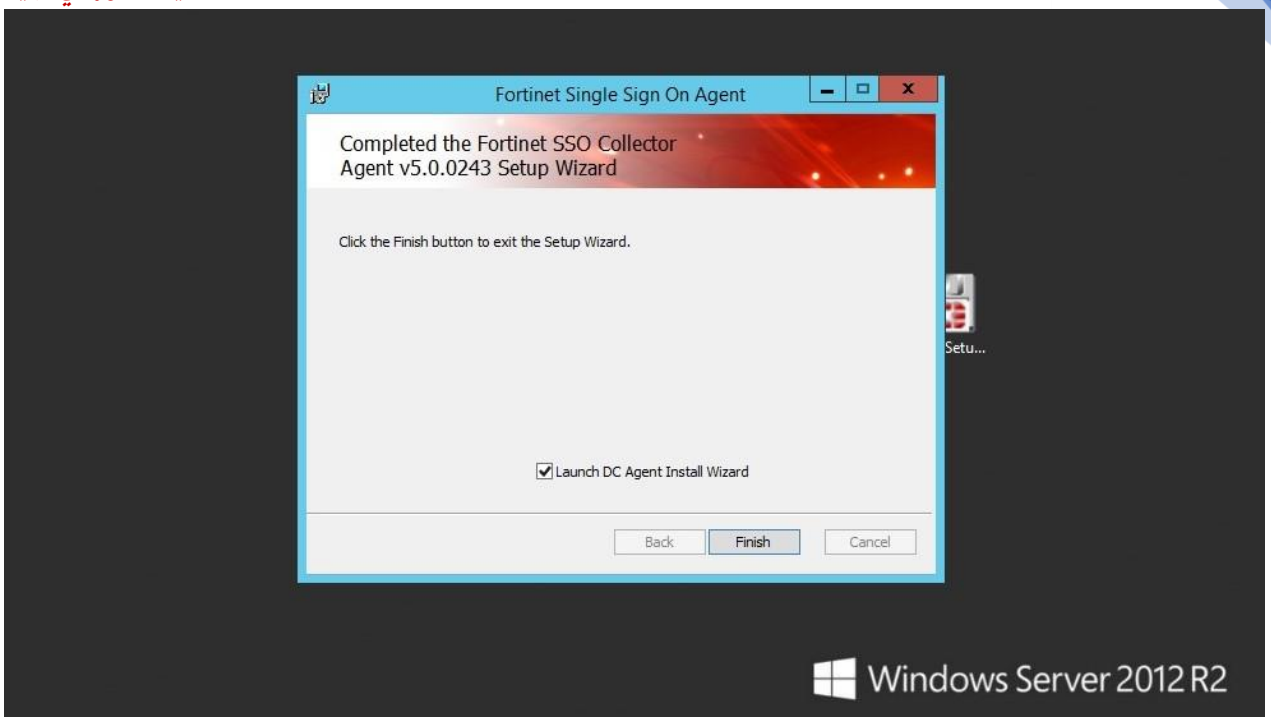


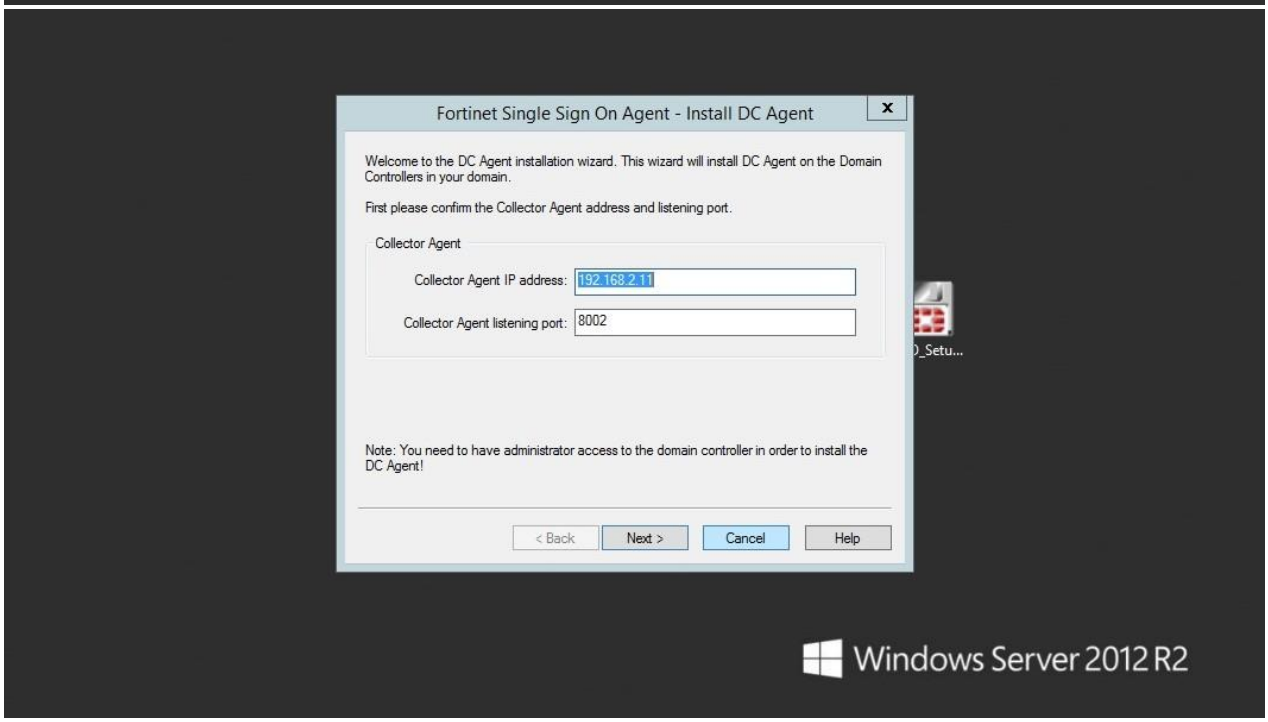
قم بكتابه كلمه السر التابعه للدومين ادمن للAD

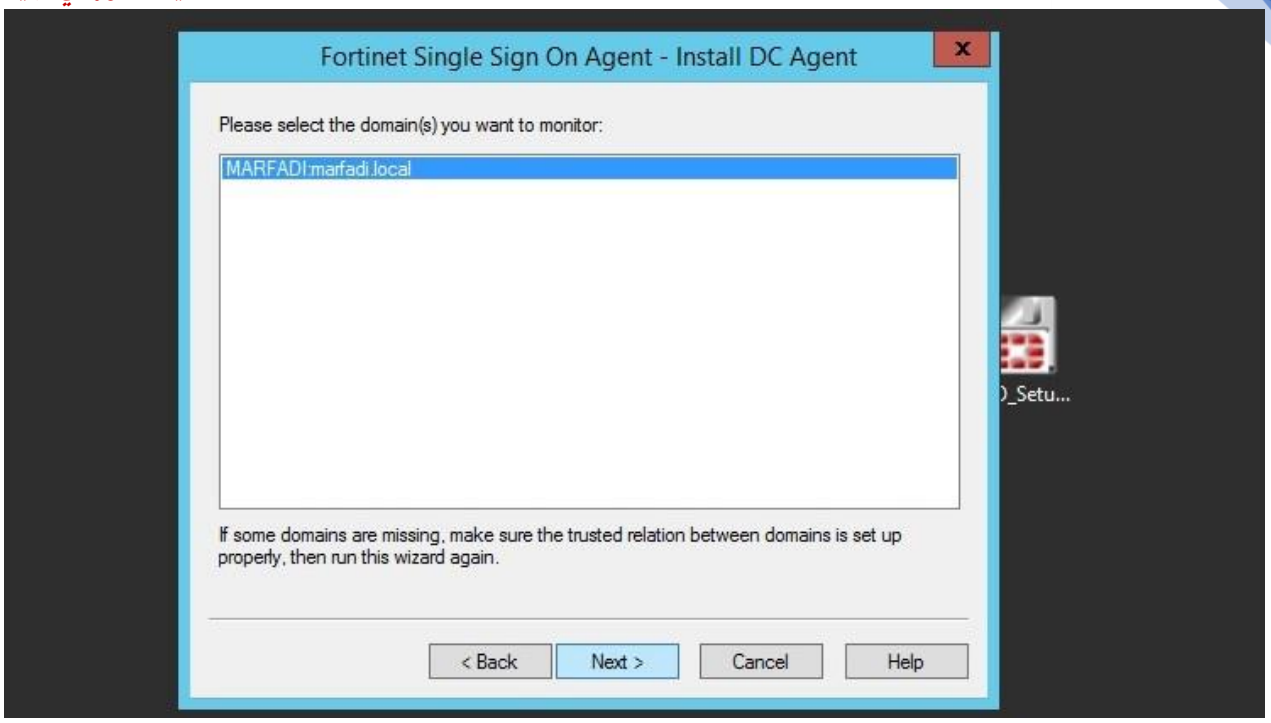




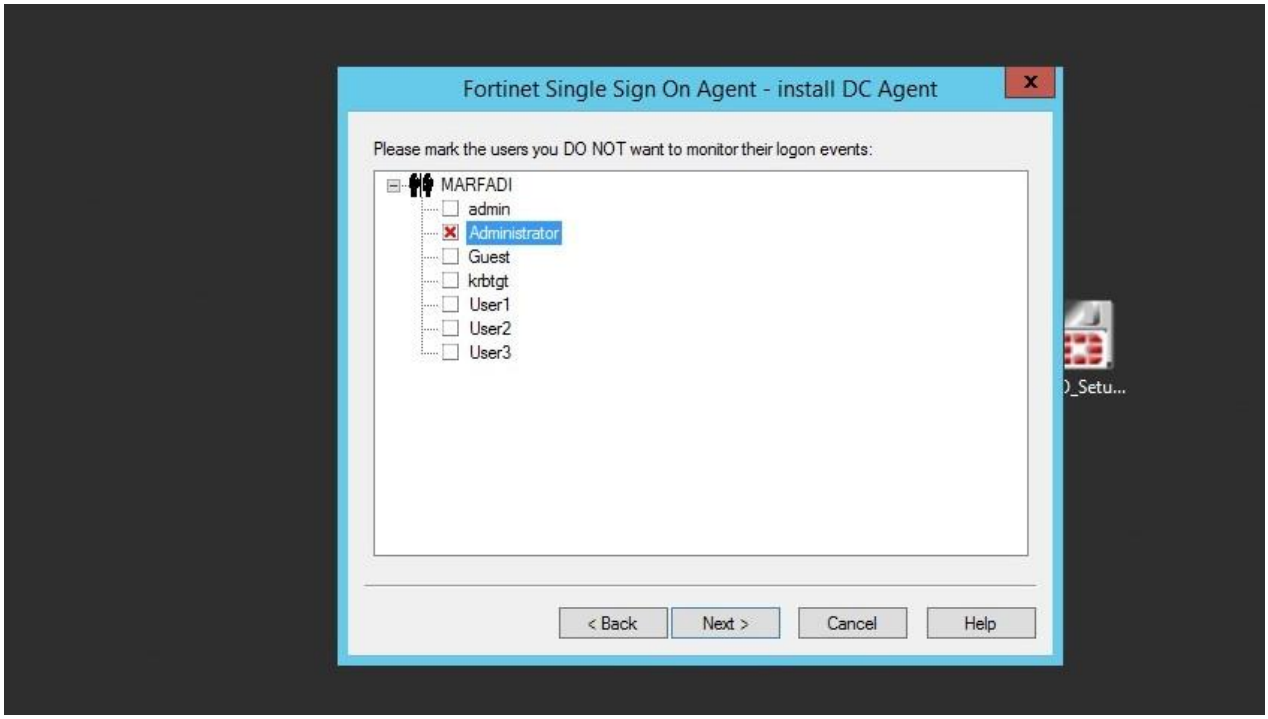


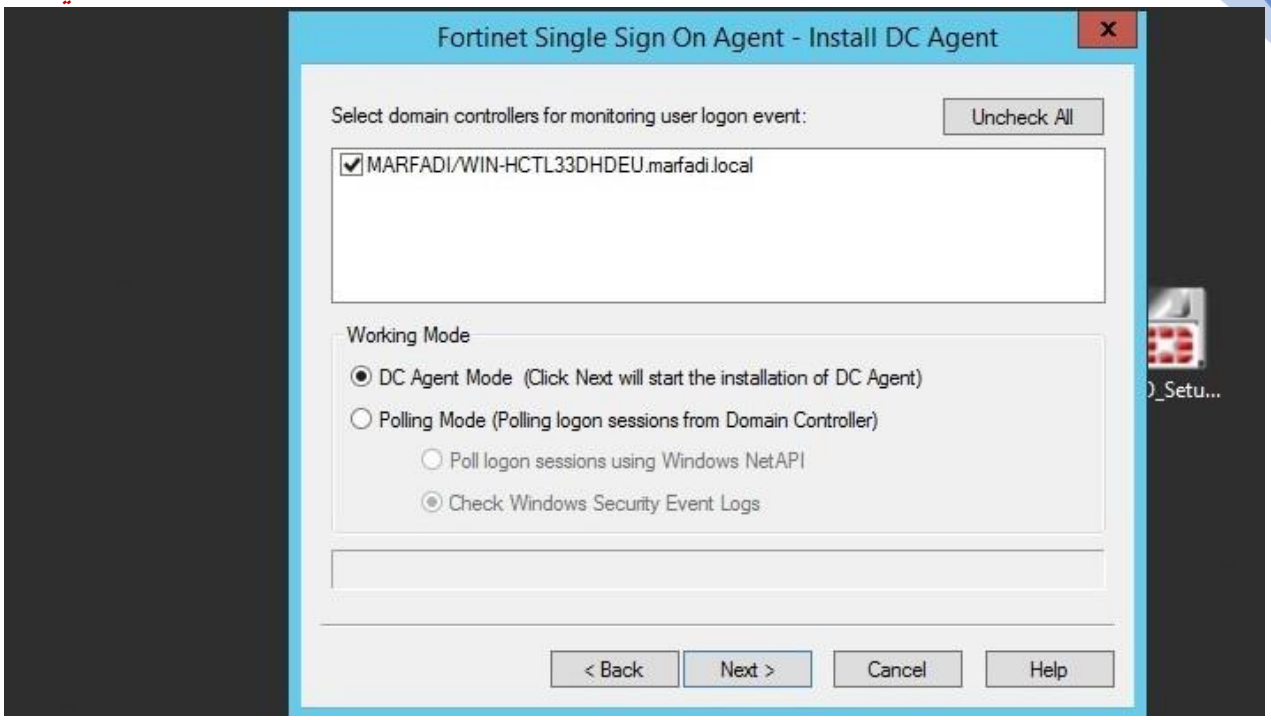

Fortinet Single Sign On Agent
Completed the Fortinet SSO Collector Agent v5.0.0243 Setup Wizard
Click the Finish button to exit the Setup Wizard.
Launch DC Agent Install Wizard
Back
Finish
Cancel
Setu...
Windows Server 2012 R2

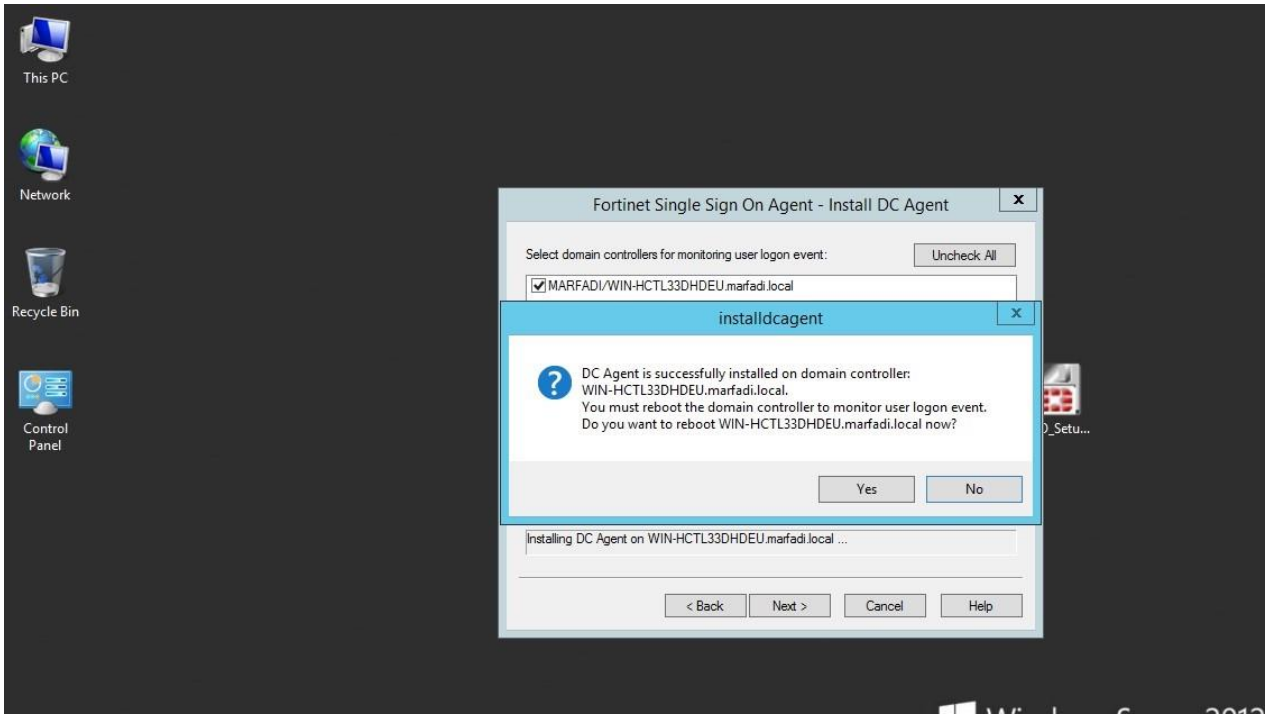

Fortinet Single Sign On Agent - Install DC Agent
Welcome to the DC Agent installation wizard. This wizard will install DC Agent on the Domain Controllers in your domain.
First please confirm the Collector Agent address and listening port.
Collector Agent
Collector Agent IP address:
192.168.2.11
Collector Agent listening port:
8002
Note: You need to have administrator access to the domain controller in order to install the DC Agent!
< Back
Next >
Cancel
Help
_Setu...
Windows Server 2012 R2

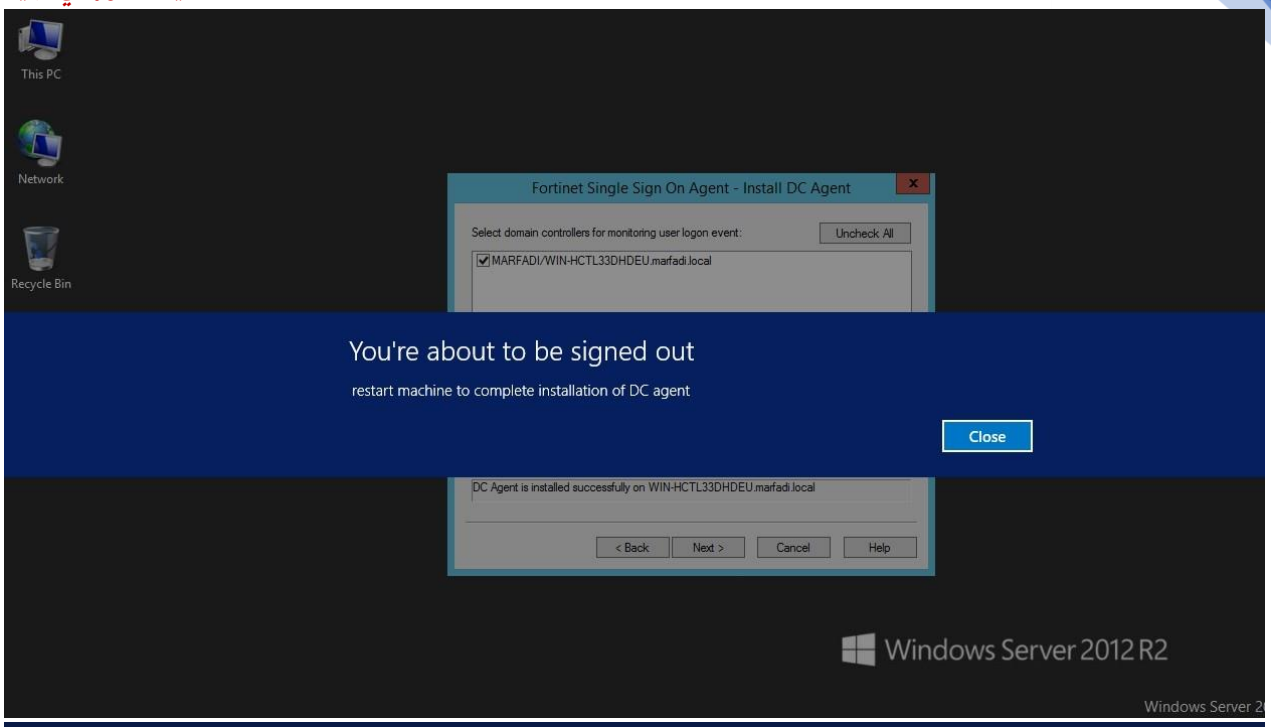


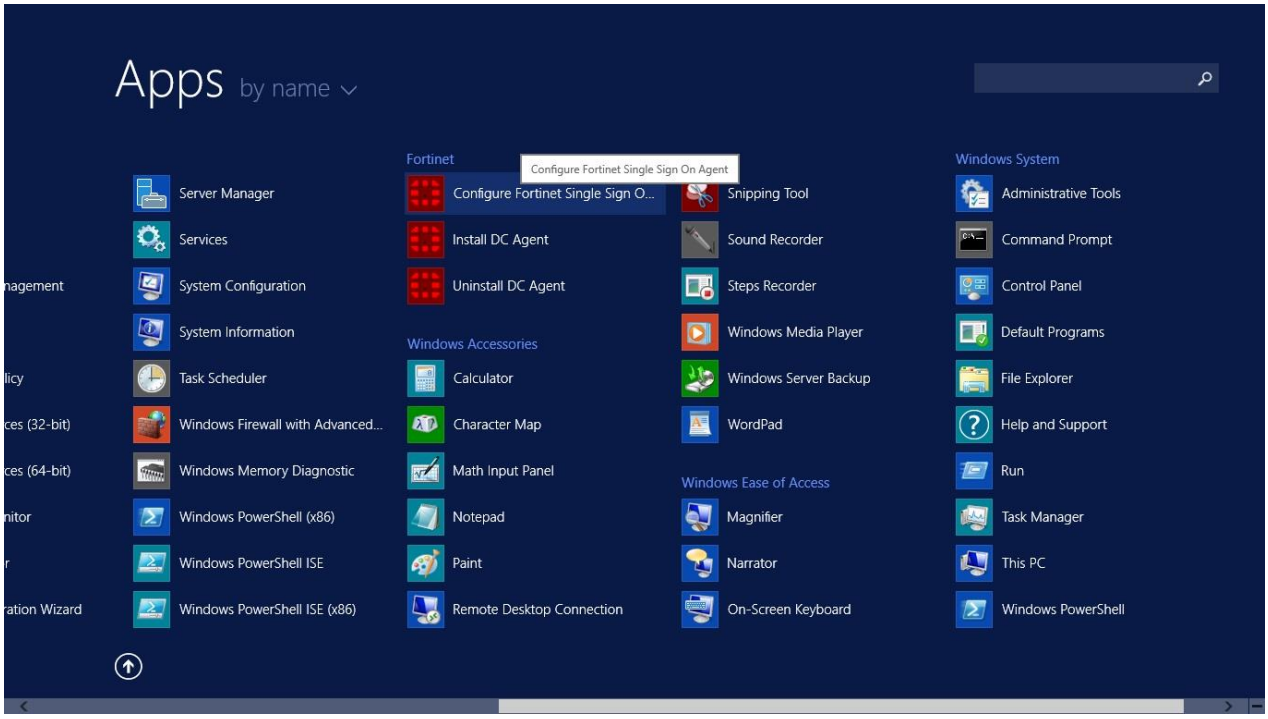
نقوم بتحديد اليوزرات المراد استثنائها من عمليه الـ monitoring عبر برنامج FSSO Agent حيث تم استثناء اليوزر Administrator

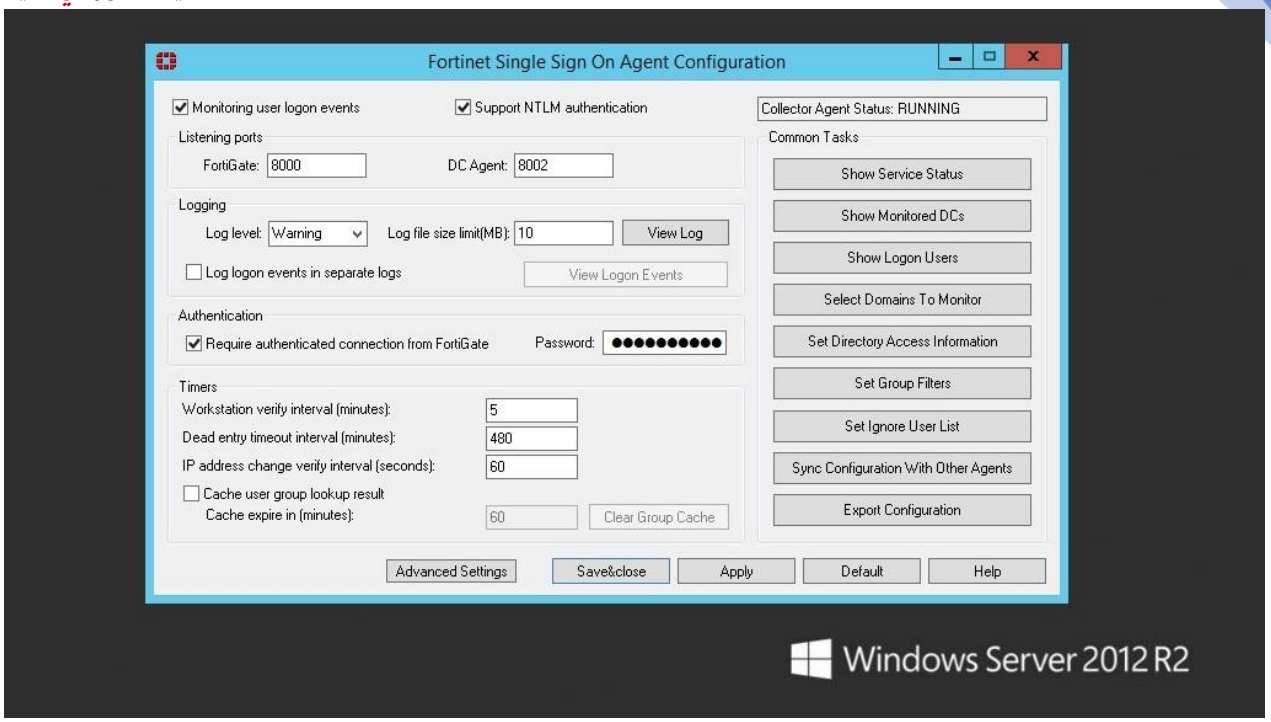


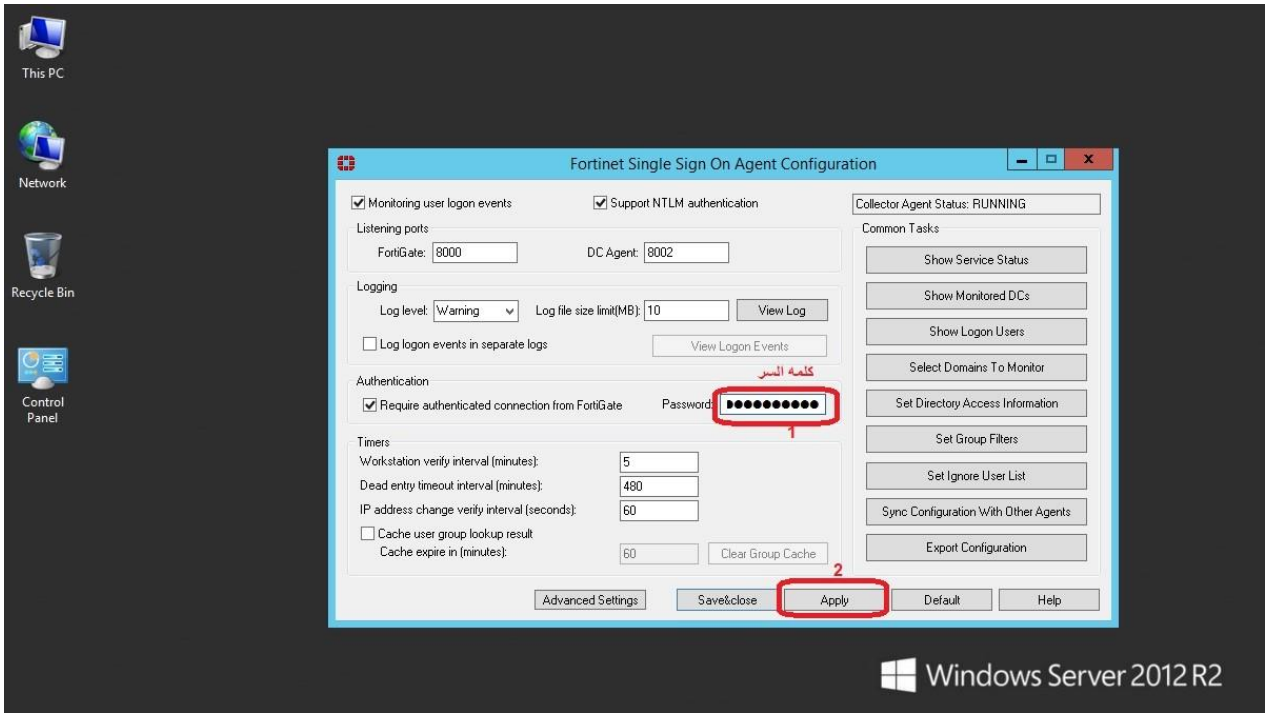

Fortinet Single Sign On Agent - Install DC Agent
Select domain controllers for monitoring user logon event:
Uncheck All
MARFADI/WIN-HCTL33DHDEU.marfadi.local
Working Mode
DC Agent Mode (Click Next will start the installation of DC Agent)
Polling Mode (Polling logon sessions from Domain Controller)
Poll logon sessions using Windows NetAPI
Check Windows Security Event Logs
< Back
Next >
Cancel
Help


This PC
Network
Recycle Bin
Control Panel
Fortinet Single Sign On Agent - Install DC Agent
Select domain controllers for monitoring user logon event:
Uncheck All
MARFADI/WIN-HCTL33DHDEU.marfadi.local
installdcagent
DC Agent is successfully installed on domain controller:
WIN-HCTL33DHDEU.marfadi.local.
You must reboot the domain controller to monitor user logon event.
Do you want to reboot WIN-HCTL33DHDEU.marfadi.local now?
Yes
No
Installing DC Agent on WIN-HCTL33DHDEU.marfadi.local ...
< Back
Next >
Cancel
Help

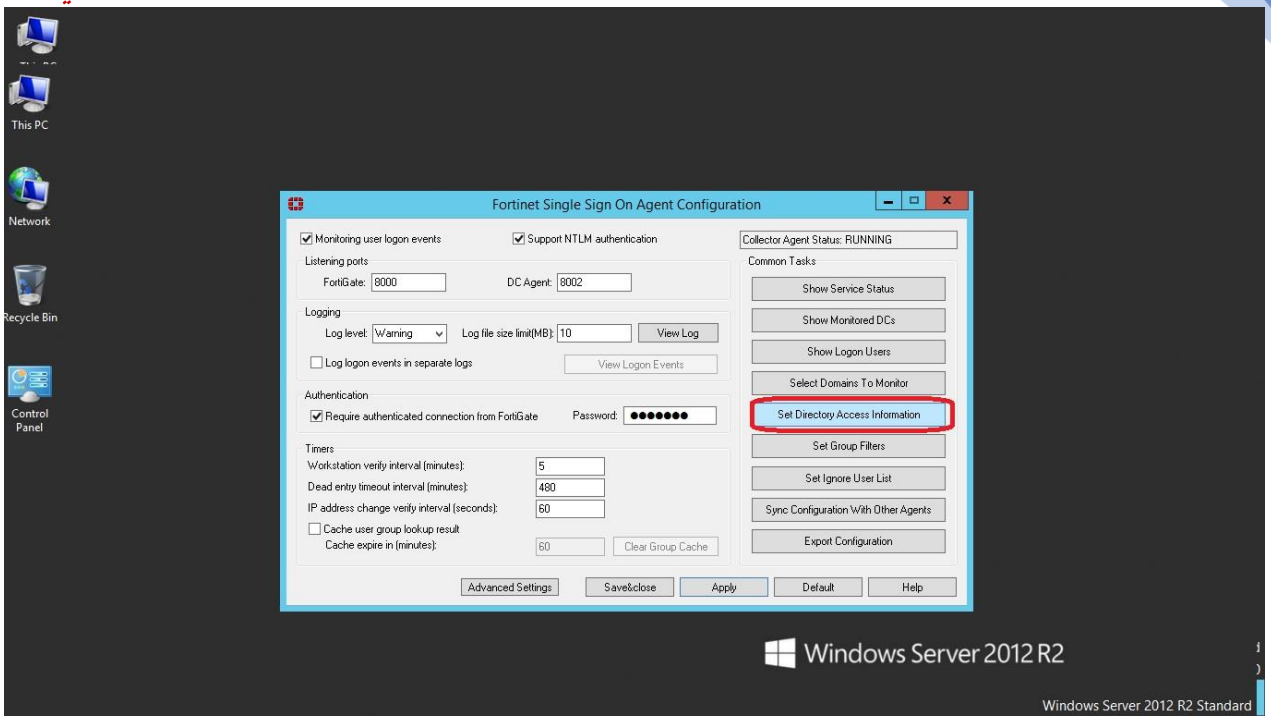

This PC
Network
Recycle Bin
Fortinet Single Sign On Agent - Install DC Agent
Select domain controllers for monitoring user logon event:
Uncheck All
MARFADI/WIN-HCTL33DHDEU.marfadi.local
You're about to be signed out
restart machine to complete installation of DC agent
Close
DC Agent is installed successfully on WIN-HCTL33DHDEU.marfadi.local
< Back
Next >
Cancel
Help
Windows Server 2012 R2

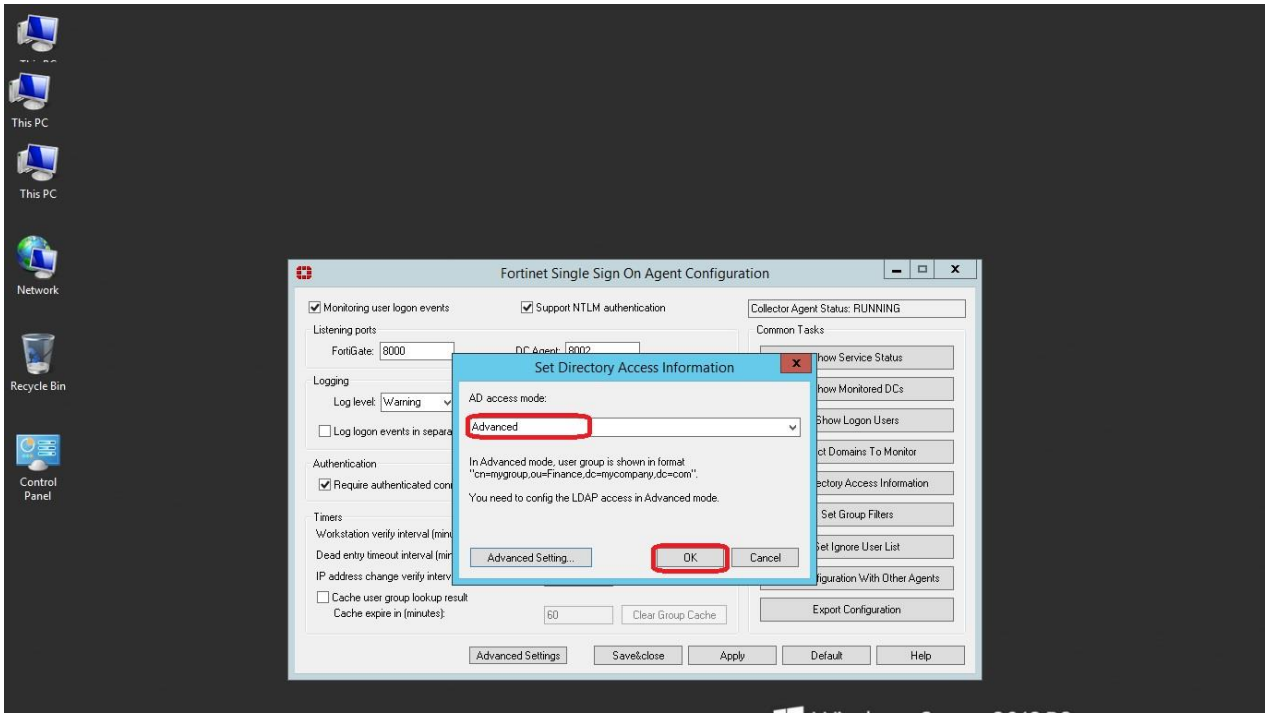

Apps by name
Server Manager
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced...
Windows Memory Diagnostic
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Fortinet
Configure Fortinet Single Sign On Agent
Configure Fortinet Single Sign O...
Install DC Agent
Uninstall DC Agent
Windows Accessories
Calculator
Character Map
Math Input Panel
Notepad
Paint
Remote Desktop Connection
Snipping Tool
Sound Recorder
Steps Recorder
Windows Media Player
Windows Server Backup
WordPad
Windows Ease of Access
Magnifier
Narrator
On-Screen Keyboard
Windows System
Administrative Tools
Command Prompt
Control Panel
Default Programs
File Explorer
Help and Support
Run
Task Manager
This PC
Windows PowerShell



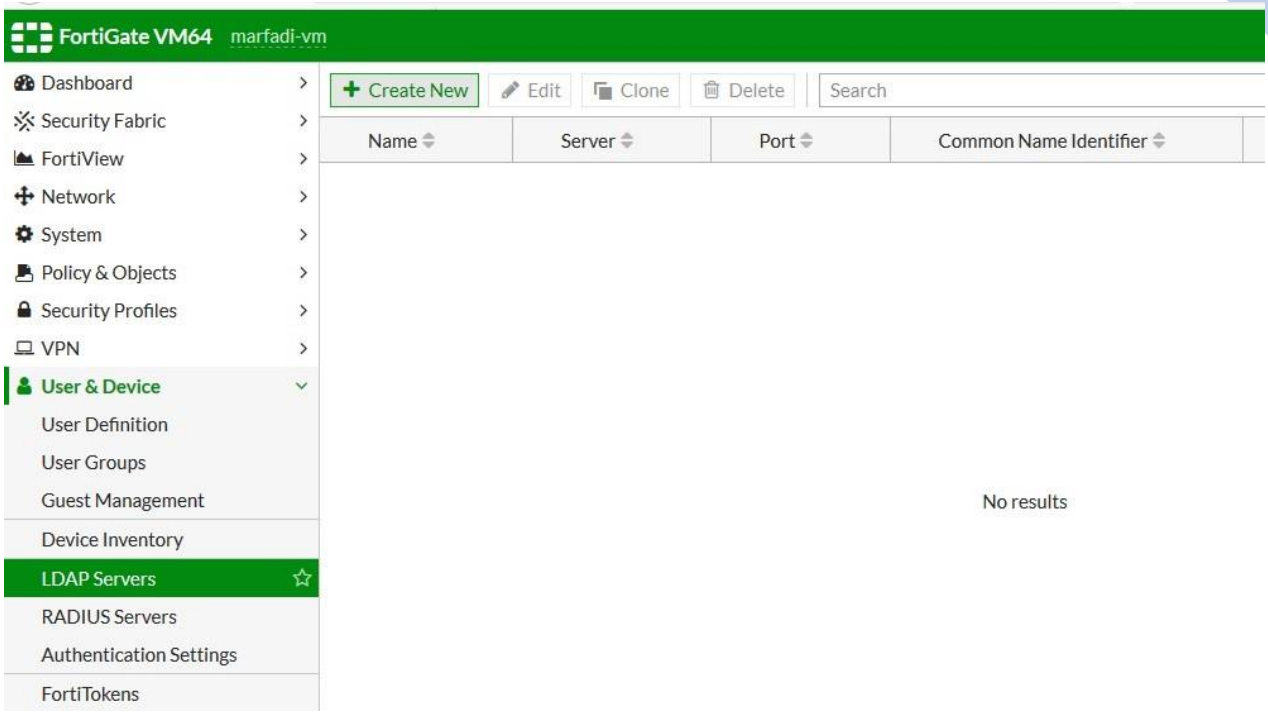


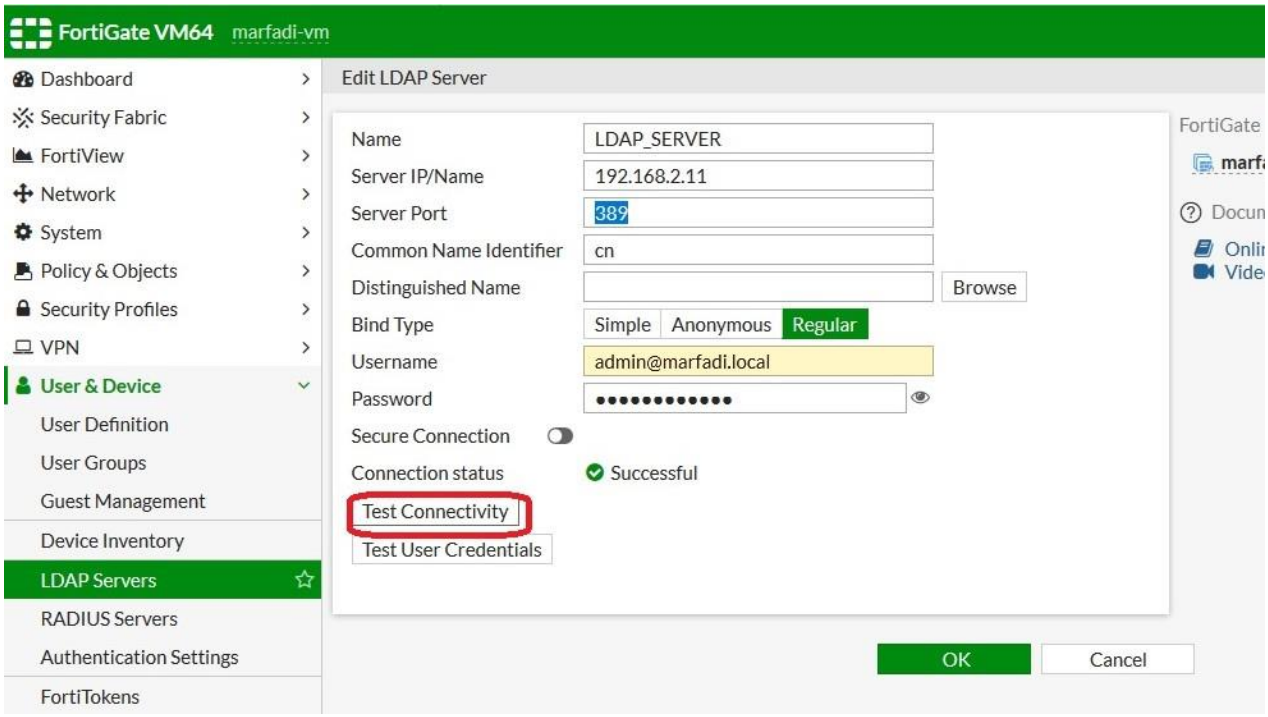
كما بالصورة أعلاه قم بكتابه باسورد (ليش شرط ان يكون نفس باسورد الدومين ادمن)حيث ستحتاج لها لعمليه الاتصال بين الفورتي جيت وبرنامج FSSO ويفضل ان يكون معقد

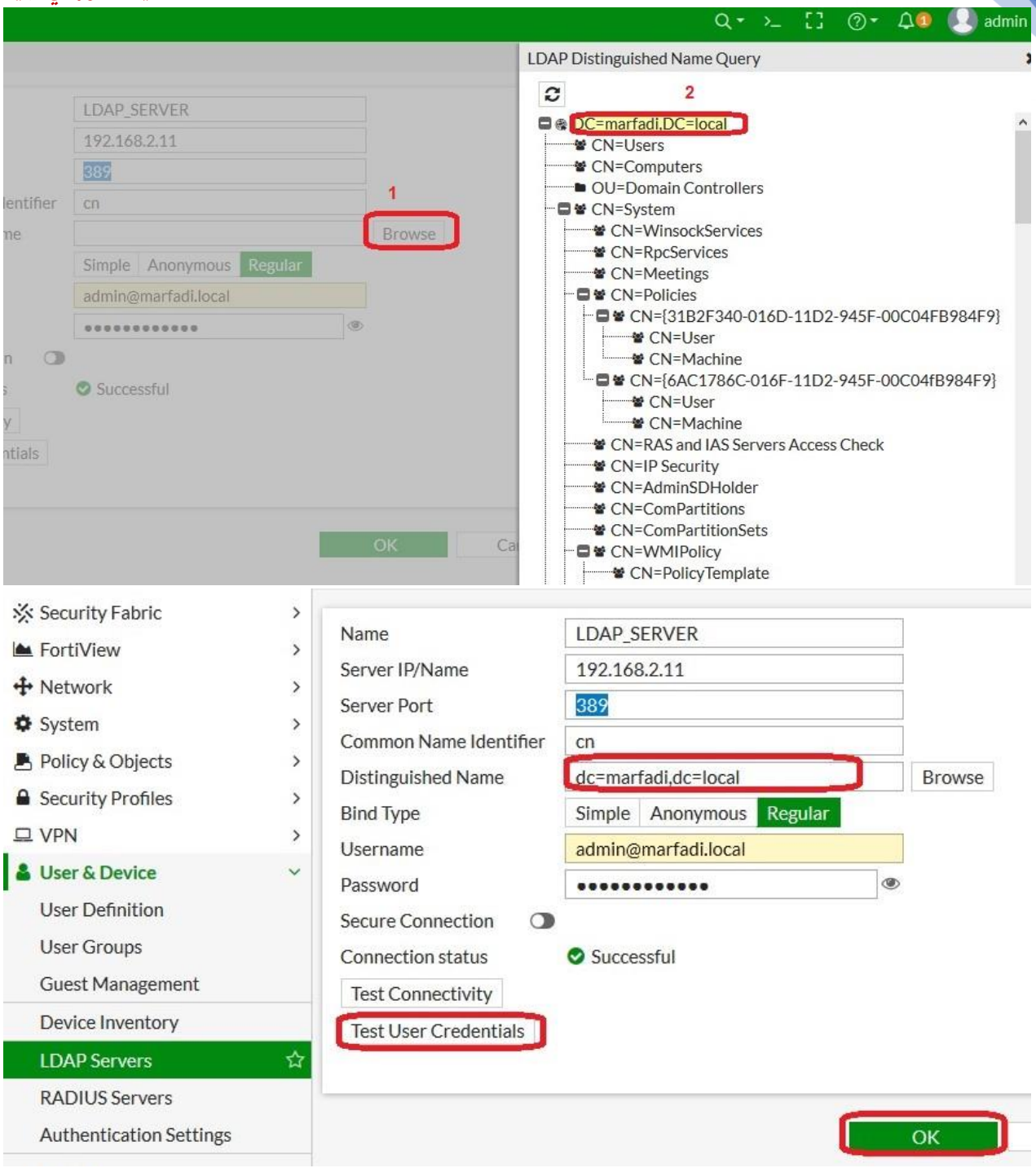


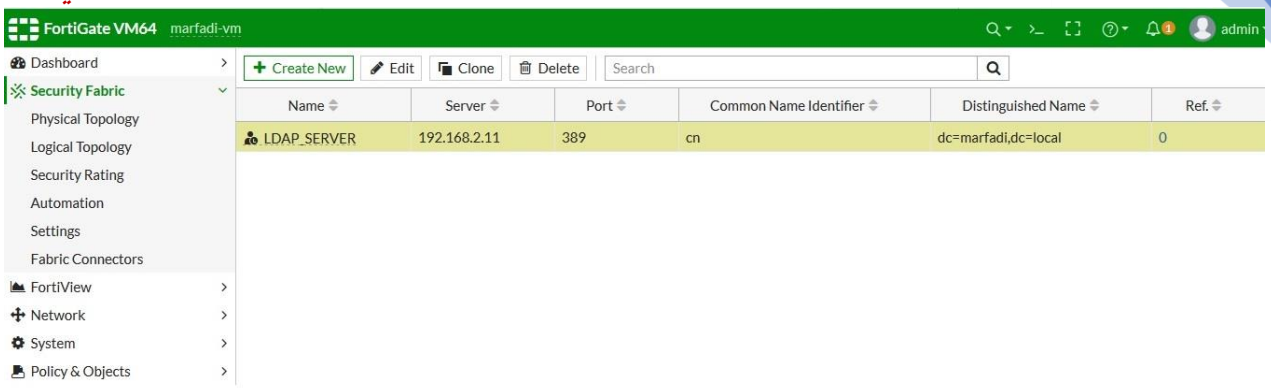


سنقوم بإنشاء LDAP SERVER كما بالصورة ادناه

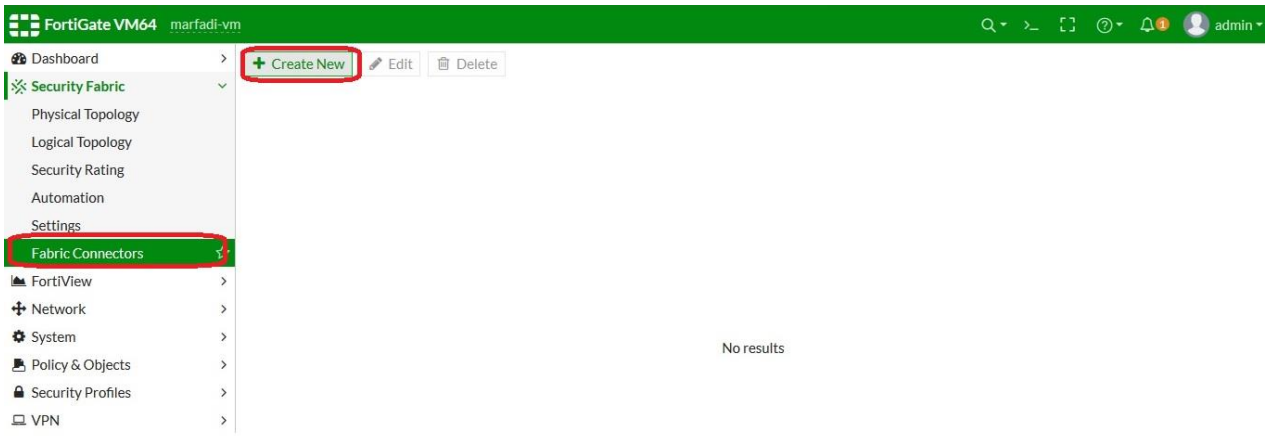

FortiGate VM64 marfadi-vm
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
User Definition
User Groups
Guest Management
Device Inventory
LDAP Servers
RADIUS Servers
Authentication Settings
FortiTokens
Create New
Edit
Clone
Delete
Search
Name
Server
Port
Common Name Identifier
No results

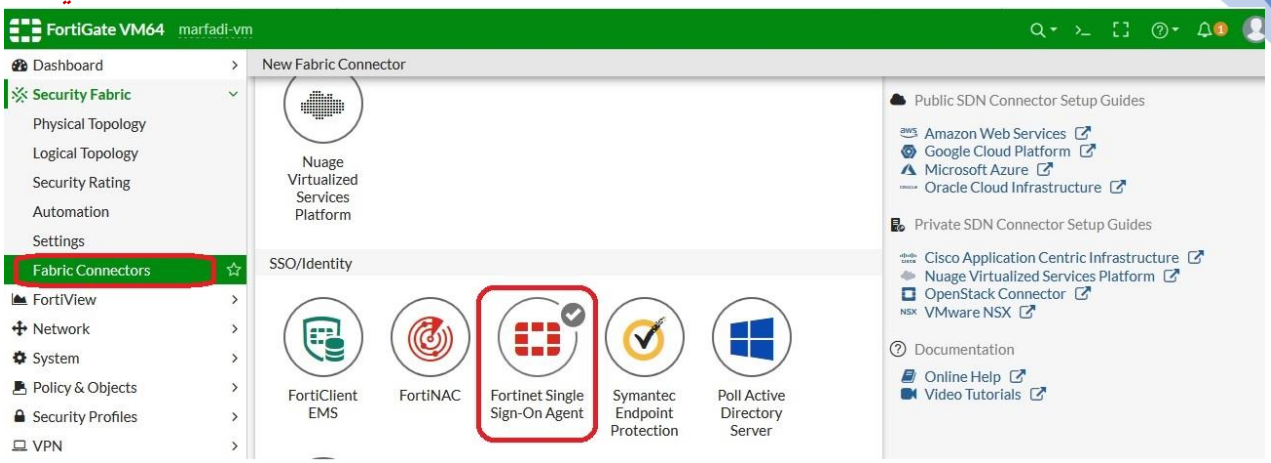

FortiGate VM64 marfadi-vm
Edit LDAP Server
Name
LDAP_SERVER
Server IP/Name
192.168.2.11
Server Port
389
Common Name Identifier
cn
Distinguished Name
Browse
Bind Type
Simple
Anonymous
Regular
Username
admin@marfadi.local
Password
Secure Connection
Connection status
Successful
Test Connectivity
Test User Credentials
OK
Cancel

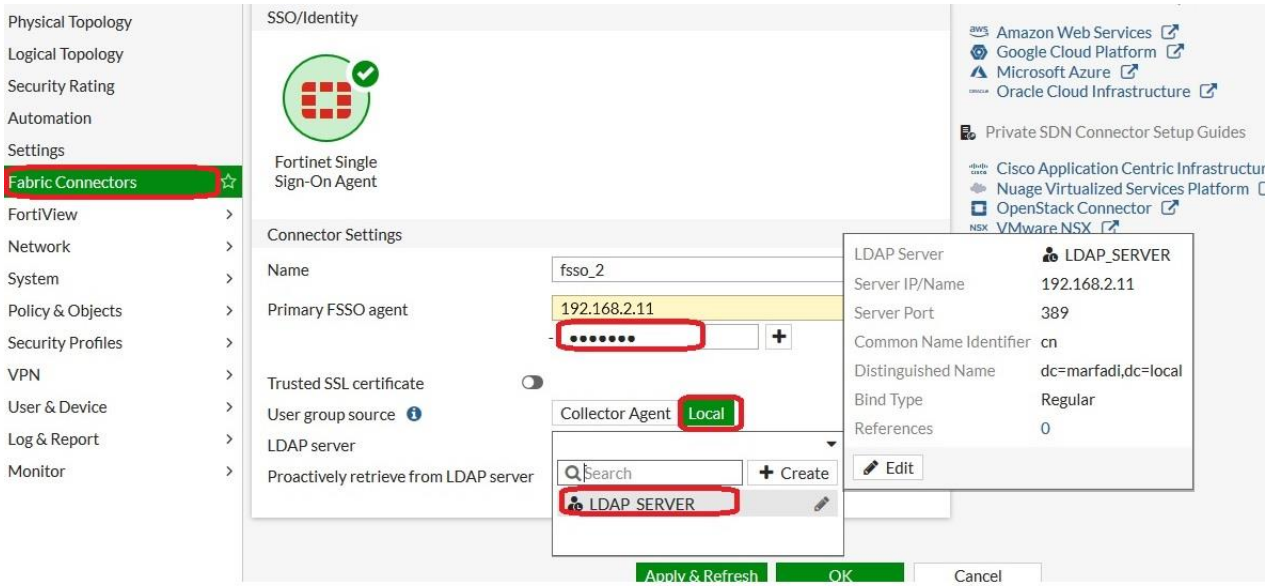

admin
LDAP_SERVER
192.168.2.11
389
cn
Browse
Simple
Anonymous
Regular
admin@marfadi.local
Successful
OK
1
LDAP Distinguished Name Query
2
DC=marfadi,DC=local
CN=Users
CN=Computers
OU=Domain Controllers
CN=System
CN=WinsockServices
CN=RpcServices
CN=Meetings
CN=Policies
CN={31B2F340-016D-11D2-945F-00C04FB984F9}
CN=User
CN=Machine
CN={6AC1786C-016F-11D2-945F-00C04fB984F9}
CN=User
CN=Machine
CN=RAS and IAS Servers Access Check
CN=IP Security
CN=AdminSDHolder
CN=ComPartitions
CN=ComPartitionSets
CN=WMIPolicy
CN=PolicyTemplate
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
Name
LDAP_SERVER
Server IP/Name
192.168.2.11
Server Port
389
Common Name Identifier
cn
Distinguished Name
dc=marfadi,dc=local
Browse
Bind Type
Simple
Anonymous
Regular
Username
admin@marfadi.local
Password
Secure Connection
Connection status
Successful
Test Connectivity
Test User Credentials
OK



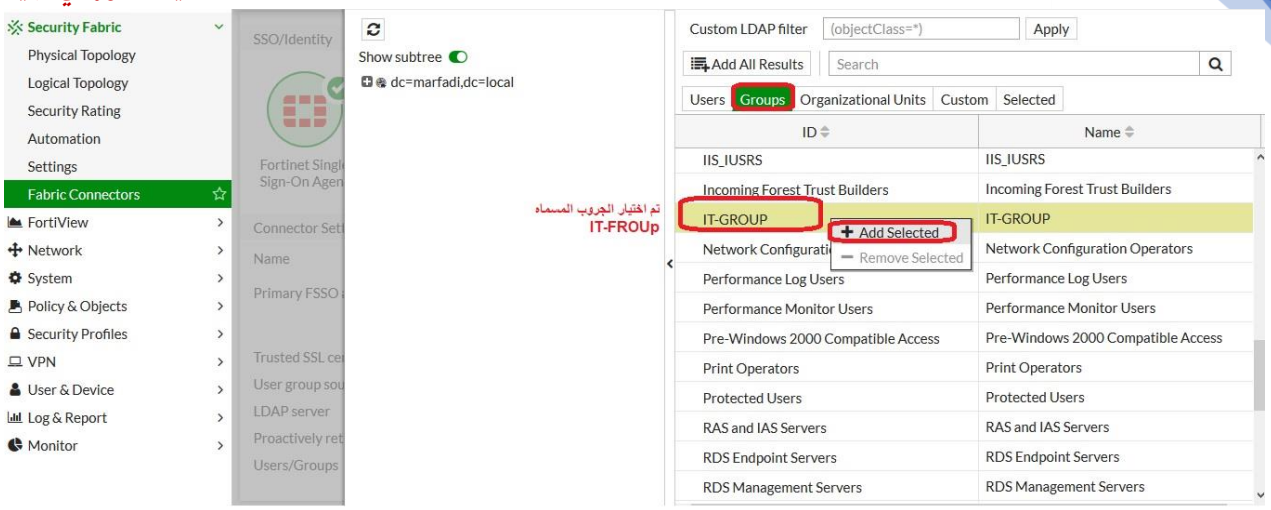
تم انشاء LDAP SERVER بنجاح باسم LDAP_SERVER والذي سنستخدمه لاحقا ..



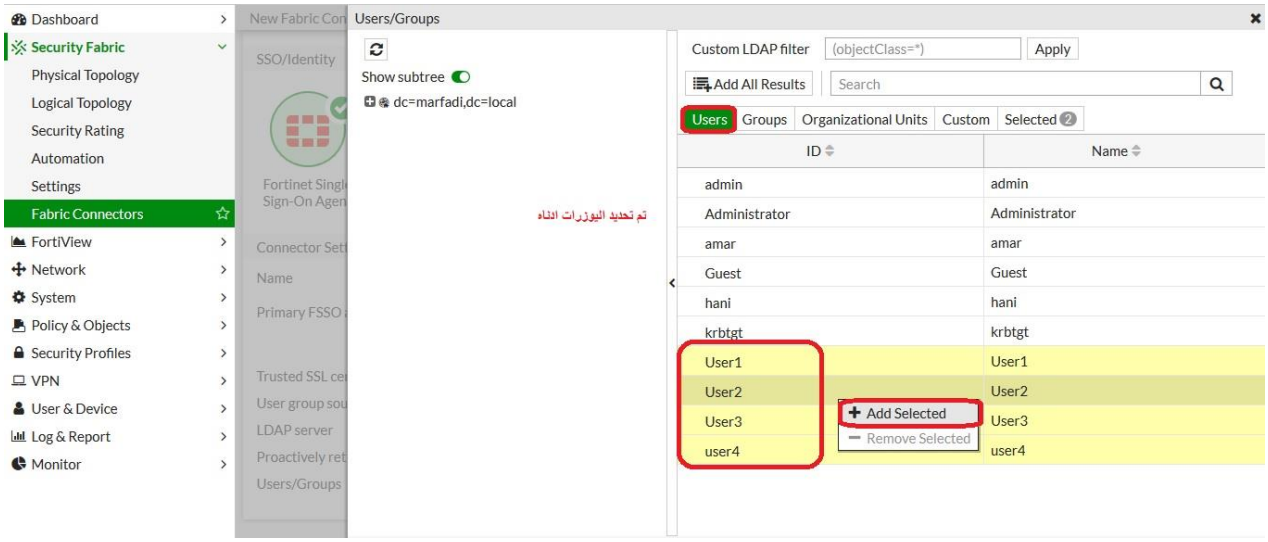




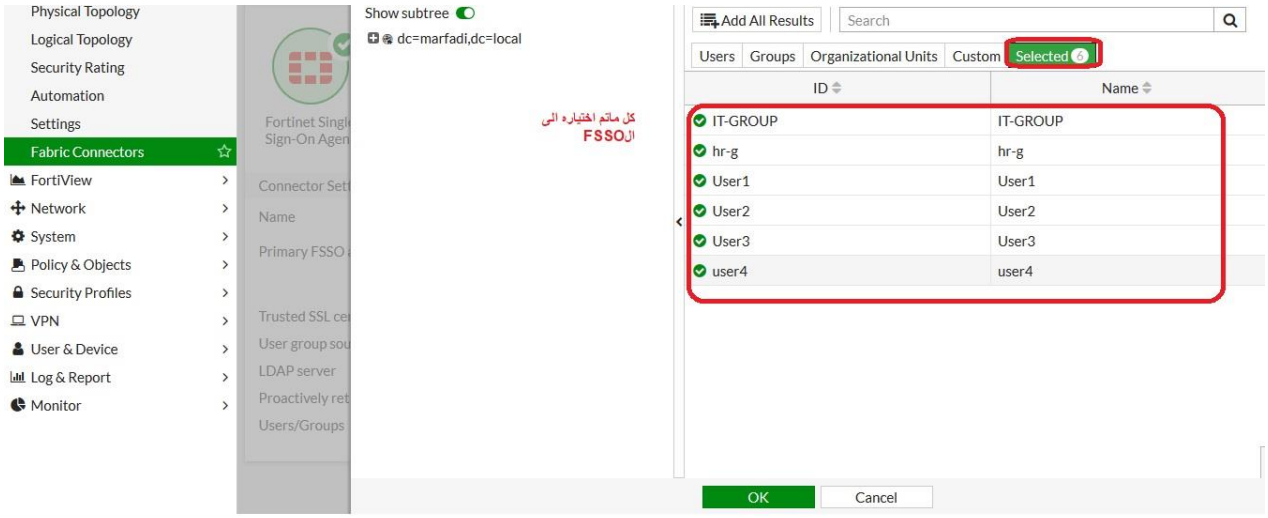
هنا الباسورد هي نفسها التي قمنا بإنشائها في برنامج FSSO على سيرفر الدومين (AD)وهناك طريقتين للحصول على اليوزرات والجروبات التي موجودة على سيرفر الAD اما نقوم باختيار الخيار Local كما بالصورة أعلاه ومن ثم نختار الLDAP SERVER الذي قمنا بإنشاء ه سابقا ..



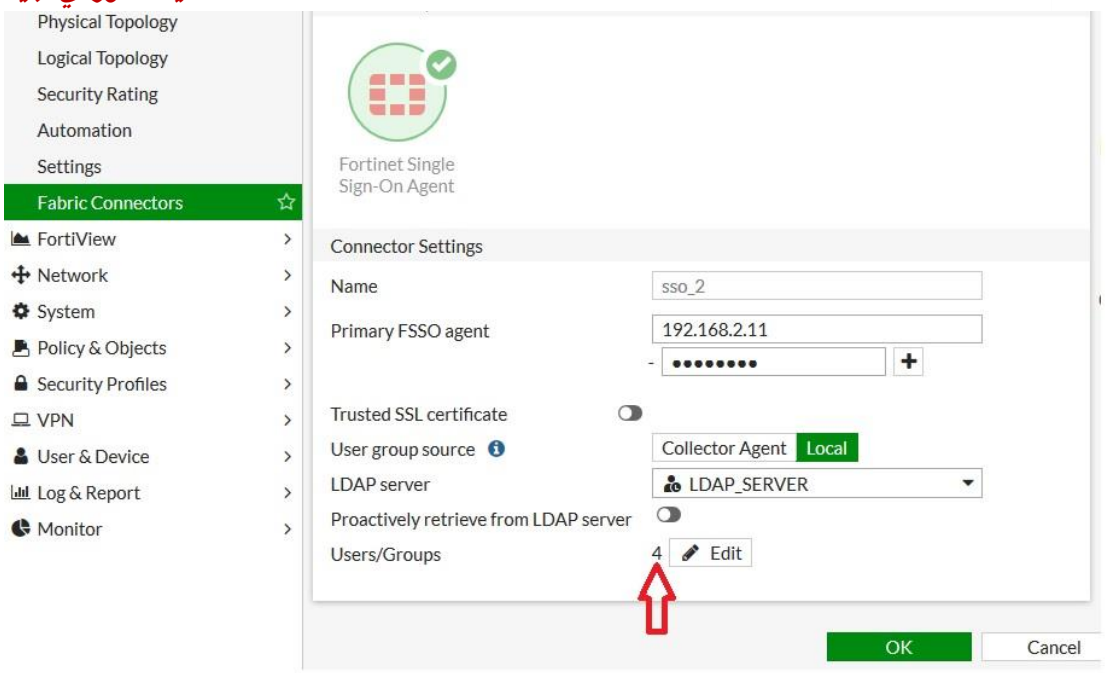
كما بالصورة أعلاه سنقوم بتحديد الجروبات واليوزرات الموجودة في الAD والتي تريد أضافتها (intergrated)مع الفورتي جيت



بعد تحديد اليوزرات المطلوب أضافتها الى الفورتي جيت



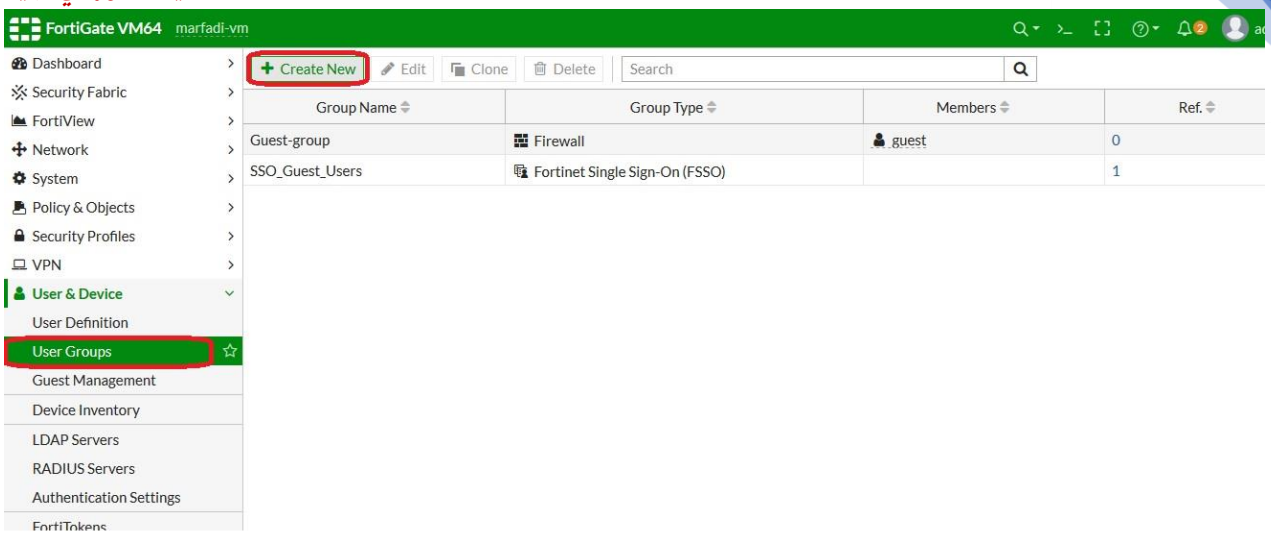
كما بالصورة أعلاه تبين بأن عدد العناصر التي تم أضافتها هي 6

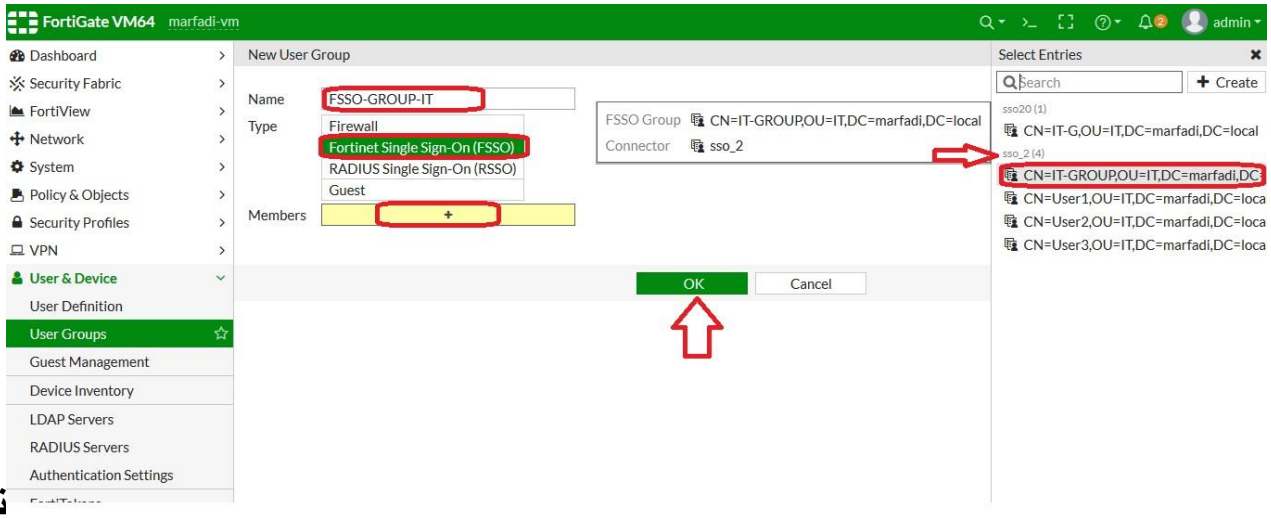


تلاحظ العدد هنا 4 عناصر تم إضافتها ومن ثم نختار OK

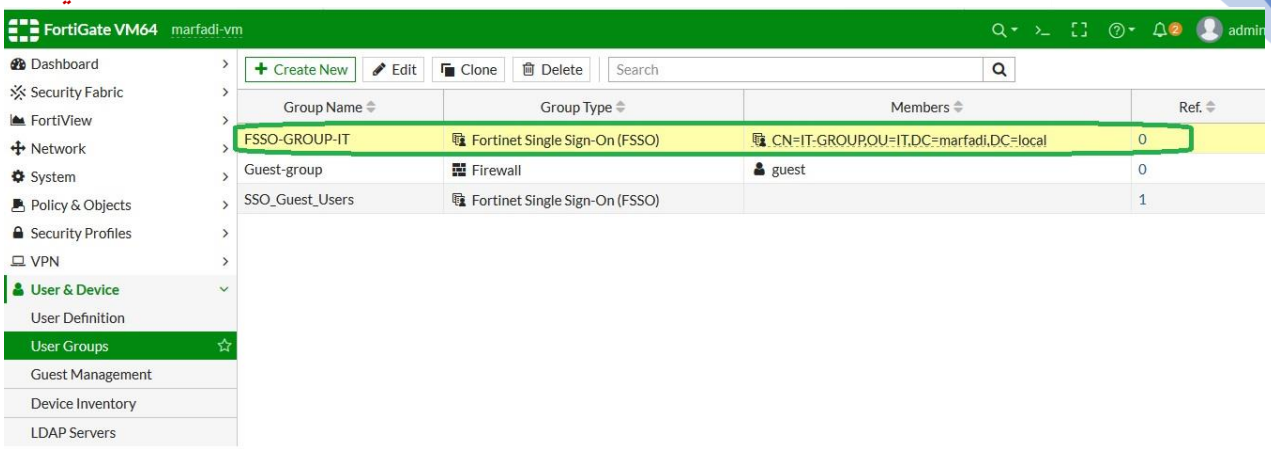
لو كان السهم باللون الأحمر فذلك يعني بأن الاتصال بين الفورتي جيت والـAD غير سليم نتأكد بأن لفايروول على سيرفر الـAD مقفول ..

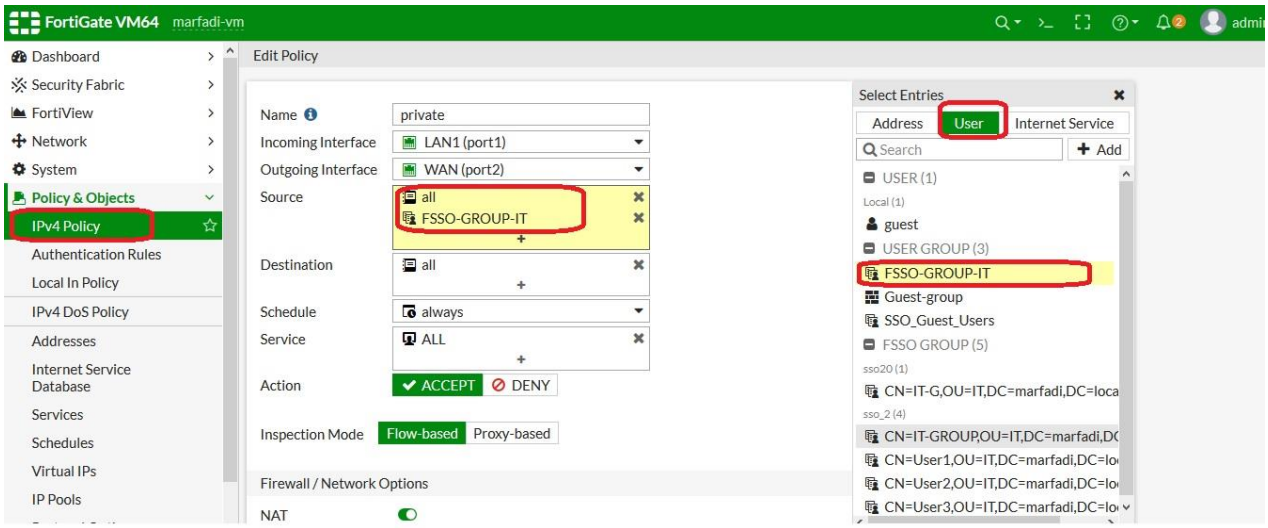
الان سنقوم بإنشاء جروب من نوع FSSO ونقوم بأضافه اليوزرات او الجروبات التي قمنا باختيارها سابقا (selected) في الخطوات السابقة حيث هذه الجروب سيتم تطبيق بوليسي معينه عليها لاحقا ..



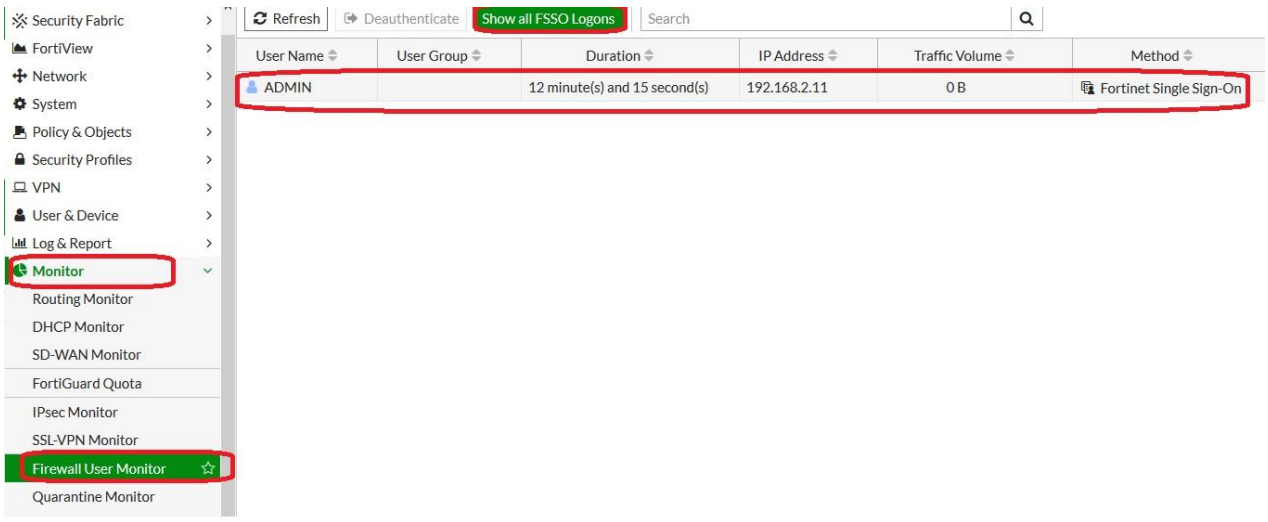


تم اختيار الجروب المسماة IT-GROUP والموجودة على AD



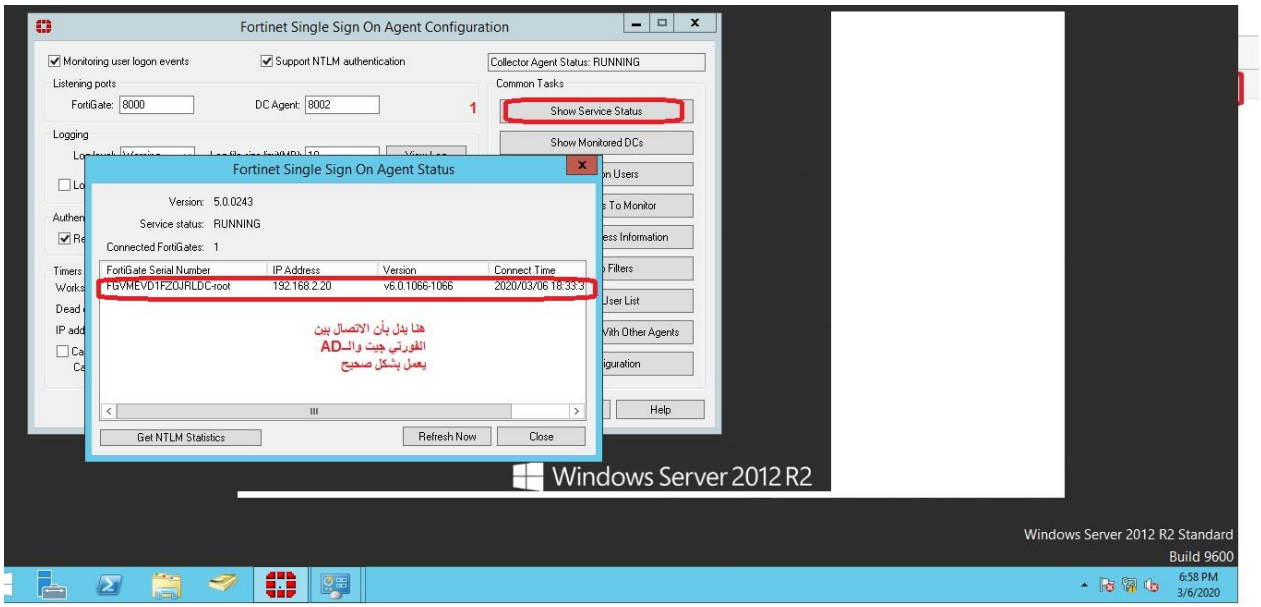


تم تطبيق البوليسي على الجروب من نوع FSSO واسمها FSSO-GROUP-IT والتي قمنا بانشائها سابقا ...

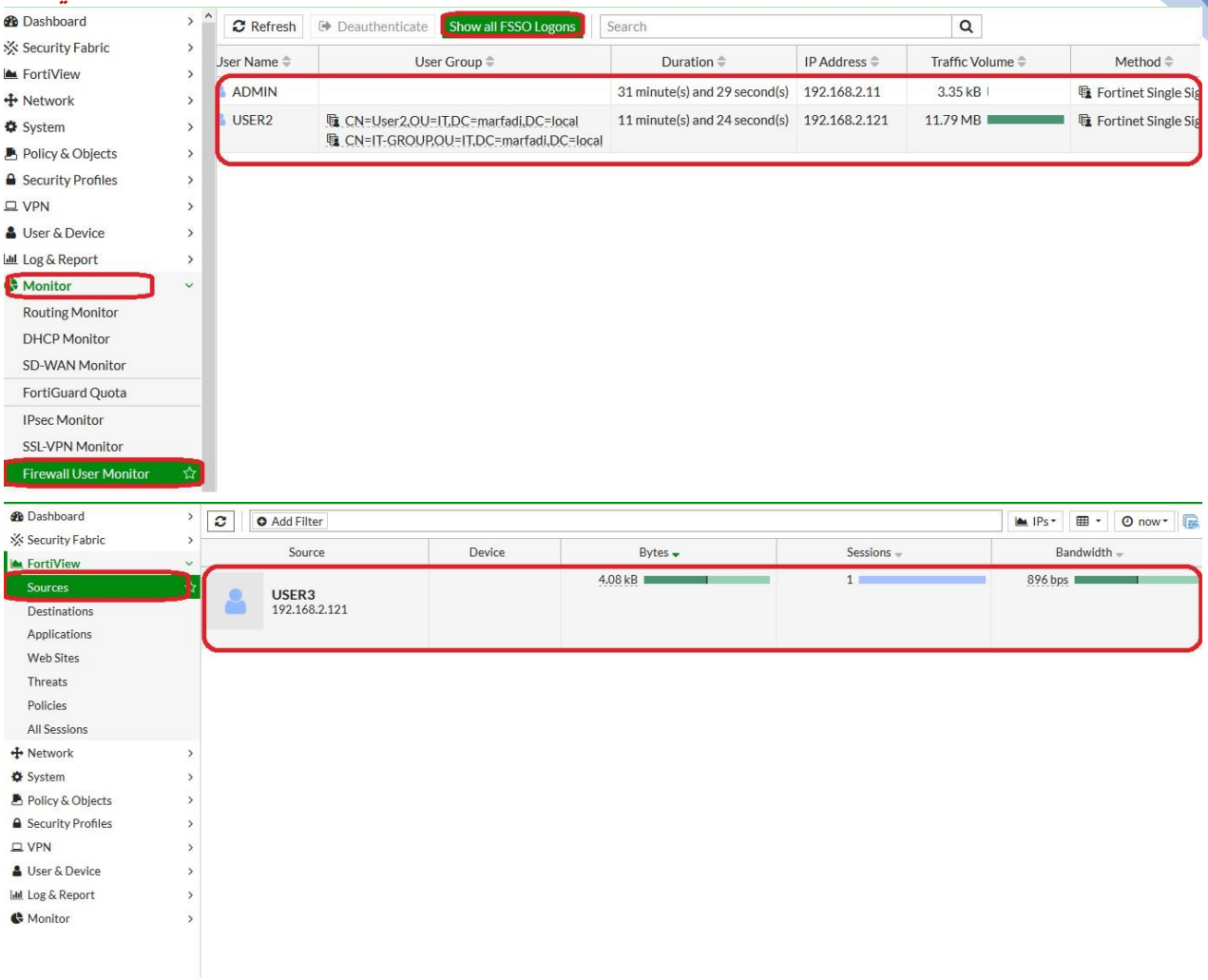


لمراقبه اليوزرات التي ضمن fsso ...

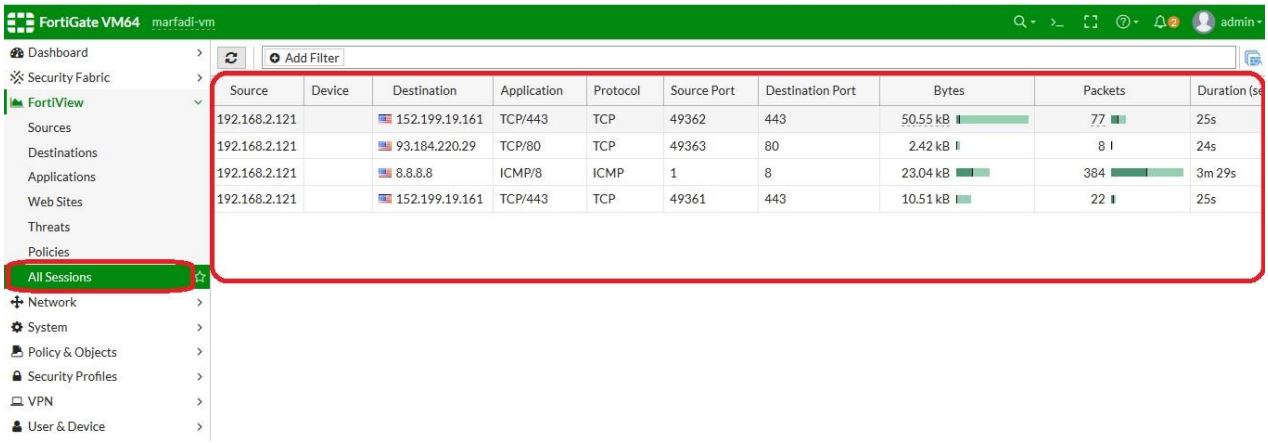
كما بالصورة ادناه يتبين بأن الاتصال بين الفورتي جيت والـ AD سليم ..



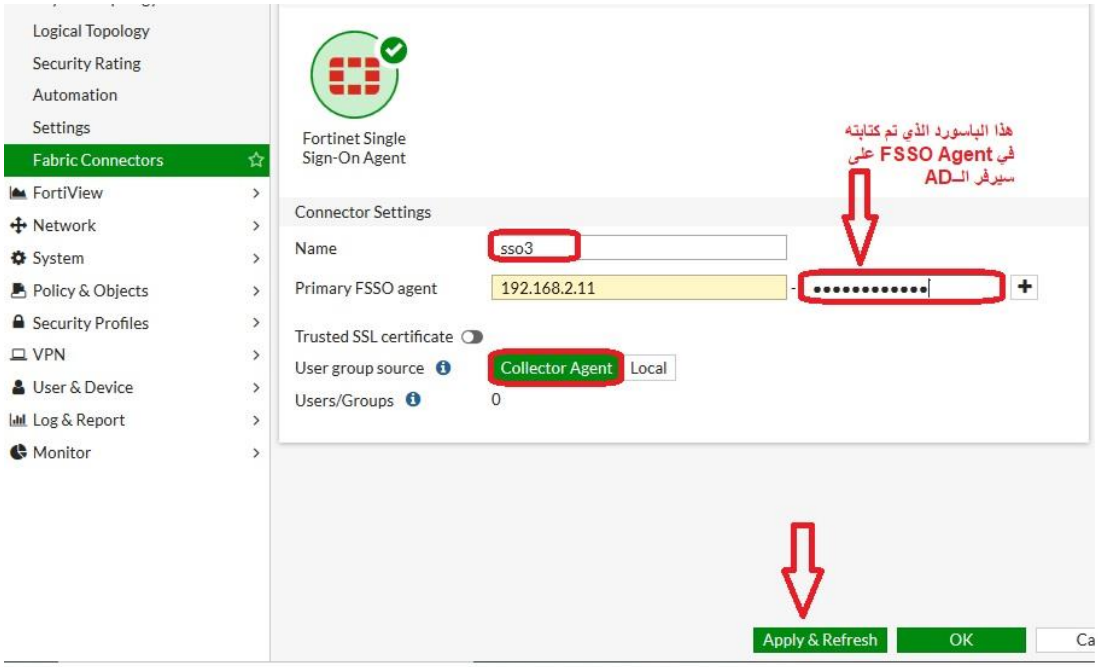
كما قلنا سابقا لو تريد مراقبه اليوزرات التي ضمن FSSO من حيث المده التي يعمل عليها والايبي وحجم الترافيك كما بالصورة ادناه ...

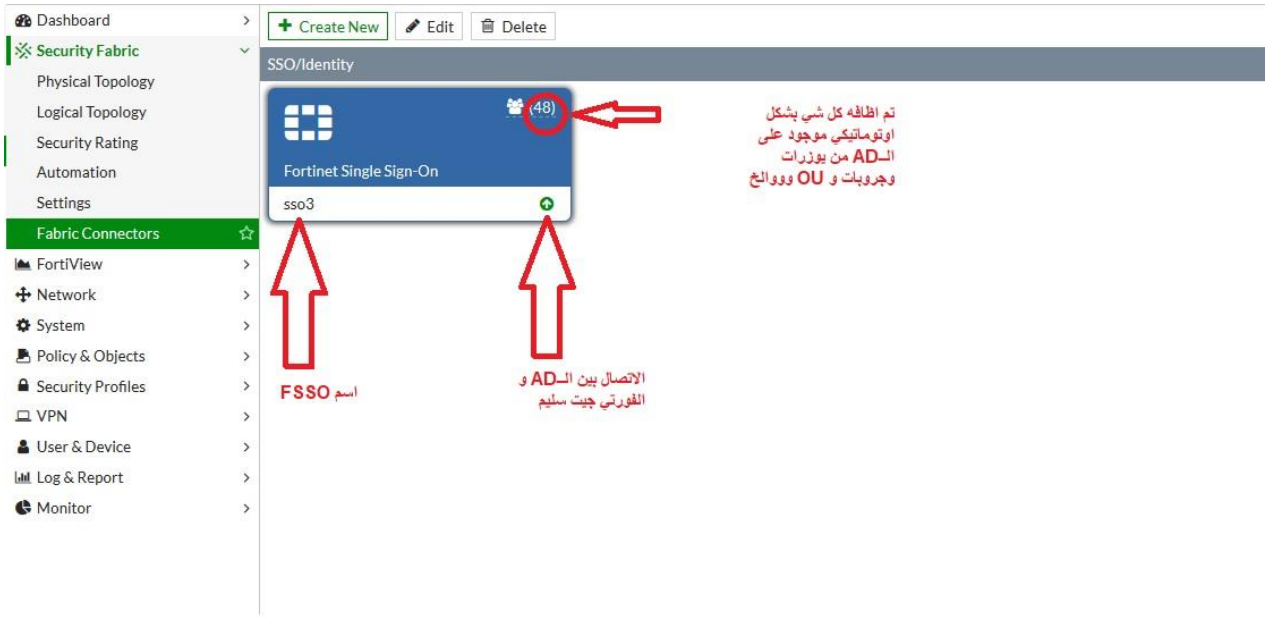


يظهرلك كل الجلسات المستخدمة وحجم الترافيك والمده ..



❖ هذه هي الطريقة الثانية(خيار اخر) لعمل integration عبر اختيار الـــCollector Agent





كما بالصورة أعلاه تم أضافه كل الجروبات والOU الموجودة على الاكتف دايركتوري الى الفورتي جيت (عددها 48 عنصر)...

Antivirus

ماهي أنواع الـ antivirus DataBase ؟

١. Normal antivirus signatures Database :هذا النوع موجود في أي جهازفورتي جيت انت تشتريه بغض النظرعن نوعه حيث الداتا بيزالموجودة فيه بيتم اعدادها من قبل الفورتي جارد(FortiGuard) من قبل فريق البحث لشركه الفورتي نت حيث تحتوي الـ database لهذا النوع على اشهرأنواع الفايروسات حيث الجهازعندما يقوم بالفحص يقوم بعمل مقارنه ما بين الملفات التي تصل اليه من خارج الشبكة وبين ال signatures الموجودة في الداتا بيزفلووجد بأن الملف له signature متشابه مع التي موجودة لديه في الـDB فيقوم الجهازباعتبارهذا الملف على انه فايروس وبيعمل له الـ action المناسب .

٢. Extended :هذا النوع متوفرفي اغلب موديلات فورتي جيت (ليس جميعها)حيث بتحتوي على النوع الأول (Normal)+DB على الفايروسات الغيرفعاله اوغيرنشطه حيث ممكن هذا الفايروسات ممكن تتنشط ويعاد نشاطها مره أخرى فهذا يكون الفورتي جيت لديه معلومة عن هذا النوع من الفايروسات ..

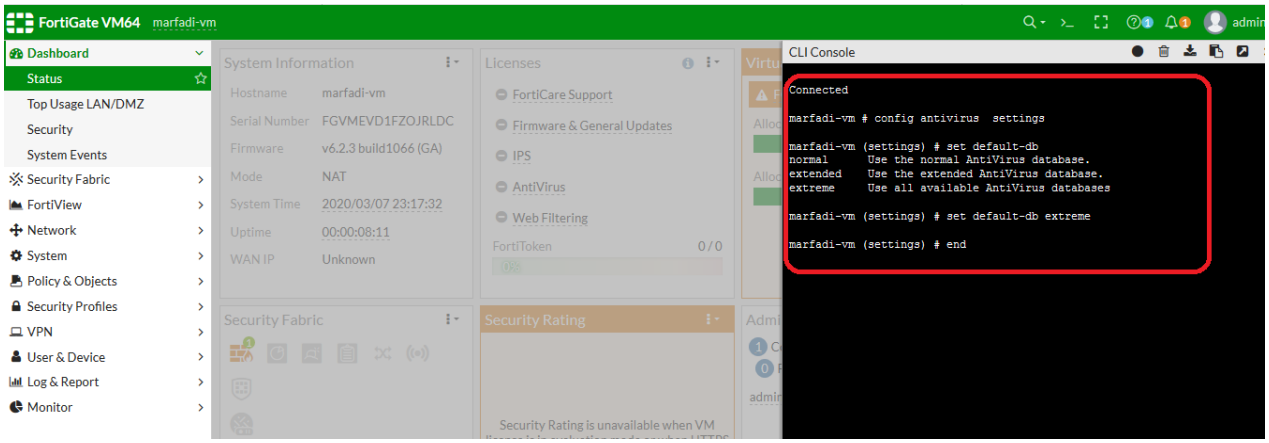
٣. Extreme :موجود هذا النوع من قواعد البيانات على بعض اجهزه الفورتي جيت حيث هي قاعده بيانات ضخمه وبتحتوي على DB النوعين السابقين +قاعده كبيره من الفايروسات حيث تكون مساحه هذا النوع كبيره جدا ولكنها توفراكبرامان وحمايه للشبكة .

حيث أي جهازقبل ماتشتريه يمكنك معرفة ماذا يدعم من قاعده بيانات من الفايروسات من الأنواع السابقة ..

- ملاحظة :نسخه fortigate VM لا يوجد بها licence للـ Antivirus .

كيف تفرق بين قواعد بيانات الفايروسات على جهاز الفورتي جيت ؟

بيتم ذلك عبر الcli ويجب ان يكون على جهاز حقيقي



كما بالصورة أعلاه تبين بأن الجهازيدعم جميع الأنواع الثلاثه حيث

بعد كتابه الامر

#set default-db ?

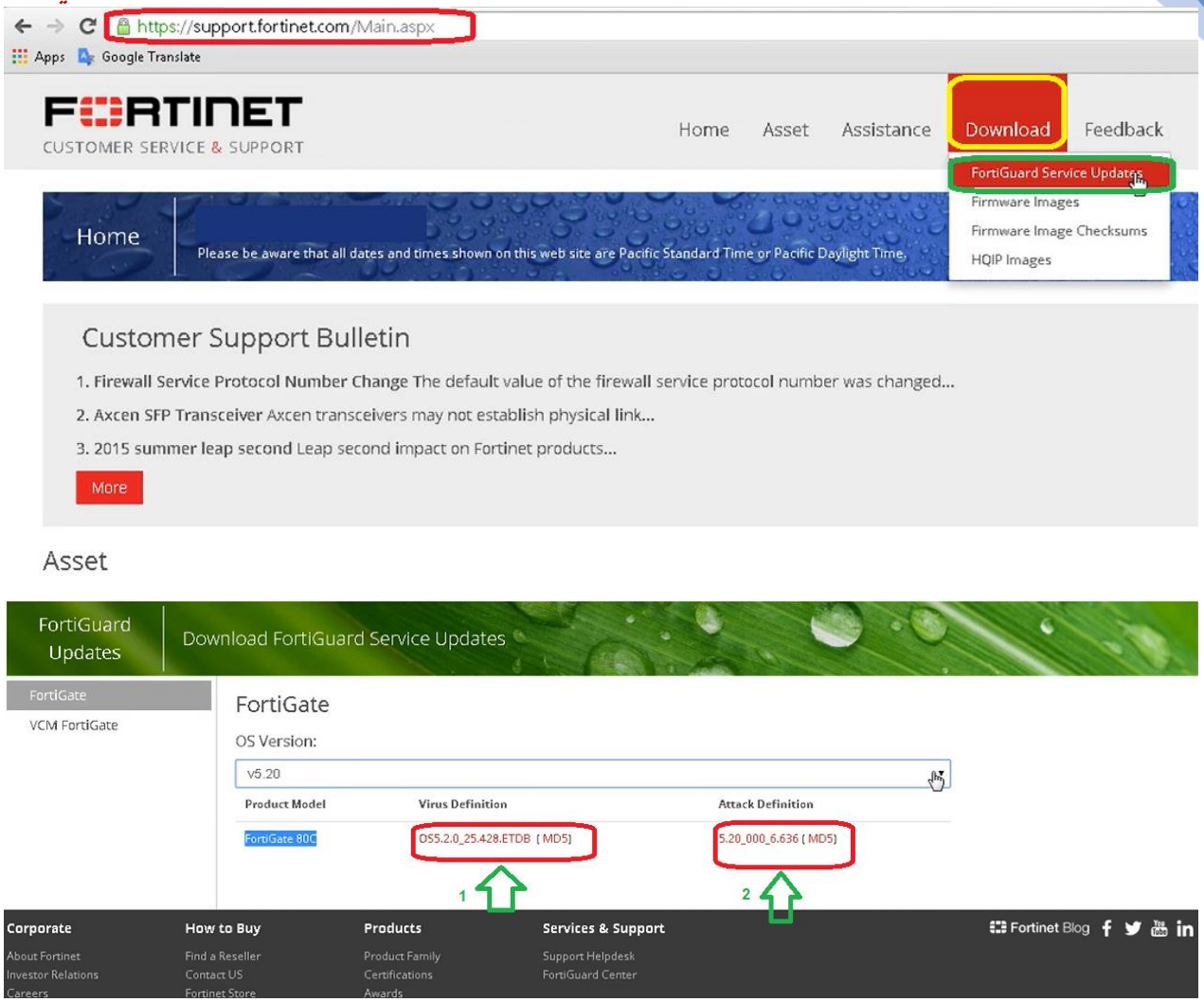
ثم تكتب ؟ سيقوم بإظهارلك كل انواع القواعد الذي يدعمها الجهازويمكنك اختيار النوع المناسب لك

مثلا extreme

حيث الـ extreme هو النوع الأفضل والاقوى ..

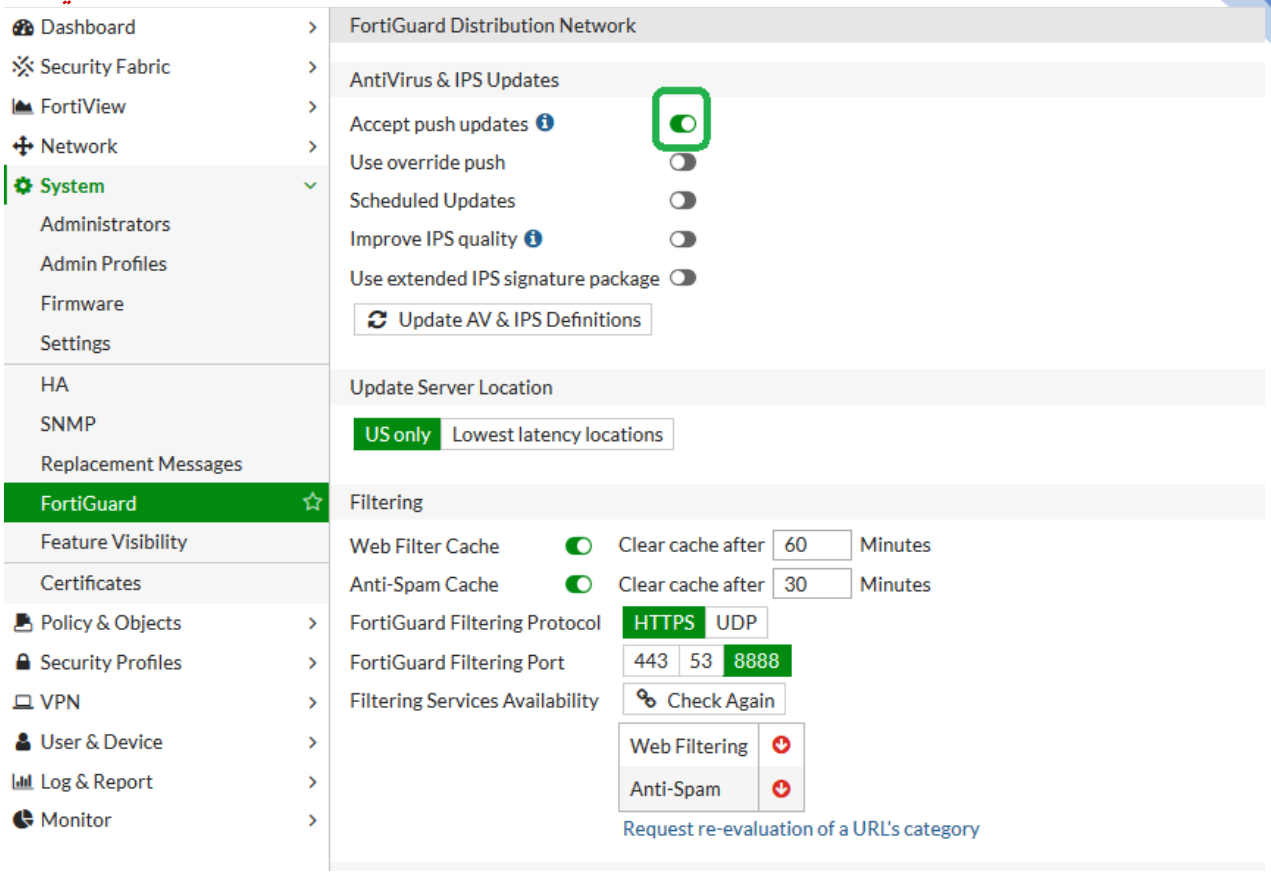
كيف بيتم عمليه التحديث للAntivirus DB ؟

a) Manual:ستقوم بتحميل ملف من الملفات عبر(fortiGuard service update)وتعمل لهذا الملف upload للجهازويقوم بتحديث الAntivirus DB



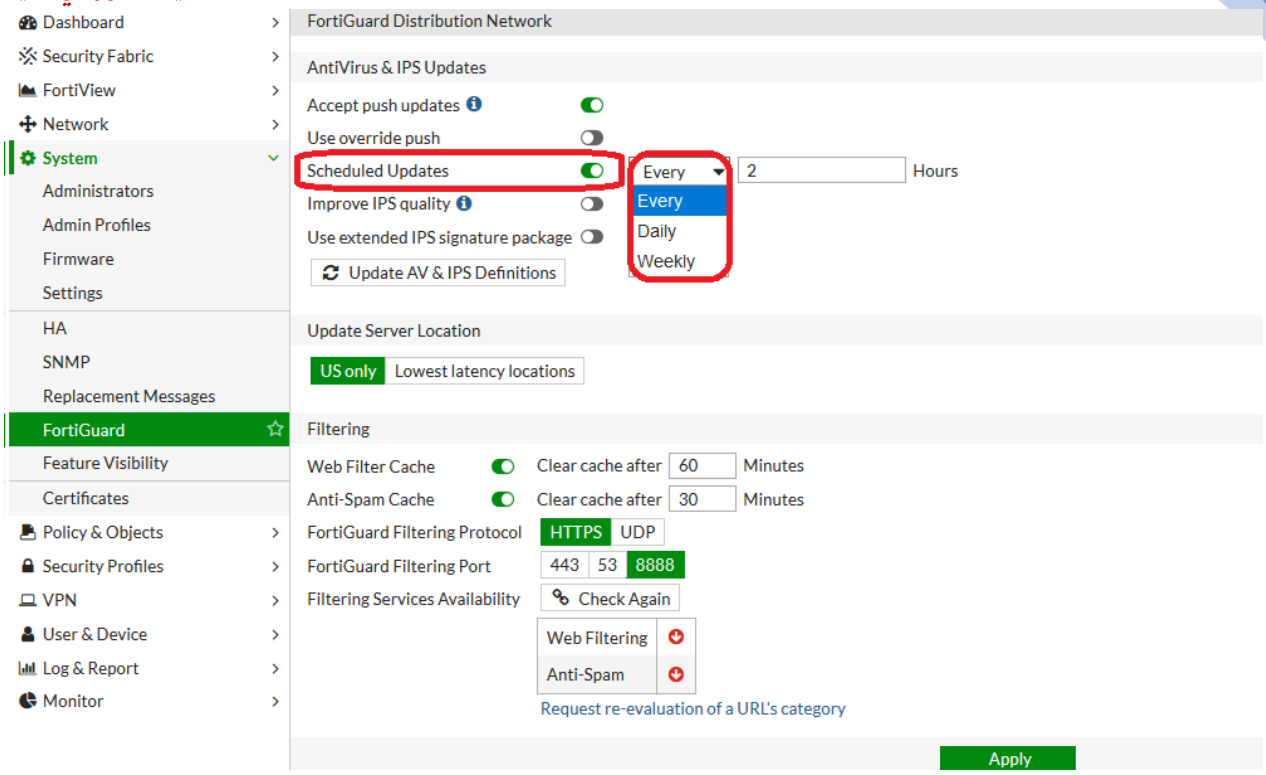
ثم نقوم بتحميل ال2 ملفات المشار اليهم بالون الأخضر ومن ثم نقوم بعمل لهم Upload من الفورتي جيت فايروول .

b) Automatic : جعل الفورتي جيت يعمل على تنزيل التحديثات من FDN(fortiGuard) بمجرد وجود تحديثات جديده .وبهذا يصبح الDB UP to Date .



حيث تقوم بتفعيل للخيار Accept push updates بحيث أي تحديث جديد موجود على FDN بيتم تنزيلها تلقائيا الى الفورتي جيت فايروول بدون تدخل منك .

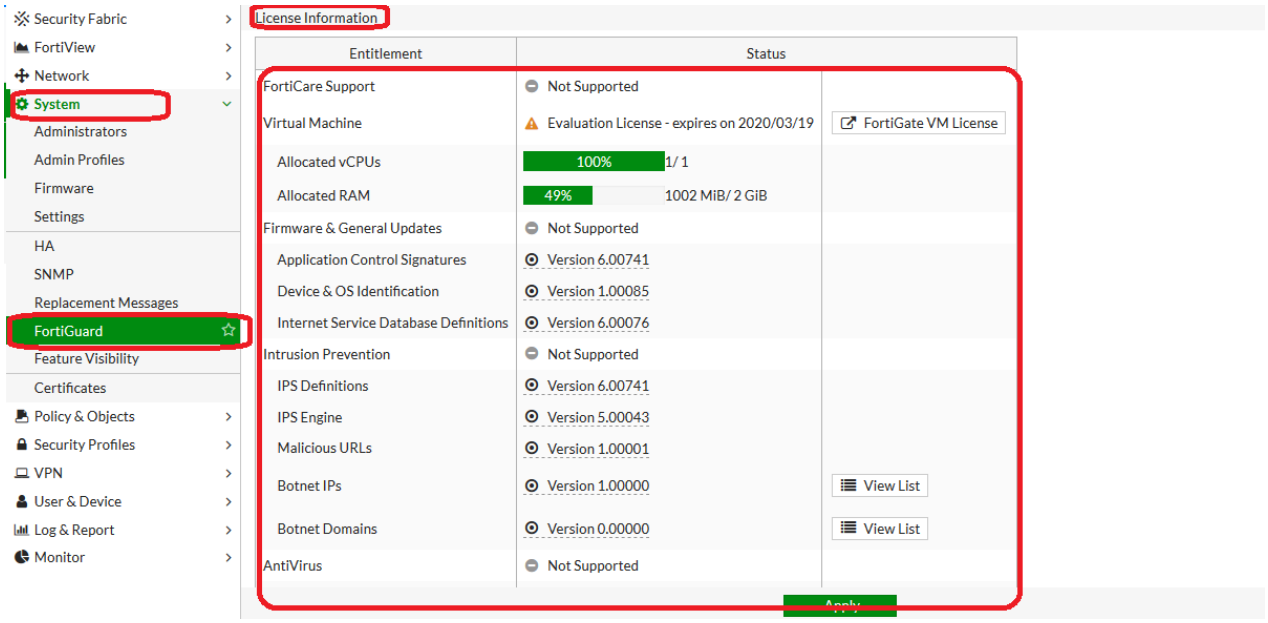
او يمكنك عبر خيار اخر بأنك تعمل schedule updates وتحدد الأيام الذي يقوم فيها الفورتي جيت بتنزيل التحديثات من FDN .

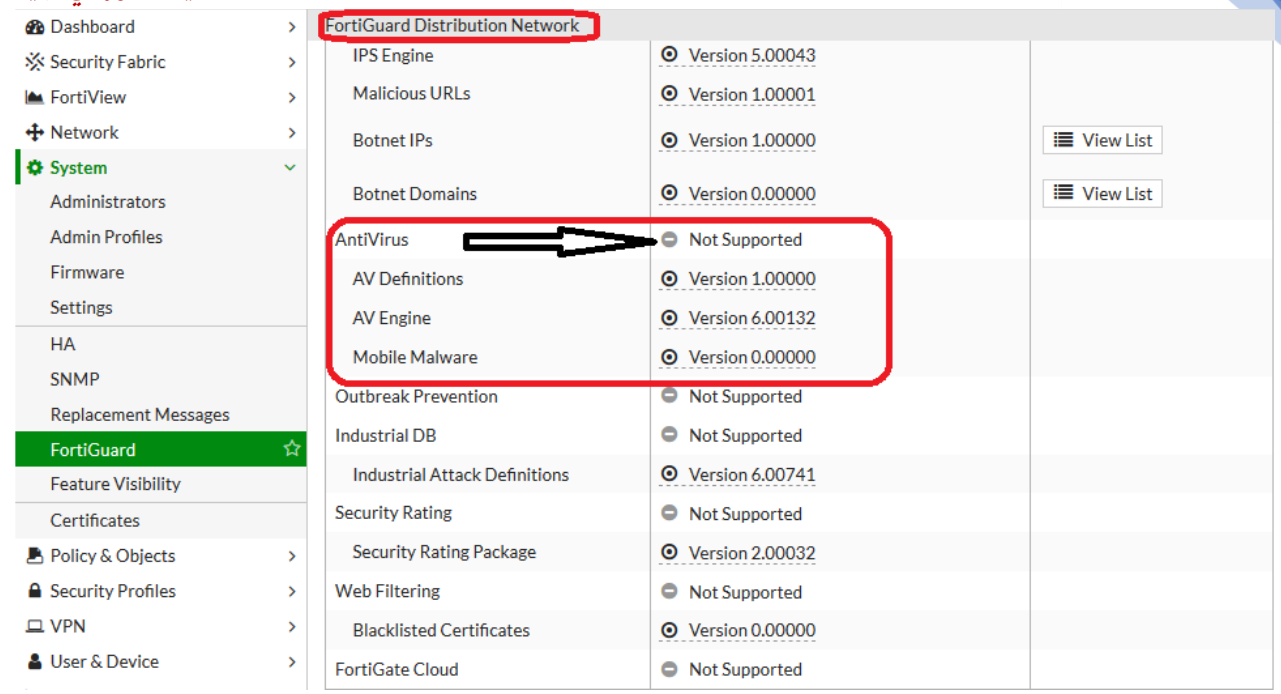


مثلا يمكنك تحديد أيام واوقات معينه لعمل التحديث (أوقات خارج الدوام)

حيث ان الـ antivirus بدون تحديث ليس له أي قيمه ...

لمعرفة الـ licenses التابع لجهاز الفورتي جيت ككل



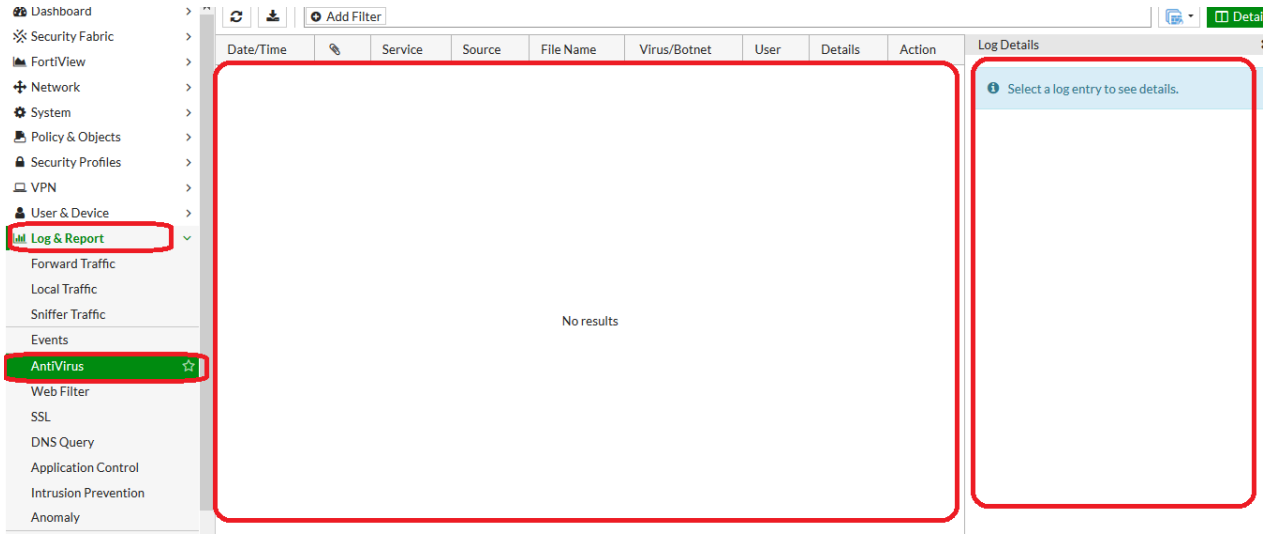


كما بالصورة أعلاه تبين بأن الترخيص للـ Antivirus غير موجود نظرا لأن نسخه عباره عن VM تجريبي ...

حيث يحتوي الـ Antivirus على

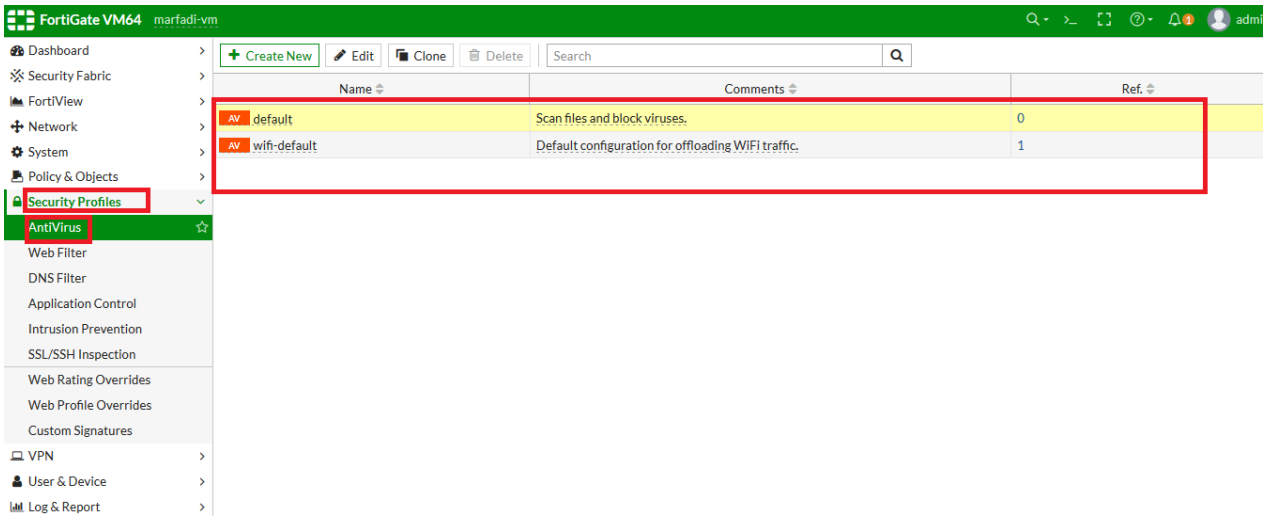
AV Definitions و AV Engine و Mobile Malware

أي شي قام جهاز الفورتي جيت بعمل له Detection بيتم تسجيله كما بالصورة ادنا ه



الوقت والتاريخ لعمليه اكتشاف الفايروس ويحدد له المصدرواسم الملف المعمول له detected وما هو اسم الفايروس ومن هو اليوزر الذي حصل عنده الـ detection وبعض التفاصيل وماه والـ action الذي حصل لهذا الفايروس ..

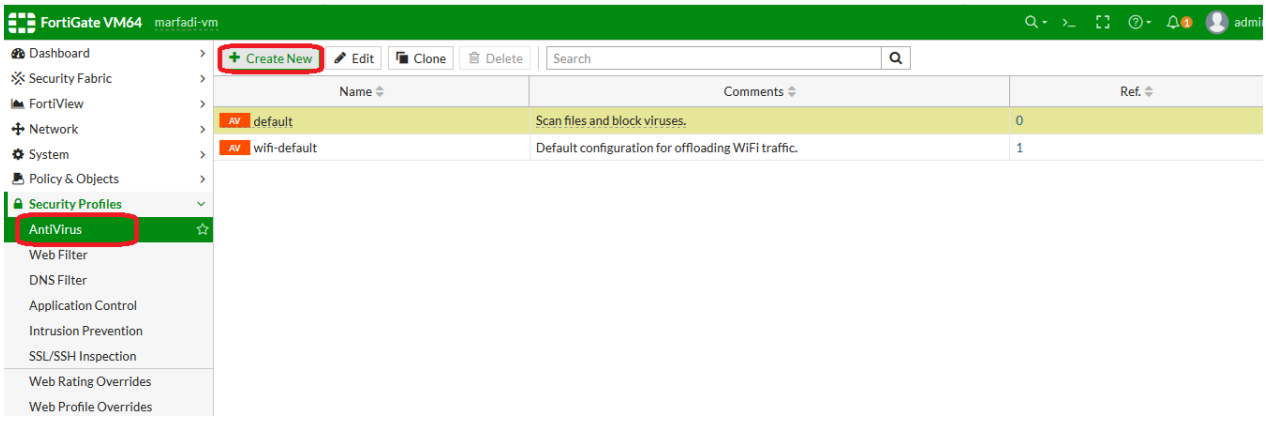
❖ طريقة تفعيل الـ antivirus على الفورتي جيت وعمل حمايه للشبكة من أي تهديدات :

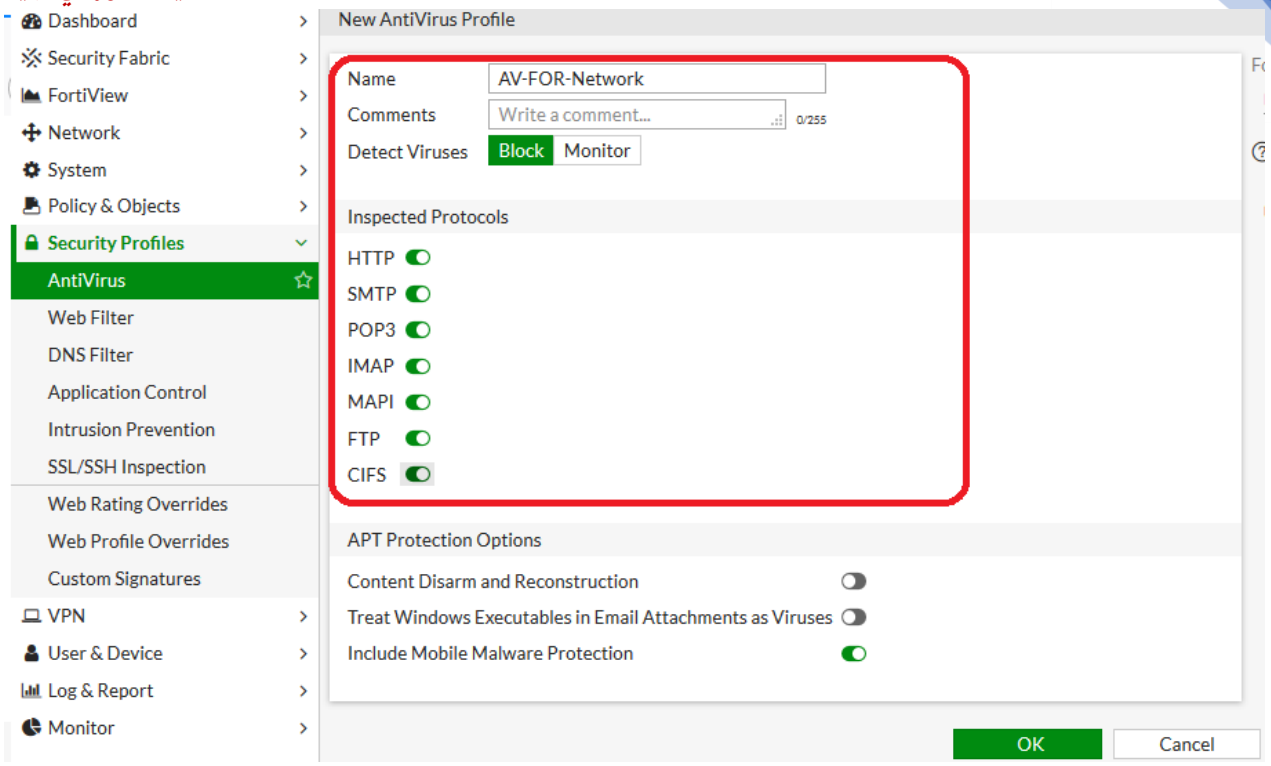


كما بالصورة أعلاه يتبين بأن 2 بروفايل موجود بشكل افتراضي ولا يمكن حذفهما ..

ويمكنك انشاء بروفايلات جديد وتخصصها كما تشاء ومن ثم سيتم اختيارها لاحقا في البوليسي ...

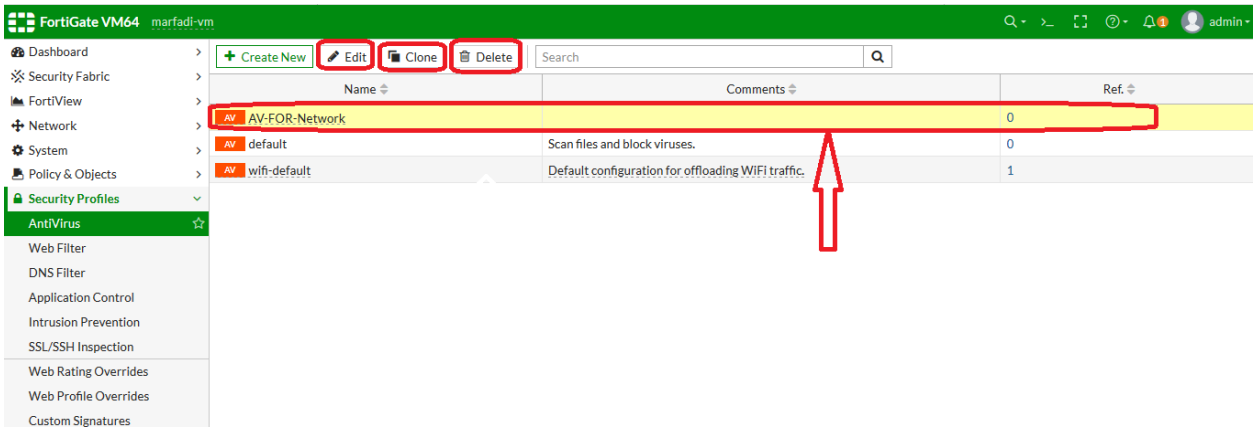
➢ طريقة انشاء بروفايل جديد لـ antivirus :





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 الفورتي جيت بان هذا الملف مصاب

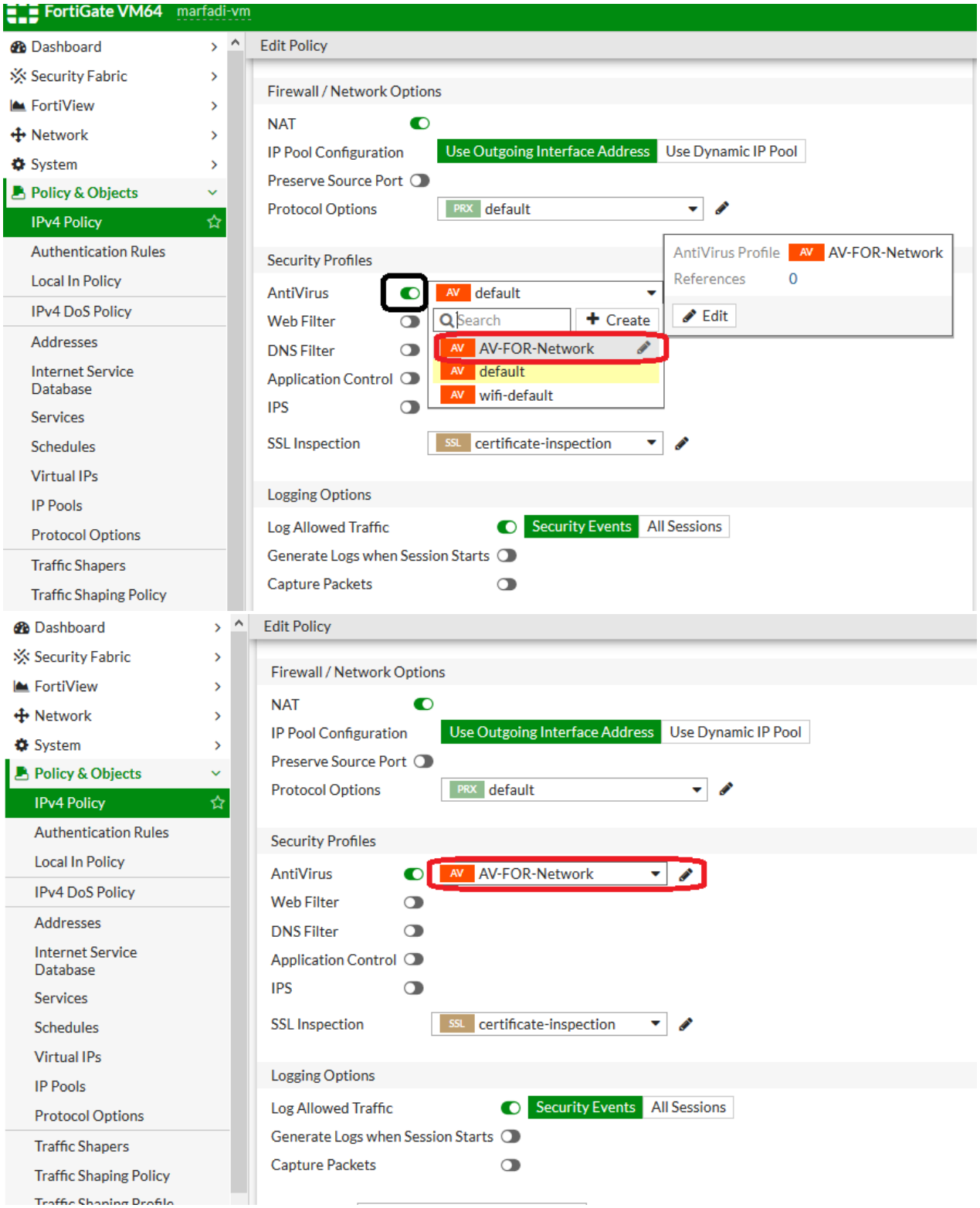
ومن ثم تحدد البرتوكولات التي سيتم عمل لها فحص من قبل الAV



كما بالصورة أعلاه تم انشاء بروفايل جديد باسم AV-FOR-Network

حيث يمكنك حذف او نسخ او التعديل عليه كما هي الأسهم المشار اليها في الصوره أعلاه ..

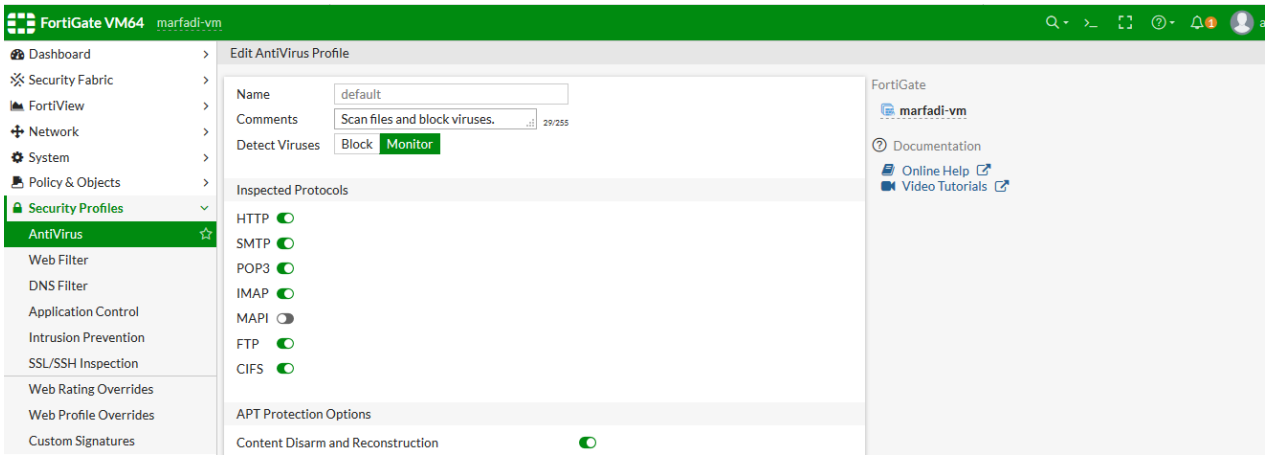
➢ طريقة اختيار البروفايل مخصص في البوليسي :



تم تحديد البروفايل المسمى AV-FOR-Network والذي قمنا بإنشائه مسبقا ..

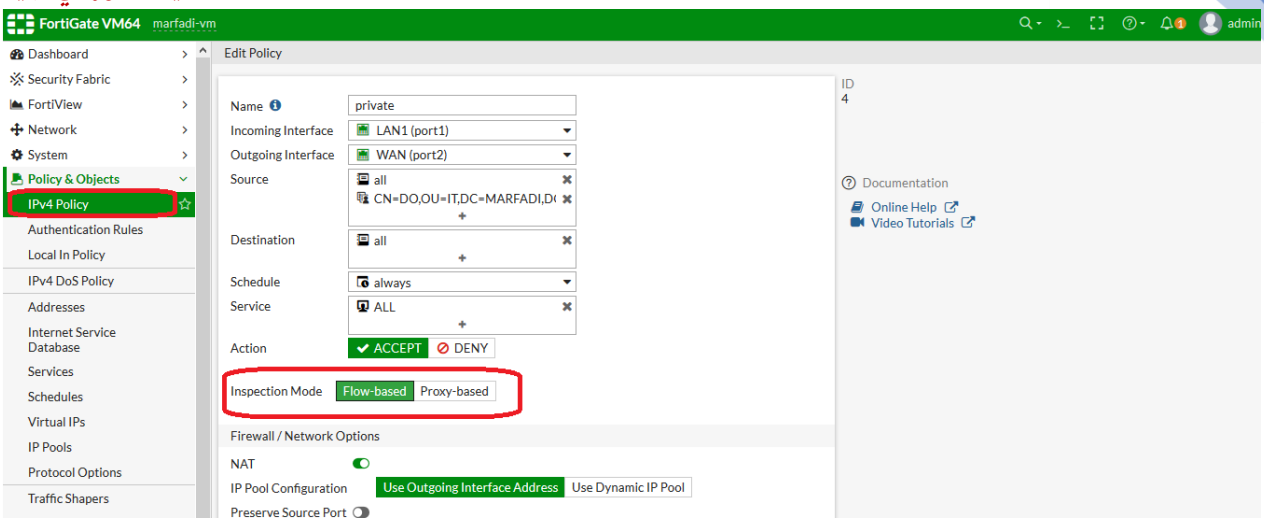
يجب ان تقوم بتفعيل الـ antivirus في كل بوليسي وذلك للأهمية ..

في حالة اردت تعمل حمايه للفورتي جيت بحيث لا يستطيع احد انشاء بروفايلات جديده مثل app control اوAV اوweb filter ..الخ



تلاحظ كما بالصورة أعلاه بأن خيار الحذف والتعديل والإضافة غير متاح بعد قيام بإلغاء تفعيل الخاصية التالية: Multiple security profiles ..

➢ Antivirus Mode :



Flow base mode	Proxy base mode
	الفحص الأكثرشمولا والاعمق و الاطول وقت حيث يتم تقسيم الملفات(للباكت) الى أجزاء
يأخذ نسخه من الملفات ويحصل لها caching على الفورتي جيت قبل تسليمه الى الكلاينت حيث لا يوجد عمليه تقسيم للباكت ثم يقوم بإرسالها الى محرك مكافح الفايروسات ليتم عمل فحص لها ففي حالة كانت سليمه فأنه يتم تسليمها الى المستلم اما لوكانت مصابه فيتم حذف الملف المصاب	يعتمد على مبدا الـ buffering أي التخزين المؤقت أي ان كل الباكت والملفات التي تصل للفورتي جيت لا يتم تخزينها بشكل مؤقت على جهاز الفورتي جيت
	في حالة لم يجد أي أصابه للملف بعد عمليه الفحص يتم ارساله الى الهدف اما في حالة وجود أصابه في الملفات يأخذ action معين ويعمل رساله للهدف كنوع من التحذير بأن الملف مصاب
	لأي Default buffering=10 m

	جهاز فورتي جيت . فلو كان الملف حجمه اكبر من 10 ميجا فأن هناك حالتين اما يتم عمليه تمرير الملف الى الهدف بدون فحص او ان يتم عمل له Block . يمكن التعديل على قيمه الـbuffering size

❖ 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 داخليه فيمكن استخدام الـ flow base لأنه اسرع وبنفس الوقت الهجمات التي تكون في الشبكات الداخليه اقل بكثير من الهجمات التي تأتي من خارج الشبكة(الانترنت) .

ممكن تستخدم flow base لو كان سرعه الانترنت لديك بسيطة فالأفضل تستخدم الـ flow base لأن عمليه الفحص تكون اقل بعكس عمليه الـ proxy التي تكون عمليه الفحص ادق ولهذا يتم استهلاك الانترنت ..

❖ ماهي طريقة عمل مكافح الفايروسات في الفورتي جيت (يتعامل المكافح بالفورتي جيت مع أي ملف على شكل مراحل)؟

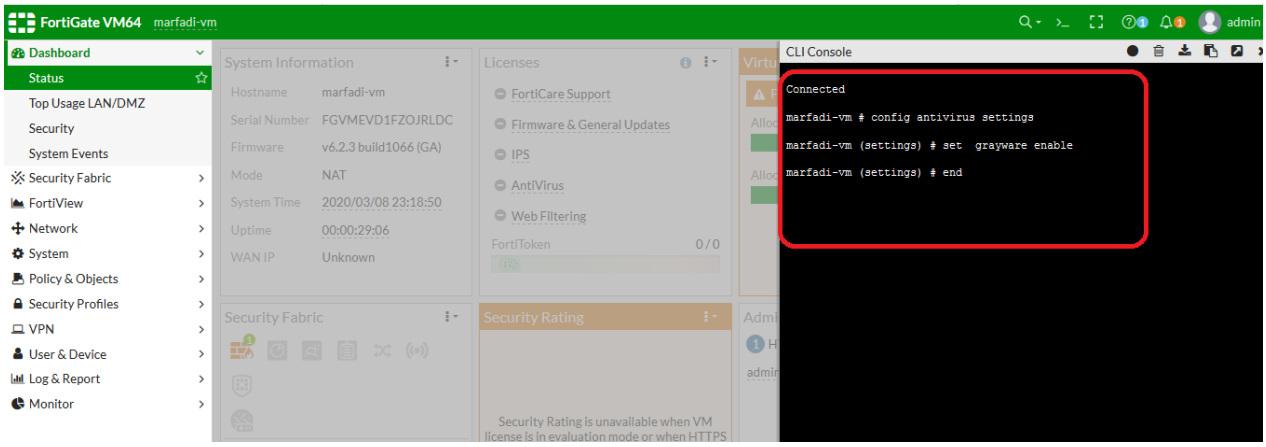
المرحله الأولى Antivirus protection ويسمى بالتهديدات الصريحه:

محرك البحث(DB) لدى مكافح الفايروسات أولا يقوم بالبحث على التهديدات الصريحه حيث لو قمت باستلام ملفات وهذه الملفات بتحتوي على تهديد صريح (malware)فيتم عمل action مناسب .

المرحله الثانية specific function (Grayware):

تعتبر هذه المرحله الثانية من مراحل تعامل مكافح الفايروسات التابع لفورتي جيت ،في هذه االمرحله يتم البحث عن البرمجيات التي تعتبر (Grayware) حيث الملفات او البرمجيات في هذه الحالة لا تعتبر مؤذيه أي انها غير صريحه بالتهديد و لا امنه .

هذه الخاصية بشكل افتراضي غير مفعله باجهزه الفورتي جيت فلو تريد تفعيلها لزياده نسبه الأمان فيكون ذلك عبر CLI كما بالصورة ادناه ..

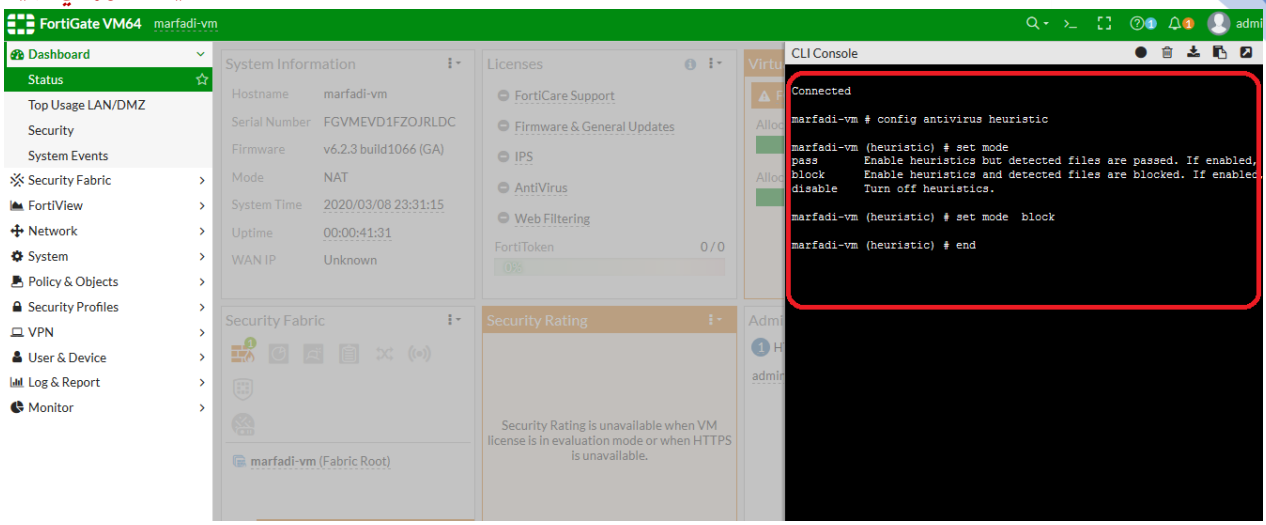


المرحله الثالثه Heuristics (الاستدلال) :

لو تم تفعيل هذه الخاصية فأن AV لو وجد 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 ...

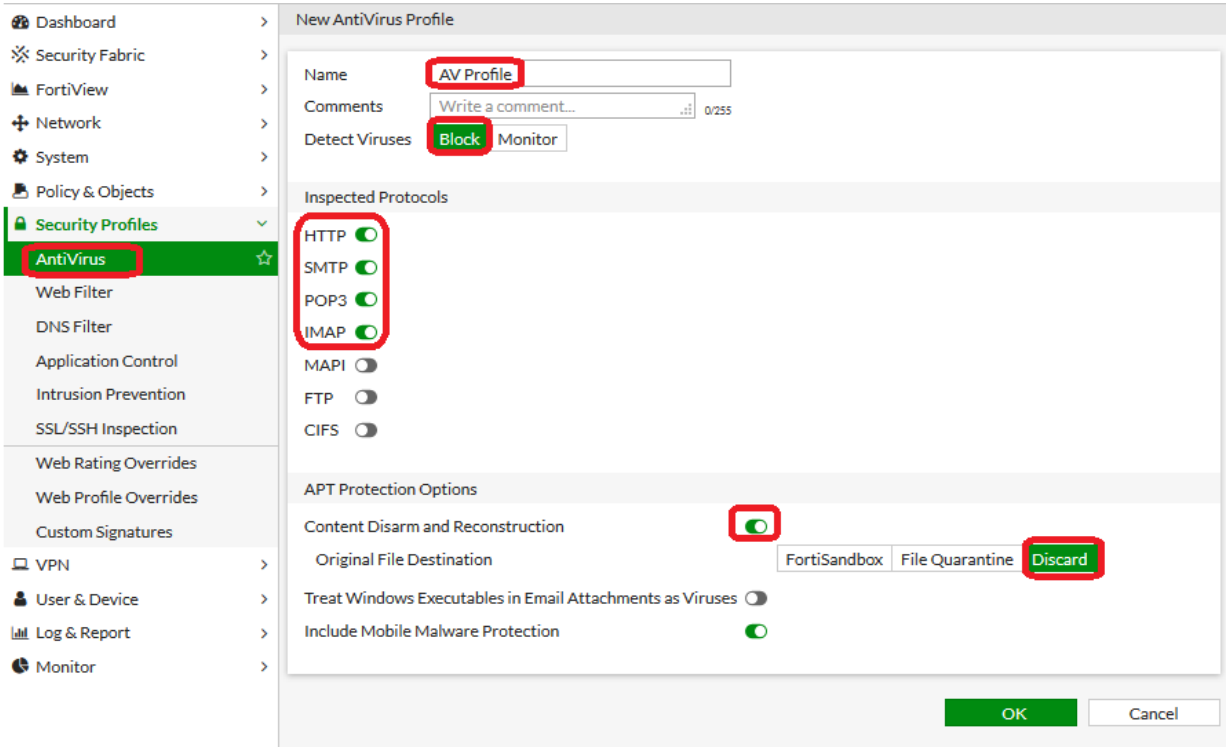
ولتفعيل هذه الخاصية عبر CLi



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: بيجعل الفورتي جيت يأخذ أي ملف(...,pdf,doc)

وفحصه والتأكد من احتوائه على الهايبرلينك ،حيث فكره الهايبرلينك هي ملف ضارداخل ملف عادي وعند تمكين هذا الخياربيتم التعامل مع هذا الملف ،حيث يقوم الفورتي جيت بحذف الهايبرلنك واصبح لديك الملف الحقيقي فقط فهو حسب الخيارات أعلاه بيقول 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 الفورتي جيت وفي هذه الحالة يجب ان يكون لديك هارد داخل الفورتي جيت .

Discard :حذف الملف الأصلي .

Treat Windows Executables in Email Attachments as Viruses : هذا الخياربيقوم بحذف الملفات المرفقة التي تصل عبر الايميل فيها exe او msi او أي ملف تنفيذي .

➢ Web filtering

عباره عن التحكم في المحتوى الذي يصل الى المستخدم او الذي يصل اليه المستخدم .

او بمعنى أوضح عباره عن فلتره الhttp 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 ففي فتح المواقع مثل اليوتيوب والألعاب.
٣- تسريب المعلومات الهامه خارج الشركة
٤- التعرض للهجمات عبر المواقع
٥- تجنب أي مسؤليه قانونيه بسبب تنزيل احد الموظفين لبرمجيات غير مصرحه .

الهجات التي تصل عبر الويب :

- البرامج التجسسيه 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 الـstreaming media (audio+video)

Web filtering mode

يوجد لدى فورتي جيت 3 أنماط مختلفه :

١) Proxy:بيعتمد على الـ Buffering أي عمليه تخزين البيانات لفتره محدده لحين إتمام عمليه الفحص ثم تمرير البيانات الى الهدف (اليوزر)

دقيق في عمليه الفحص ولكنه بطئ بسبب عمليه الـbuffering.

اعداداته كثيره .

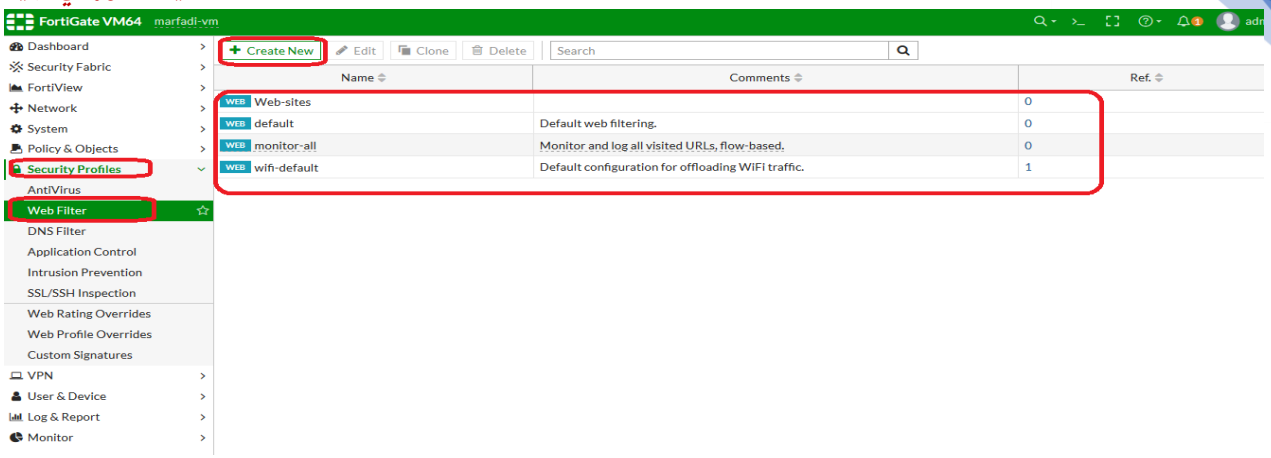
٢) Flow:لا يعتمد على الـBuffering حيث يمرر البيانات الى الهدف بدون تخزين حيث انه اقل دقه من البروكسي ويعتبر اسرع نمط .

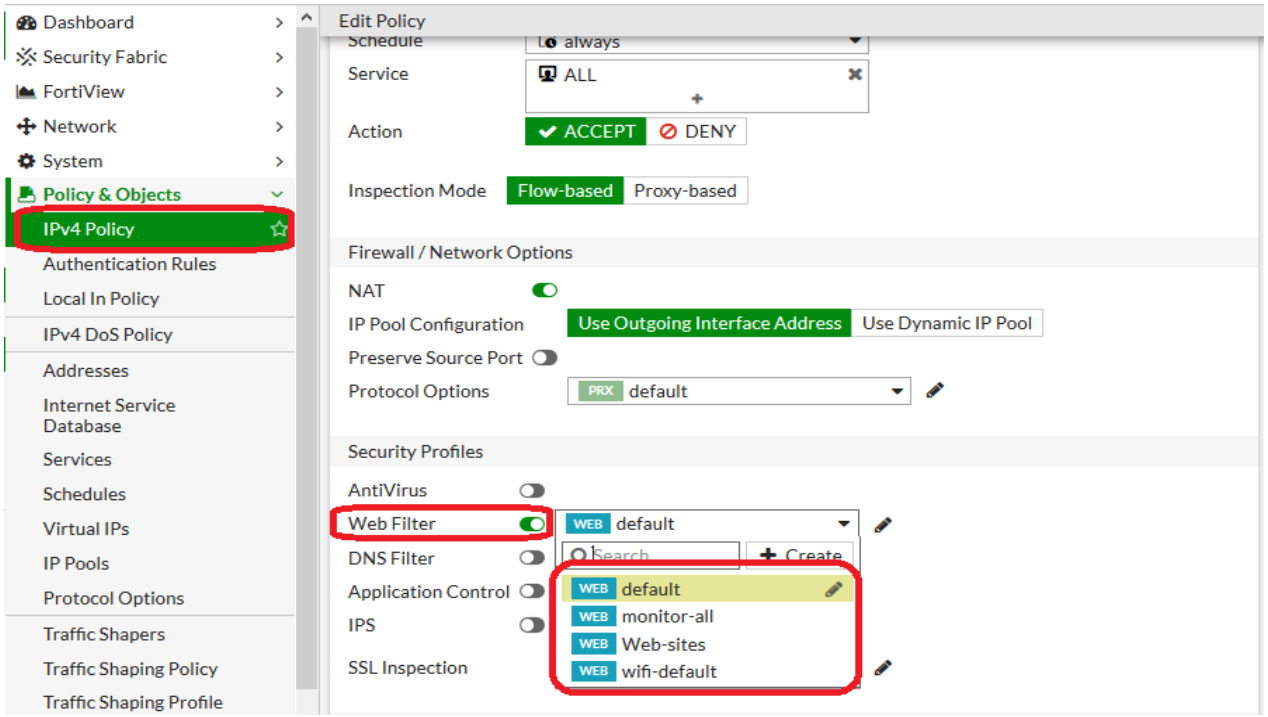
٣) DNS:لا يعتمد على الـBuffering حيث يقوم بعمليه تحويل من اسم الى ايبي حيث شركه فورتي نت لديها dns server ويمكن الاعتماد عليه لعمليه فلتره المواقع ،حيث يعتبر هذا النمط دقيق لأنه يعتمد على الـ dns server التابع لفورتي نت حيث يتعبر سريع ولكن ليس اسرع من ال flow mode

حيث يعتبر اقل اعدادات .

- ملاحظة :عمليه الفحص تكون على ايبي الموقع واسم الموقع

حيث ستقوم بإنشاء بروفايل خاص ب web filtering وتخصصه لناس معينين.





تم تطبيق بروفايل معين في الـweb filter على بوليسي معينه ..

➢ ماهي الخيارات المتاحة على الفورتي جيت بخصوص الـweb 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 :تمكنك من فلتره المحتوى المطلوب بناء على كلمات محدده على صفحة الويب او أنماط معينه او جمل معينه

٣) fortiGuard web filter :يمكنك بوساطتها ان تتحكم بملائين المواقع من خلال التصنيفات التي معموله عبر شركه فورتي جيت

➢ شرح مفصل للأنواع المذكورة أعلاه :

١) fortiGuard web filter :

عباره عن حل بيتم ادارته من قبل شركه فورتي نت حيث لا يمكنك الاستفاده منه الا لو قمت بعمليه تجديد الاشتراك كل سنه ..

حيث لو لم تكن مشترك بهذه الخدمة فانك لن تقدر التحكم بالمواقع بحسب التصنيف.

حيث الـ vm لا تكون مفعله ولذا لا يمكننا استخدام النوع fortiGuard web filter .

فمثلا لو تريد اغلاق مواقع الـ social networking التي تقدر بمئات المواقع فأنه من الصعب اغلاقها 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،...)

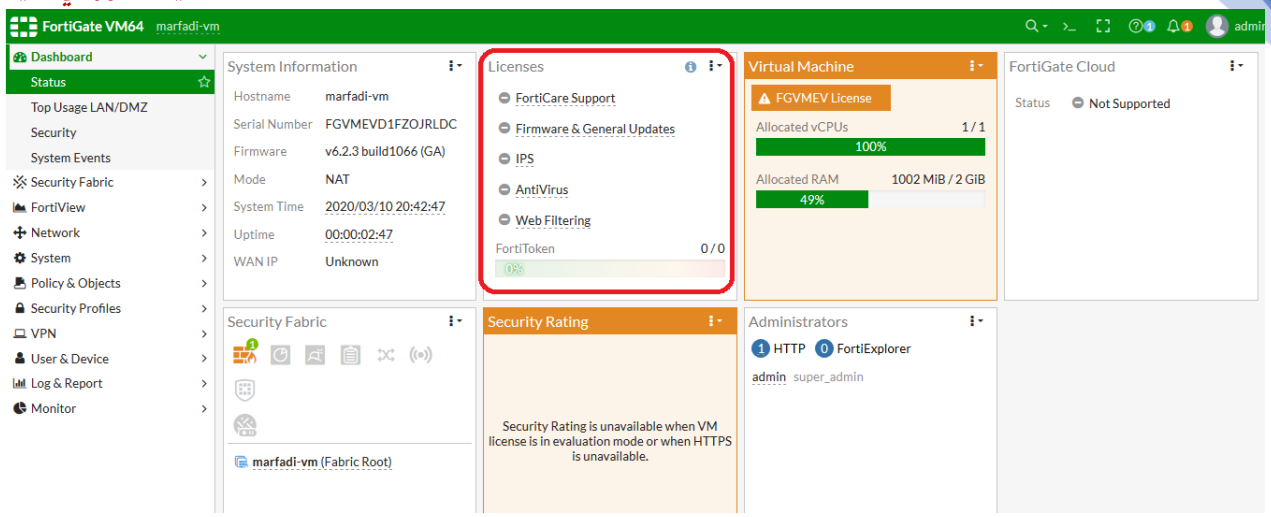
➢ ماهي علاقه فورتي جار بالفورتي جيت :

اليوزر عندما يطلب أي موقع فأن الفورتي جيت يأخذ الطلب ويرسله لأقرب سيرفر لفورتي جارد بشرط ان يكون جهاز الفورتي جيت مشترك (License).

فلو كان الطلب (الموقع) الذي طلبه اليوزر ممنوع(Block) فيقوم سيرفر فورتي جارد بإرسال رساله الى جهاز الفورتي جيت بأن الموقع محجوب والذي بدوره يقوم بإظهار رساله لليوزر بأن الموقع مغلق .

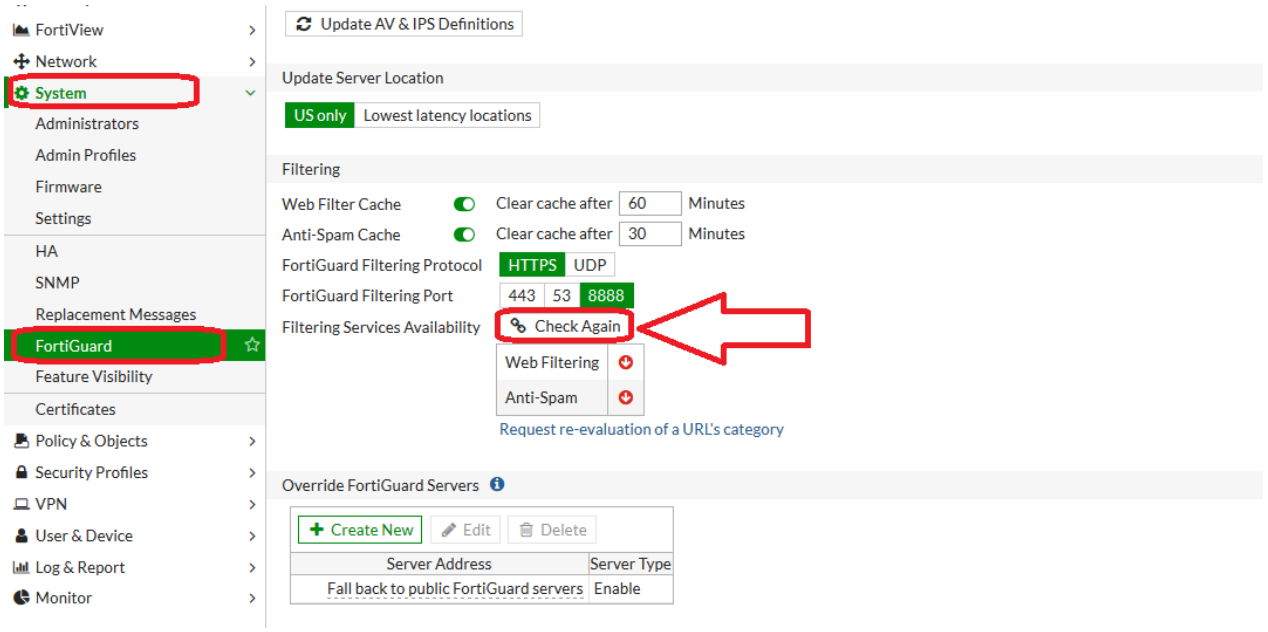
حيث يعتبر الفورتي جيت وسيط بين اليوزر والفورتي جارد سيرفر

يجب ان تتأكد بان الفورتي جيت متوصل بشكل سليم مع الفورتي جارد وأيضا لديك ترخيص (license).

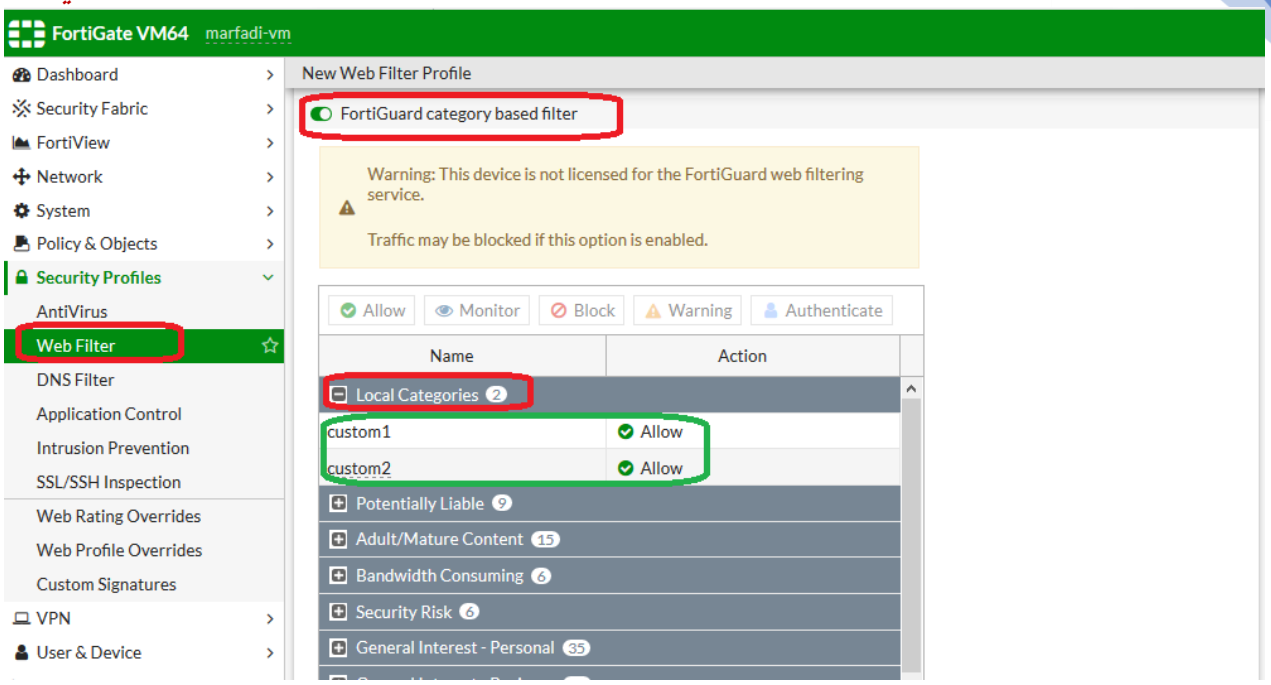


يجب ان تتأكد بأن ال licenses شغال بشكل سليم كما بالصورة أعلاه

وأيضا تتأكد من الـ connectivity بين الفورتي جيت والفورتي جارد كما بالصورة ادناه



➢ كيفيه التعامل مع الـــ fortiguard category في الـــ web filter :



نلاحظ بأن رساله الخطأ توضح بأن الفورتي جارد ليس متاح على الfortigate vm حيث يجب ان تكون مشترك بخدمه الفورتي 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

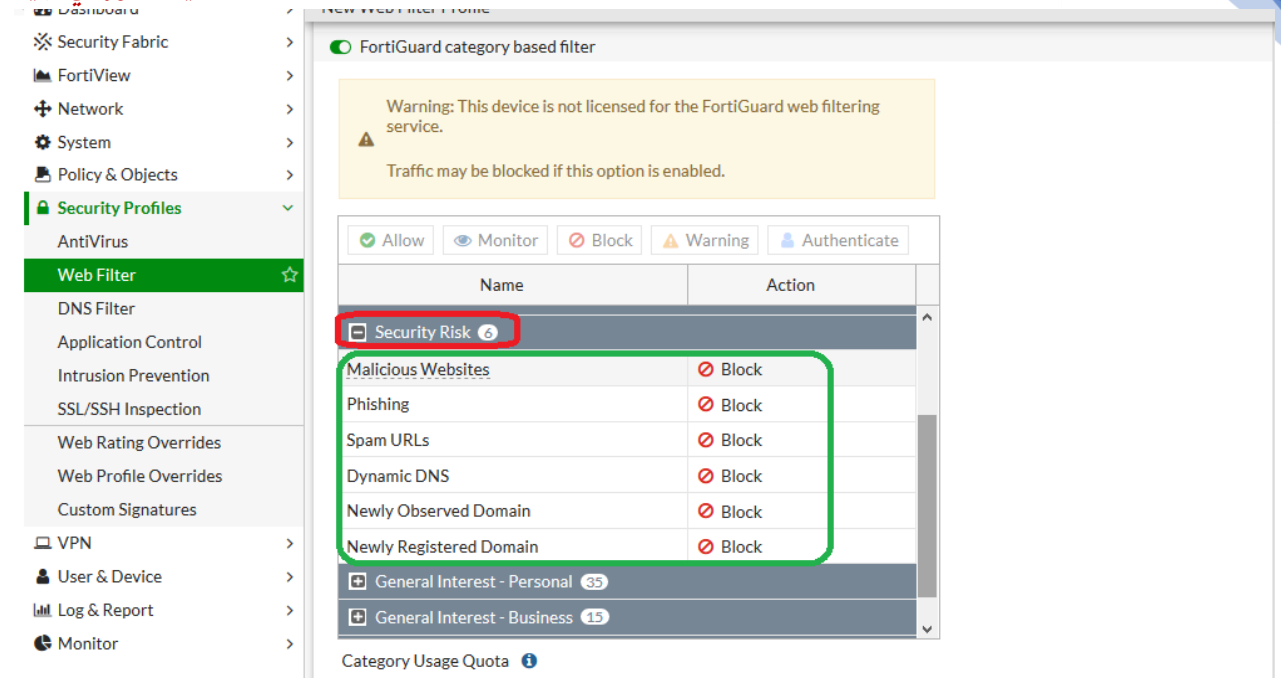
Spam

Spam URL

Dynamic DNS

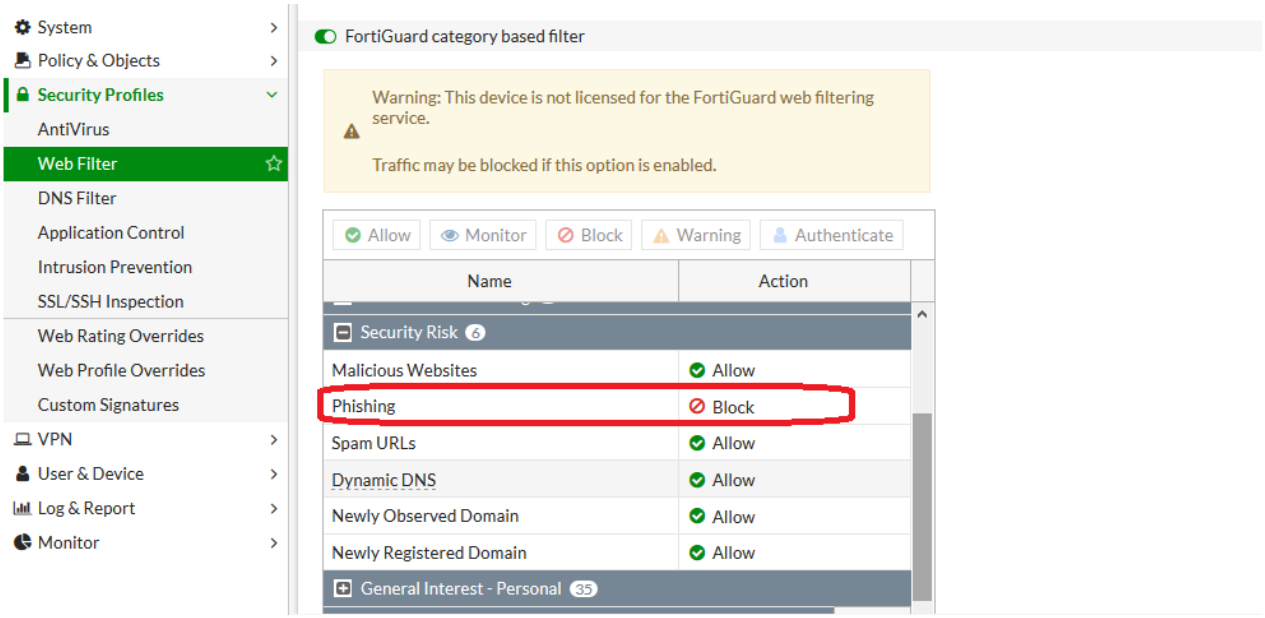
New observed Domain

New Registered Domain

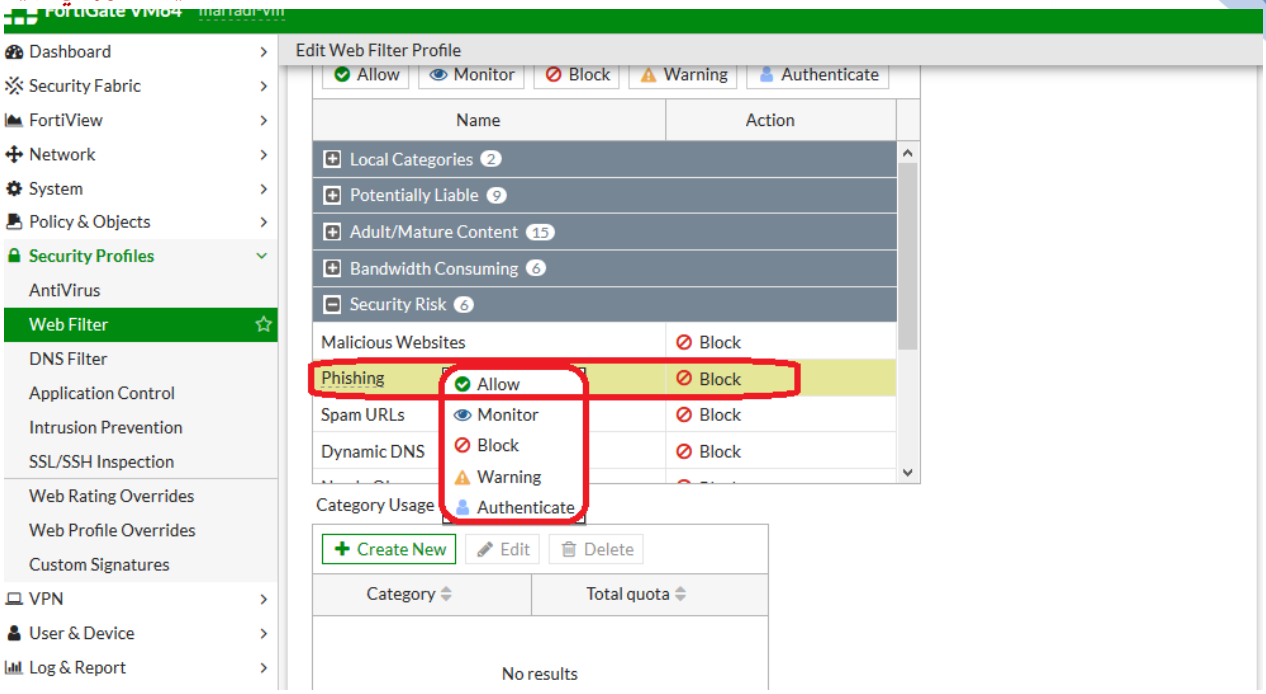


فلو تريد اغلاق كل مواقع phishing فأنه يجلب عليك ان تقوم بإغلاق التصنيف المسمى phishing

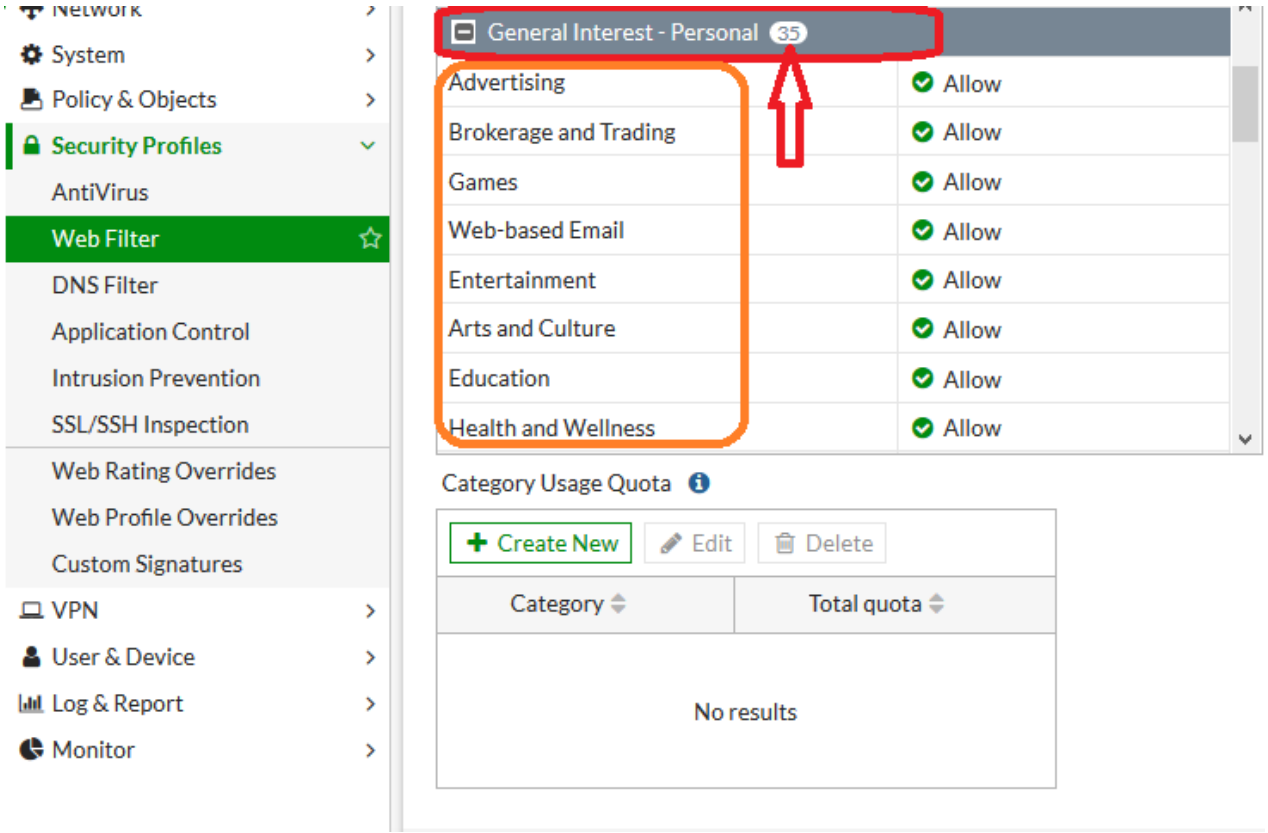
وهكذا كما بالصورة ادناه

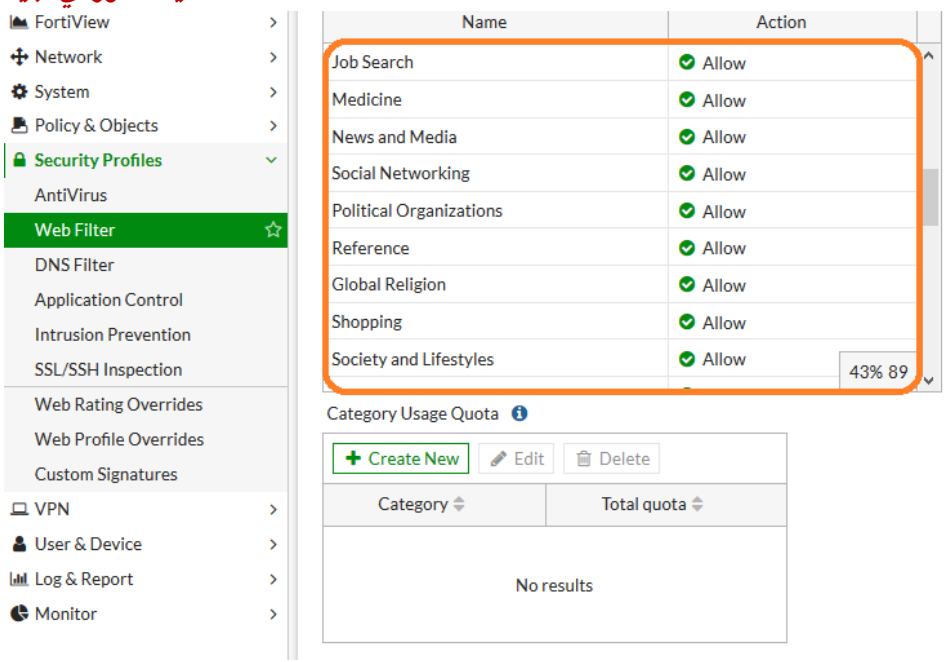


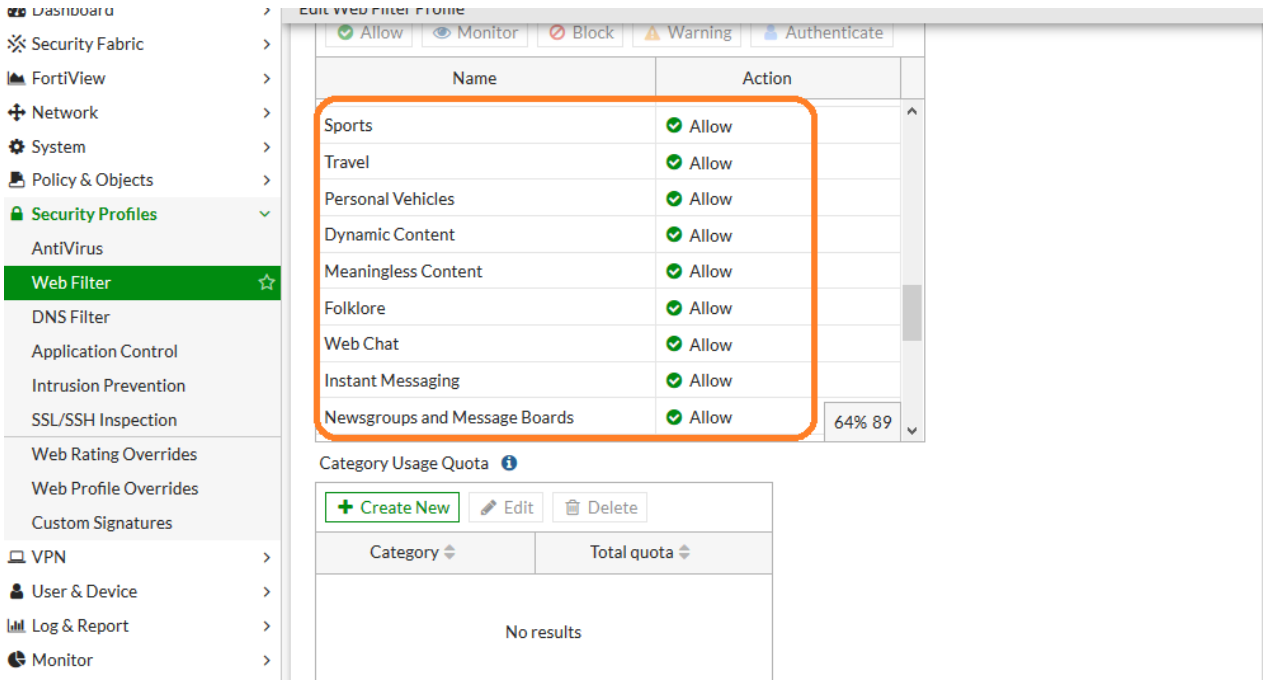
حيث بمجرد النقر على sub categories بالزر الأيمن يظهر لك الـ actions المراد اختياره مثل Allow ,Monitor,Block,Warning,Authenticate

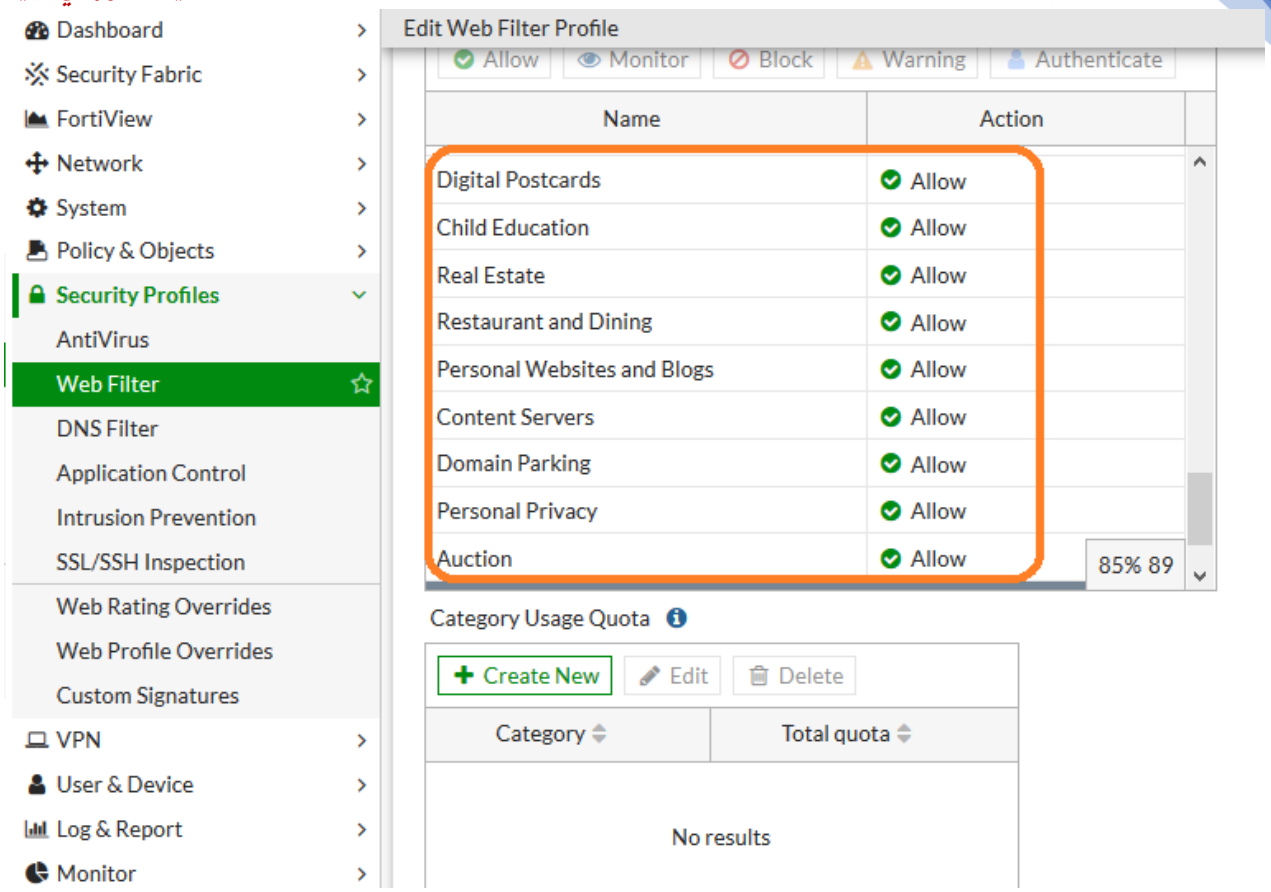


مثلا التصنيف General Interest-Personal (35) يحتوي على 35 تصنيف فرعي كما بالمربع البرتقالي




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
Medicine
News and Media
Social Networking
Political Organizations
Reference
Global Religion
Shopping
Society and Lifestyles
Allow
43% 89
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
Allow
Monitor
Block
Warning
Authenticate
Name
Action
Sports
Travel
Personal Vehicles
Dynamic Content
Meaningless Content
Folklore
Web Chat
Instant Messaging
Newsgroups and Message Boards
Allow
64% 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 الصحه .

News and Media :يحتوي على مواقع الاخبار.

Personal Vehicles:يحتوي على مواقع الشاحنات والسيارت

Personal Privacy : يحتوي على المواقع الشخصيه

Sports :مواقع الرياضه

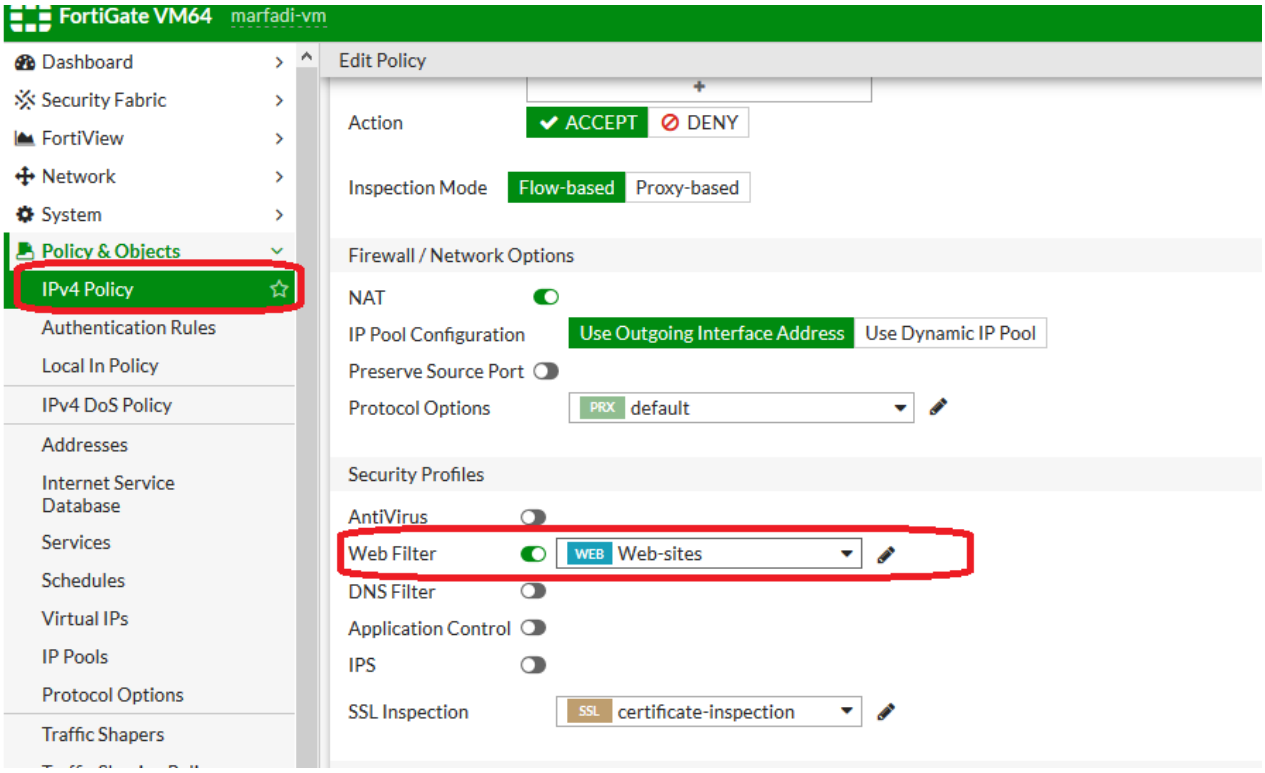
Shopping : مواقع التسويق

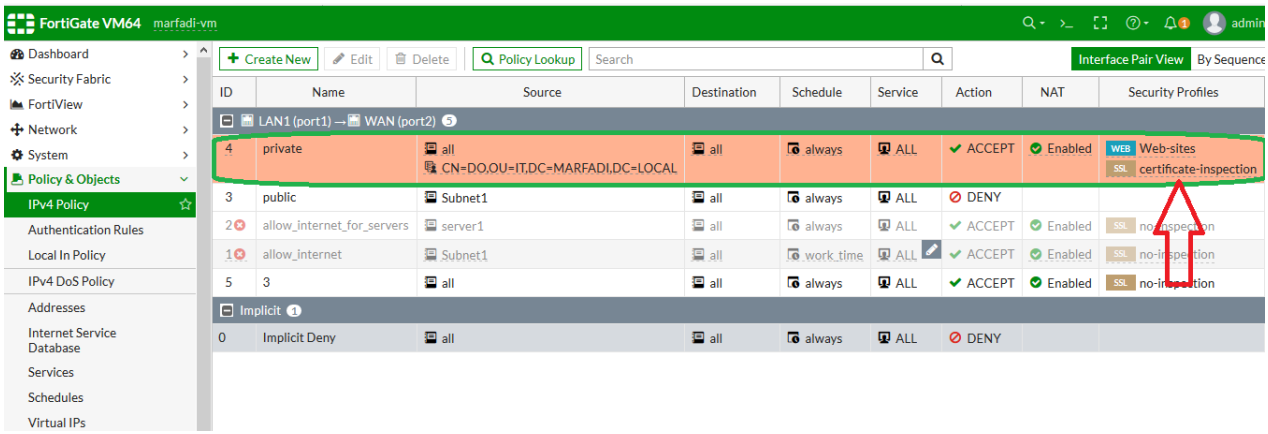
Social Networking :الشبكات الاجتماعية مثل الفيسبوك والتويتروالجوجل بلاس

Games :مواقع الالعاب

Web Chat : مواقع الشات حيث يختلف عن app chat

حيث تقوم باختيار الـ actions المناسب ثم تقوم بإعطاء اسم للبروفايل ومن ثم تنشى بوليسي وتختارهذا البروفايل لهذا البوليسي لكي يتم تطبيقه ..



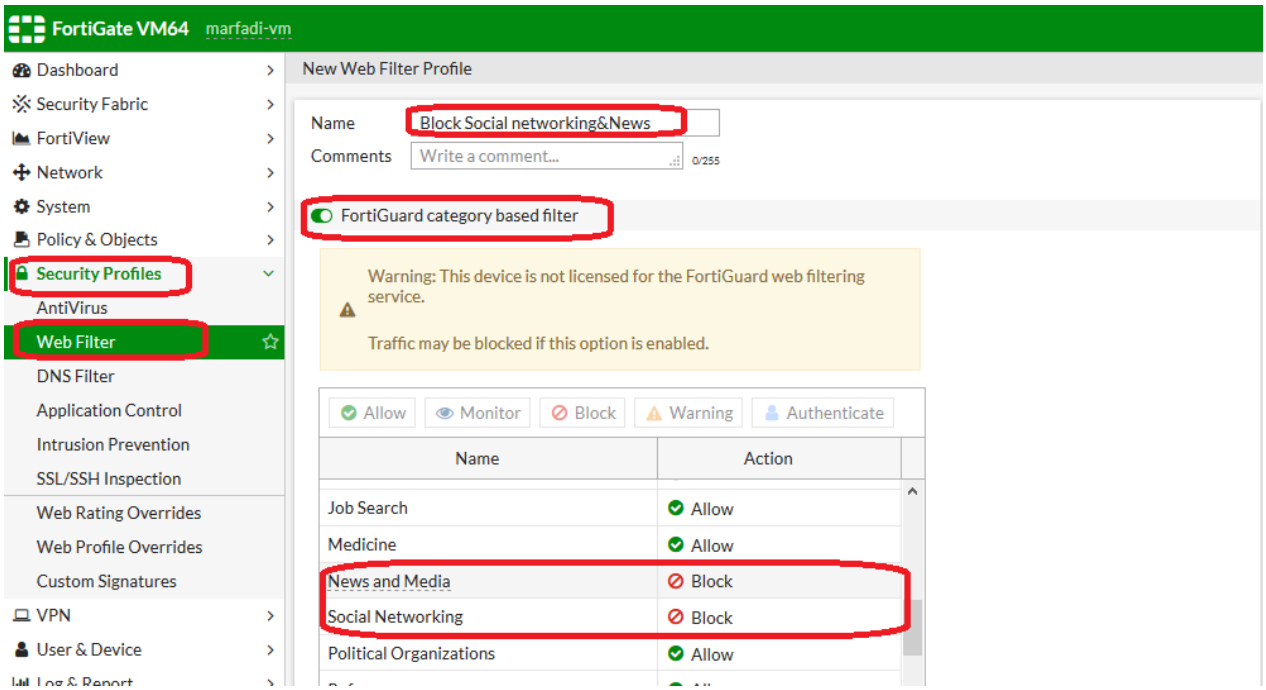


مثال :

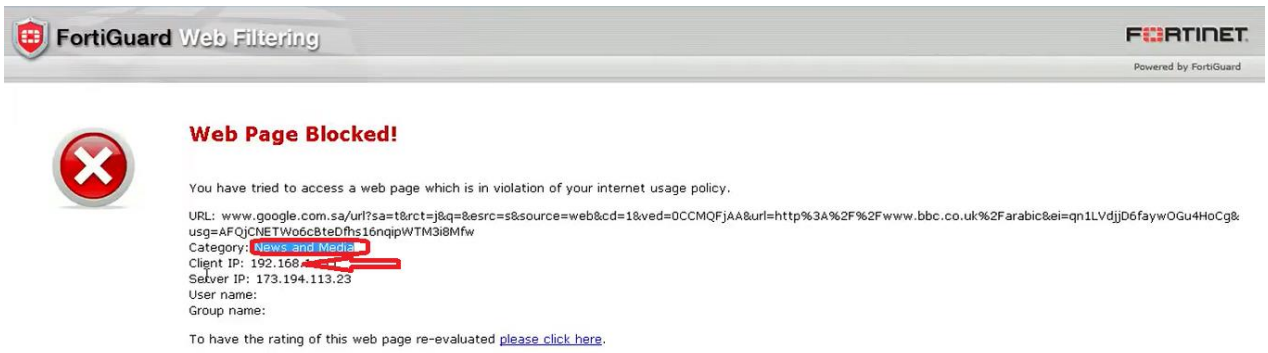
لو تريد اغلاق مواقع التواصل الاجتماعية مثل الفيسبوك وتويتروأيضا اغلاق مواقع الاخبار مثل صحافه 24 و موقع bbc.com وغيرها ..

فأننا سنقوم أولا بإنشاء بروفايل باسم Block social networking&News

وسنقوم بالسماح لكل الـ categories ماعدا الـ social networking و New and media سوف نقوم بإغلاقها كما بالصورة ادناه ..



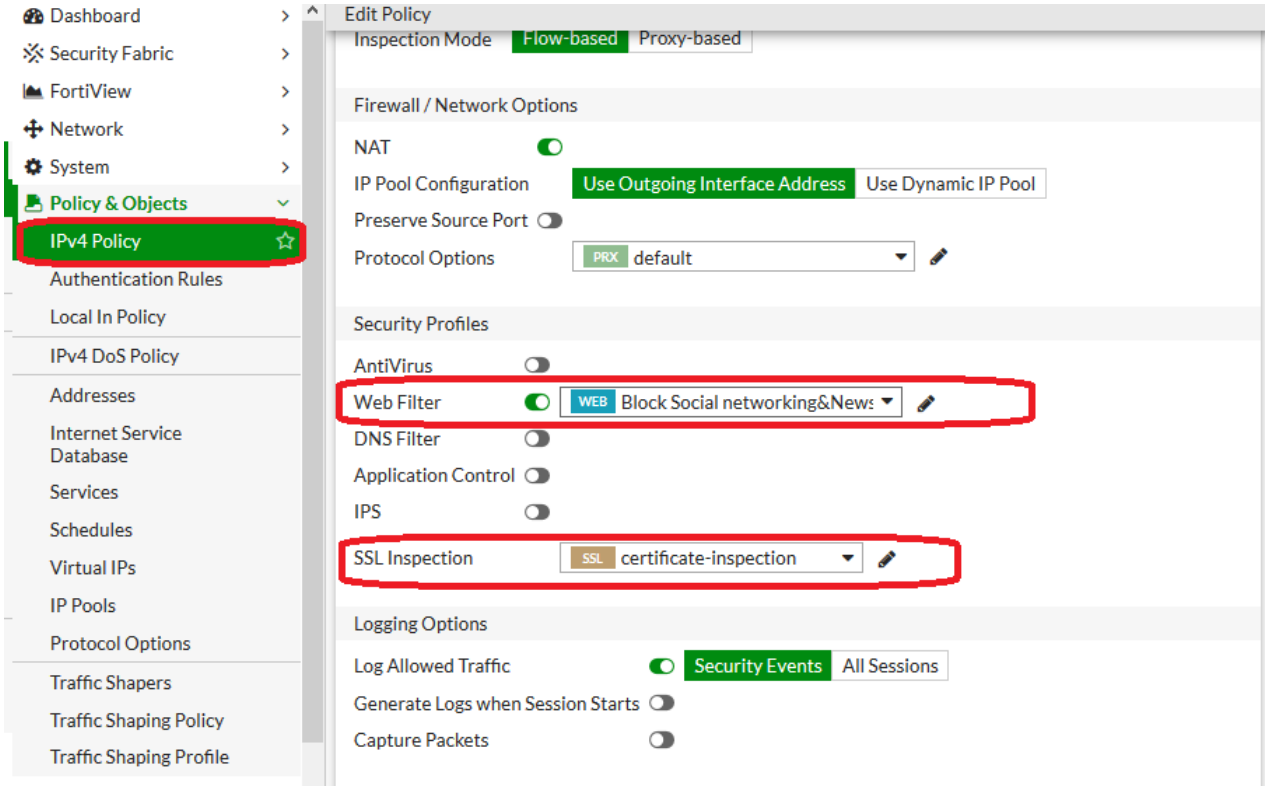
فعند محاوله فتح أي موقع اخباري مثل BBC فأنه ستظهر لك رساله بان الموقع مغلق بالإضافة الى المعلومات بايبي الجهاز 192.168.2.121 الذي حاول يفتح الموقع وأيضا ال category الذي ينتمي لها هذا الموقع هو News and Media والذي تم اغلاقه بواسطتها ..



فلو قمت بفتح موقع الفيسبوك https:\\facebook.com فانه 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

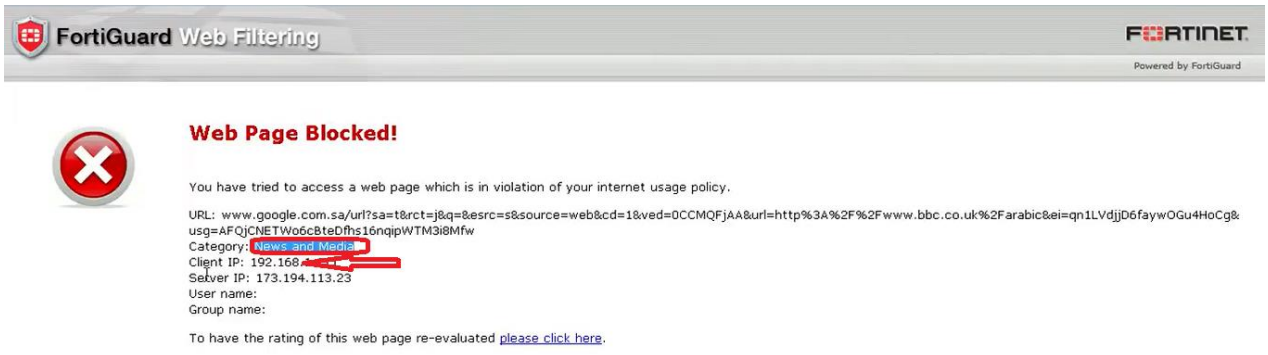
ssl inspection=certificates-inspection وبذلك تجعل الفورتي جيت يقوم بفحص أي موقع https وبهذا سوف يتم غلق المواقع الاجتماعية.

اي ان أي شخص يريد الوصول الى موقع ضمن تصنيف الشبكات الاجتماعية او المواقع الإخبارية سواء كان http او https فانه سوف يتم اغلاقها ..

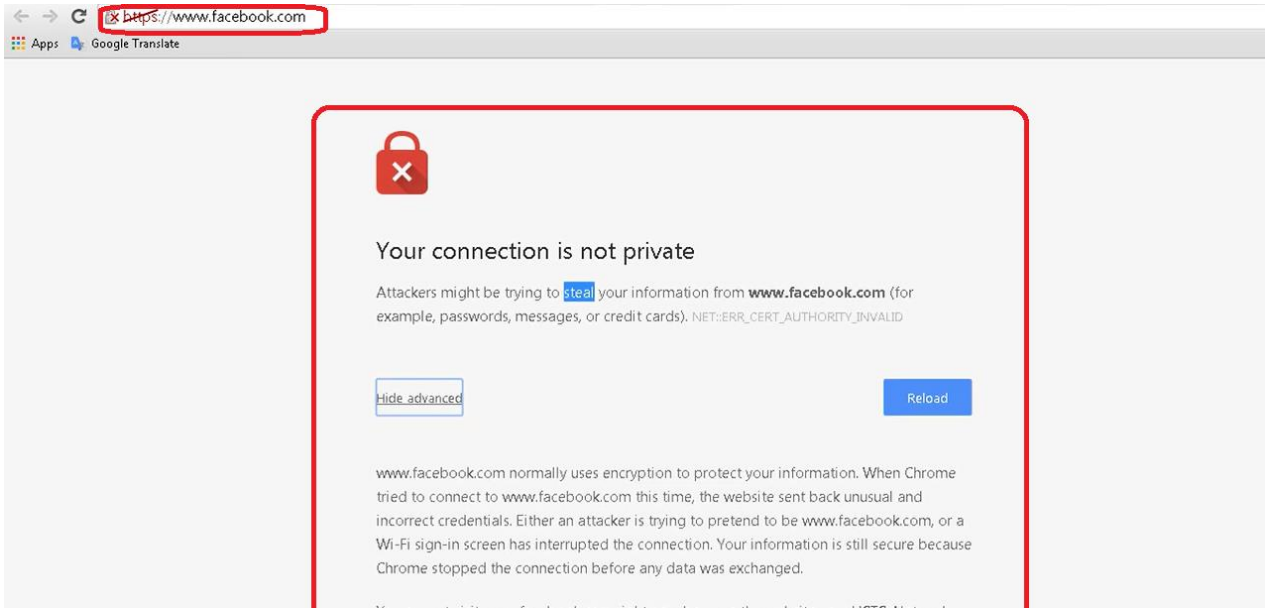


ملاحظة :

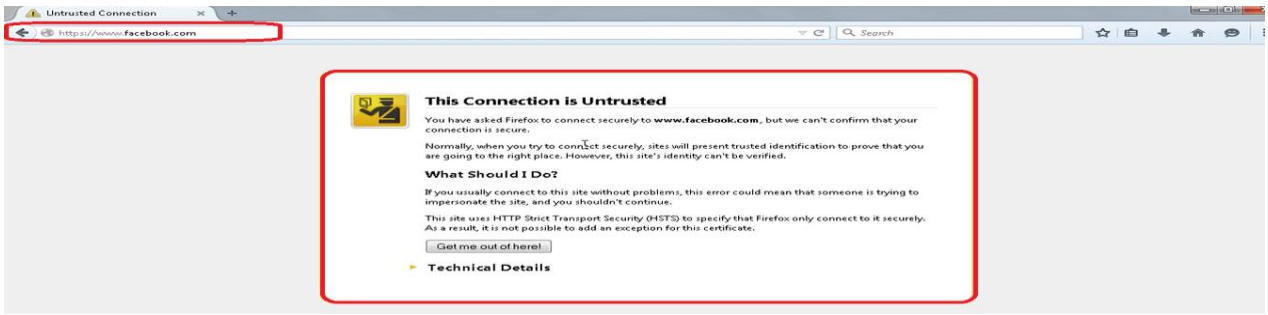
لوكان الموقع المراد الوصول اليه http وهو ضمن التصنيف المعمول له Block فسوف تظهر رساله الغلق(Web page Blocked) من فورتي جيت كما بالصورة ادناه

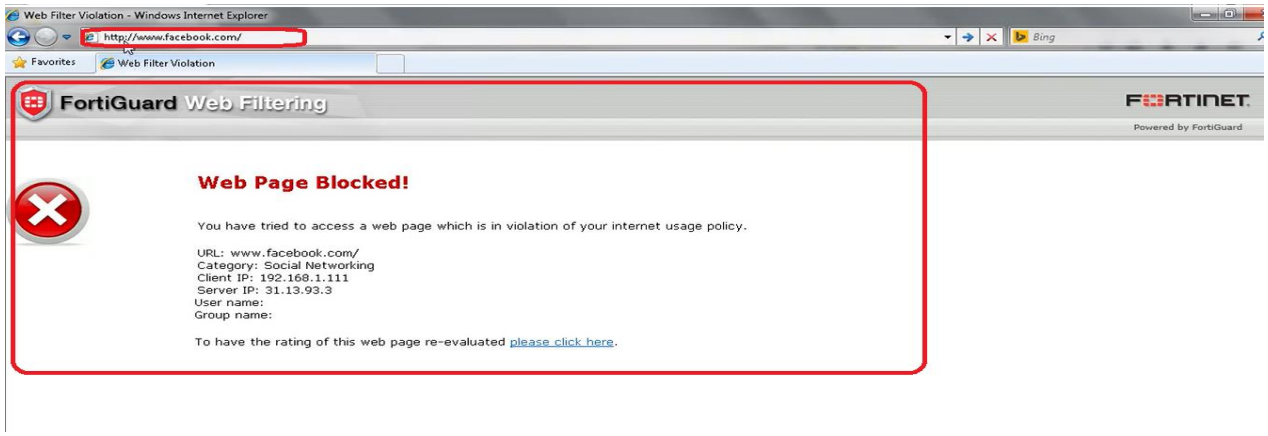


اما لو قمت بتفعيل خاصيه ssl inspection فأن رساله الغلق Web page Blocked لن تظهر بهذا الشكل(باغلب المتصفحات) مع مواقع الhttps بل تظهر لك رساله الخطأ كما بالتالي وذلك بحسب المتصفح



وهذا عن طريق متصفح اخر لنفس الموقع





اما عن طريق متصفح Internet explorer ظهر لك رساله الWeb Page Blocked كما بالصورة أعلاه ..

وفي جميع الأحوال لن تستطيع الوصول الى تلك المواقع سواء http او https

الخلاصة :

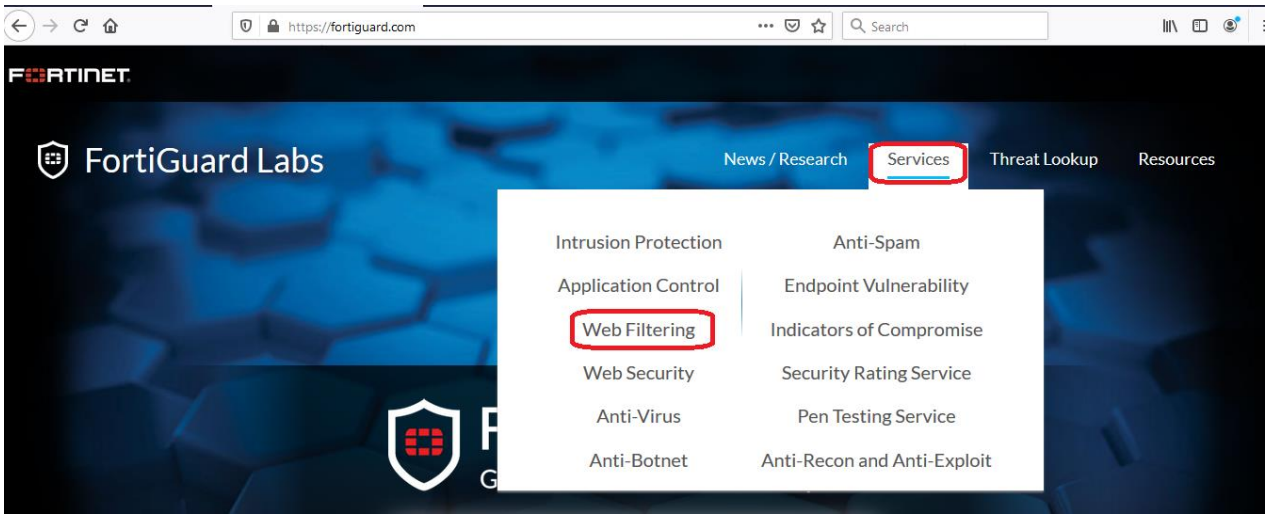
بواسطة fortiguard categories سوف تستطيع اغلاق آلف المواقع بحسب تصنيفها بنقرزر واحده بدون الحاجه الى كتابه المواقع يدويا ...

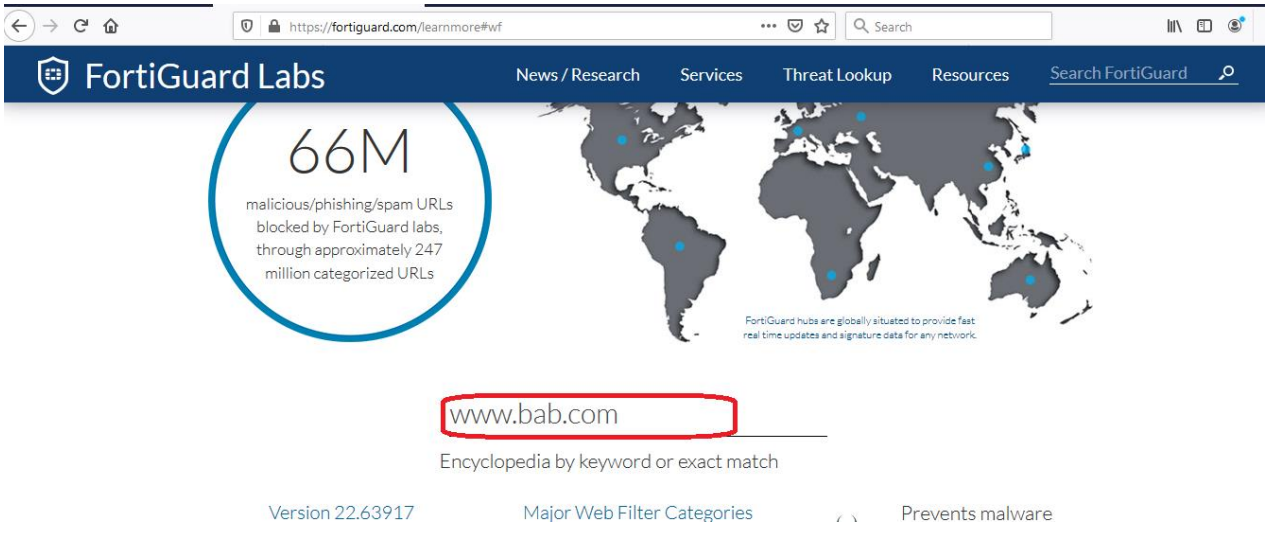
طريقة معرفة تصنيف أي موقع ..

مثلا موقع www.bab.com لو تريد معرفة تصنيفه

نقوم بالدخول الى الموقع التالي https://fortiguard.com

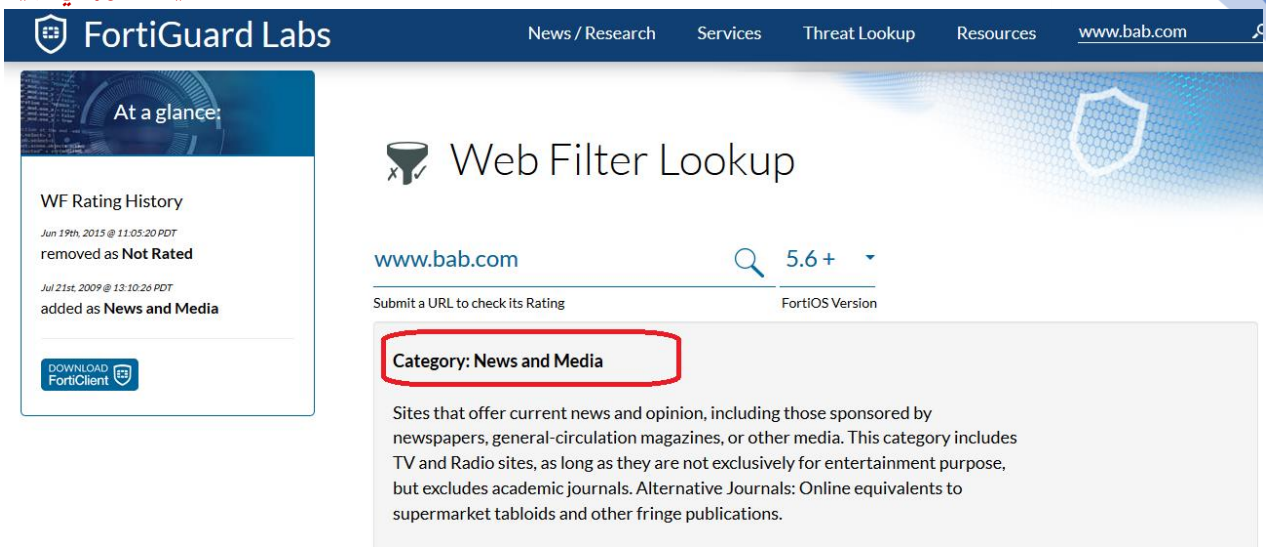
ثم كما بالصورة التالية





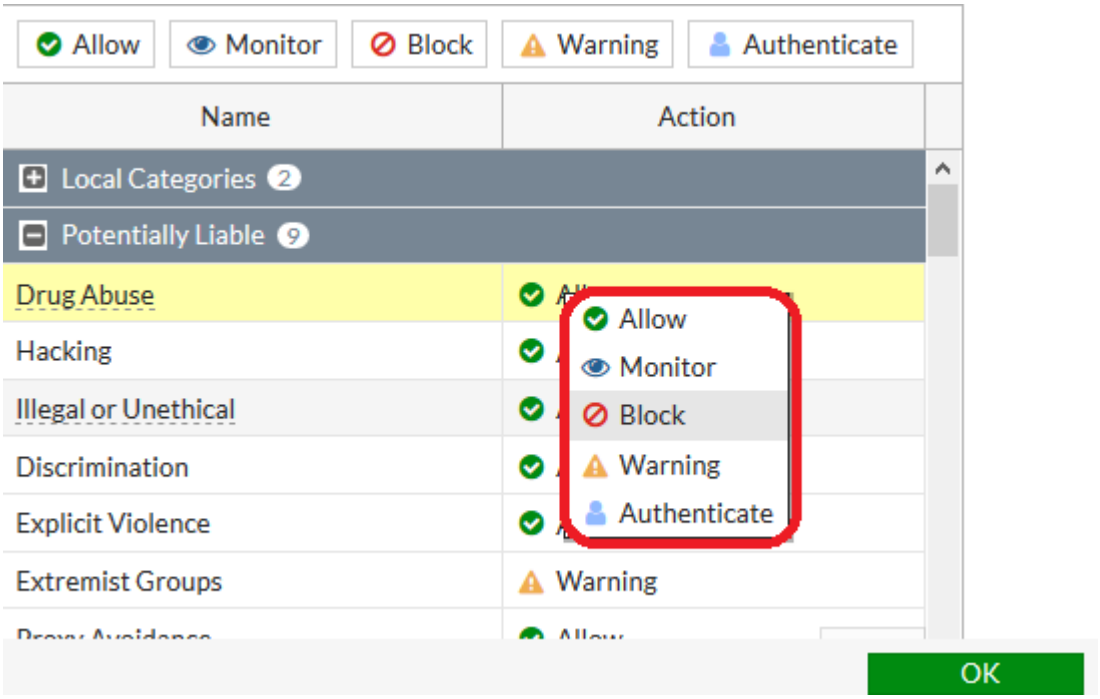
نكتب المواقع المراد معرفة الـ category التابع له ثم enter

سوف يظهر لك التصنيف للموقع كما بالصورة ادناه



اذا الموقع www.bab.com يقع ضمن التصنيف news and Media .

أنواع الـــ action :



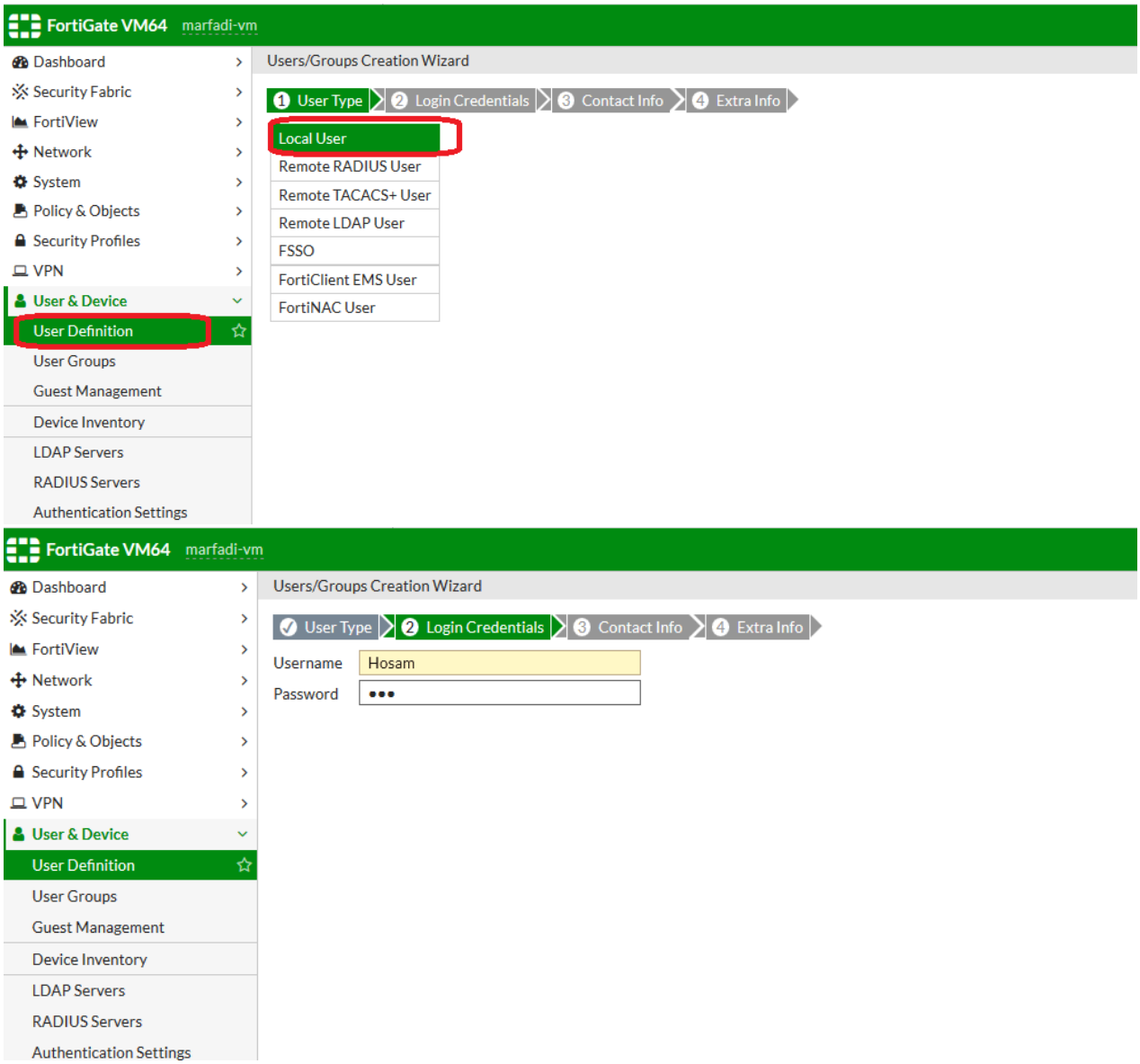
١- Allow :السماح للوصول لأي موقع يندرج تحت الـ category التي عملت لها allow

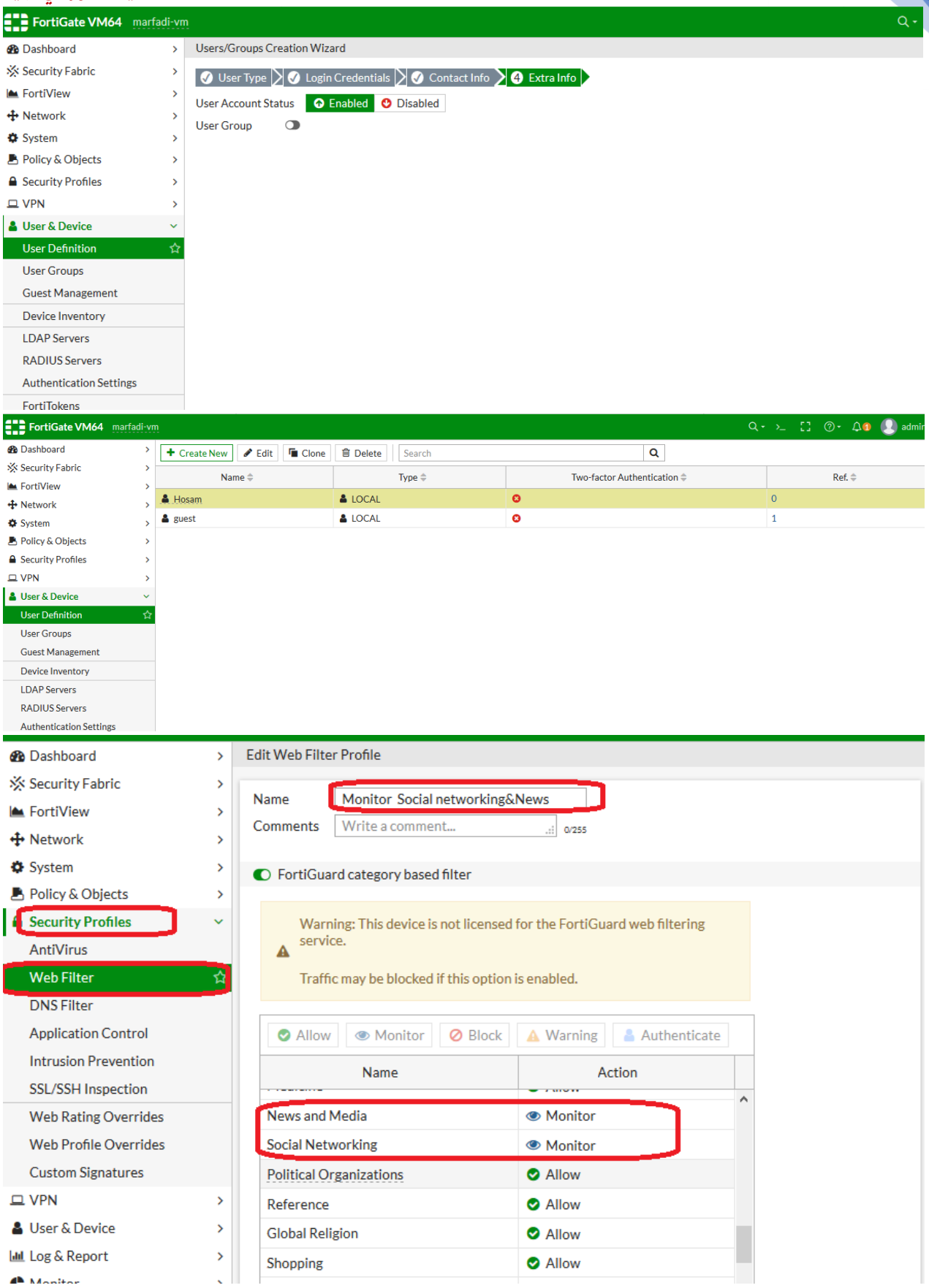
٢- Block : منع الوصول لأي موقع يندرج تحت الـ category التي عملت لها block

٣- Monitor :مراقبه أي شخص من الوصول الى أي موقع يندرج تحت category قمت بعمل لها monitor ..

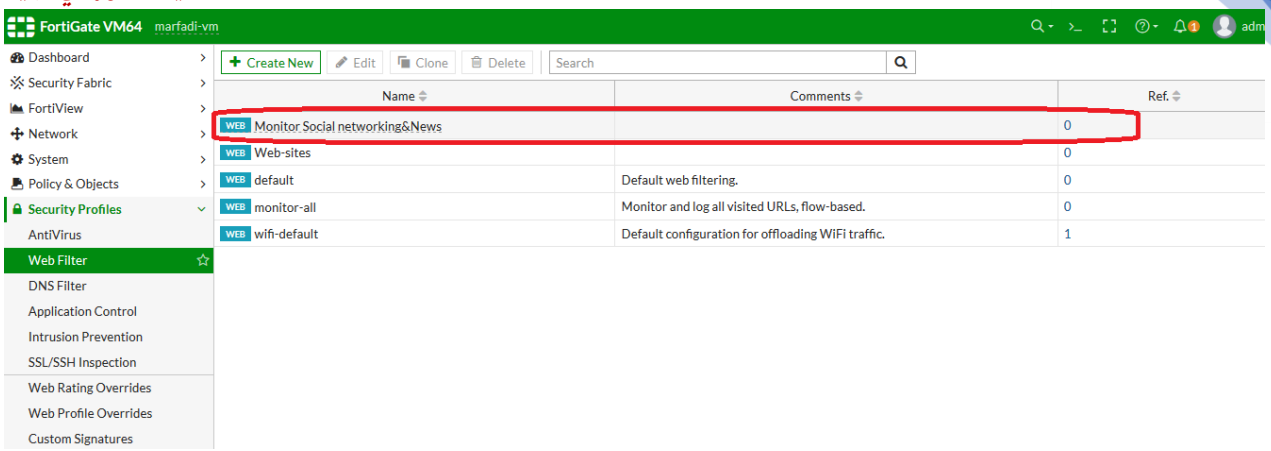
حيث المراقبة سوف تكون في الـ logs حيث سيظهرلك ماذا فتح من موقع ومتى ومن الشخص الذي فتح الموقع ولكن بشرط يجب ان يكون اليوزرموجود في local users (حسابات محليه)التابع للفورتي جيت أي ان اليوزرلو أراد الوصول الى الانترنت يجب ان يقوم بإدخال اليوزرينم وباسورد حيث سيتم عمل Monitor لهذا اليوزرات فقط .

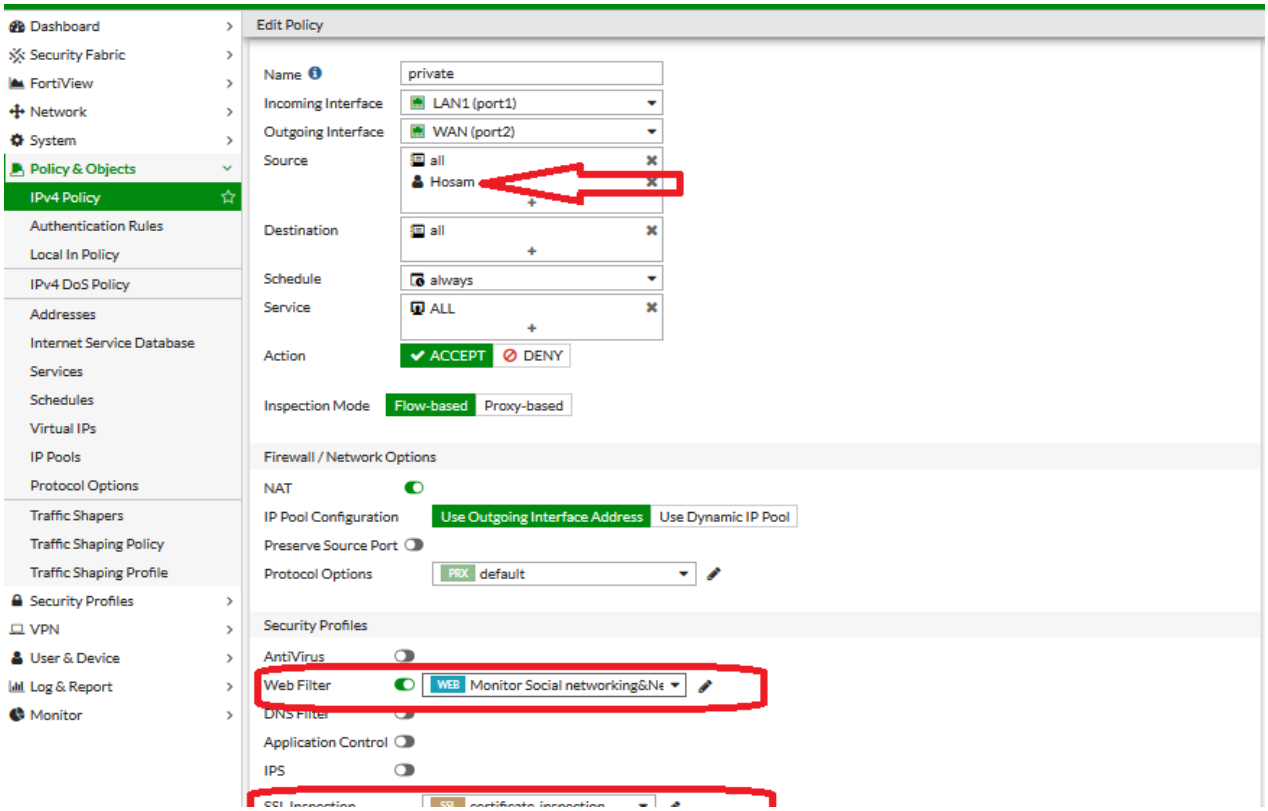
فاذا قمت بإنشاء يوزرمحلي باسم Hosam وباسورد 123 على الفورتي جيت وأريد مراقبه الـcategory المسماة social networking سوف نقوم بالتالي :





تم عمل مراقبه New and Media و Social Networking كما بالصورة أعلاه

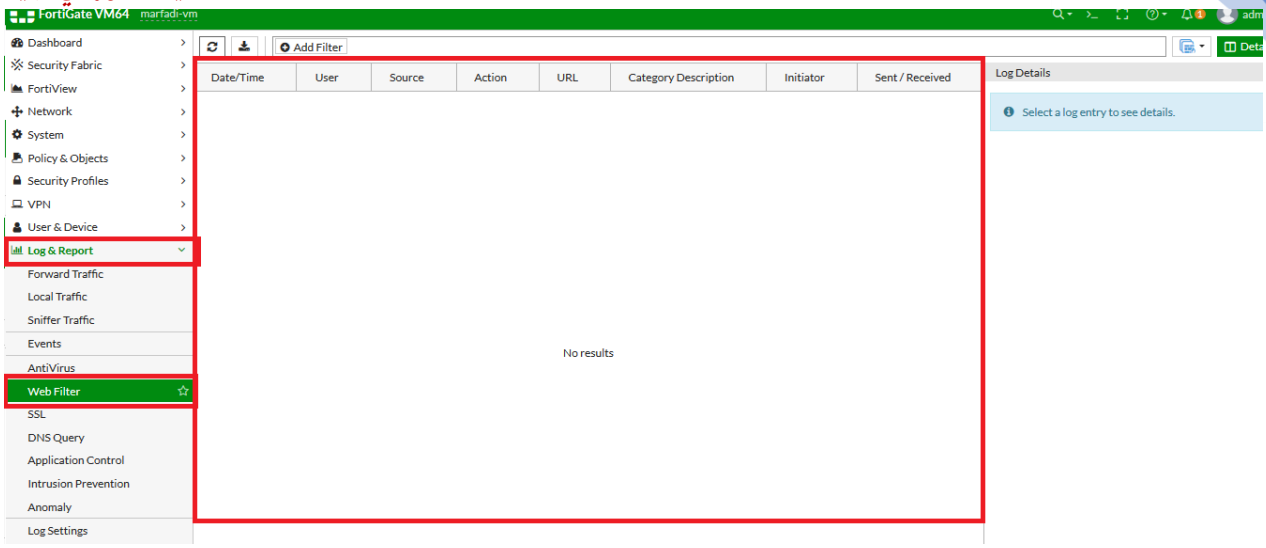




كما بالصورة أعلاه تم انشاء بوليسي بحيث يتم مراقبه اليوزر المسمى Hosam عند الوصول الى Social networking & new and Media

حيث المفترض عندما يقوم اليوزر Hosam بفتح موقع مثل فيسبوك او صحافه نت او غيرها من المواقع ضمن التصنيف الـSocail networking & new and Media

فانه سوف يطلب منه يوزرنيم وباسورد وبد إدخالها من قبل hosam فان الموقع سوف يفتح طبيعي ولمراجعه الـ logs لليوزر



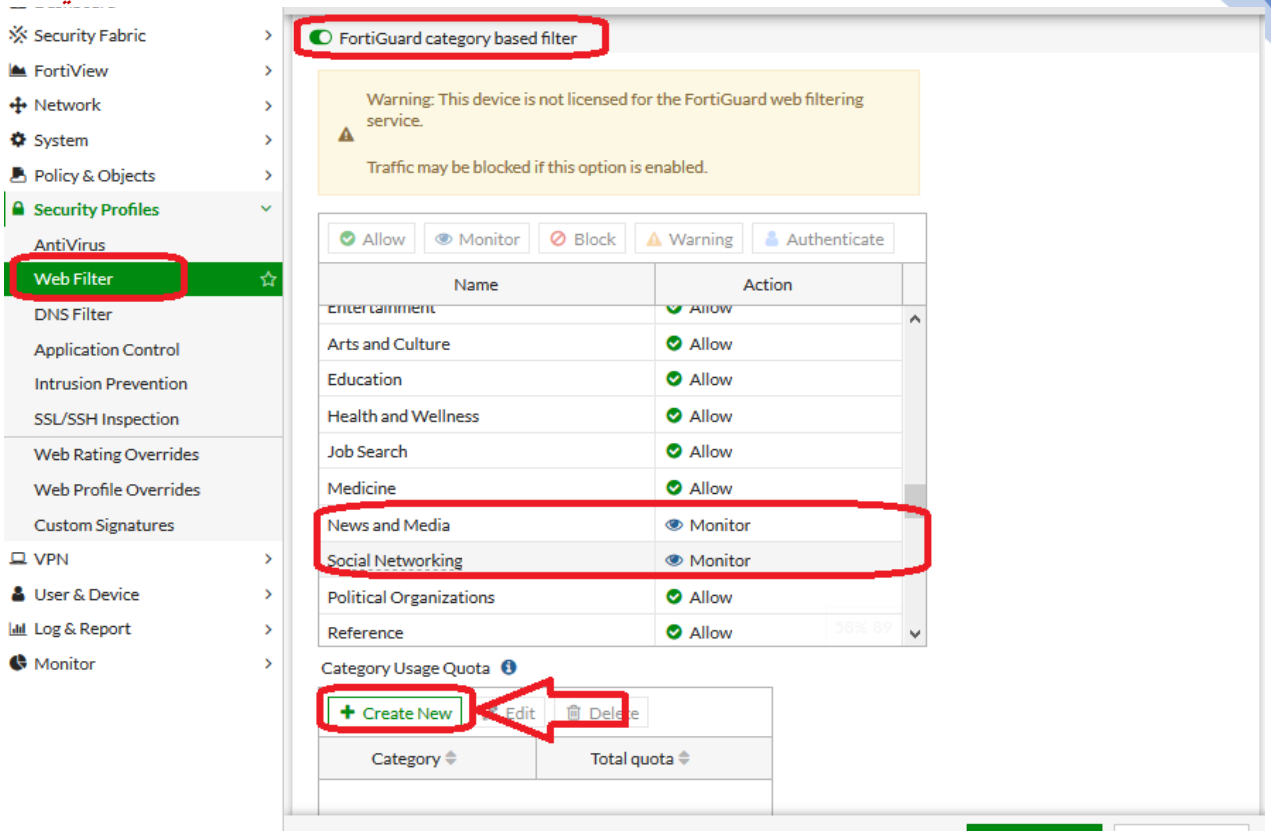
حيث يظهر لك الوقت واسم اليوزر والـ action والموقع الذي تم الوصول اليه من قبل اليوزر والـ category المندرج تحتها هذا الموقع وغيرها من المعلومات ..

أي ان يوزر معمول له Monitor فاني ممكن اطلع على الـ logs كما بالصورة أعلاه ..

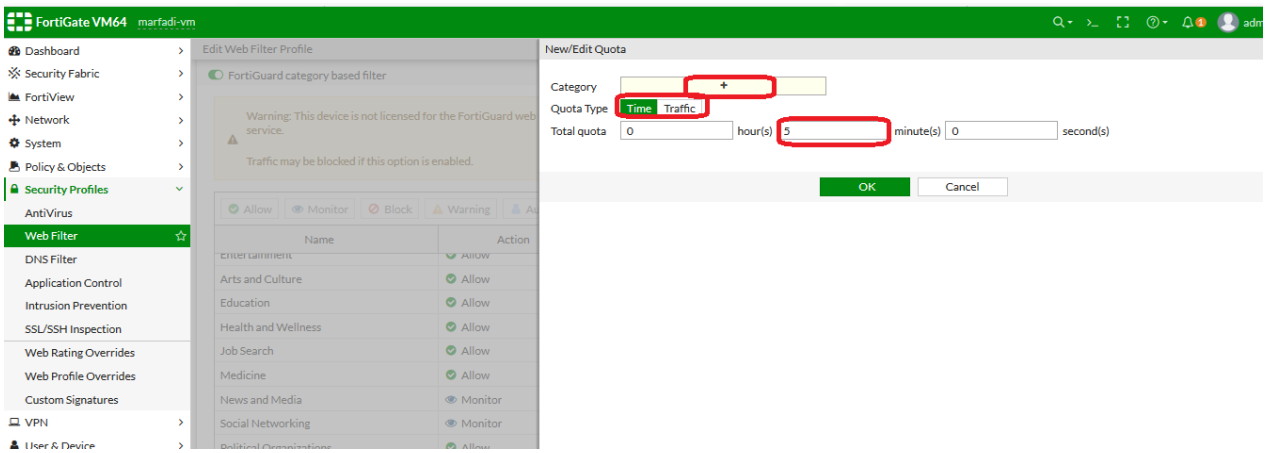
لو كنت تريد فتح مثلا مواقع معينه مثل الفيسبوك وتويتر لفتره محدده ولكن بدون تحديد الوقت (مثلا 15 دقيقه في اليوم لكل يوزر) ليس محدد الوقت المسموح، بل أي وقت سوف يستخدمه اليوزر سوف يتم اعطاءه 15 دقيقه فقط بغض النظر عن الوقت وبعدها سوف يتم عمل block لتلك المواقع ..

فمثلا بعض الموظفين سوف يفتحوا المواقع صباحا لمده ربع ساعه والبعض الاخر ظهرا والخ وهكذا حيث سيتم حساب وقت كل يوزر على حده وبعد انتهاء الوقت سوف يتم عمل Block لهذه الـ category .

- يوجد في الفورتي جيت خاصيه جميله جدا اسمها الـ Quota حيث يتم تطبيق الـquota على الـ category التي الـ action لها Monitor او authenticate او warning فقط

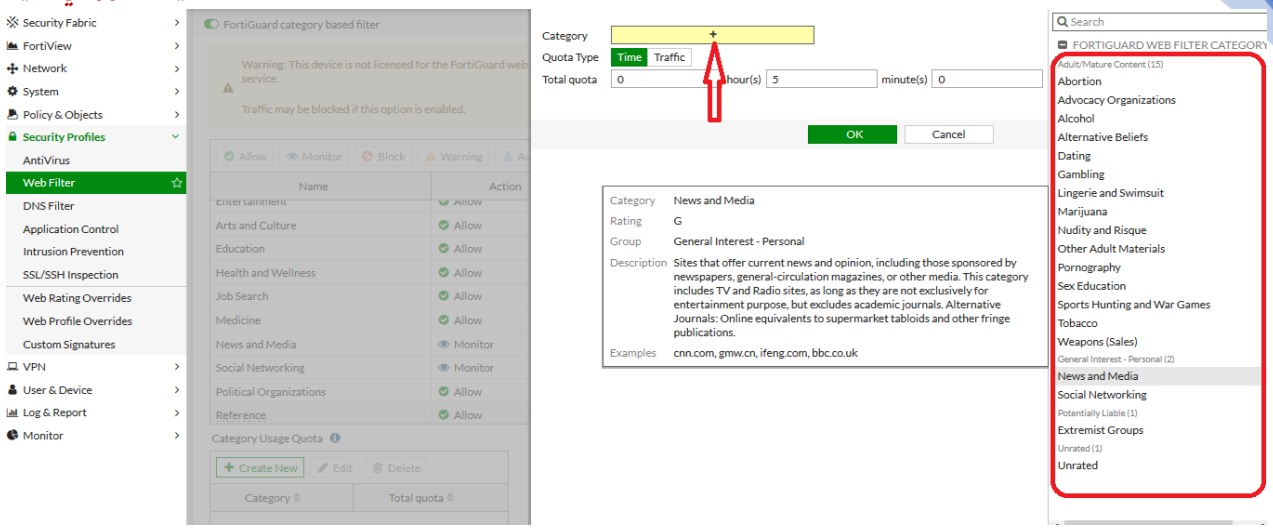


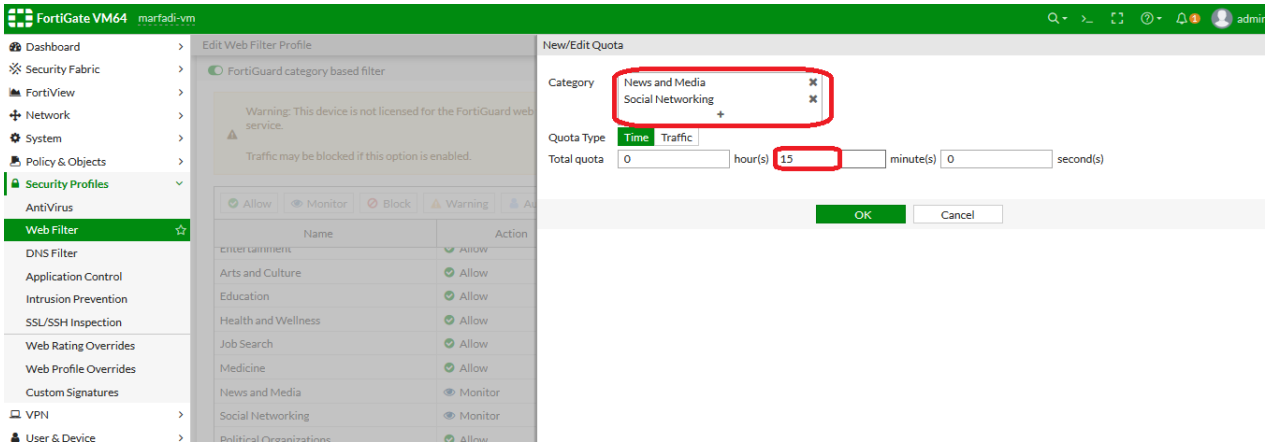
عندما اريد انشاء Quota وذلك بالنقر على الخيار Create New فأنه يجب ان تكون الـ category من احدى الأنواع الثلاثه التي ذكرت سابقا لكي أتمكن من انشاء الـquota



نقوم بتحديد نوع الـQuota هل بالوقت ام بالترافيك(بالحجم)

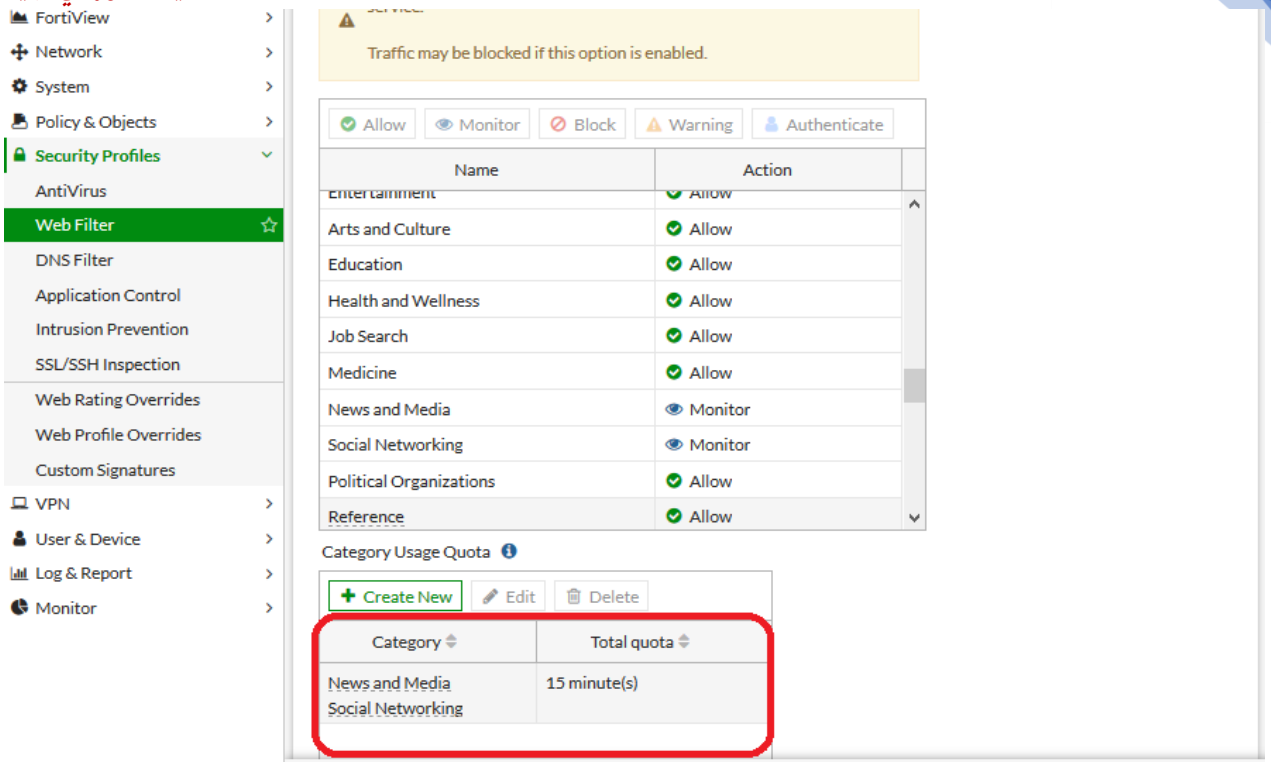
ونقوم بتحديد الـ category المراد تطبيق quota عليها .





تم السماح 15 دقيقه لليوزر من الوصول الى مواقع الاخبار ومواقع التواصل الاجتماعي فقط ...

حيث بمجرد انتهاء الـ15 دقيق للموظف فانه سيتم عمل Block لتلك الموافق مباشره ..

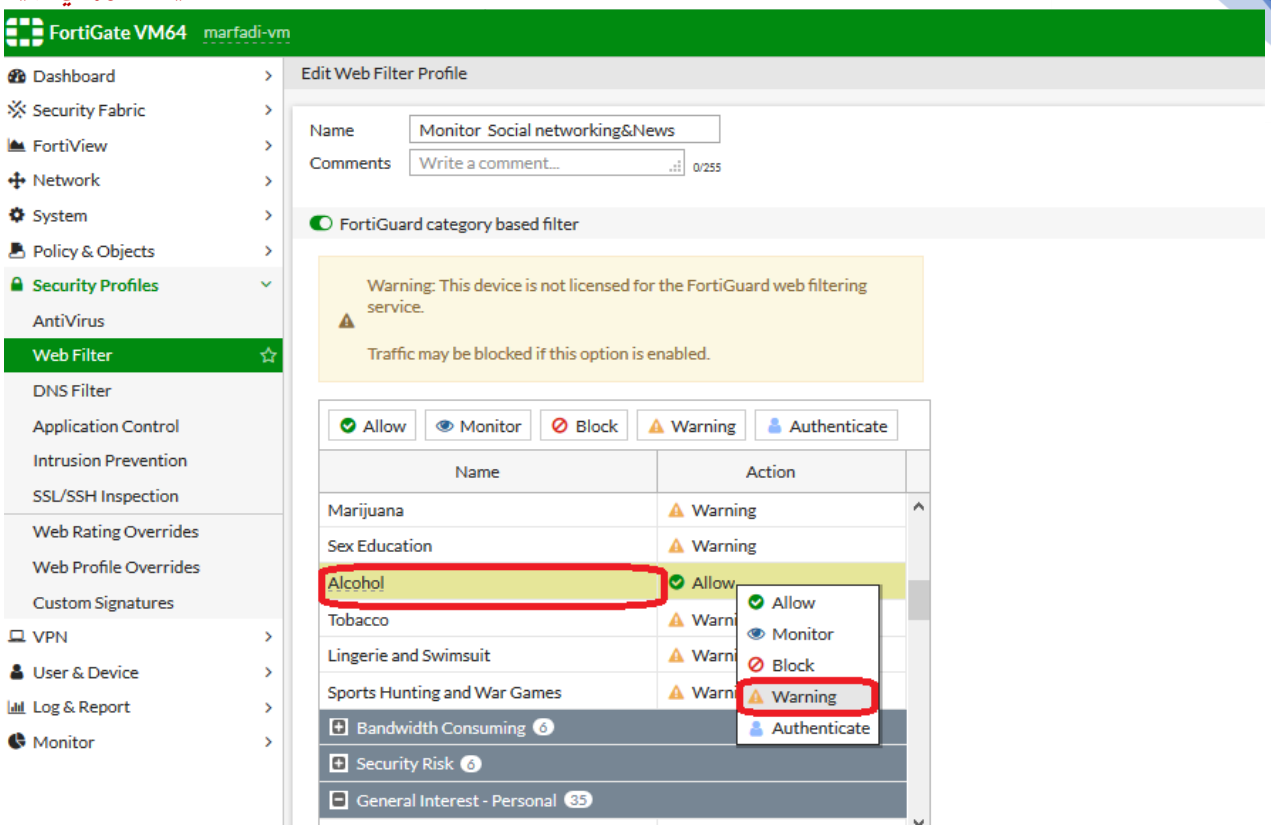


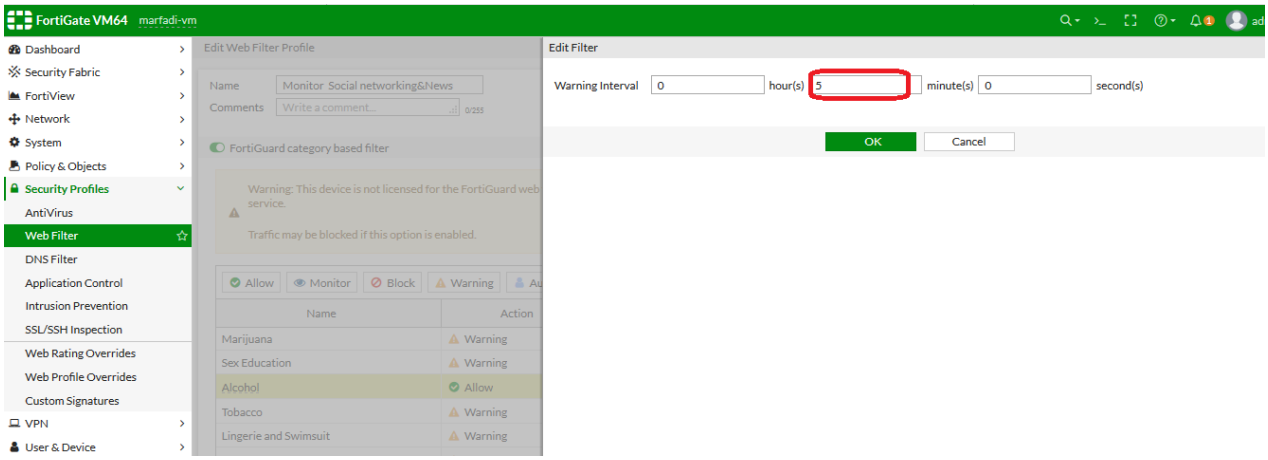
Warrning :معناها بأنه تم اغلاق الموقع في الشبكة حيث ستظهرلك رساله تحذيريه لليوزرتوضح بان الموقع الذي قمت بطلبه محجوب لو تريد فتحه سوف تفتحه على مسؤليتك وستصبح متراقب من قبل الفورتي جيت

حيث سيظهررساله تحذيريه 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 Alchol

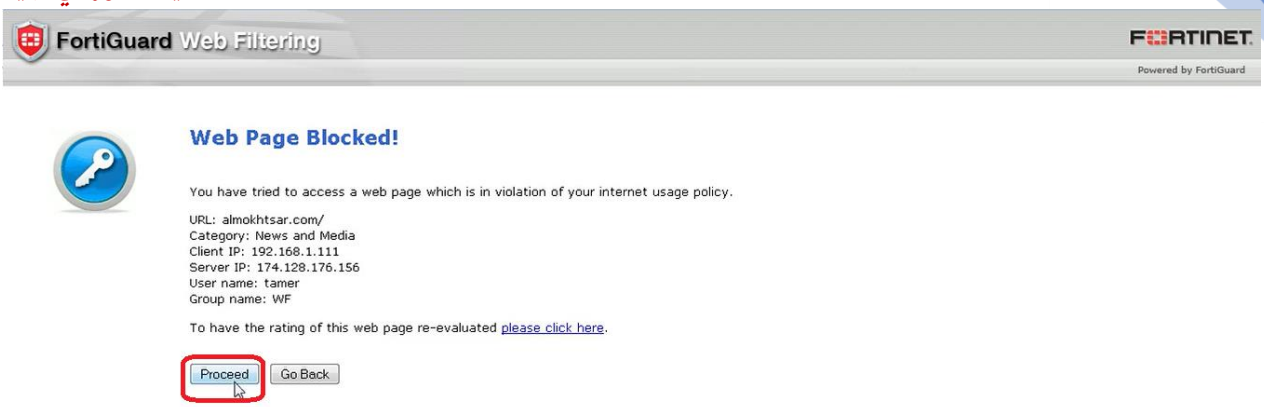
فمجرد تنقربالزر الأيمن على الـ Alchol وتختارالـaction=warning فأنه سوف تفتح لك نافذه كم بالتالي





حيث كل 5 دقائق يظهرلك رساله تحذيريه لو انت لا زلت فاتح أي موقع ضمن التصنيف المحدد سابقا (Alchol).

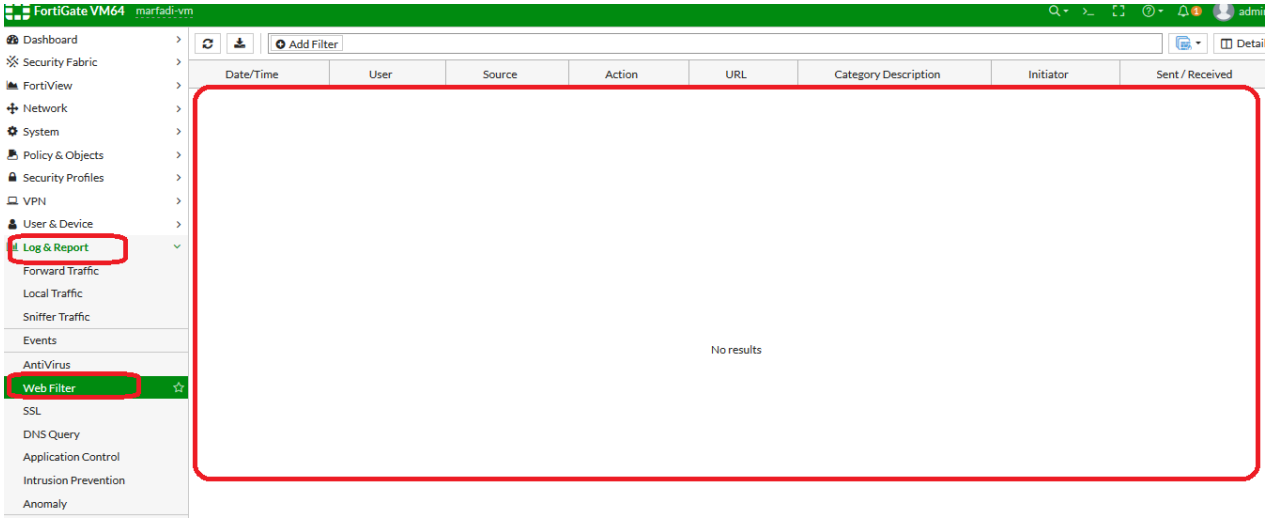
حيث لو قام المستخدم بفتح أي موقع ينتمي لهذا التصنيف سوف تظهرله رساله الـ Block كما بالصورة التالية



فلو تريد ان تفتح الموقع فقم باختيار الخيار Proceed .

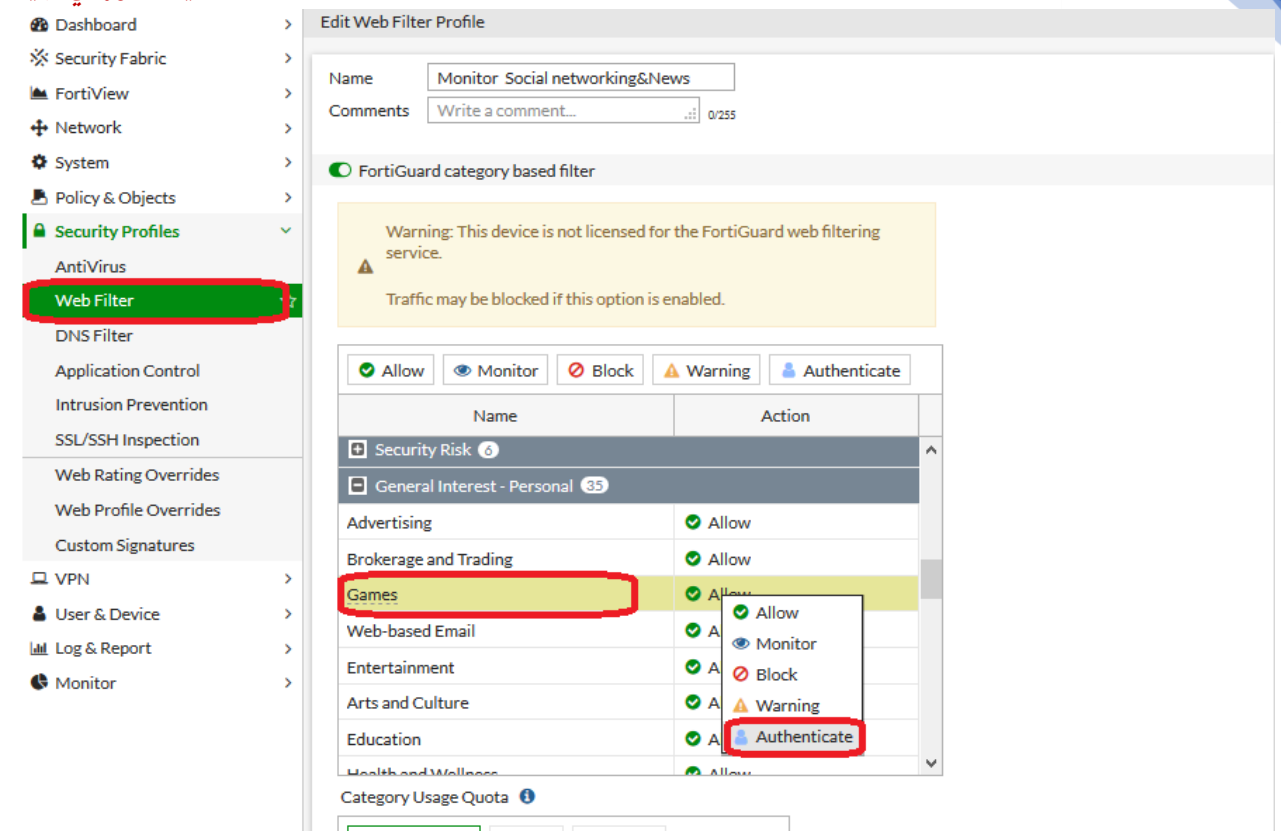
فبعد 5 دقائق سوف يتم اغلاق الصفحة ثم ظهور رساله الـ Web Page Blocked فلو تريد ان تفتح الموقع على مسؤليتك فثم باختيار Proceed.

حيث يصبح كل المواقع المندرجه متراقبه عبر الفورتي جيت ويمكن استعراض كل الـ logs كما بالتالي :

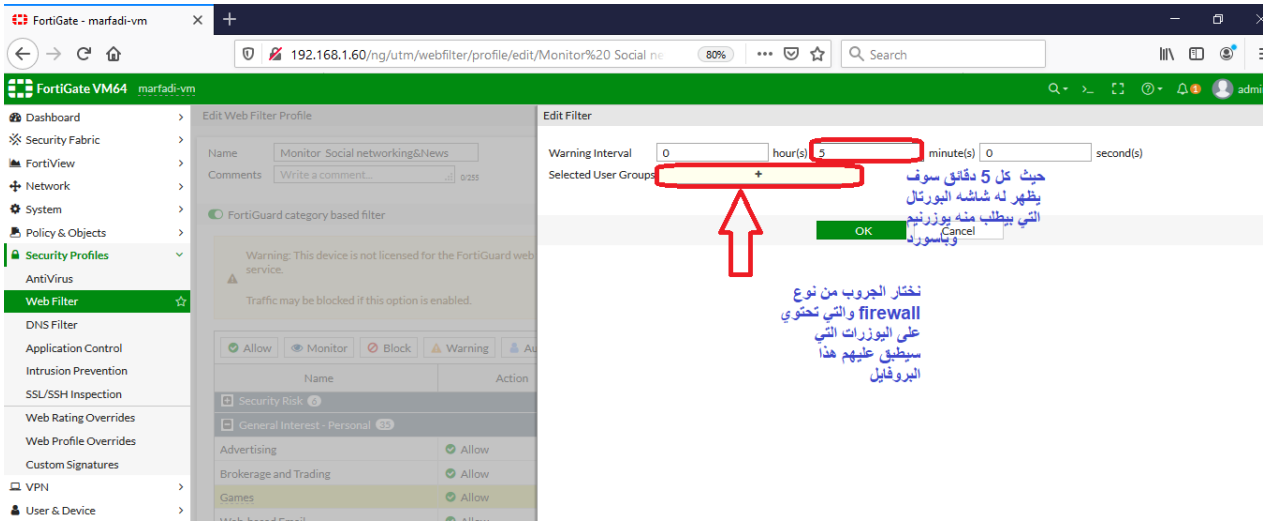


Authenticate : متى تريد ان تجعل البورتال يطلب يوزرنيم وباسورد ؟

حيث أي احد يحاول يفتح أي موقع يندرج تحت الـ category المعمول لها Authenticate فأنه سوف يطلب منه يوزرنيم وباسورد .



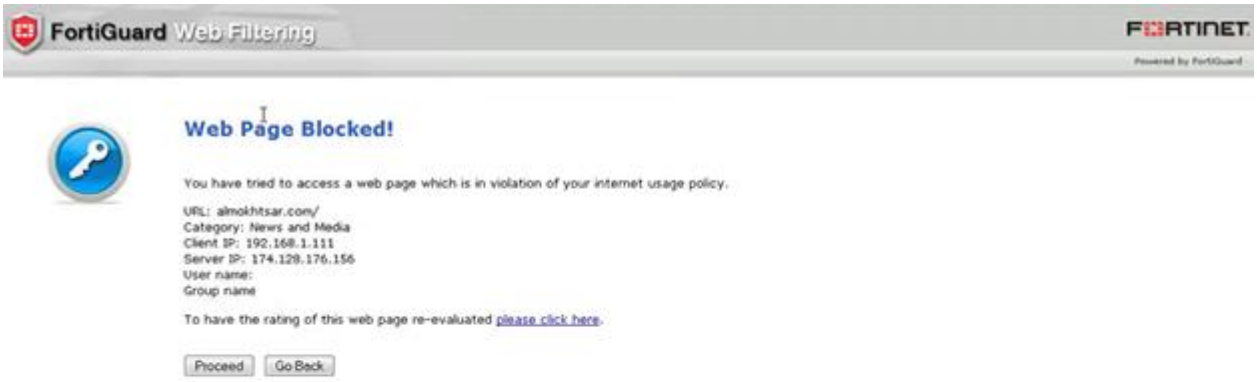
قمنا بإنشاء action نوعها Authenticate على الـ category المسماة Games



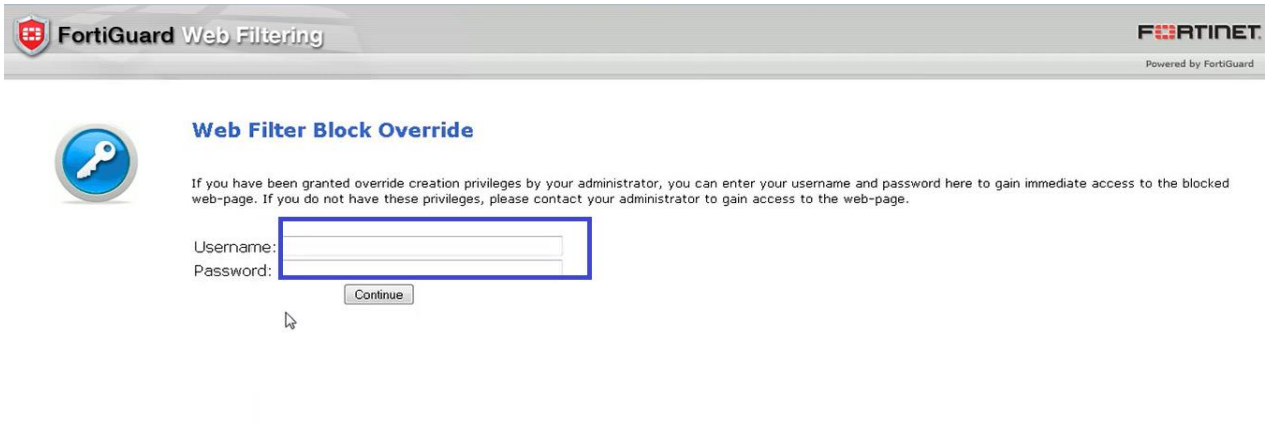
حيث أي يوزرمن الجروب المختاره سوف يفتح موقع من مواقع الألعاب سوف يظهرله نافذه البورتال (يوزرنيم وباسورد)..الخ

الخلاصة :

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 يظهرله البورتال اللي بيطالب منه اليوزرنيم والباسورد لكي يعمل reauthentication ويستطيع الوصول الى تلك المواقع ...



ثم بعد النقرعلى الزر proceed فأنه سوف تظهرلك الشاشة التالية



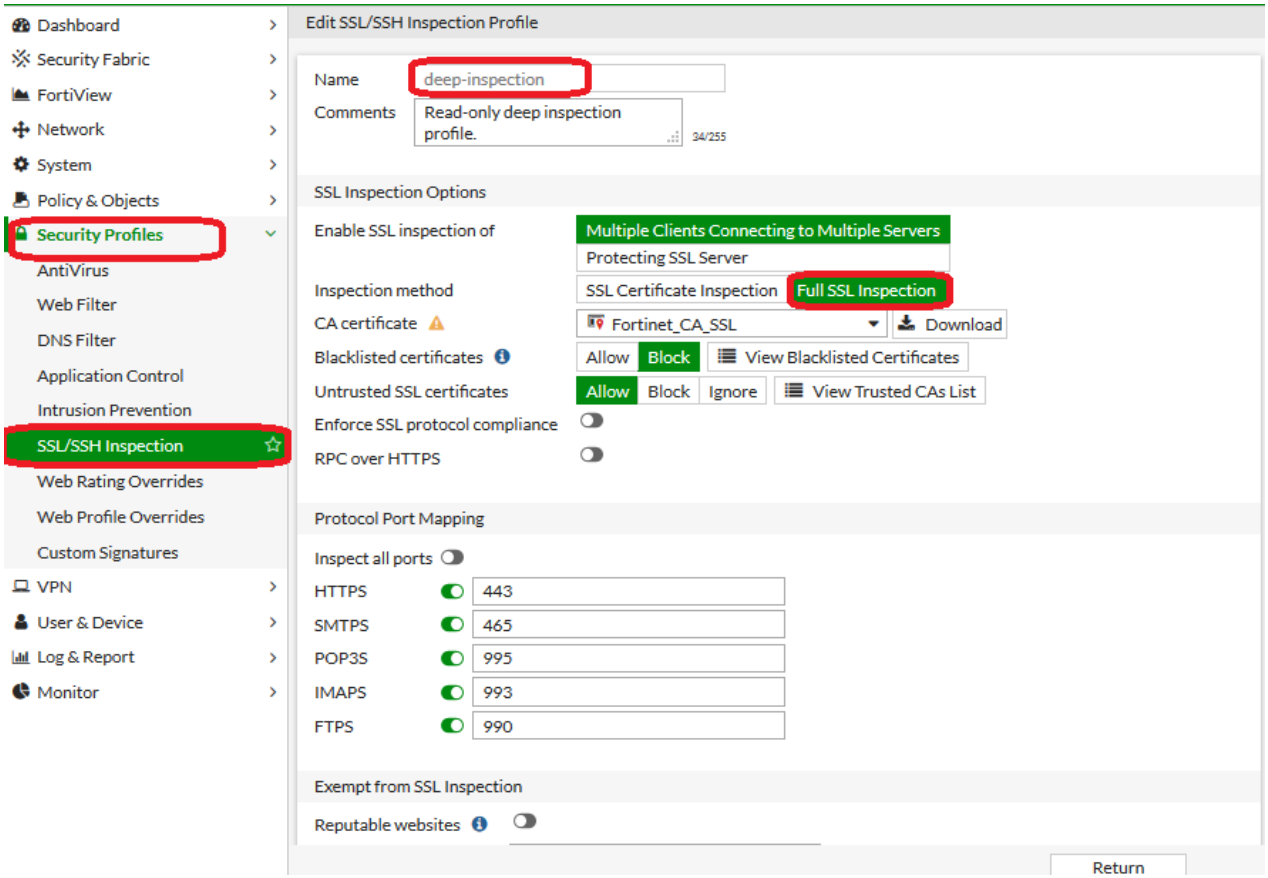
فيجب عليك ادخال اليوزرنيم والباسورد لأحد اليوزرات التي تنتمي للجروب المحدده.

ملاحظة :

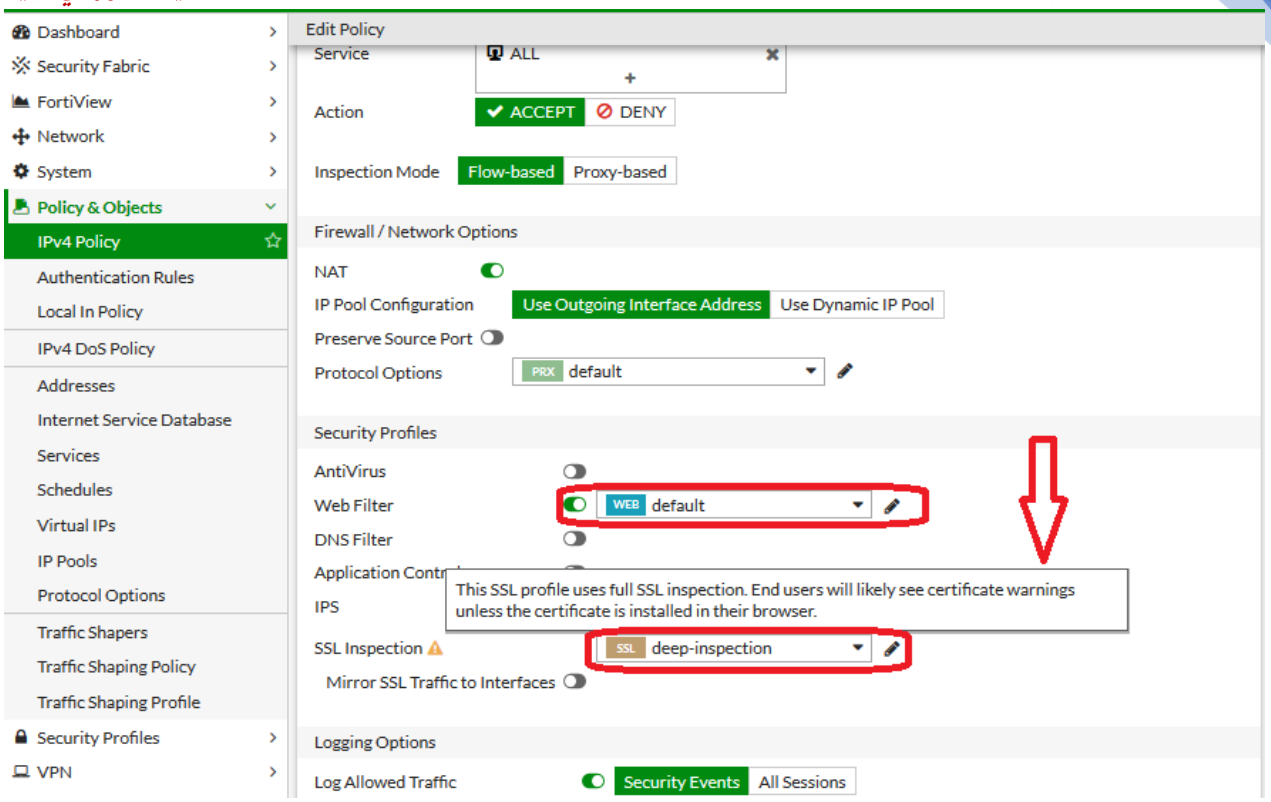
الـwarning يعتبرنفس الـauthenticate الا انه في حالة الـauthenticate يطلب منك يوزرنيم وباسورد ..

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 معينه لـ ssl أي للمواقع التي تكون https وليس http يجب ان تكون مضبط الاعدادات بشكل سليم لكي يعمل معك الـ web filtering أيضا يجب ان تكون عامل الشهادة certificate بشكل سليم ومستوردها على متصفحات واجهزه الكلاينت ..

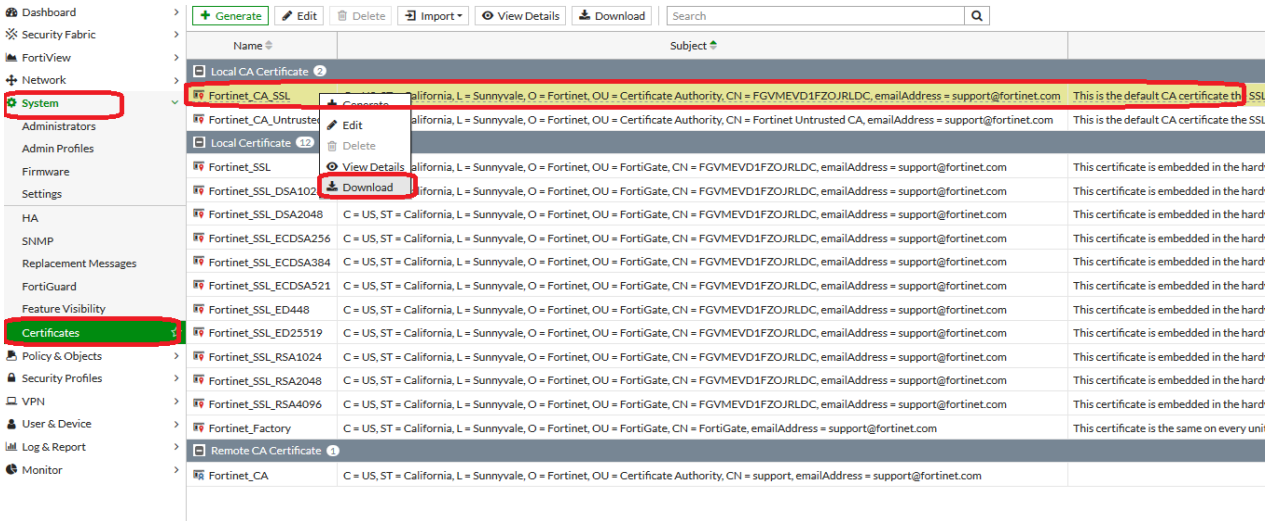


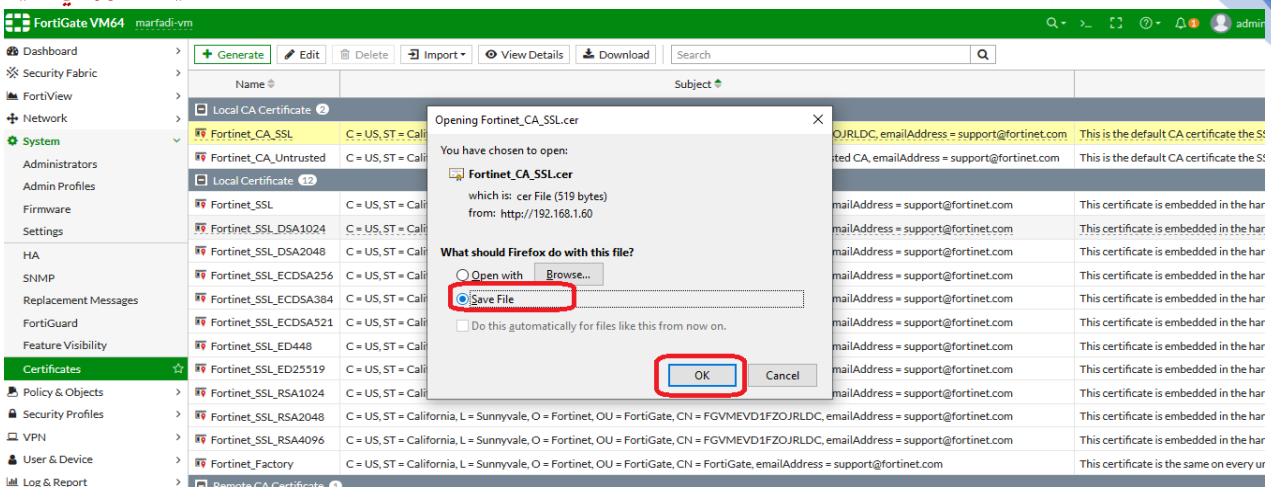
ننشئ ssl/ssh inspection ونجعلها Full SSl Inspection ثم نختارها في البوليسي كما بالصورة التالية :



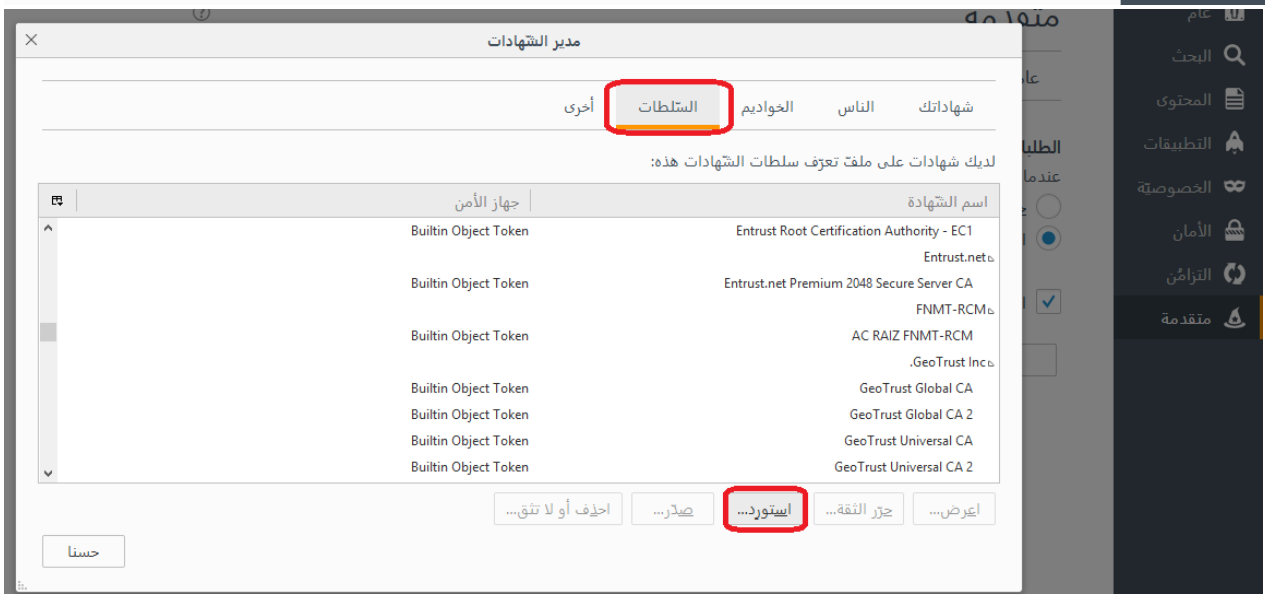
نلاحظ بأننا اخترنا البروفايل المسمى deep-inspection والذي تم تجهيزه سابقا ونلاحظ بأن هناك hint يقول فيها عند اختيار full SSl inspection فان اليوزرات سوف يحتاجوا ان تقوم باستيراد تلك الشهادة على متصفحاتهم ..

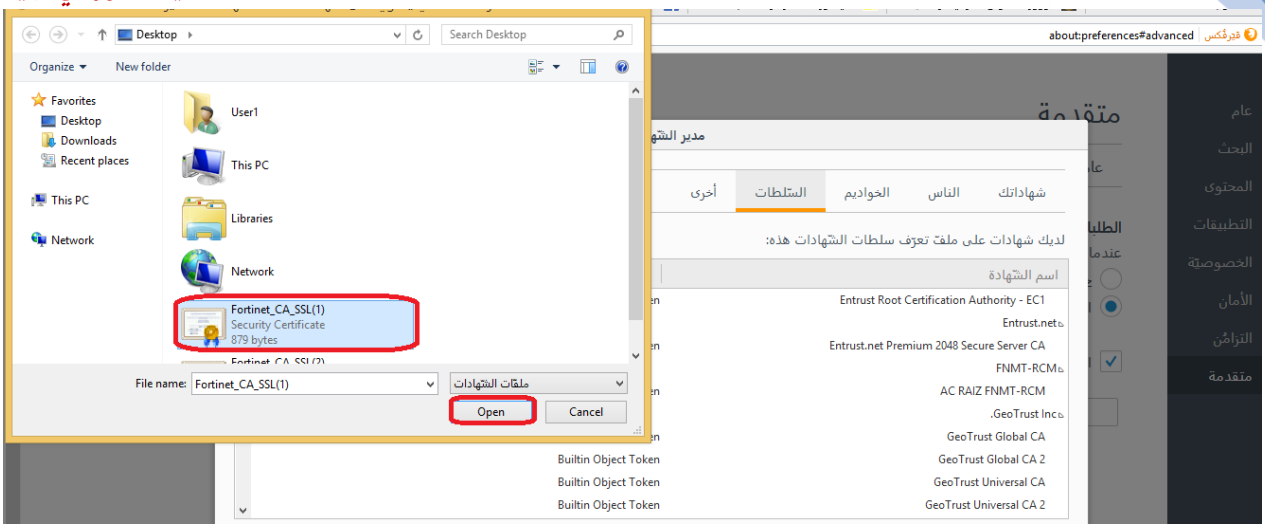
الآن سوف نقوم بتصدير الشهادة من الفورتي جيت كالتالي :

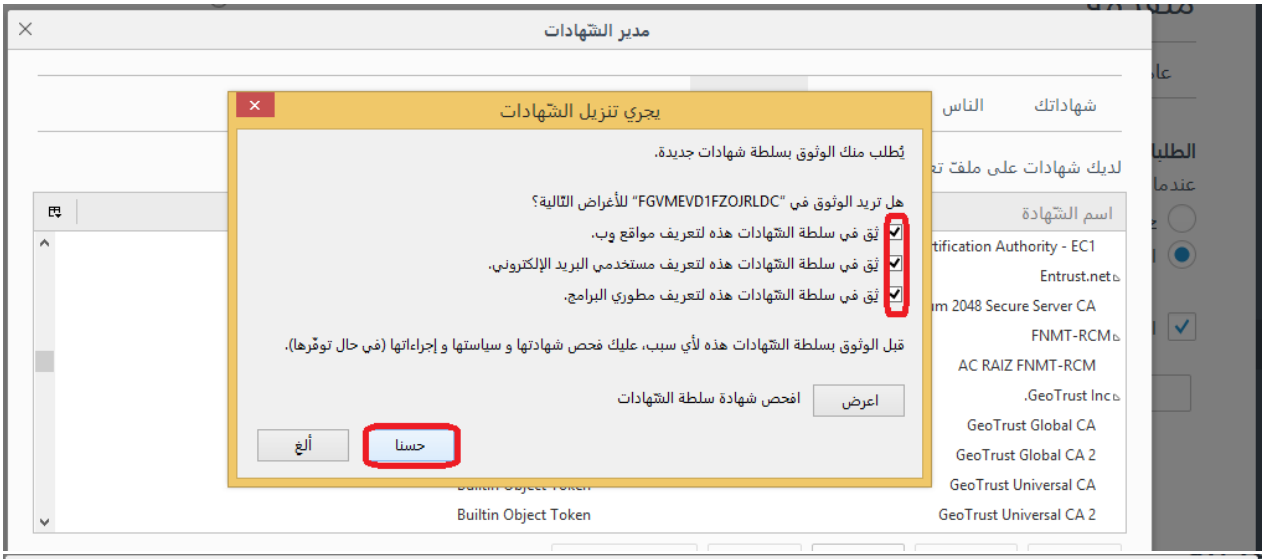


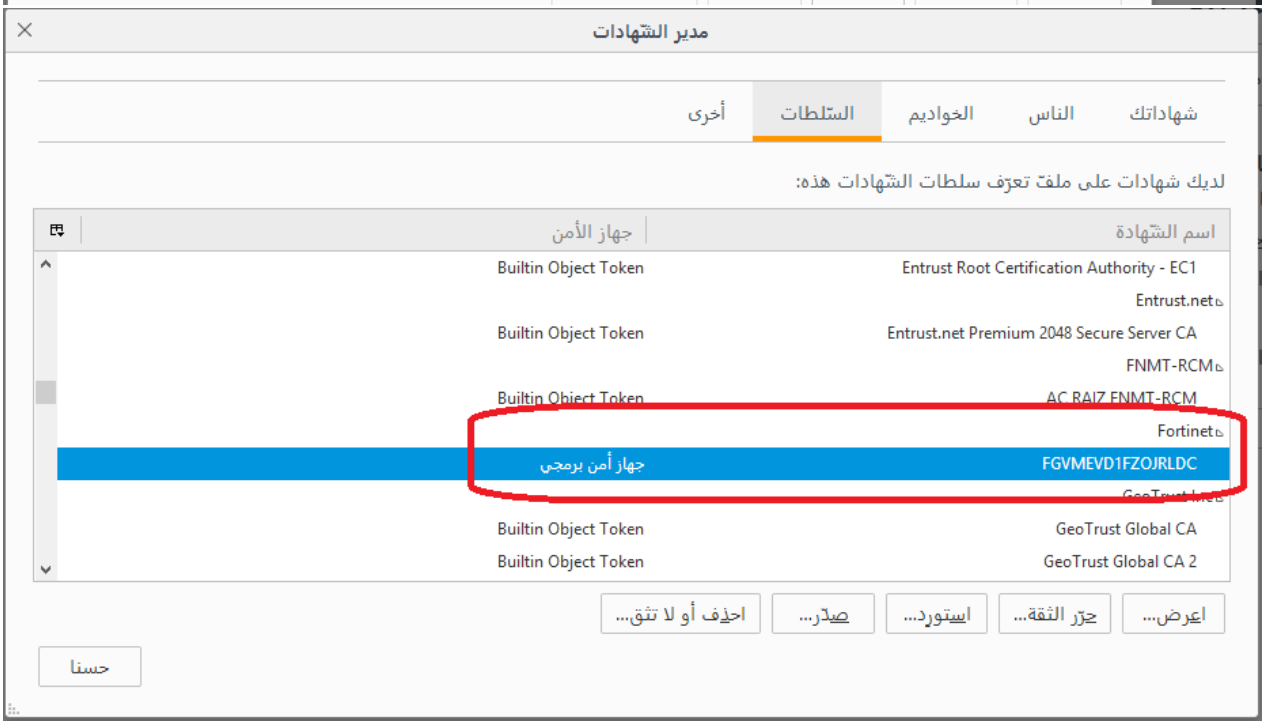


نقوم بنسخها على اجهزه الموظفين ثم نستوردها على متصفحاتهم كما بالخطوات التالية




Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
Recent places
This PC
Network
User1
This PC
Libraries
Network
Fortinet_CA_SSL(1)
Security Certificate
879 bytes
File name: Fortinet_CA_SSL(1)
ملفات الشهادات
Open
Cancel
about:preferences#advanced
متقدمة
مدير الشهادات
شهاداتك
الناس
الخوادم
السلطات
أخرى
لديك شهادات على ملف تعرّف سلطات الشهادات هذه:
اسم الشهادة
Entrust Root Certification Authority - EC1
Entrust.net
Entrust.net Premium 2048 Secure Server CA
FNMT-RCM
AC RAIZ FNMT-RCM
GeoTrust Inc.
GeoTrust Global CA
GeoTrust Global CA 2
GeoTrust Universal CA
GeoTrust Universal CA 2
Builtin Object Token

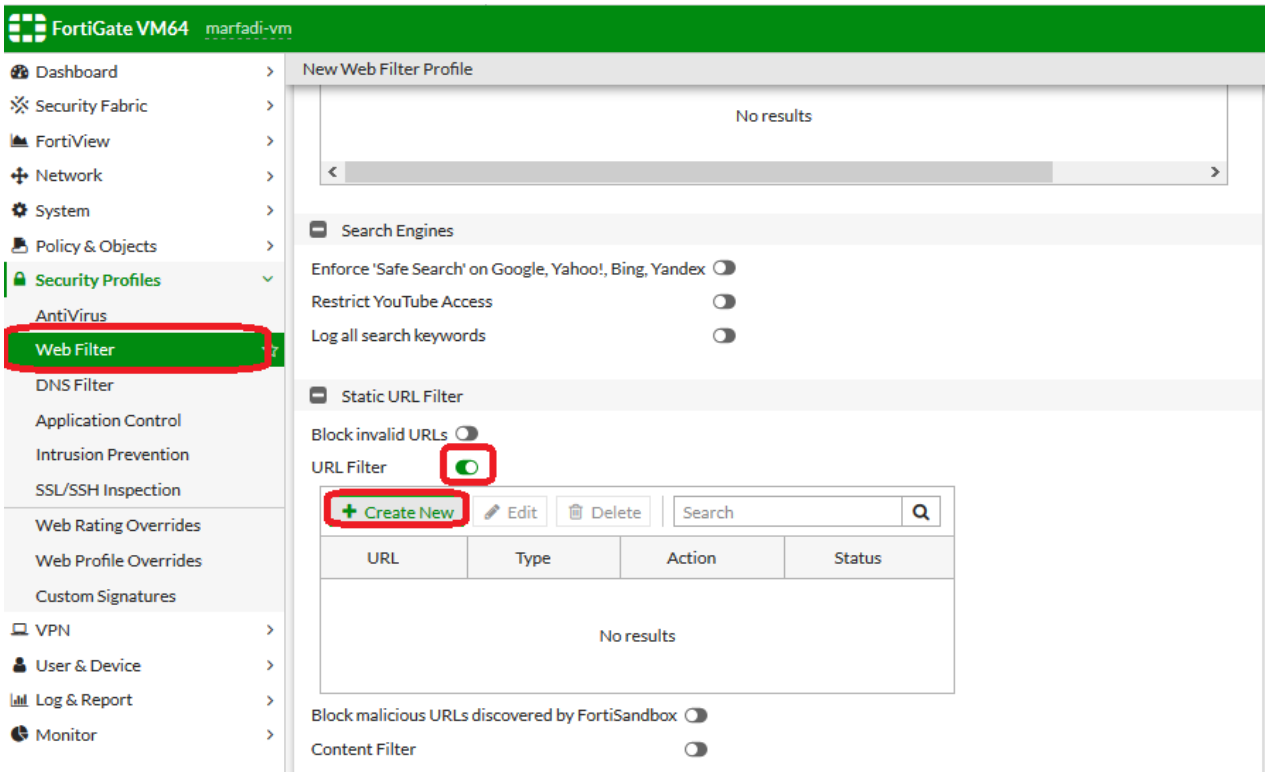

مدير الشهادات
يجري تنزيل الشهادات
يُطلب منك الوثوق بسلطة شهادات جديدة.
هل تريد الوثوق في "FGVMEVD1FZOJRLDC" للأغراض التالية؟
ثِق في سلطة الشهادات هذه لتعريف مواقع وب.
ثِق في سلطة الشهادات هذه لتعريف مستخدمي البريد الإلكتروني.
ثِق في سلطة الشهادات هذه لتعريف مطوري البرامج.
قبل الوثوق بسلطة الشهادات هذه لأي سبب، عليك فحص شهادتها و سياستها و إجراءاتها (في حال توفّرها).
اعرض
افحص شهادة سلطة الشهادات
ألغِ
حسنا


مدير الشهادات
شهاداتك
الناس
الخوادم
السلطات
أخرى
لديك شهادات على ملف تعرّف سلطات الشهادات هذه:
اسم الشهادة
جهاز الأمن
Entrust Root Certification Authority - EC1
Builtin Object Token
Entrust.net
Entrust.net Premium 2048 Secure Server CA
Builtin Object Token
FNMT-RCM
AC RAIZ FNMT-RCM
Builtin Object Token
Fortinet
FGVMEVD1FZOJRLDC
جهاز أمن برمجي
GeoTrust Global CA
Builtin Object Token
GeoTrust Global CA 2
Builtin Object Token
اعرض...
جدّد الثقة...
استورد...
صدّر...
احذف أو لا تثق...
حسنا

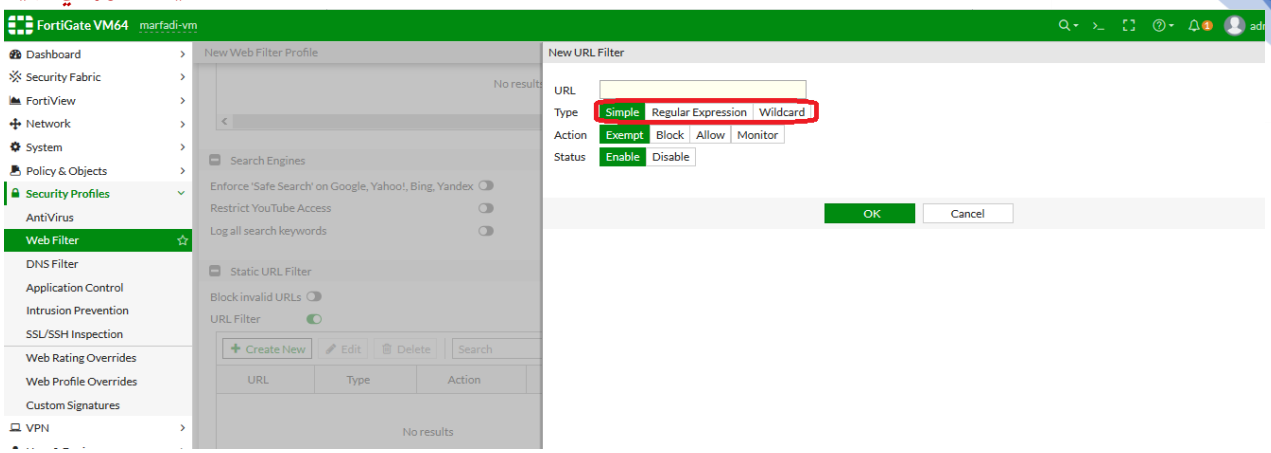
نلاحظ بالصورة أعلاه بأن الشهادة تم استيرادها بنجاح وعند النقر عليها نقرتين تظهر لك تفاصيل الشهادة ..

❖ Web URL filtering

توجد 4 أنواع مهمه في web URL filter



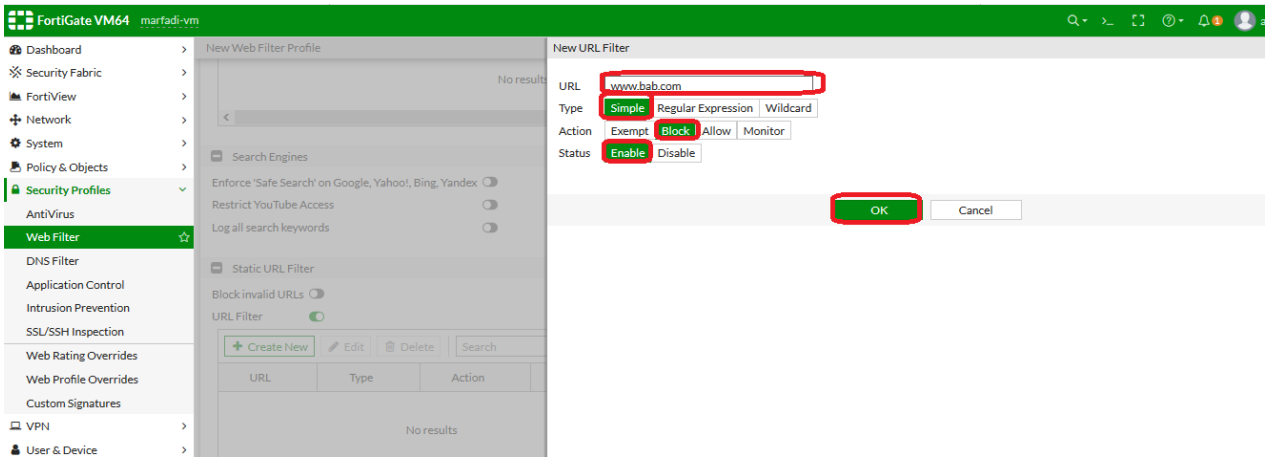
قمنا بإنشاء بروفايل جديد وتم تفعيل الخيار URL Filter ثم نقوم بإنشاء الـ static url كما بالصورة ادناه

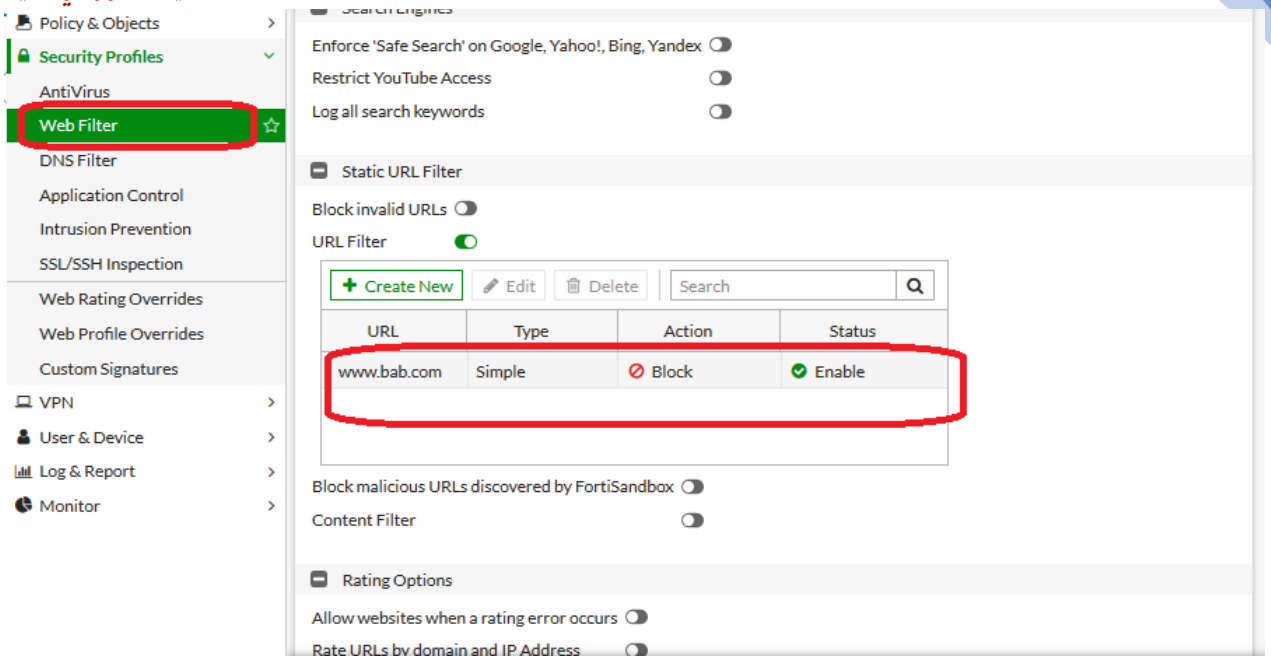


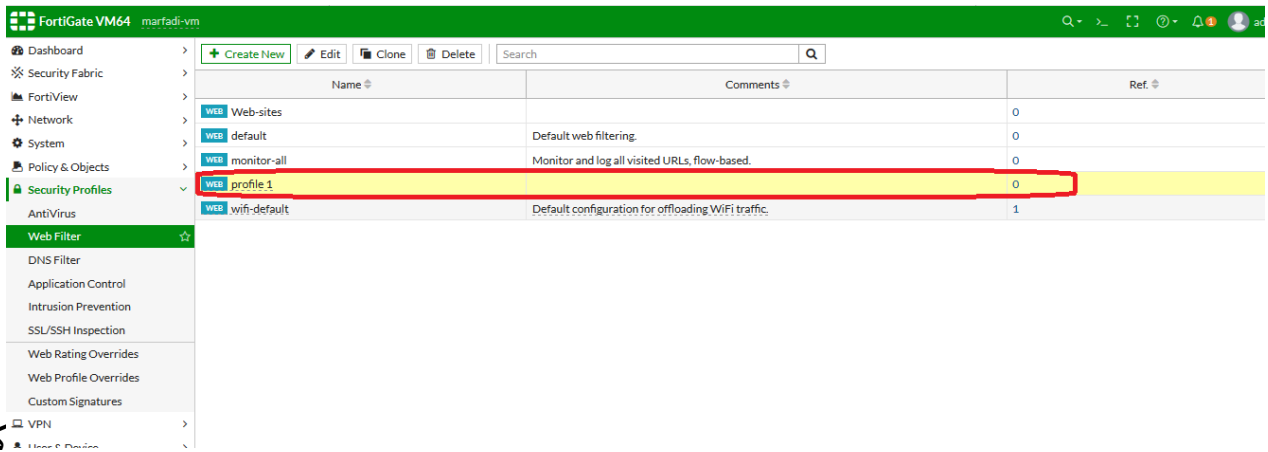
يوجد لدينا عده أنماط(أنواع-اشكال-طرق)تكتب فيها المواقع لكي تطبق عليها action معين .

١) Simple : تكتب الـ url لموقع صراحه كالتالي

www.bab.com او bab.com كل يؤدي نفس الغرض ..

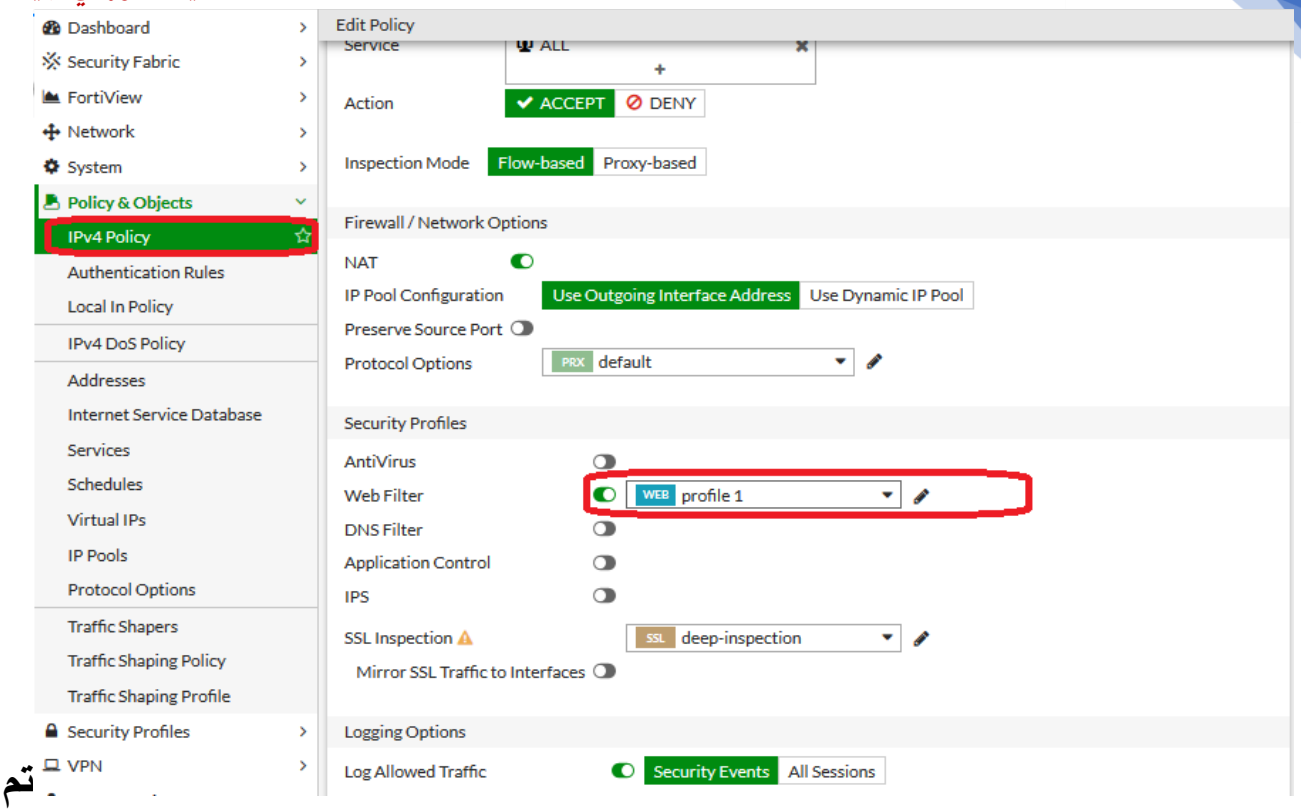






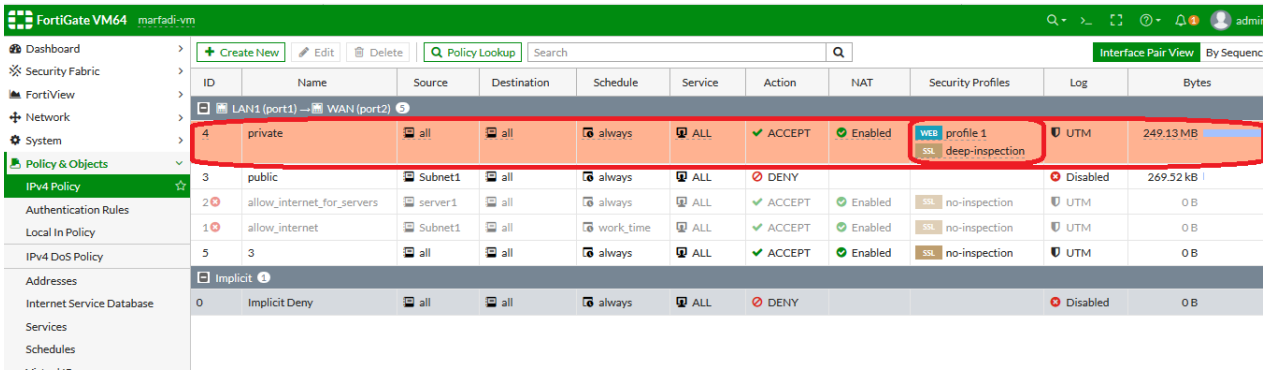
كما

بالصورة أعلاه تم انشاء البروفايل باسم profile 1



تم

تطبيق البوليسي وتم اختيار البروفايل profile 1 في Web Filter



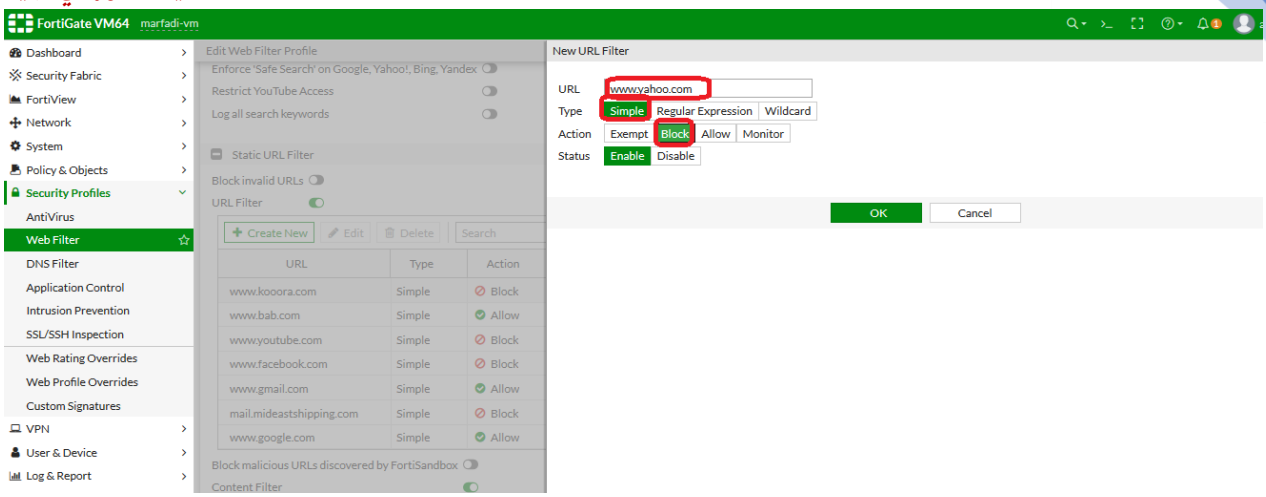
توجد عده طرق للتحكم بالويب بواسطة Static Url :

الطريقة الأولى :

ملاحظة :

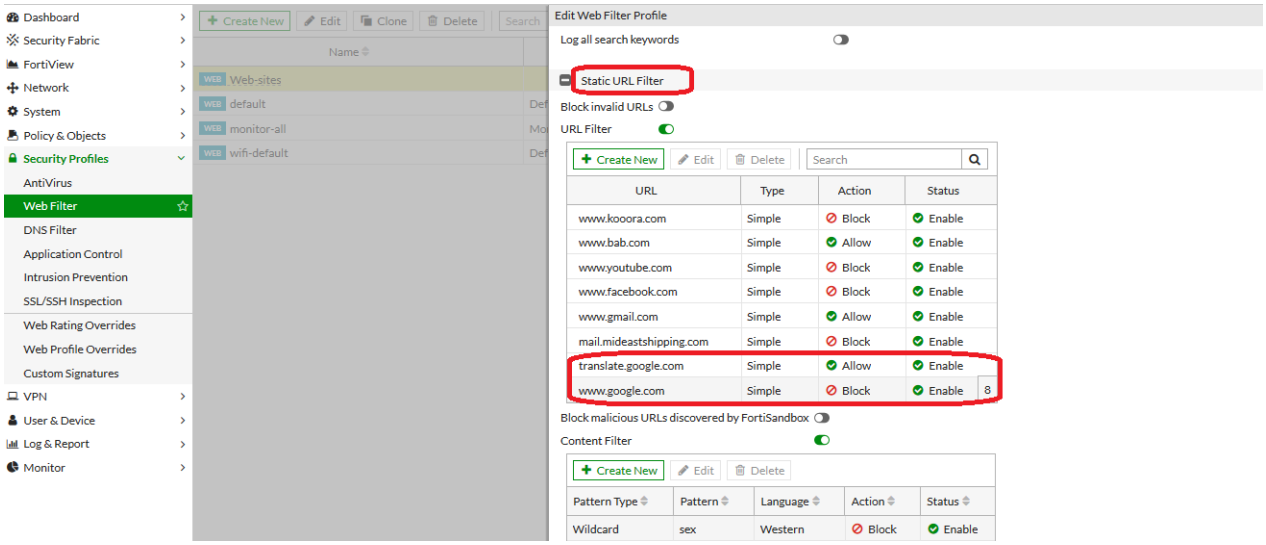
لو قمت بإغلاق للموقع www.yahoo.com

فأن أي موقع يندرج تحت هذا الموقع سيتم اغلاقه أيضا كما بالصورة ادناه



الطريقة الثانية :

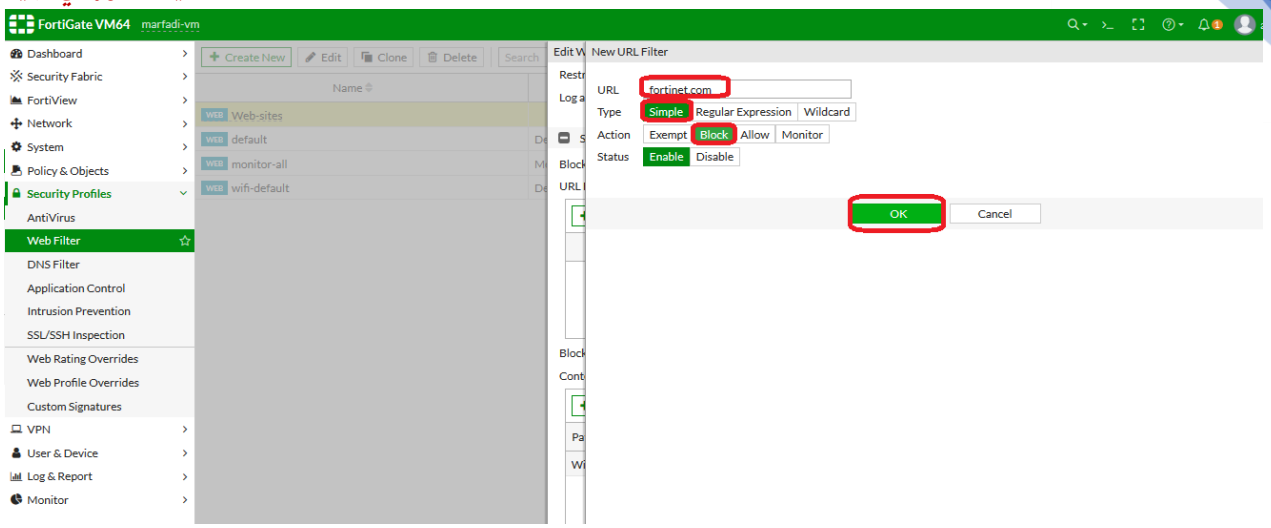
اما في حالة تريد بالتحكم بموقع معين(صفحة معينه)في الموقع عن طريق المسار او ما يسمى الـURL مثلا السماح فقط بصفحة معينه مثلا translate.google.com وهو مترجم جوجل ومنع جوجل بشكل كامل ..

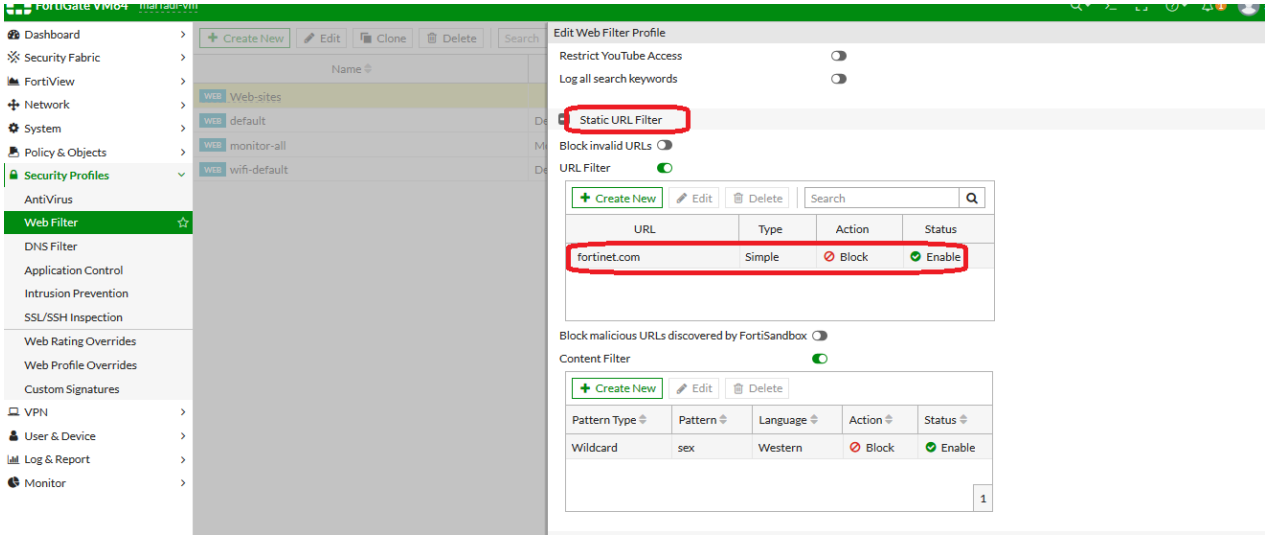


حيث قمنا بالسماح لمترجم جوجل فقط واغلاق كل شي في جوجل ...

الطريقة الثالثه :

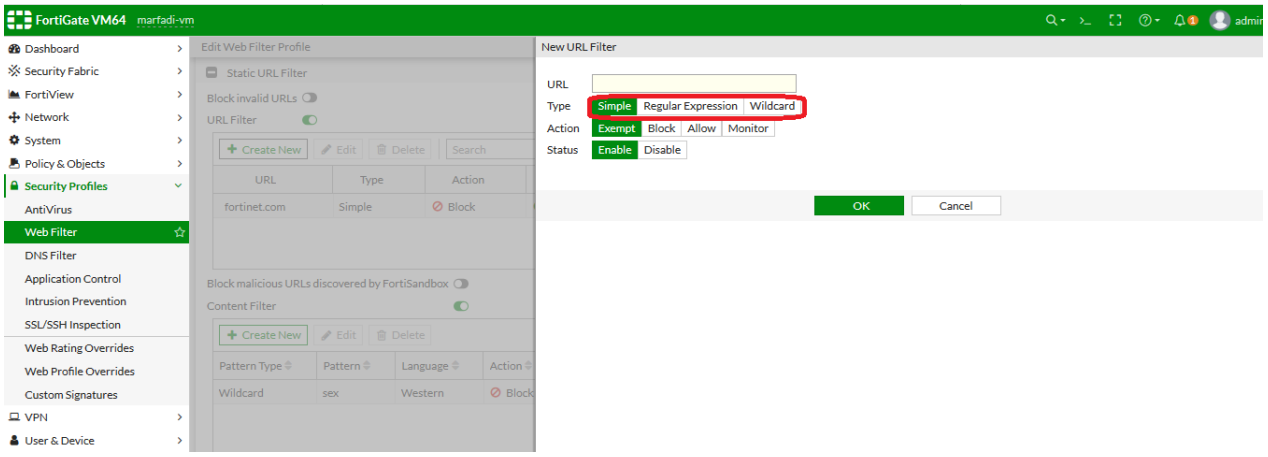
اما في حالة تريد ان تقوم بالتحكم باي موقع ينتهي مثل www.fortinet.com بغض النظرعن أي صفحة تحت هذا الموقع (Sub domain) لهذا الموقع مثل support.fortinet.com حيث انه يندرج تحت الموقع www.fortinet.com .





حيث أي sub domain يندرج تحت الموقع Fortinet.com مثل support.fortinet.com او غيرها سيتم اغلاقه بغض النظرعن اسم الموقع ...

توجد 3 أنماط استطيع ان اتحكم باي موقع في الويب فلتر:



وهي Simple -Regular Expression-Wildcard

في النوع Simple

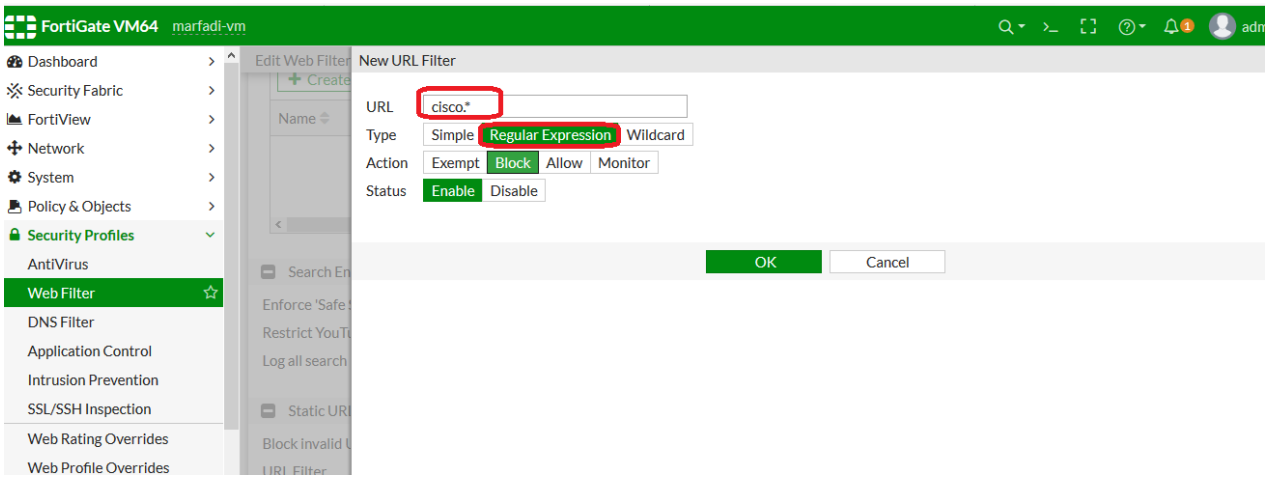
اما نكتب بالصيغه www.bab.com او bab.com مباشره

اما الأنواع Regular Expression و Wildcard فأنه تستخدم عندما تريد استخدام رموز

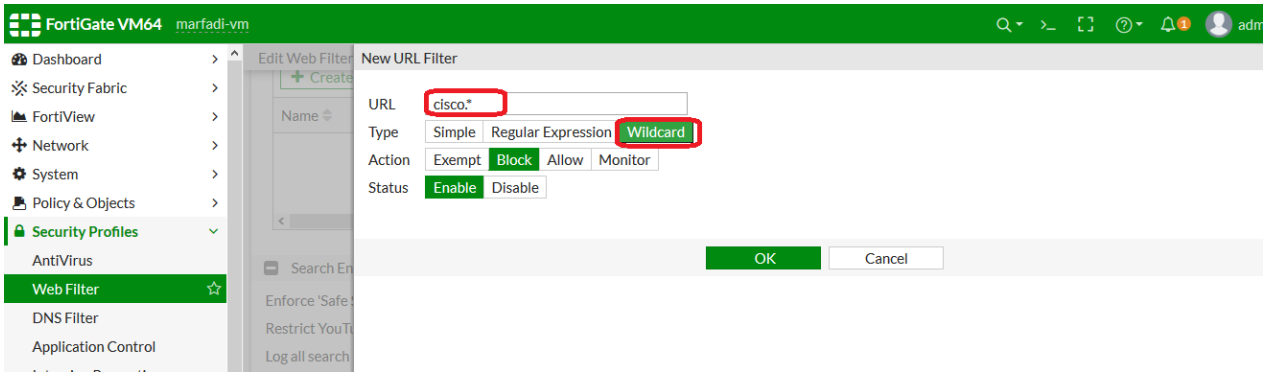
مثلا لو اردت التحكم بالدومين المسمى cisco بغض النظر هل هو cisco.com او cisco.net حيث كليهما بيفتح لك نفس الموقع ..

فبواسطة Regular Expression او Wildcard يمكنك التحكم بالدومين المسمى cisco بغض النظر هل هو com. او net. او org.

كما بالصورة ادناه



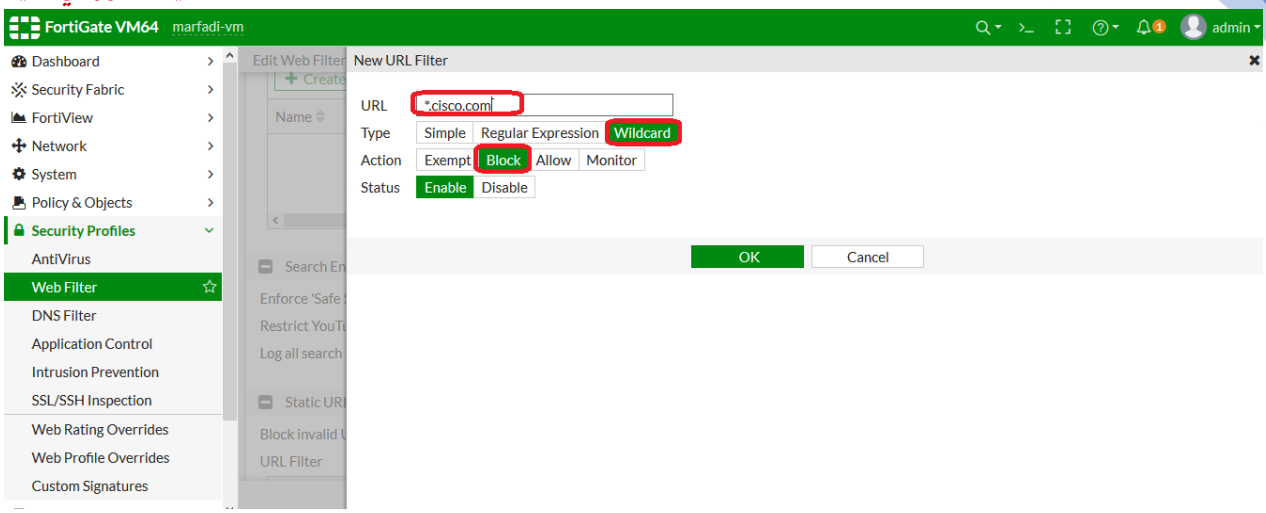
او



يمكن استخدام الرموز بالطريقة التالية

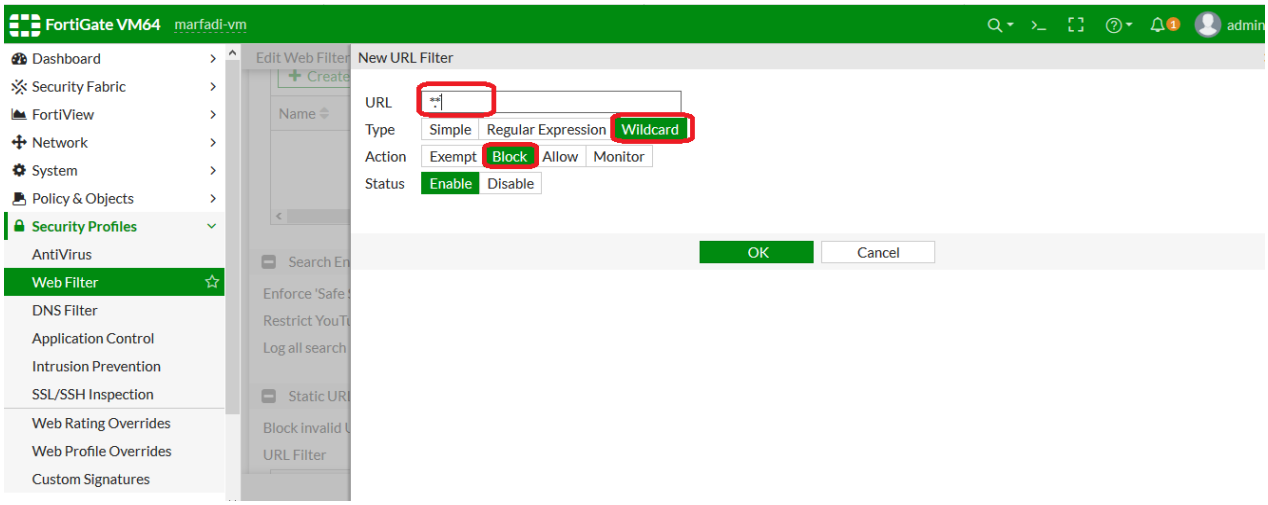
cisco.com.* أي ان أي sub domain سوف يتم التحكم به ..

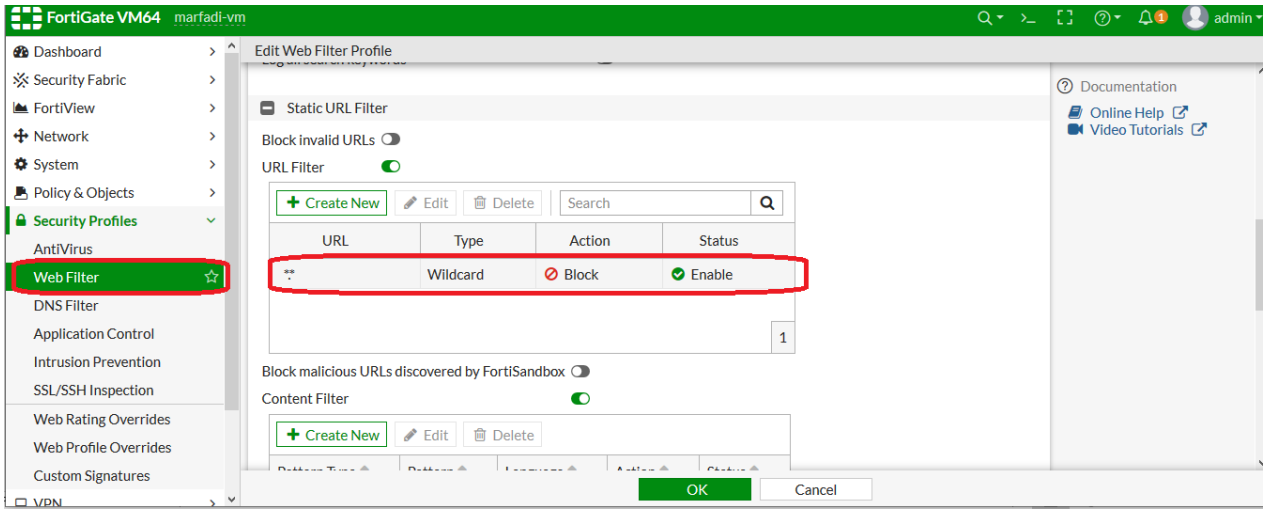
كما بالصورة التالية



فلو اردت ان تقوم بإغلاق كل المواقع

. أي قم بالتحكم باي موقع تحت أي شي ..

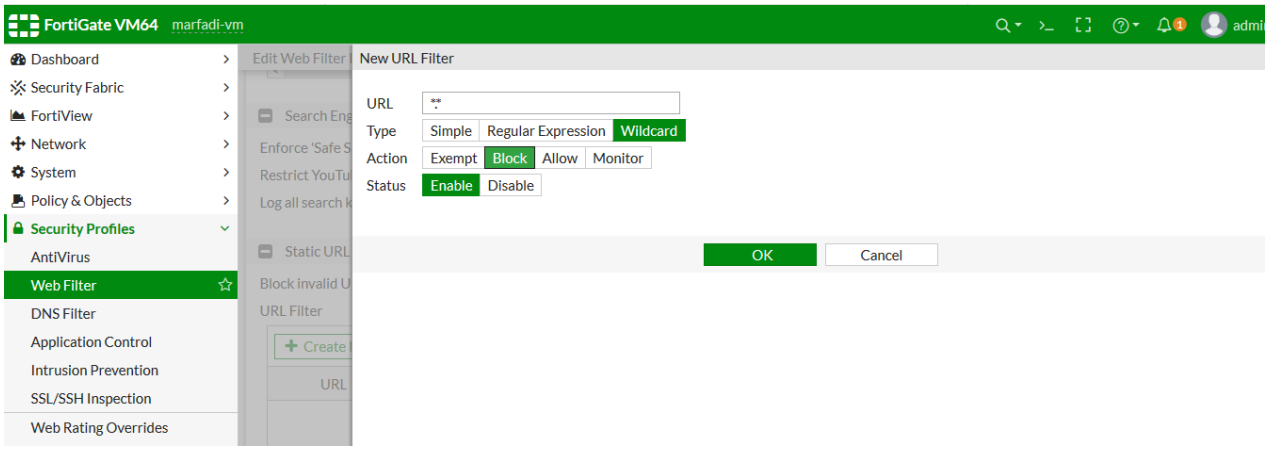


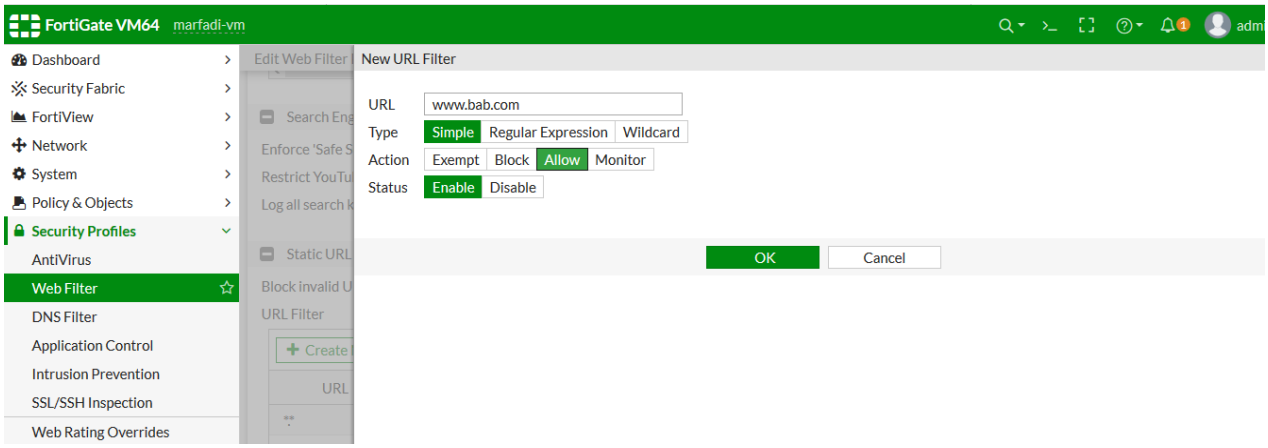


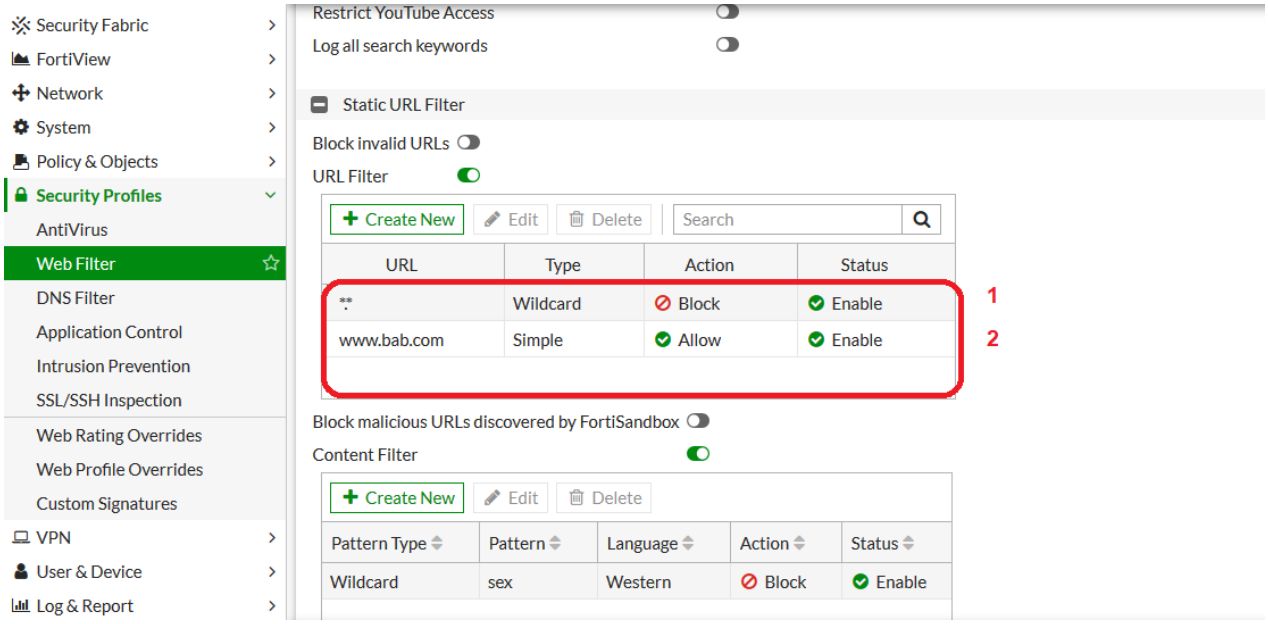
ترتيب الـ URL لها اهميه ..

حيث يتم تطبيق الـURL من الأعلى الى اسفل (يبدا بتطبيق المواقع من الأعلى وهكذا)..

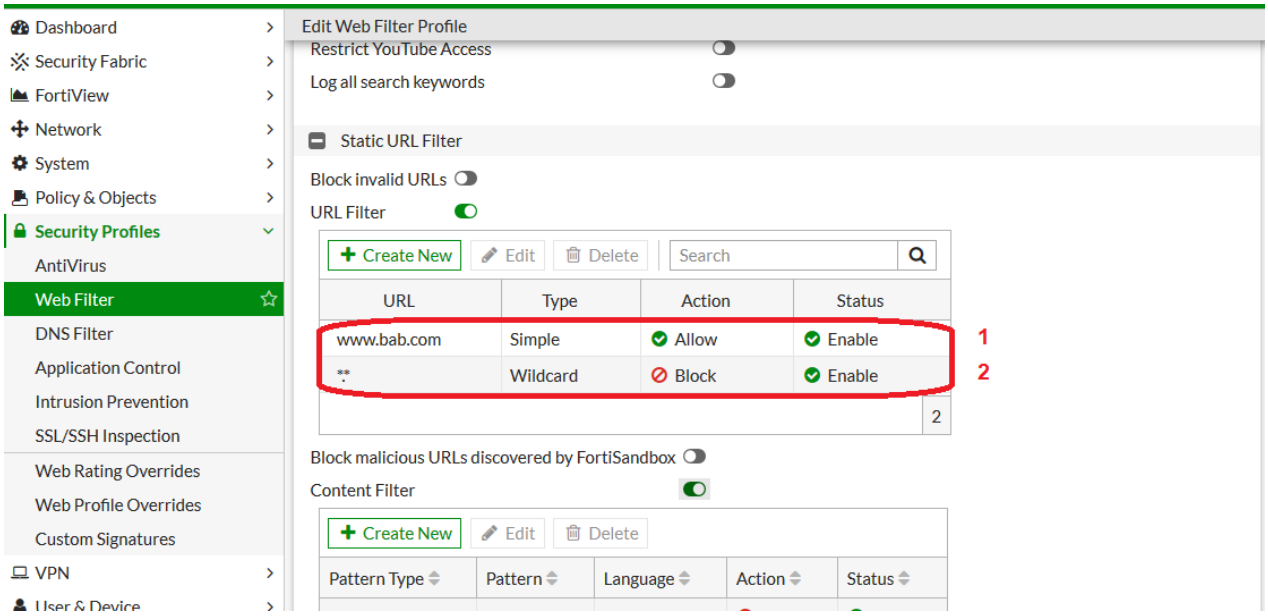
مثلا لو اردت اغلاق كل المواقع ماعدا صفحة www.bab.com







فبحسب الترتيب أعلاه فأنه سوف يتم اغلاق كل المواقع بما فيها الموقع www.bab.com اما لو قمنا بإعادةترتيب الـ URL Filter كما بالصورة التالية



فأن الموقع www.bab.com سوف يكون متاح وسيتم اغلاق باقي المواقع كامله ..

لذا ترتيب الـ URL مهم جدا جدا وهو نفس فكره الـ Policy حيث يتم تطبيقها من اعلى الى اسفل ..

Web content filter

عباره عن عمليه التحكم بمحتوى الموقع (صفحات الانترنت)بناء على الكلمات او الجمل او الرموز التي تكون داخل الصفحة .

مثلا لو كانت الصفحة تحتوي على كلمه sex اعمل لها Block حيث ان جهاز الفورتي جيت بيعمل scan للصفحة بحيث لو وجد الكلمه التي يبحث عنها فأنه يقوم بتطبيق action معين .

بشرط ان عمليه الفحص تصل الى score معين حيث يعرف الـ score بانها قيمه اورقم معين لكل كلمه او جمله اورمز داخل الفورتي جيت فلتر..

بحيث لو وصل مجموع الـ score الى الـ threeshold فان الفورتي جيت سيقوم بتطبيق الـ action المعين س واء allow او block اما اذا لم يصل الـscore لهذا الموقع الى قيمه الـ threehold فأن الـ action لا يطبق ابدا على هذه الصفحة ...

ملاحظة :

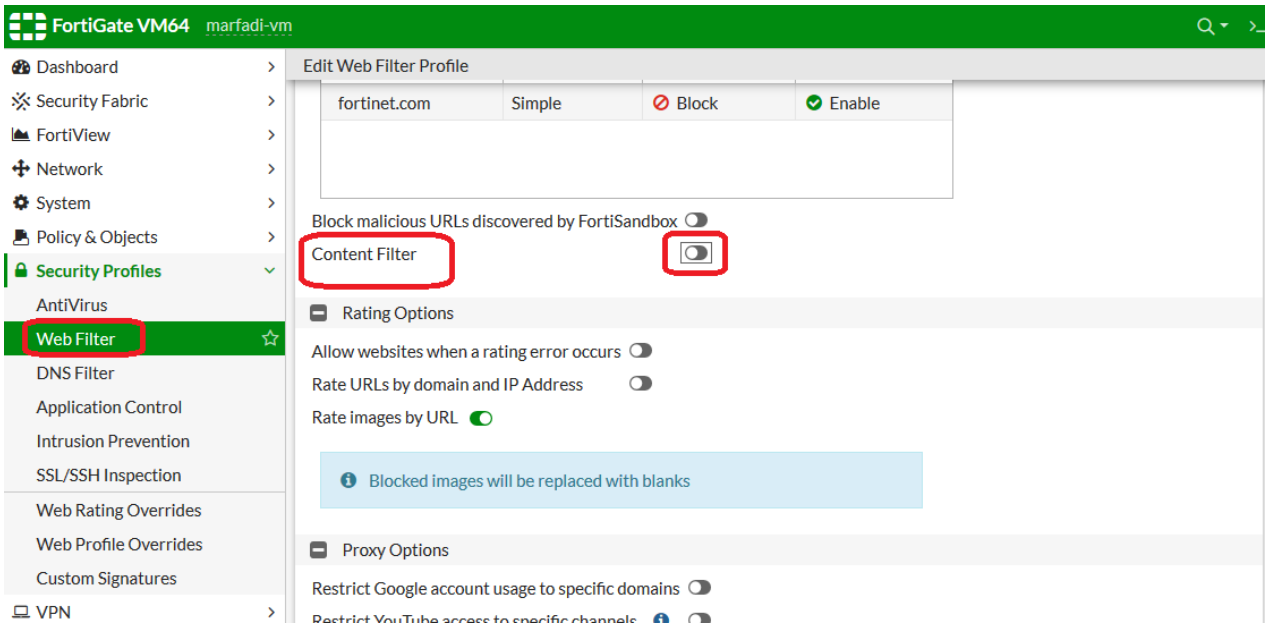
حيث الـ threeshold هو الحد وهي نتيجه جمع الـ score للكلمات او الجمل او الرموز المفلتره على الفورتي جيت الى ان تصل للحد ..

حيث الـ threeshold يساوي 10

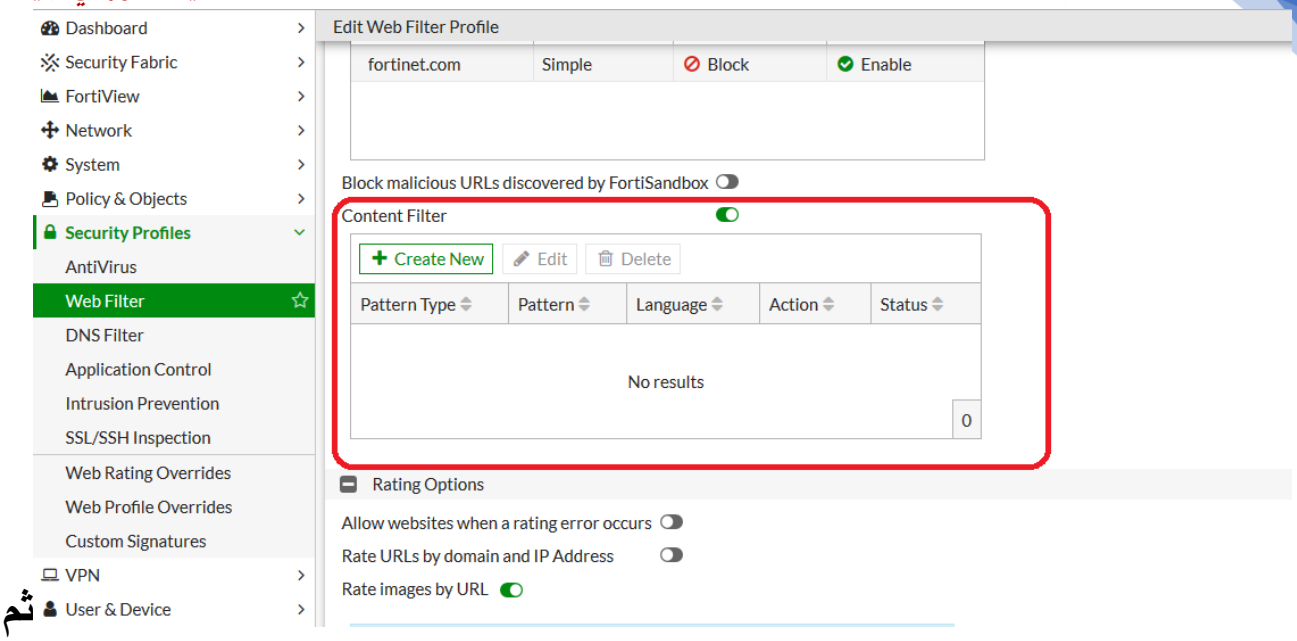
و الـ score لأي جمله اوكلمه اورمزهو الرقم 10 .

حيث أي كلمه انا عامل لها فلترعلى الفورتي جيت مثلا(sex)فلو وجدها فأن الـ score سيكون 10 ولذا يتم الوصول الى قيمه الـthreehold وبهذا سيتم تطبيق الـ action على هذا الموقع .

ملاحظة :الـ score موجود فقط على CLI وليس بواسطة الـGUI حيث يمكنك تعديل قيمه الـ score حيث القيمة الافتراضية هي 10 ويمكنك تغييرها ..

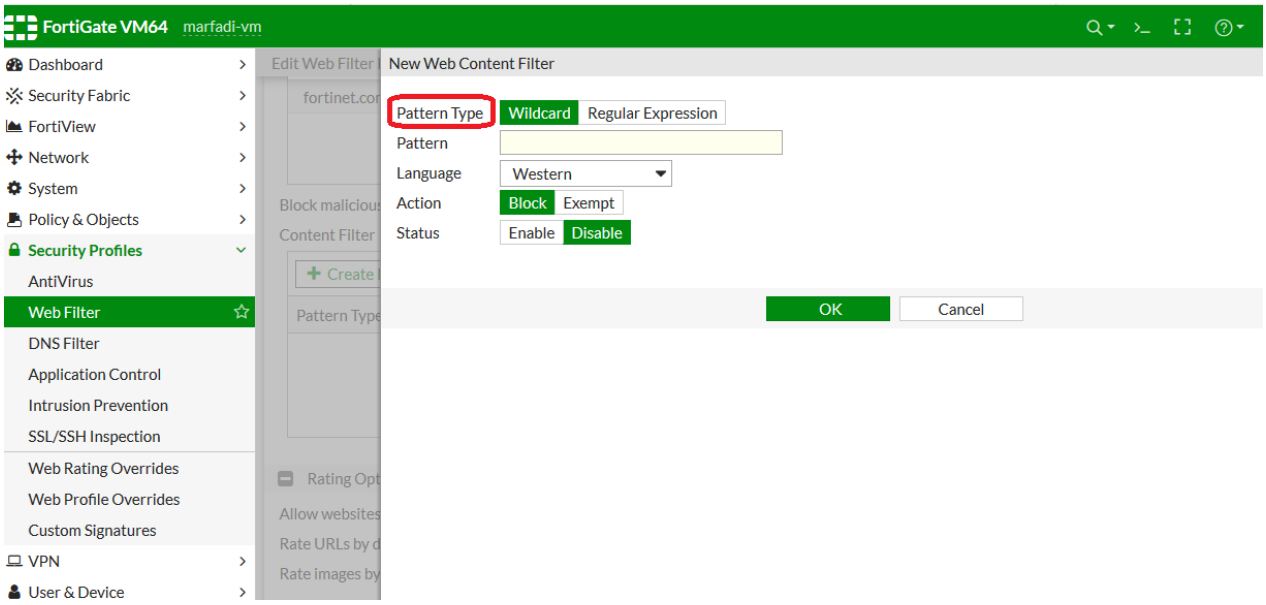


نقوم بتفعيل الخيار Content Filter



ثم

create New



حيث pattern Type نحدد النمط الذي سوف اكتب فيها الكلمه التي سنقوم بعمل لها فلتره هل Wildcard ام Regular Expression

Wildcard : للتحكم بكلمه او جمله اورمزولديك الى حد 80 حرف فقط .

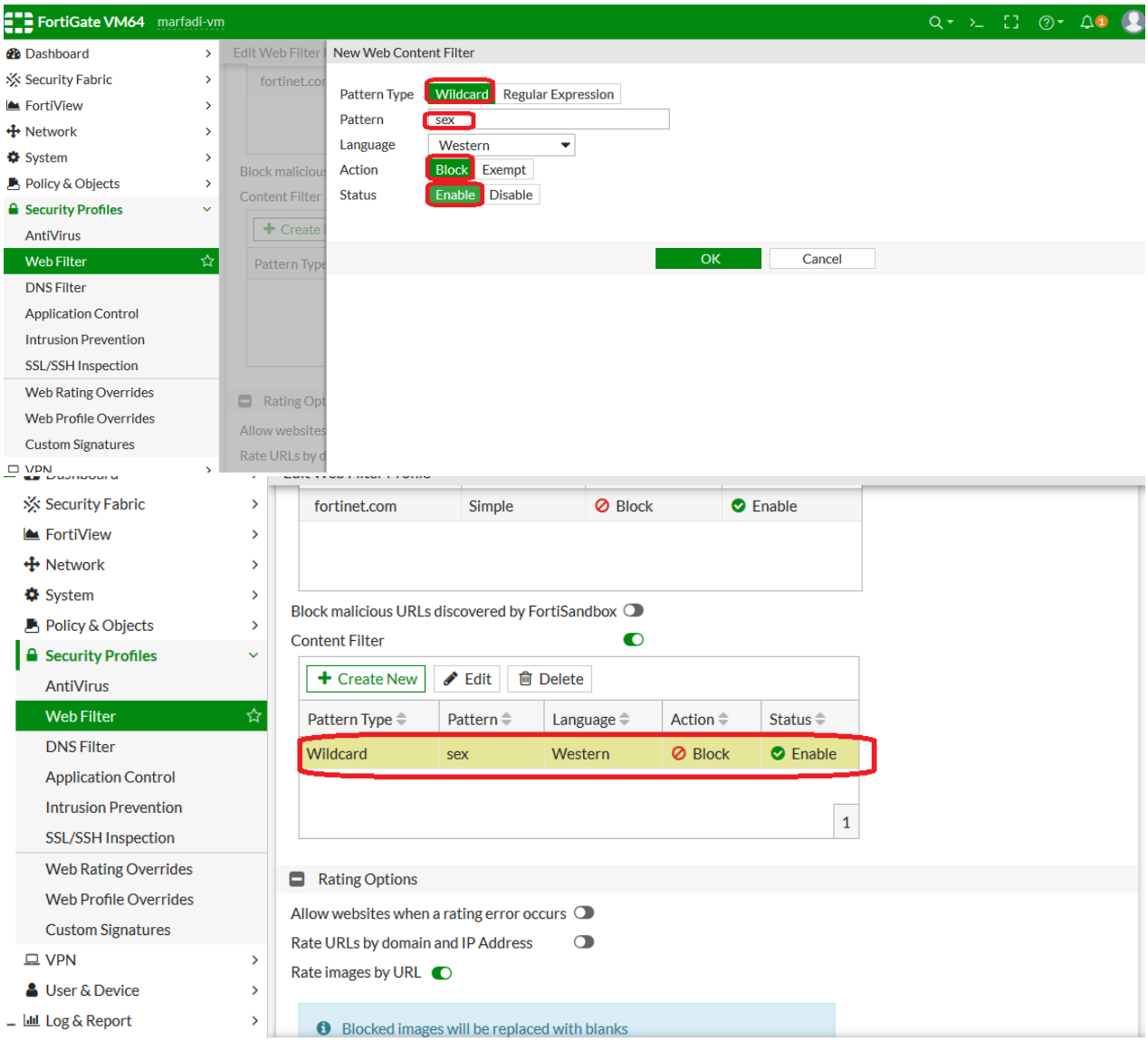
Regular Expression : حيث هنا يتم استخدام تعبيرات معينه في بعض لغات البرمجه ونحن في اغلب الأوقات نستخدم النمط الأول (Wildcard)

حيث الـ Pattern : هي الكلمه او الجمله او الرمز الذي سوف نعمل لها فلتره .

Language : اللغه التي كاتب فيها الكلمه او الجمله ولا توجد اللغه العربيه

Action : الحدث الذي سنقوم به عندما تصل الـ score الى قيمه الـ threeshold .

Status : هل تريد تطبيقها ام لا



أي صفحة تحتوي على كلمه sex سيتم عمل Block لها ..

طريقة تعديل قيمه الـ score بوسطه الـ 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 الكلمه sex والتي تم انشائها مسبقا في web filter content .

حيث قمنا بإظهار الاعدادات السابقة عبر الامر show full-configuration للكلمه sex حيث نلاحظ بأن الـscore=10

ثم نقوم بتعديل القيمة الى 9 ..

Application controller

عباره عن التحكم بالتطبيقات (السوفتوير)(البرامج)على الشبكة .
حيث الفورتي 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 ماسنانجر وواتساب

او تطبيقات browser based او التطبيقات التي تعتمد على المتصفح مثل فيسبوك او تويتر
حيث الفورتي 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 الـ web filter فبهذا انا قفلت الموقع فما الحاجه الى اغلاق الفيسبوك أيضا من الـ application control !!!

الاجابة بأني ممكن اسمح للفيسبوك عبر ال web filer ولكني 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 الـ application controller ..

حيث في application controller اقدر اتحكم في سلوكيات او خصائص التطبيق .

حيث الـ application controller بيستطيع 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).

الفورتي جيت بيعتمد على الapplication control database والتي تكون على شكل قائمه موجودة على الفورتي جيت حيث يتم تحديث تلك القائمة بشكل مستمر عبر FortiGuard App control License .

Forigate's signature هو الشي الذي بيعتمد عليه الـ app control في التحكم بالتطبيقات حيث يحتوي الـsignature على port التطبيق و services و ip's و URl لكل تطبيق .

Application control action:

يوجد لدى الفورتي جيت 4 أنواع من الـaction :

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 فأن فورتي جيت سيقوم بعمل ban لايبي اليوزر الذي حاول الوصول لهذا التطبيق .

ماهو الـــTraffic shape :

Traffic shape: تخصيص ترافيك معين لطبيق معين حيث ال traffic shaper يحتوي على 5 اشكال :

Gurantee(80k) : اضمن بأن الترافيك سوف يأخذ 80 كيلو لتطبيق معين على الأقل .

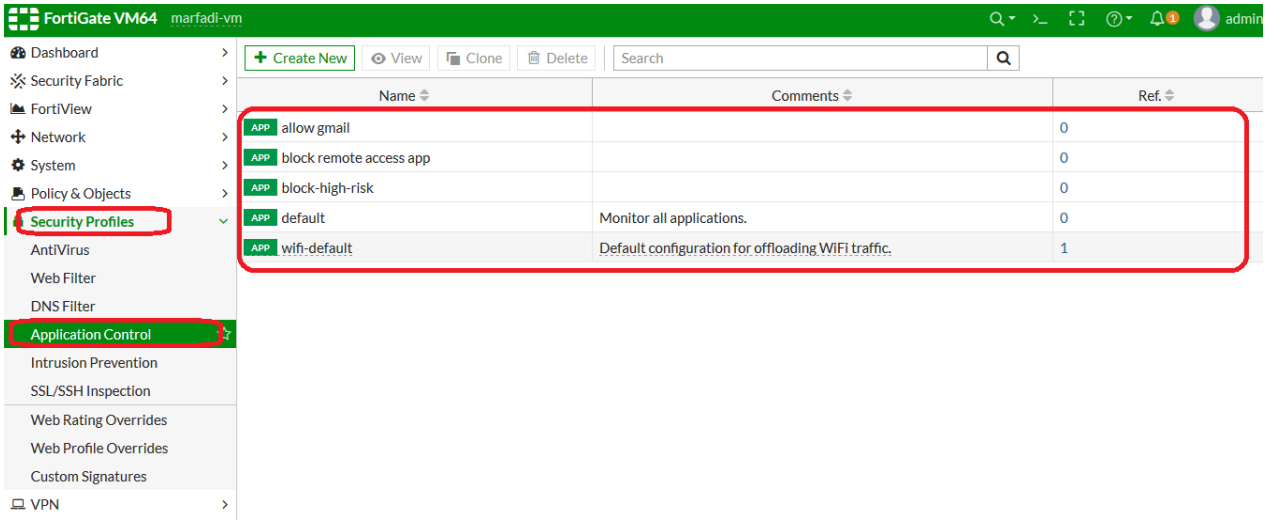
High priority :اضمن بأن لدي اعلى اولويه لترافيك بالمرور..

Low priority : اخذ اقل اولويه للترافيك

Medium priority :اخذ اولويه متوسطه

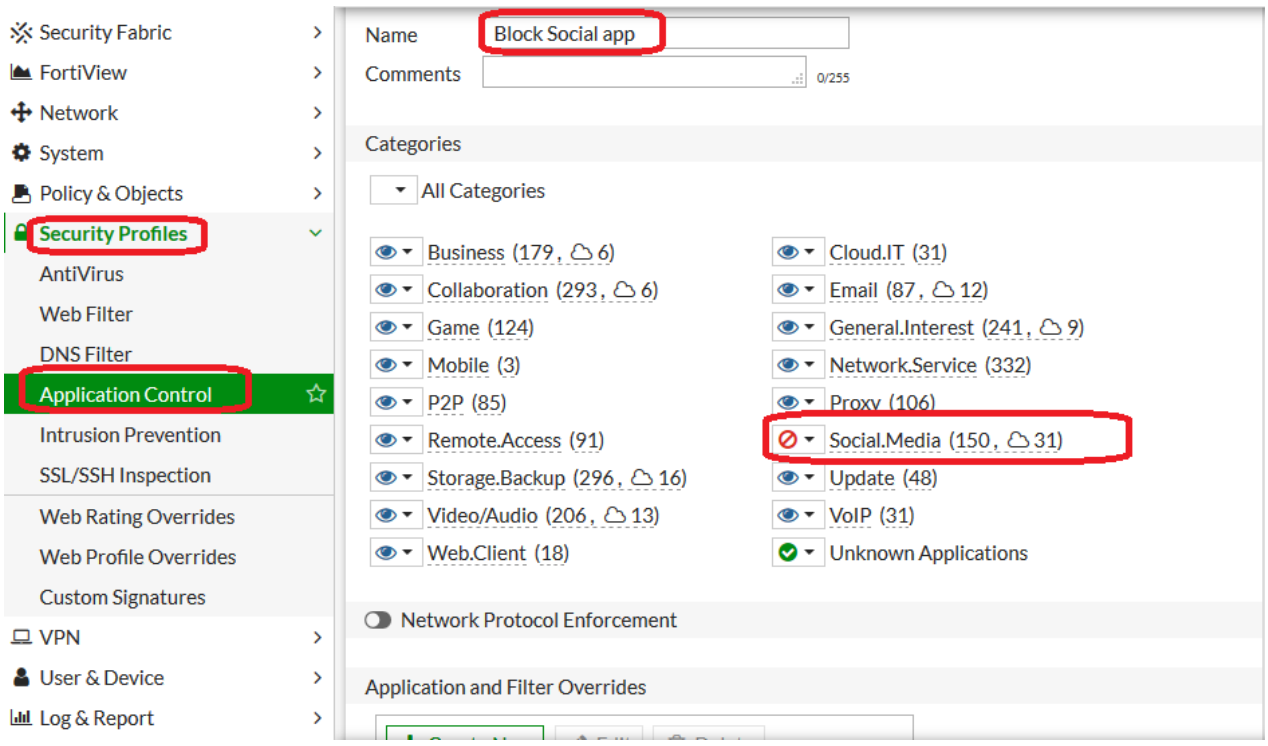
Shared : تخصيص مثلا 1 ميجا لترافيك معين حيث الناس تتشارك فيه .

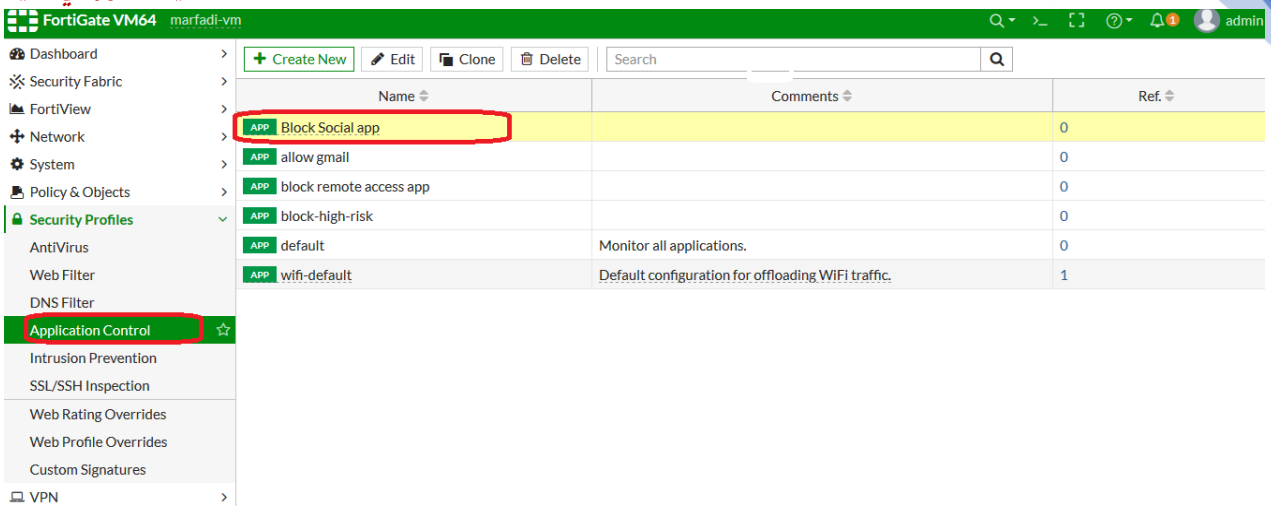
مثلا تخصيص 1 ميجا مثلا لتطبيق الفيسبوك حيث ان جميع الأشخاص في الشركة الذين سيتخدمو الفيسبوك سوف يتشاركوا ب1 ميجا .



حيث نقوم بإنشاء بروفايل معين للـapp control ولسكن اسمه Block Social app

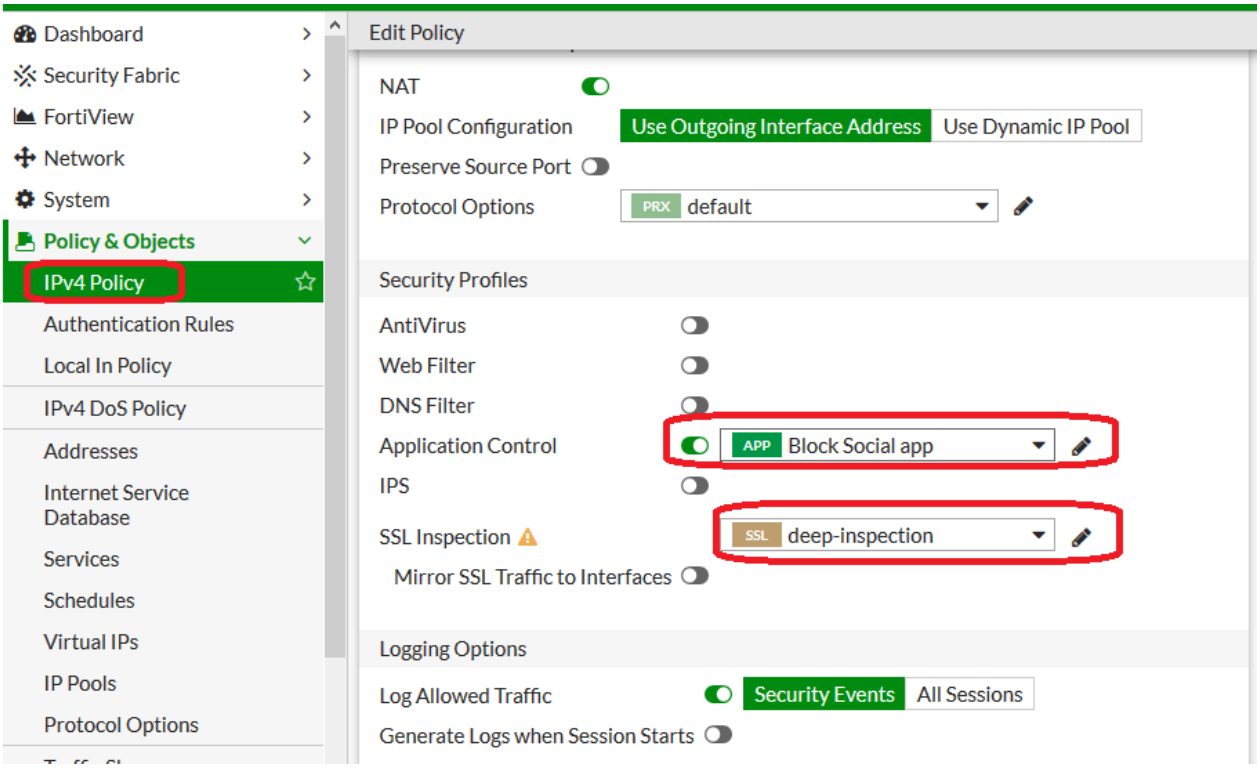
حيث سنقوم باغلاق كل التطبيقات التي تستخدم مواقع التواصل الاجتماعي مثل فيسبوك او تويتر او الخ..



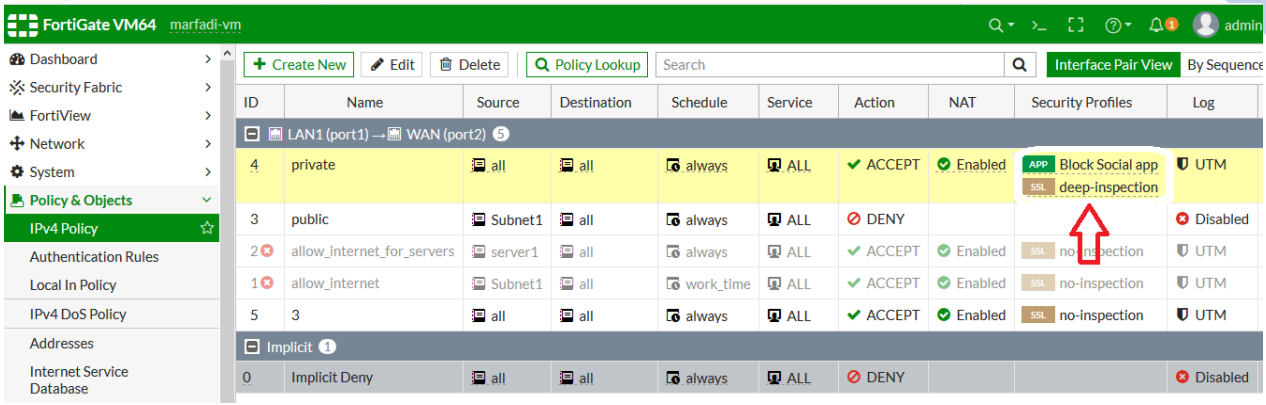


تم الانشاء ...

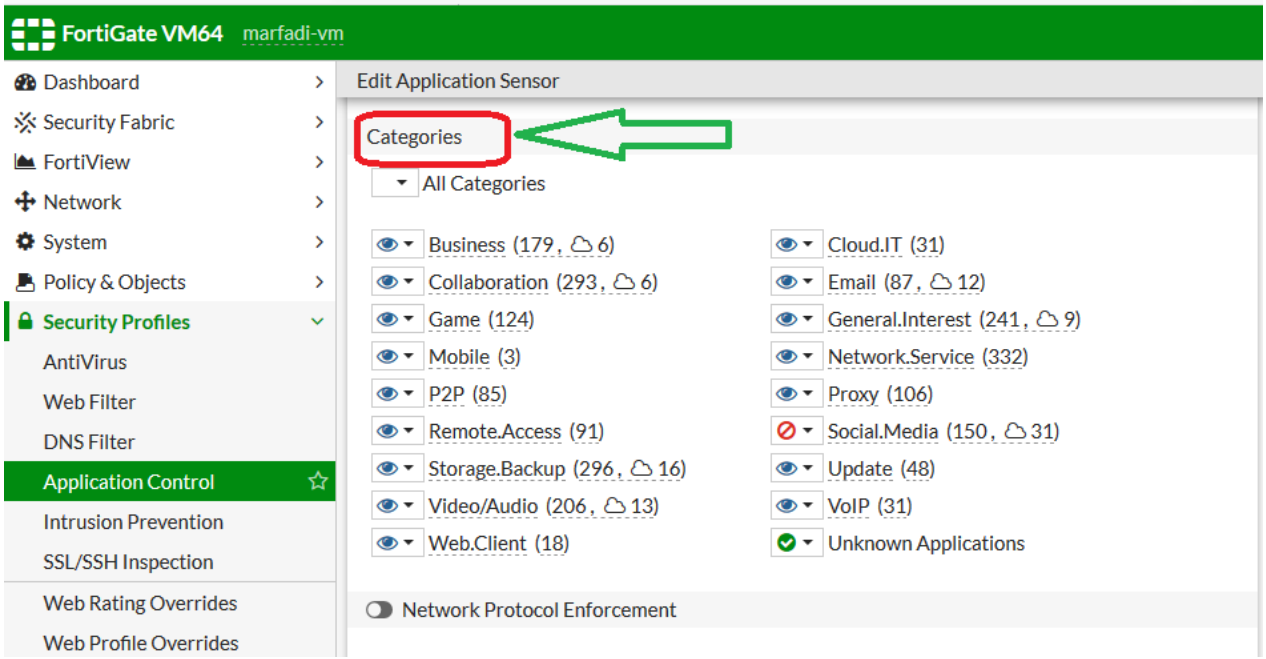
ثم عند تطبيق البوليسي نقوم بتفعيل app control واختيار البروفايل الذي أنشأناه مسبقا ..



مع التأكيد من تفعيل الخاصية SSL Inspection=deep-inspection لكي يتمكن من التحكم باي تطبيق او موقع يستخدم ssl protocol (https)..



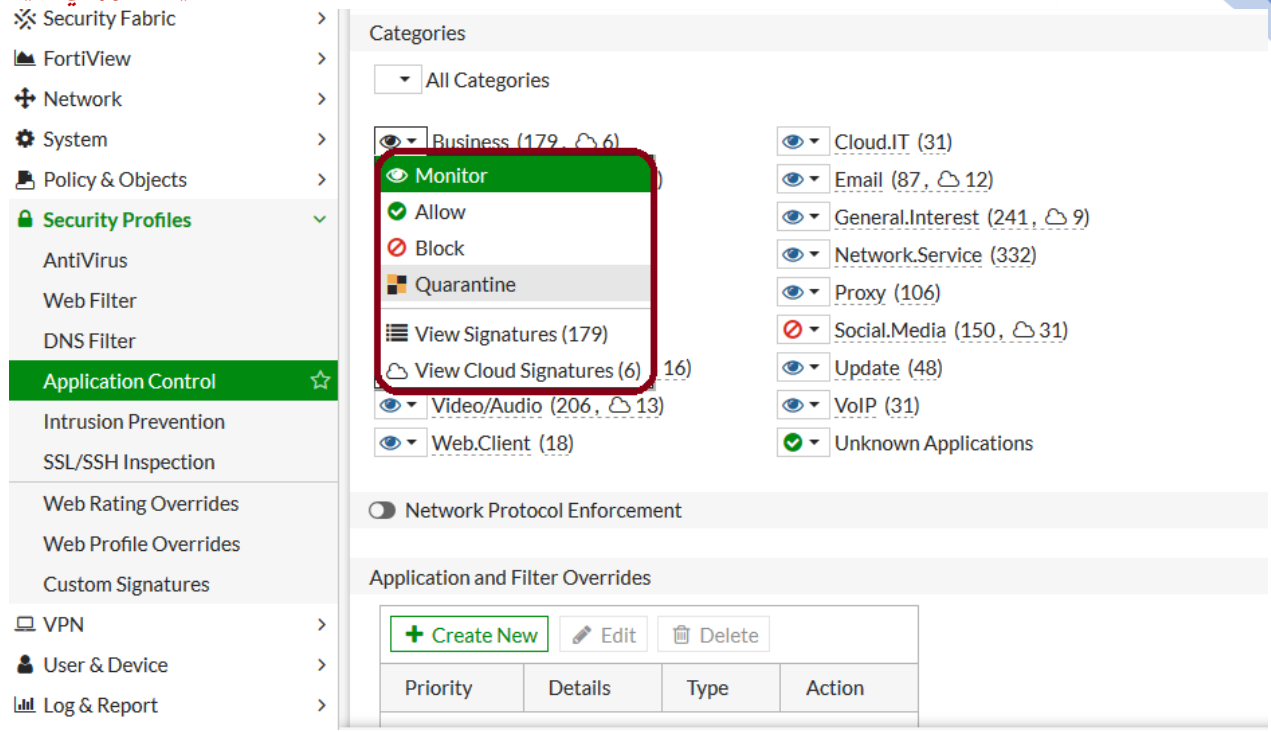
كما نلاحظ بالصورة ادناه بأن ال app control بيقسم الى categories



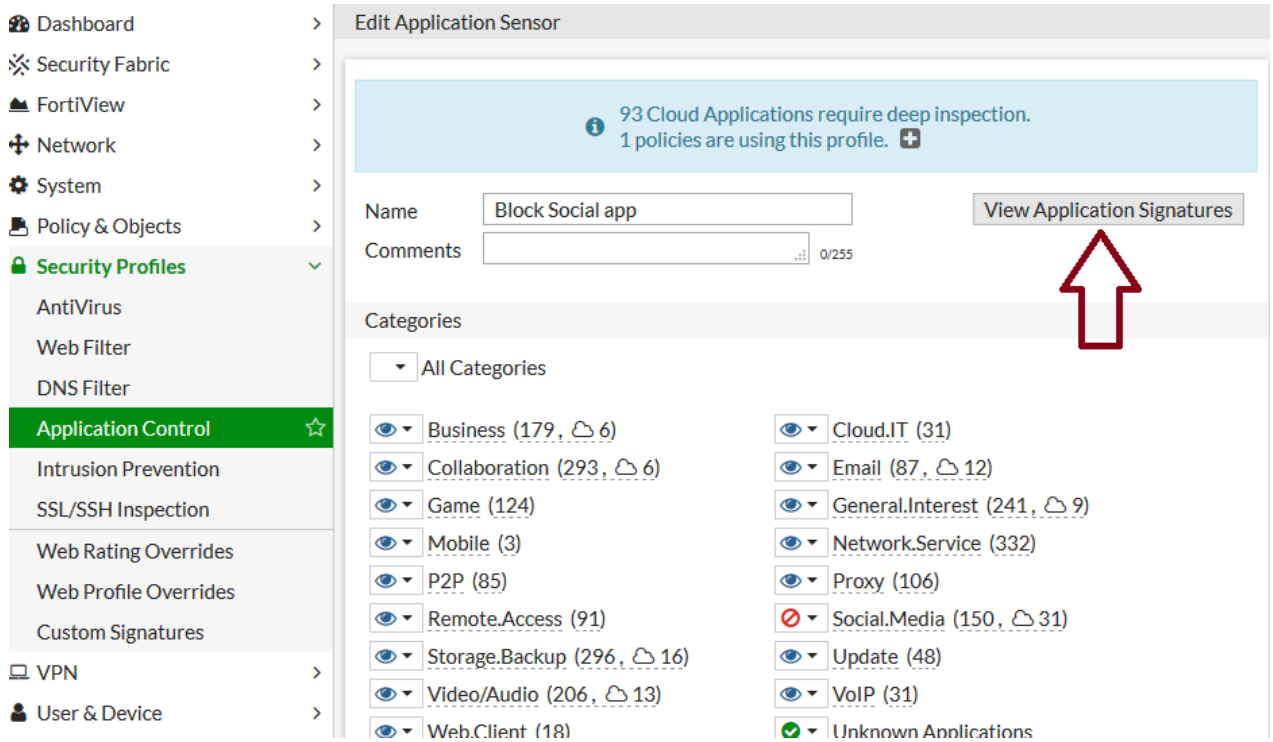
بتحتوي على تصنيفات حيث تم تقسيم كل مجموعة من التطبيقات المتشابهه في الخصائص بتصنيف معين .

ملاحظة : تم السماح لكل التطبيقات الغير معروفه(Unknown Applications)(الفورتي جيت ليس لديه signature لهذا التطبيقات) ..

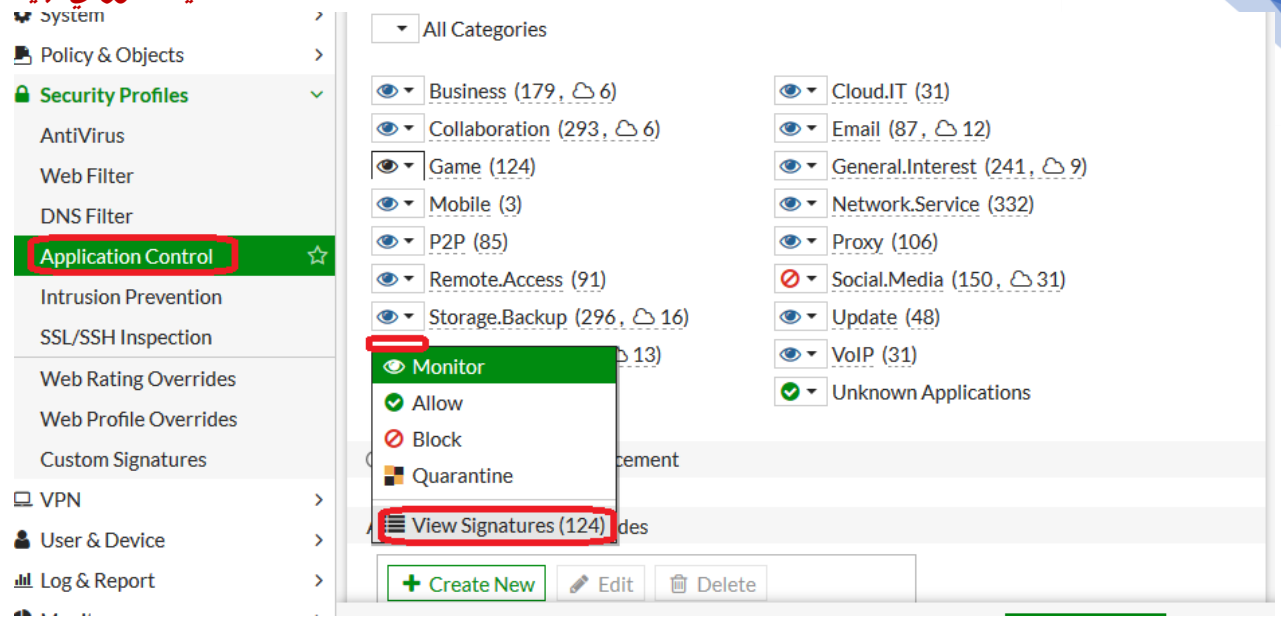
حيث بمجرد النقرعلى أي category يمكنك تطبيق أي action تريده كما بالصورة ادناه ..



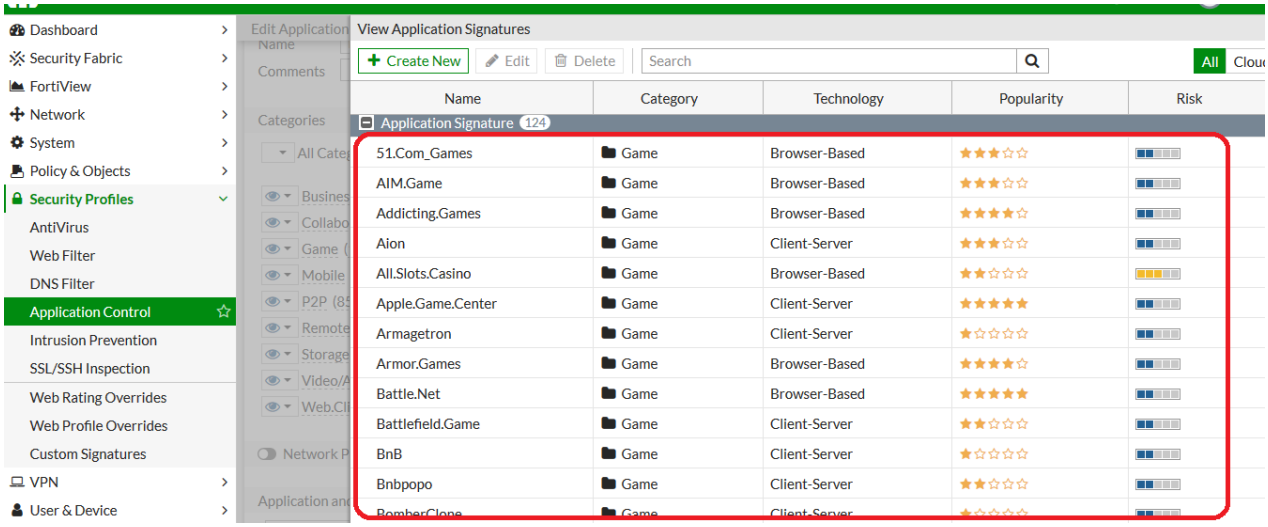
يمكن ان أقوم بتصفح كل الـsignatures(التطبيقات)التي بيتحكم بها الفورتي جيت وذلك كالتالي :



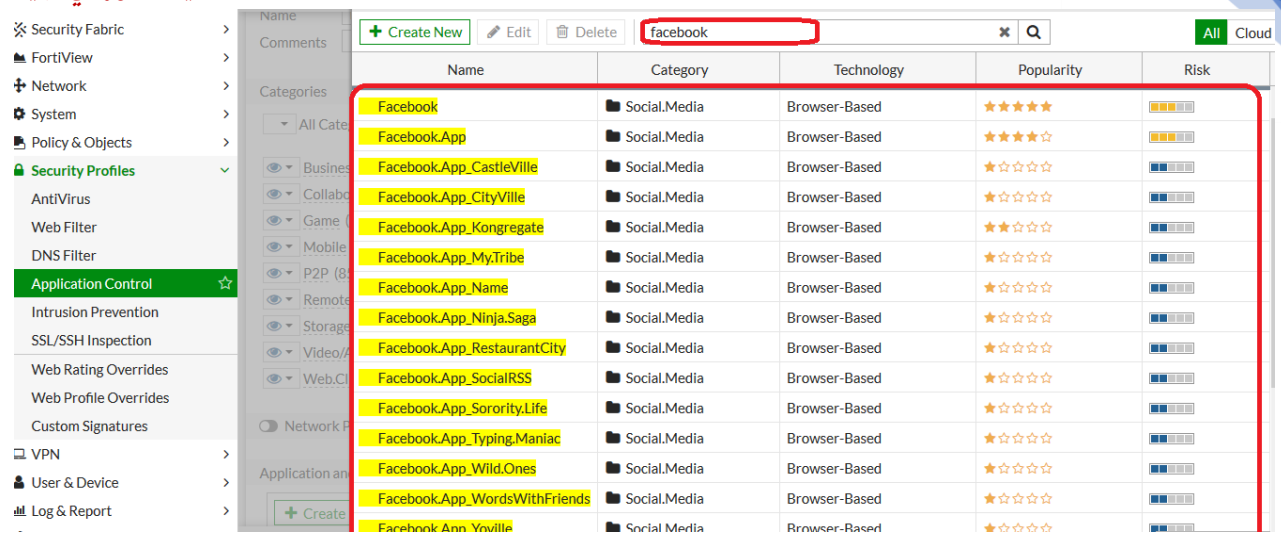
كما يمكنني ان اظهر الـ signatures لتصنيف معين كما بالصورة التالية :



حيث ستظهرلك كل التطبيقات التي تندرج تحت هذا التصنيف كما بالصورة ادناه



حيث يمكن البحث عن أي تطبيق تريده للتأكد من وجوده في هذ التصنيف ...



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 (soical 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 بـserver مثل برنامج كاسبرسكاي حيث يأخذ التحديث من السيرفر التابع لموقع كاسبر..

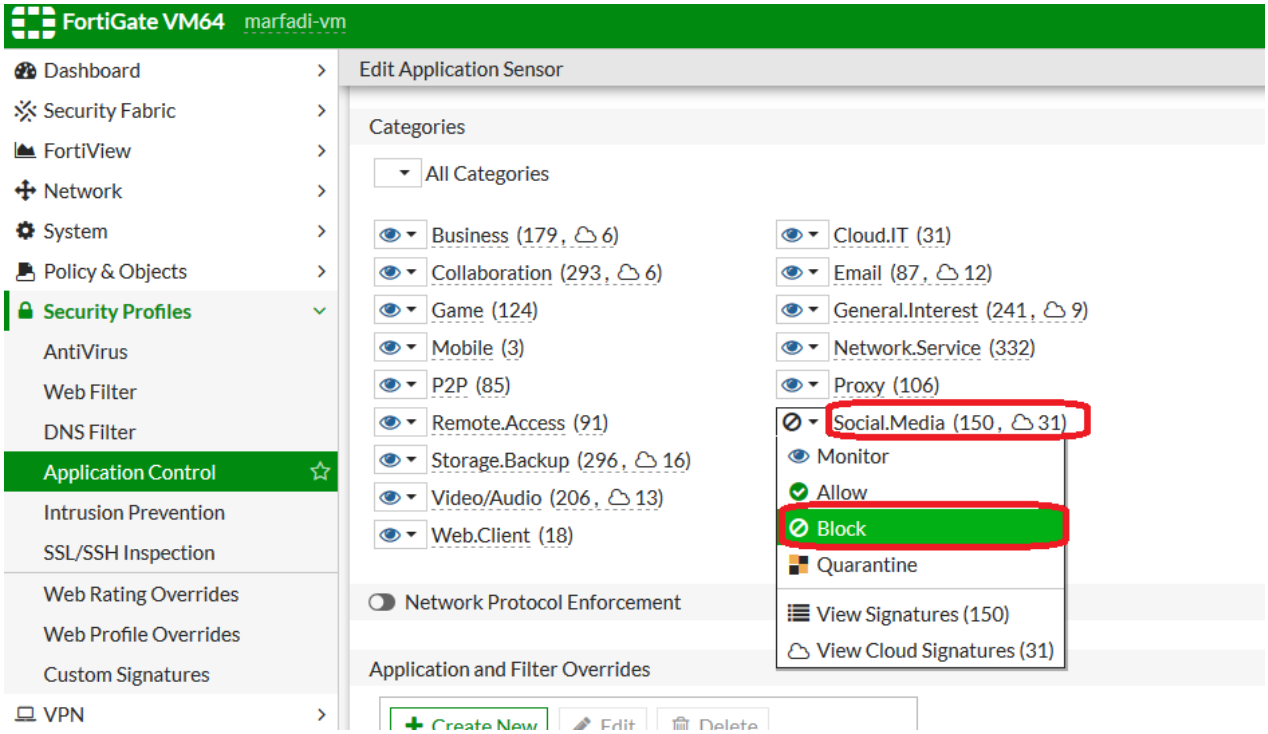
او تطبيق يعمل بتقنيه (peer -to-peer)

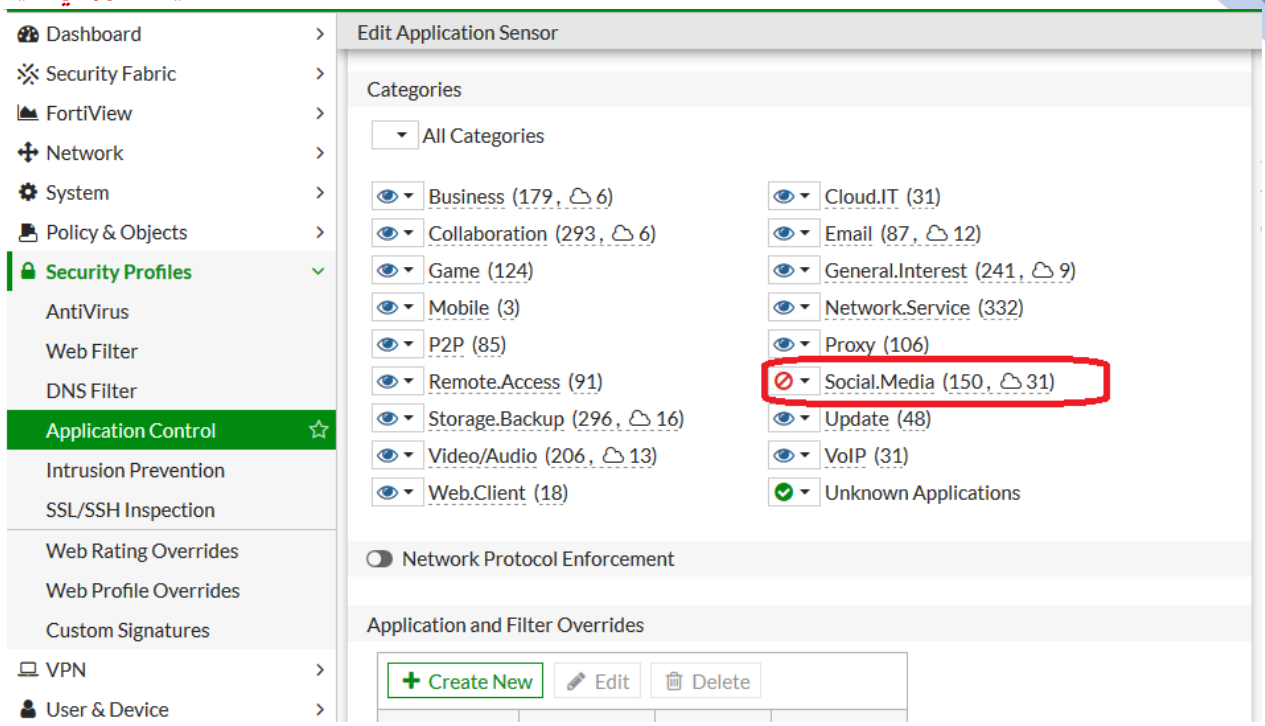
والعمود الرابع باسم popularity بمعني الشعبيه (الشهره)حيث يظهرلك نجوم بعدد شهره التطبيق ..

العمود الخامس باسم Risk ويوضح مدى خطوره التطبيق (خطر critical ،مرتفع elevated ،منخفض low ،متوسط Medium ،ليس خطر None ..)

❖ طريقة التحكم في التطبيقات عبر الـApplication control :

مثلا لو اريد اغلاق كل مواقع التواصل الاجتماعي (فيسبوك،تويتر،انستجرام ....).

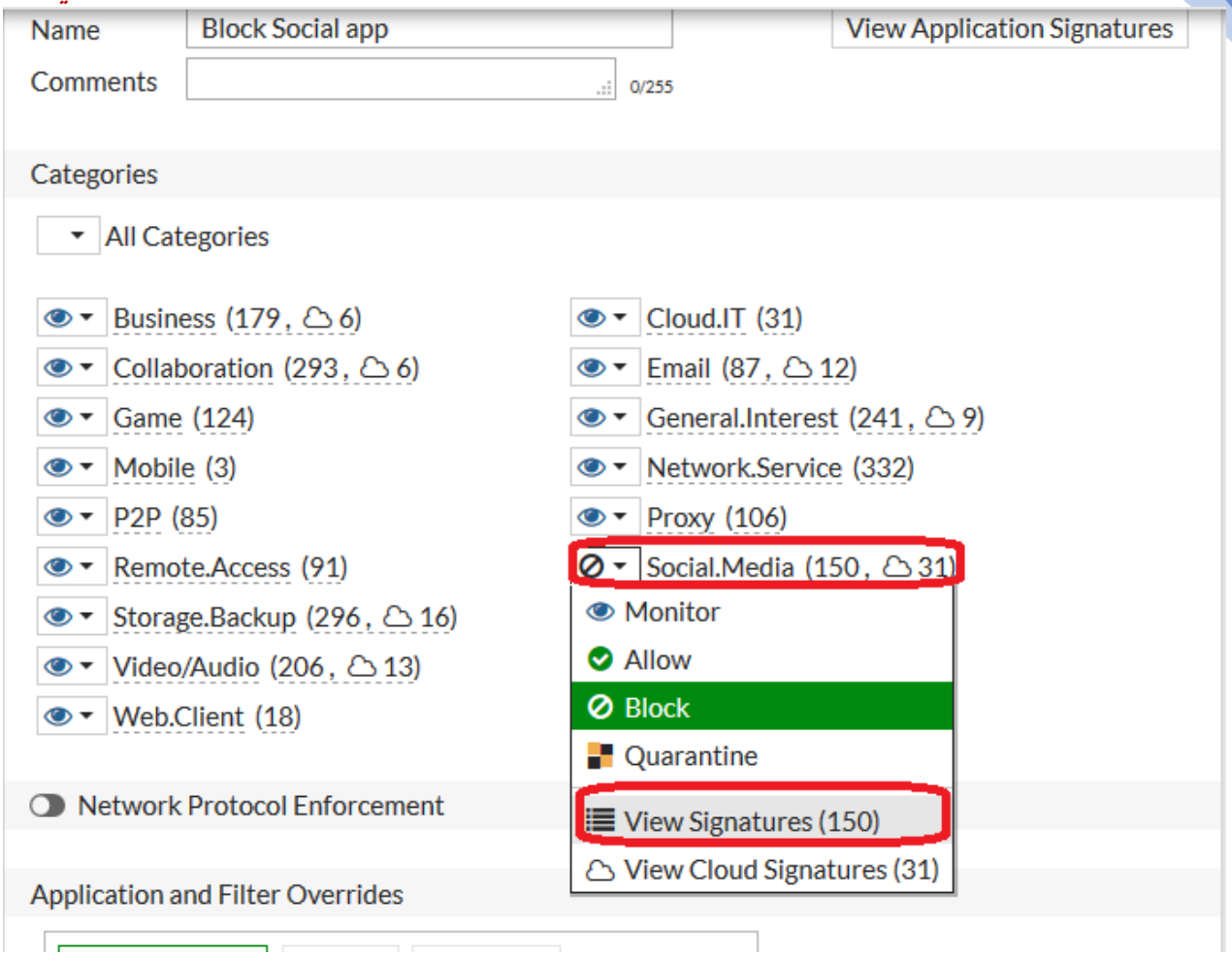


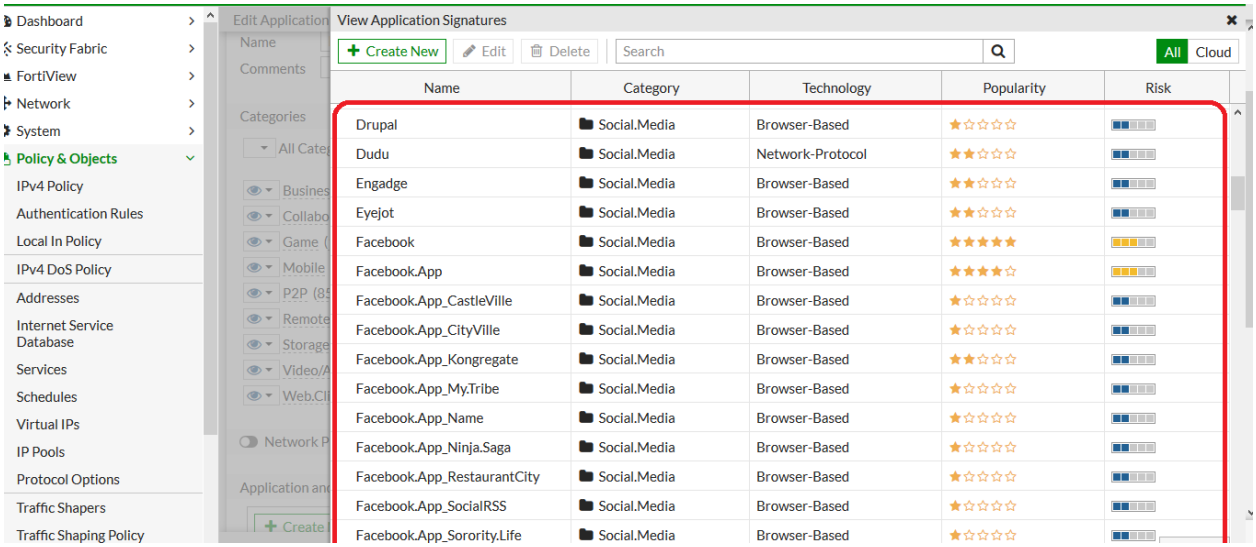


بهذه الطريقة سيتم اغلاق كل مواقع التواصل الاجتماعي ويظهرللمستخدم الرساله التالية :

كما بالصورة أعلاه يظهرلنا اسم التصنيف الذي ينتمي اليه موقع الفيسبوك (Social Media)والurl الذي حاول الوصول اليه اليوزرصاحب الايبي المحدد بالصورة ...

➢ لمعرفة ماهي البرامج(signatures)التي بتكون مندرجه تحت الـــ category :



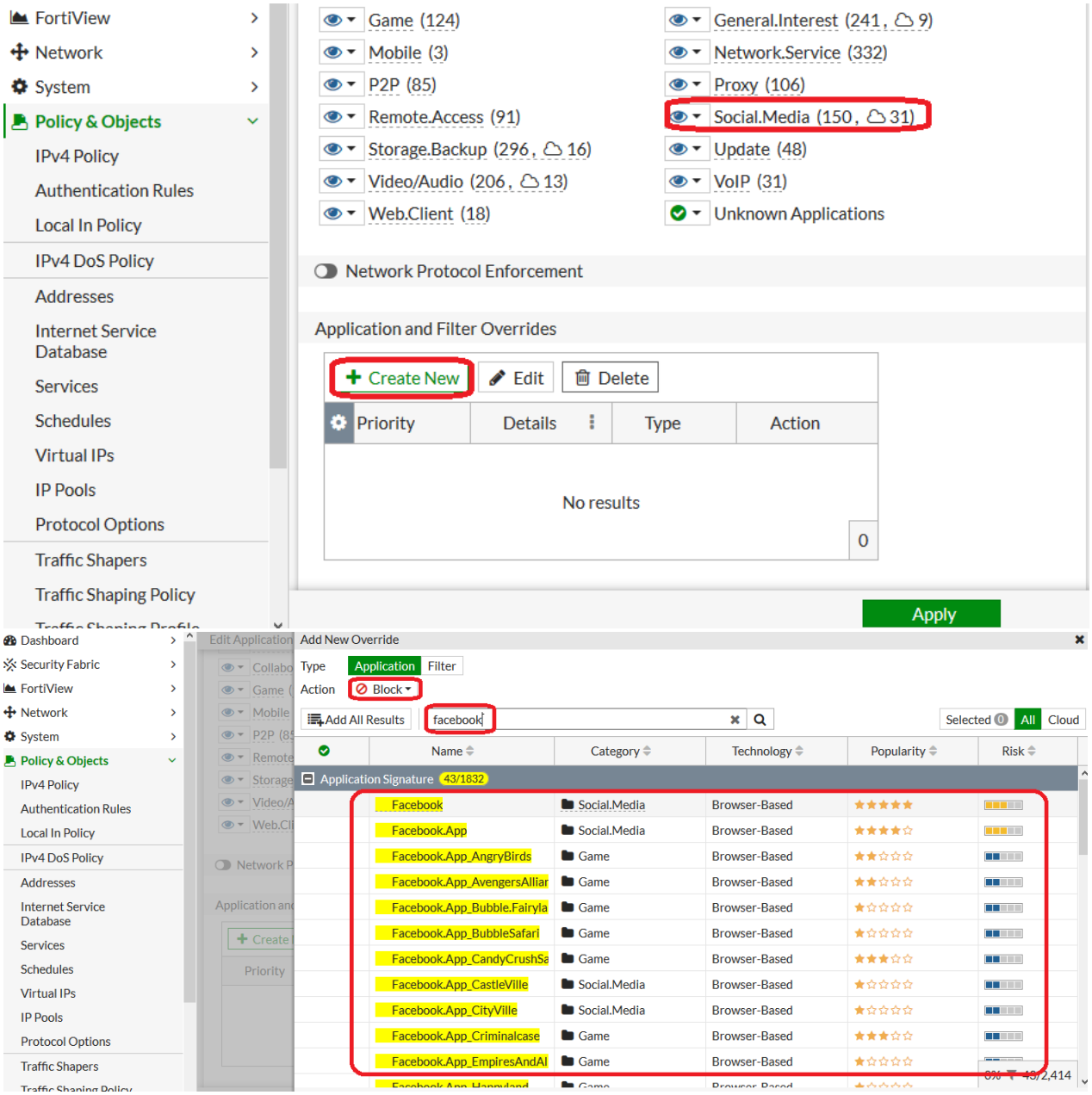


طريقة التحكم بخاصية معينه داخل الموقع وليس كل الموقع :

التحديد لتطبيق معين اولخاصية معينه داخل التطبيق يكون من الخيار

Application and Filter Overrides

مثلا اريد افتح الفيسبوك ولكن اقفل خاصيه اعجبني :



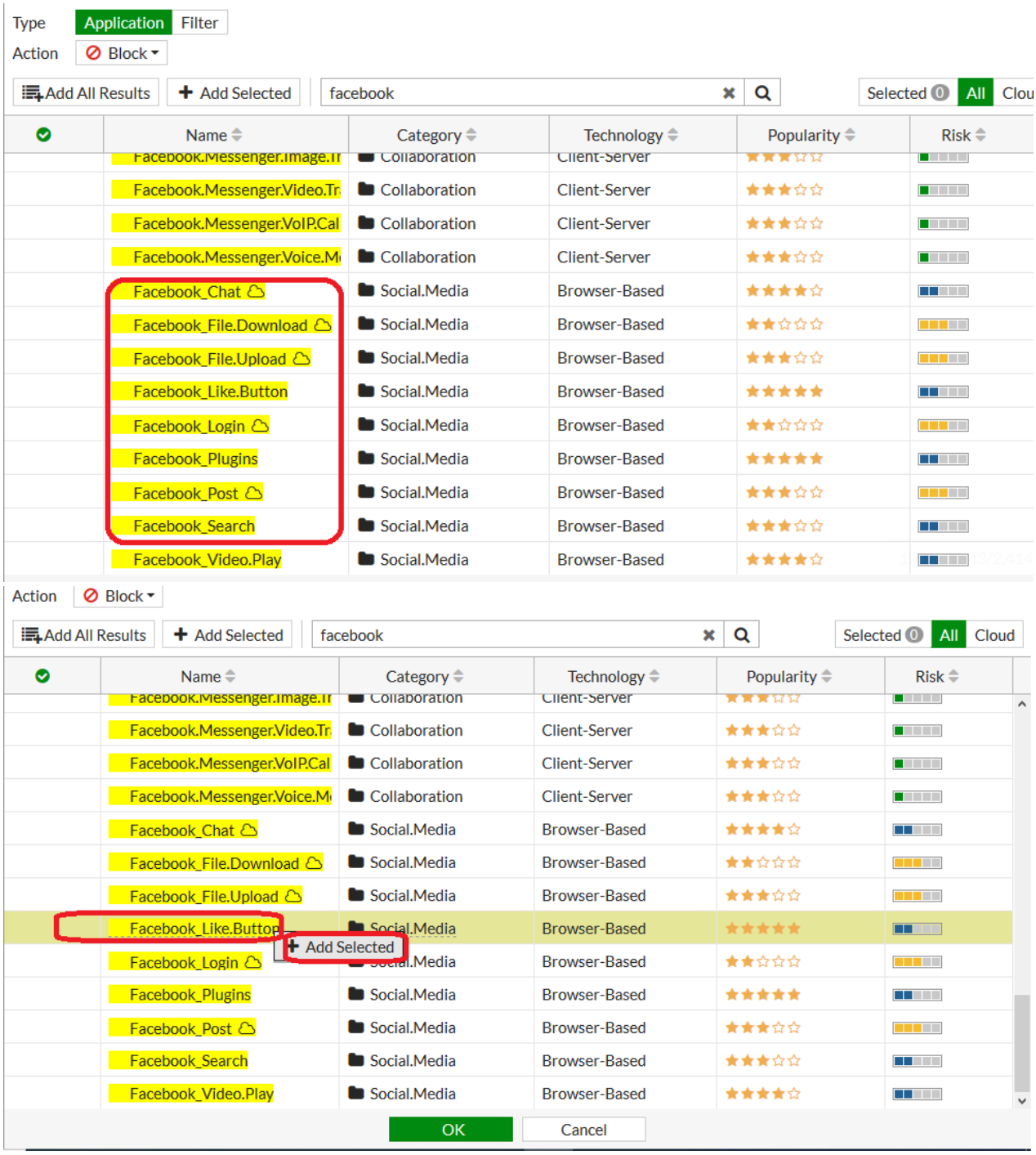
كما بالصورة أعلاه تم البحث عن التطبيق facebook في خانه البحث وظهرت كل التطبيقات التي باسم facebook

حيث اول تطبيق يظهر لك مثلا facebook بدون أي اضافات يعتبر التطبيق العام (موقع الفيسبوك كامل مع الخصائص المدرجة تحته)...

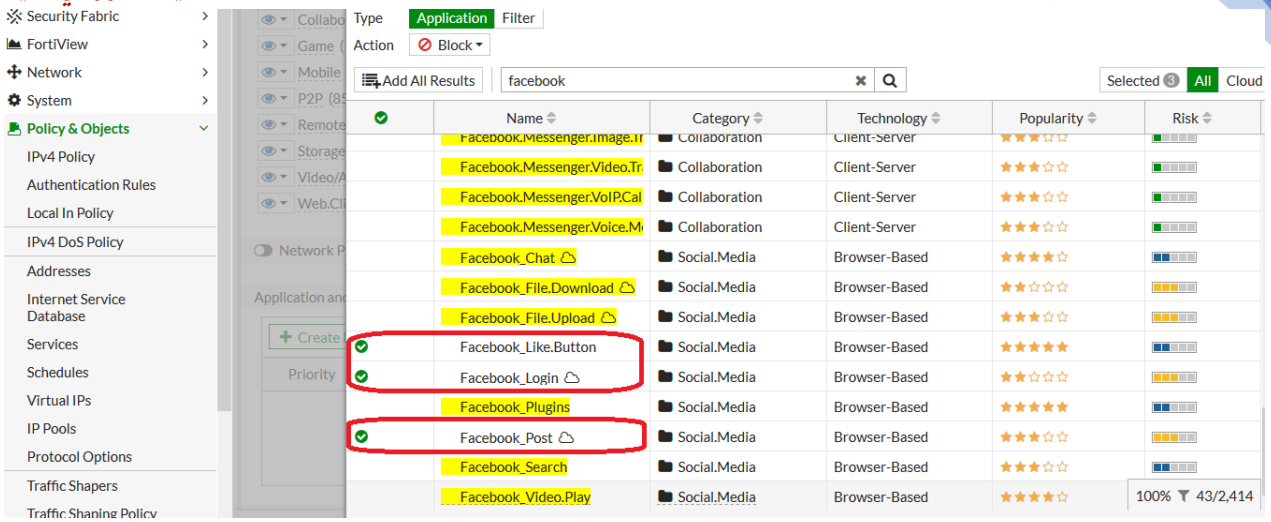
فمثلا facebook.app هذا يعني التطبيق نفسه وليس الURL

حيث الaction هو Block التي سوف نحدده للتطبيقات التي سوف نختارها كما بالصورة التالية :

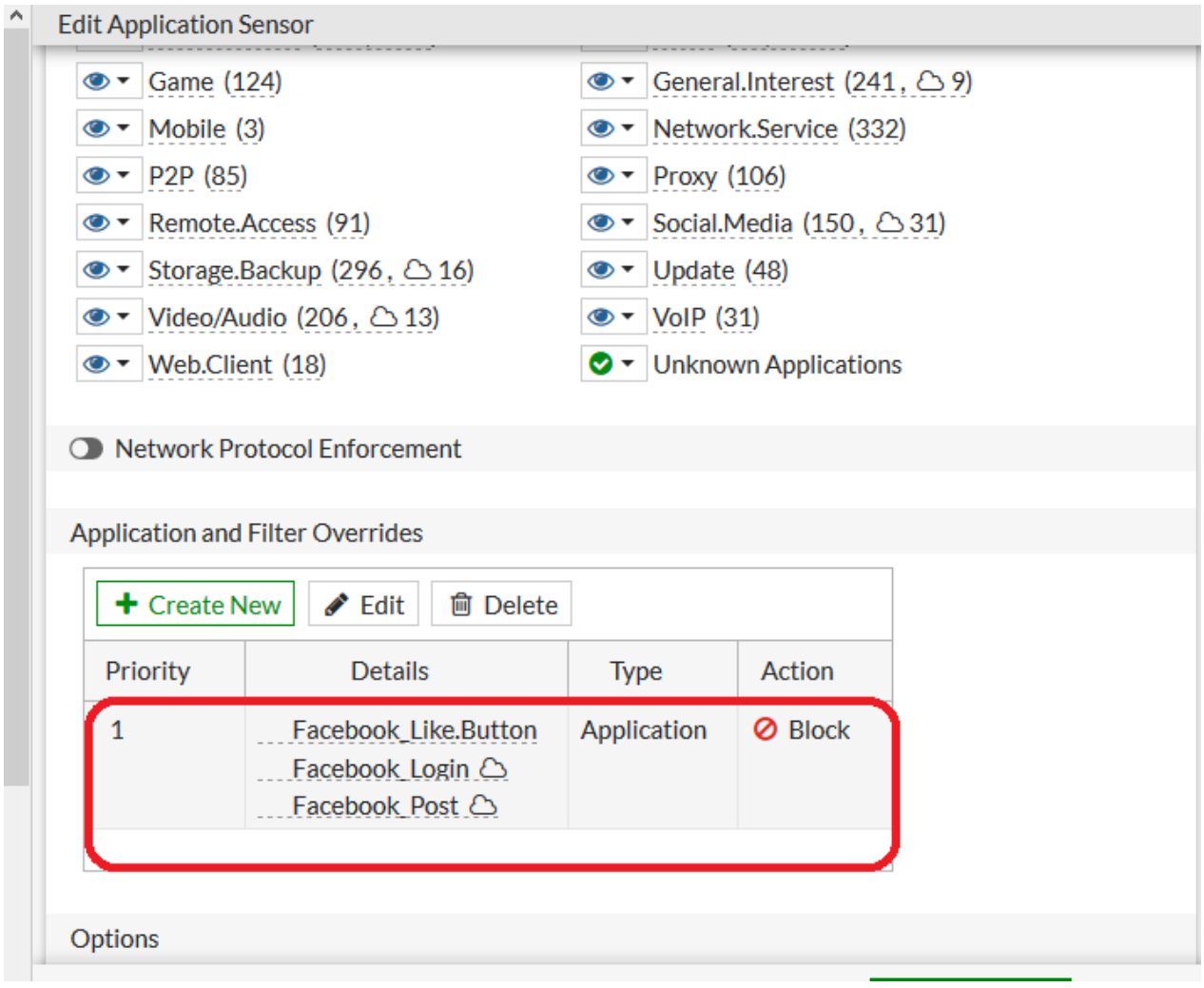
مثلا اريد اغلاق خاصيه معينه في الفيسبوك وليكن اغلاق النشروالدخول وزر اعجبني



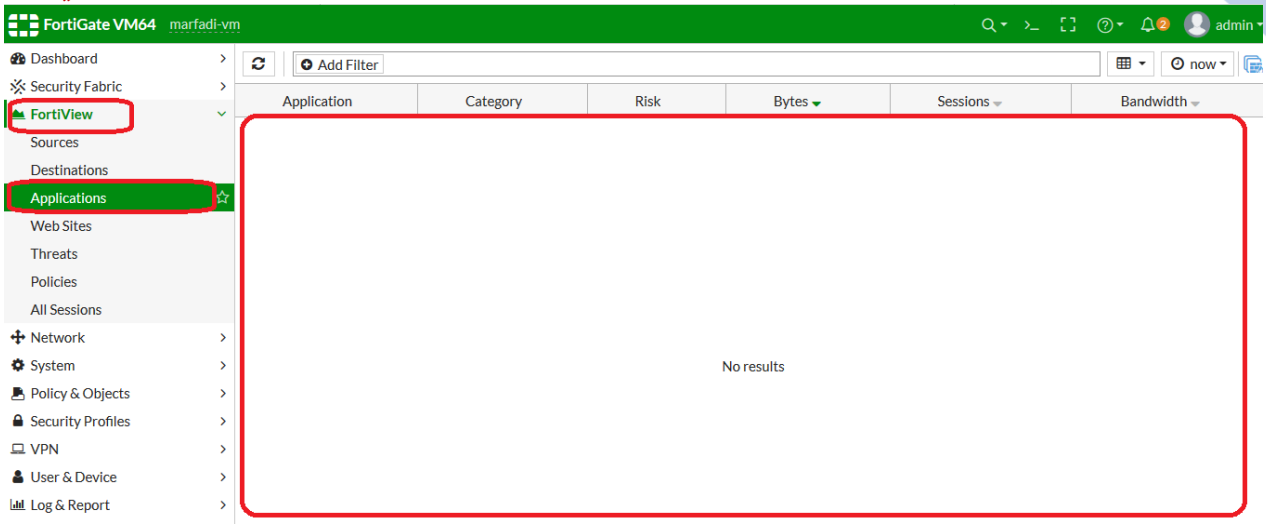
حيث نحدد بالزر الأيمن للخاصية وليكن منع زر اعجبني بالفيسبوك ثم نختار الخيار Add Selected



تم تحديد الخصائص التالية بالفيسبوك (Like ,Login,post)



لو تريد متابعه ومراقبه الlogs كما بالصورة التالية

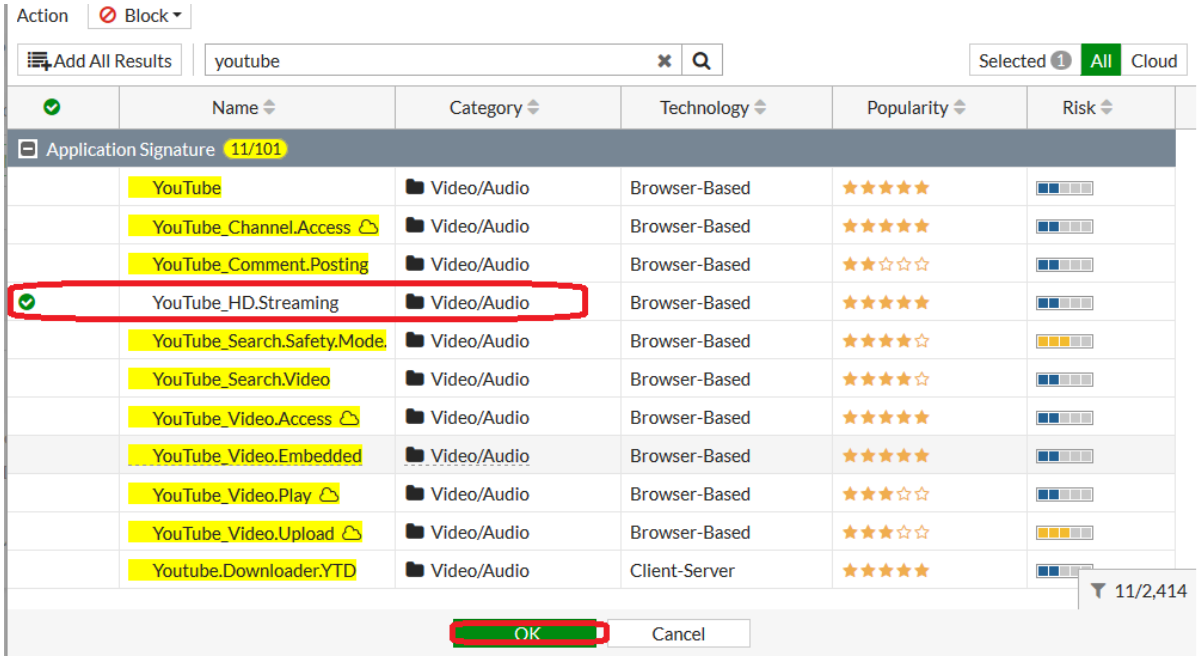


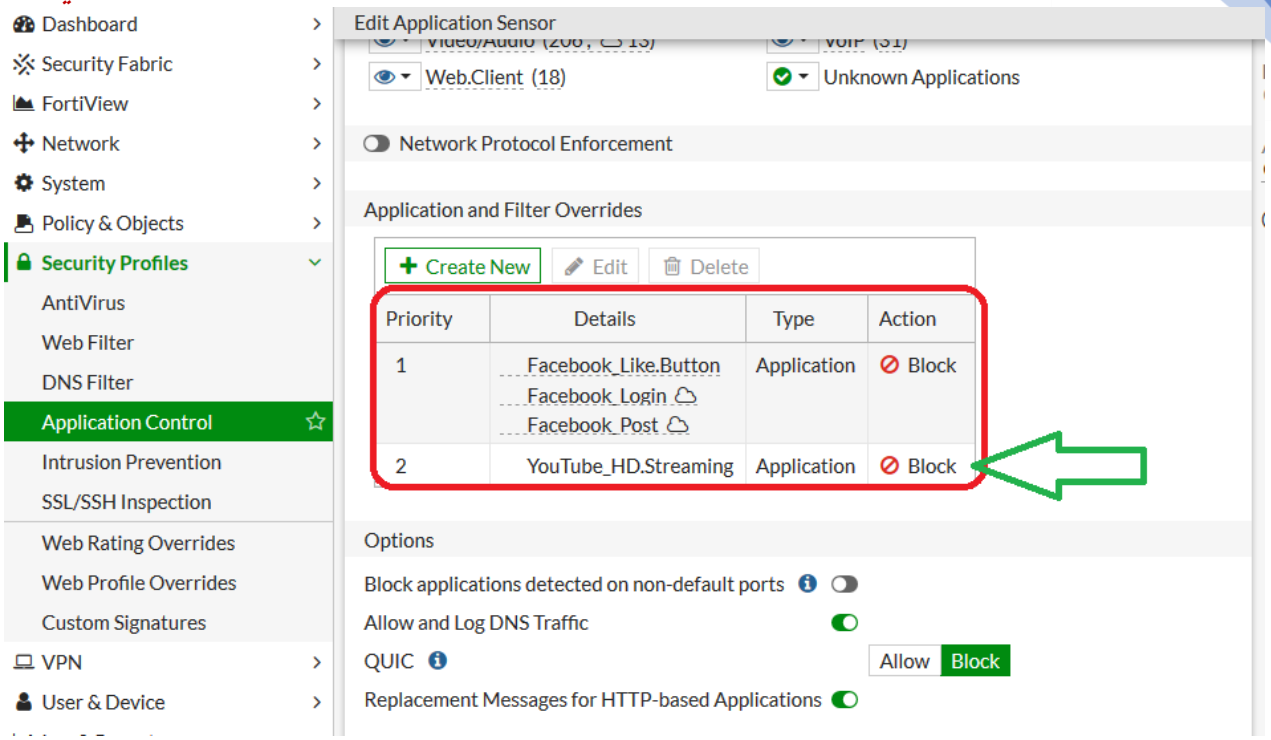
حيث يظهرلك كل التطبيقات التي حاول اليوزر الوصول اليها والتي في الأصل معمول لها Block او Monitor ...

حيث سيوضح لك اسم التطبيق والتصنيف الذي ينتمي له التطبيق ودرجه الخطوره وحجم استهلاك الانترنت ...الخ

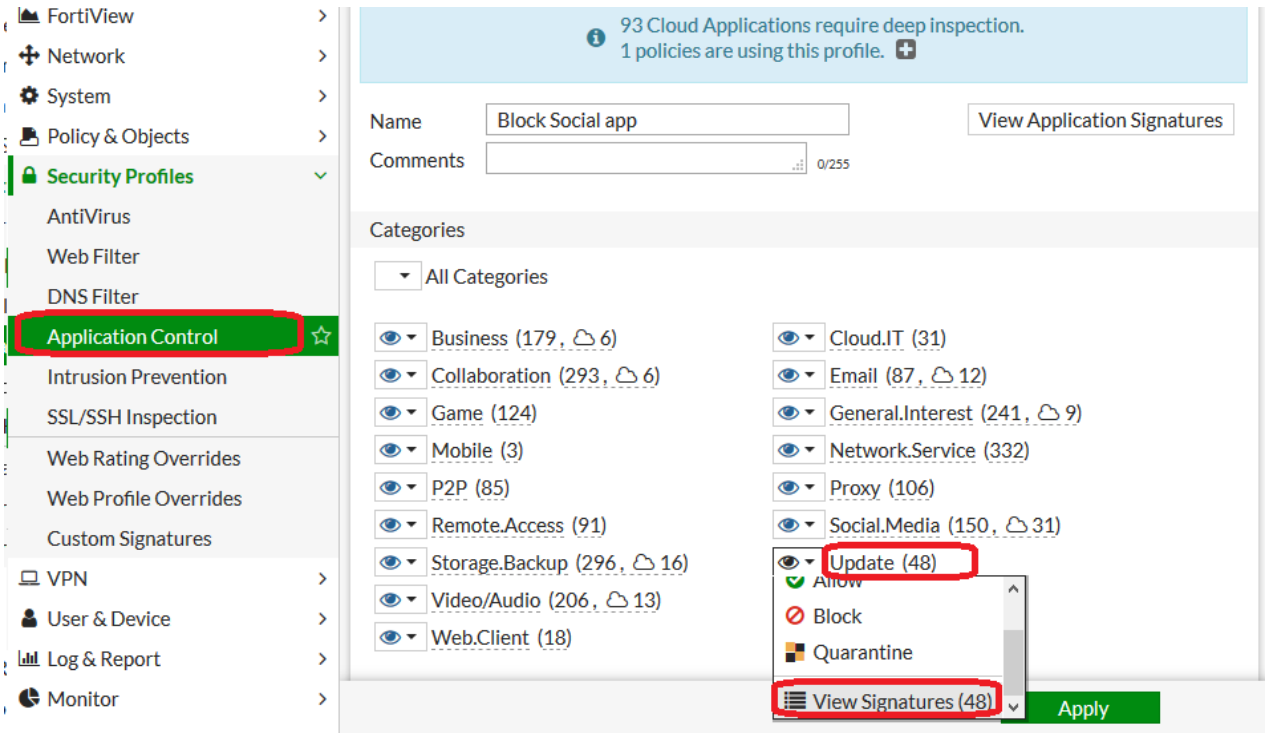
مثال اخر:

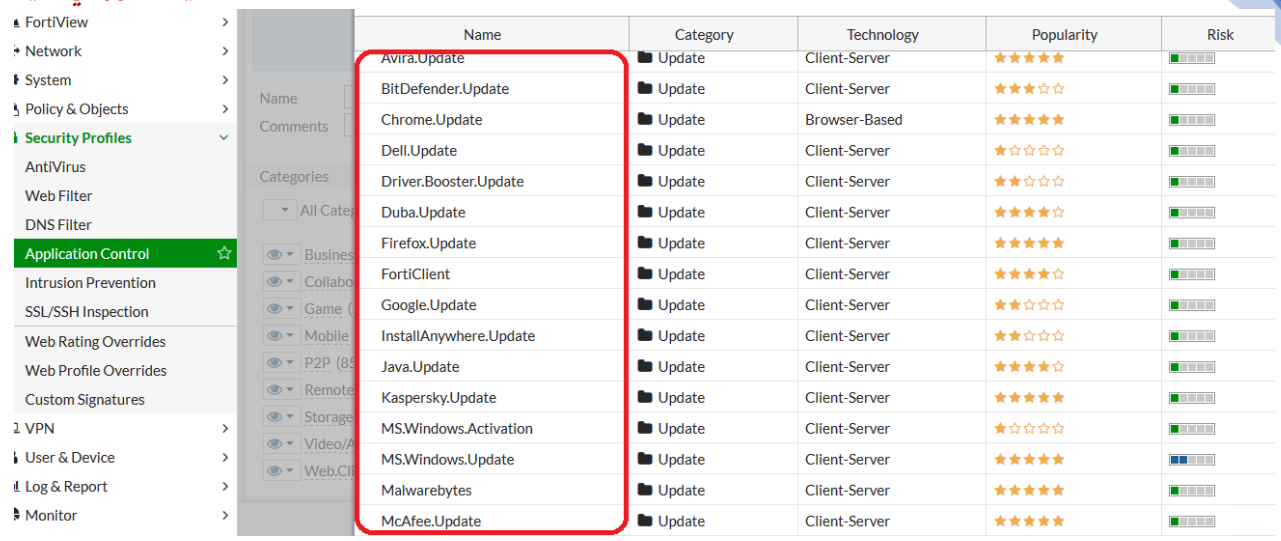
اريد اغلاق قط الفيديوهات عاليه الدقه (HD)فقط من على اليوتيوب ...





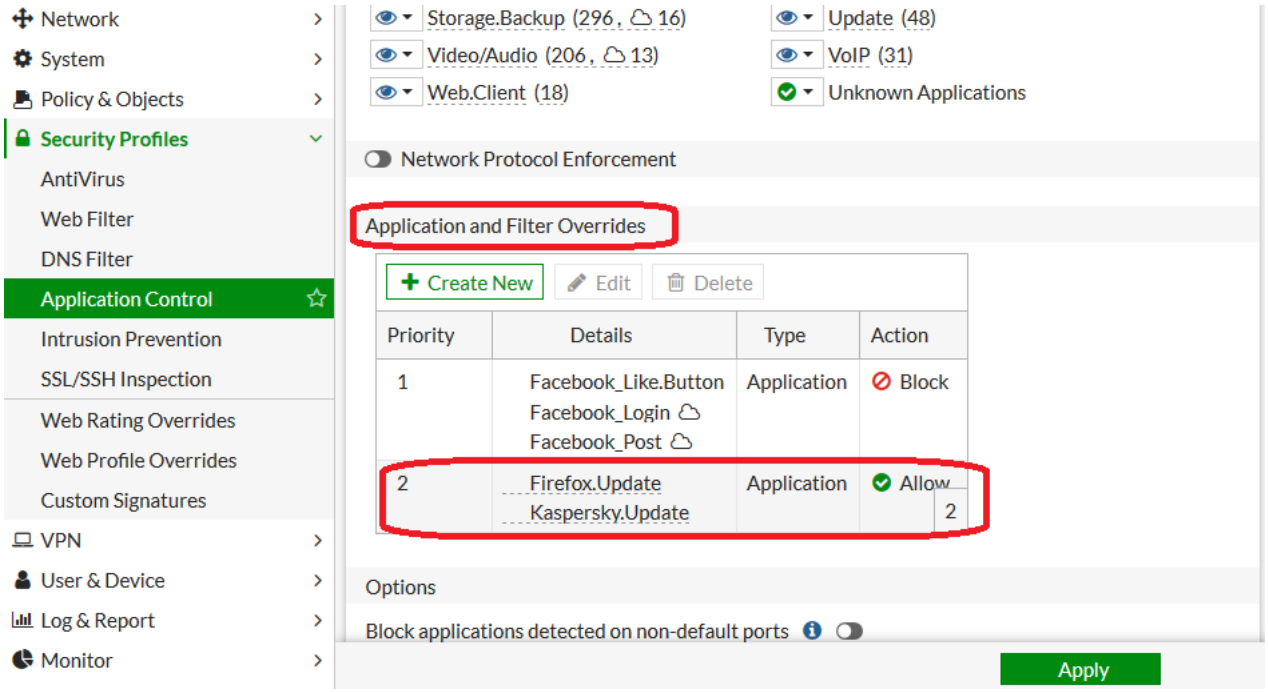
طبعا توجد تصنيف(Category)اسمها Update والأفضل ان تتركها مثلا تحديث مكافح الفايروسات او تحديث ويندوز ..الخ





فيمكنك السماح للتطبيق المناسب او منع التحديث لتطبيق ما ...

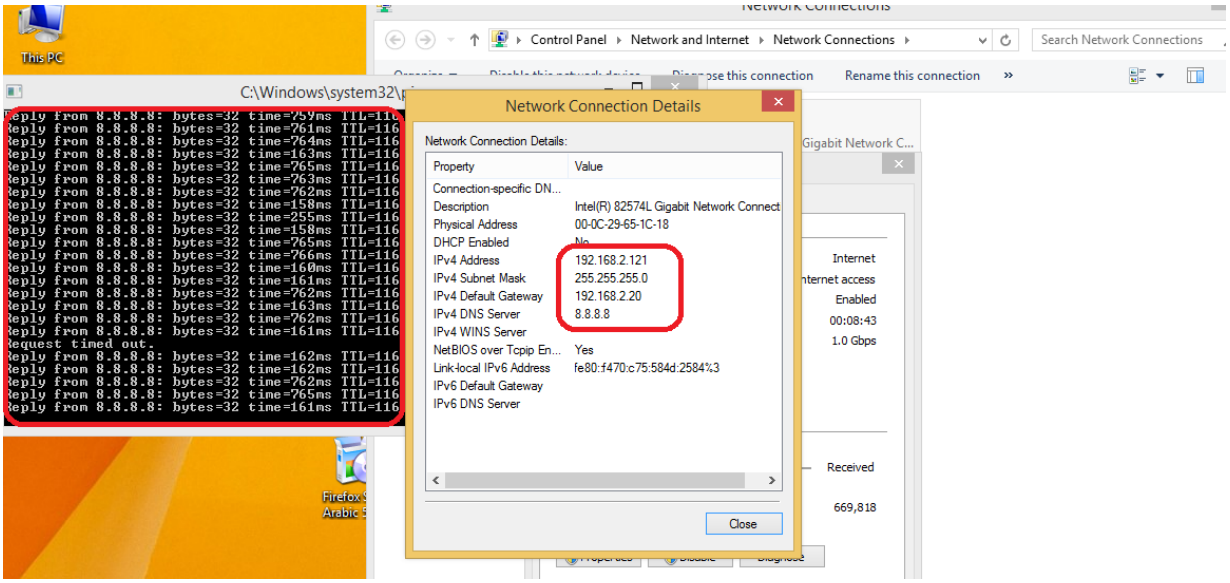
مثلا اريد السماح للكاسبروالفايرفوكس ان يعملوا تحديث



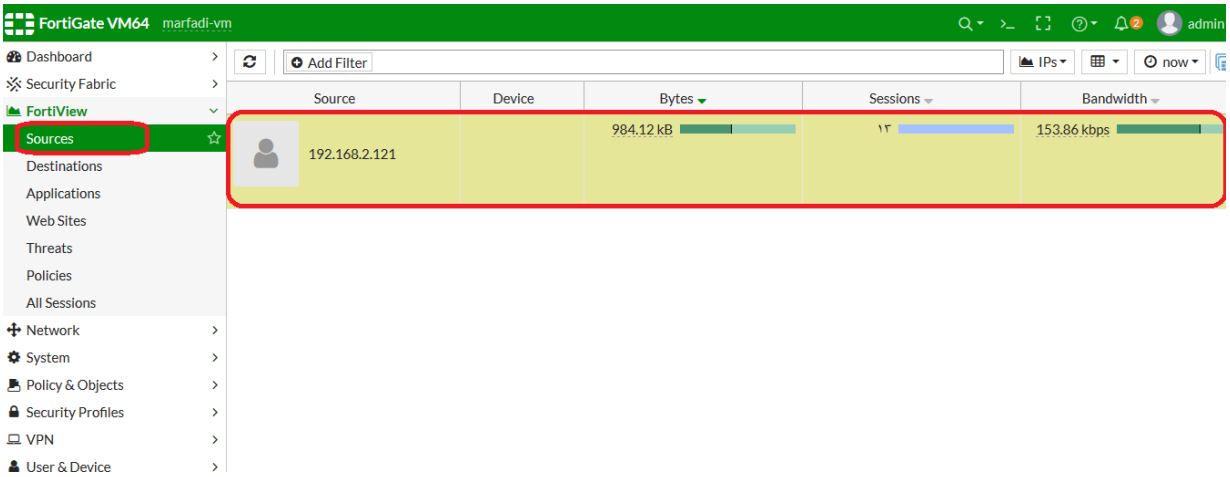
➢ طريقة عمل حظر (ban)لجهاز معين ...

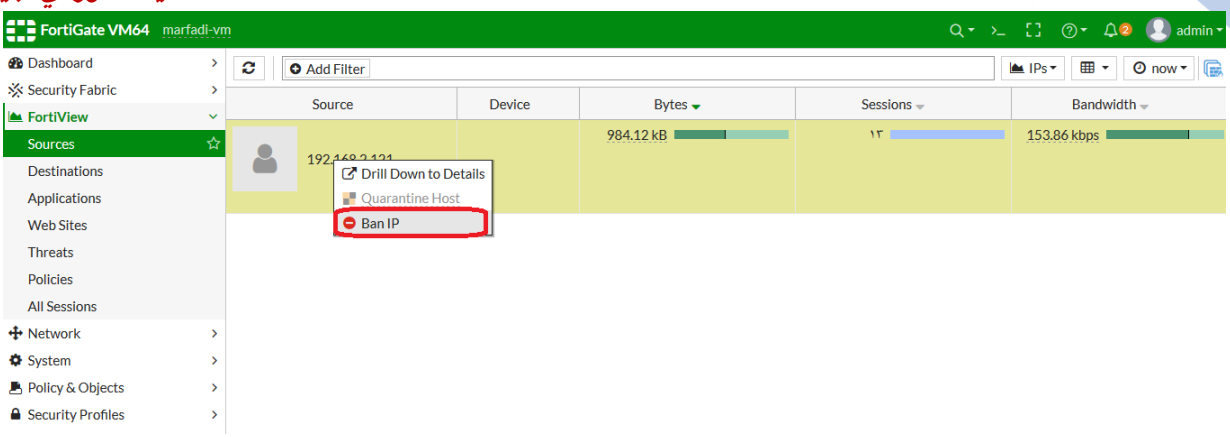
لنفترض بأن الجهازصاحب الايبي 192.168.2.121 نريد عمل له حظر..

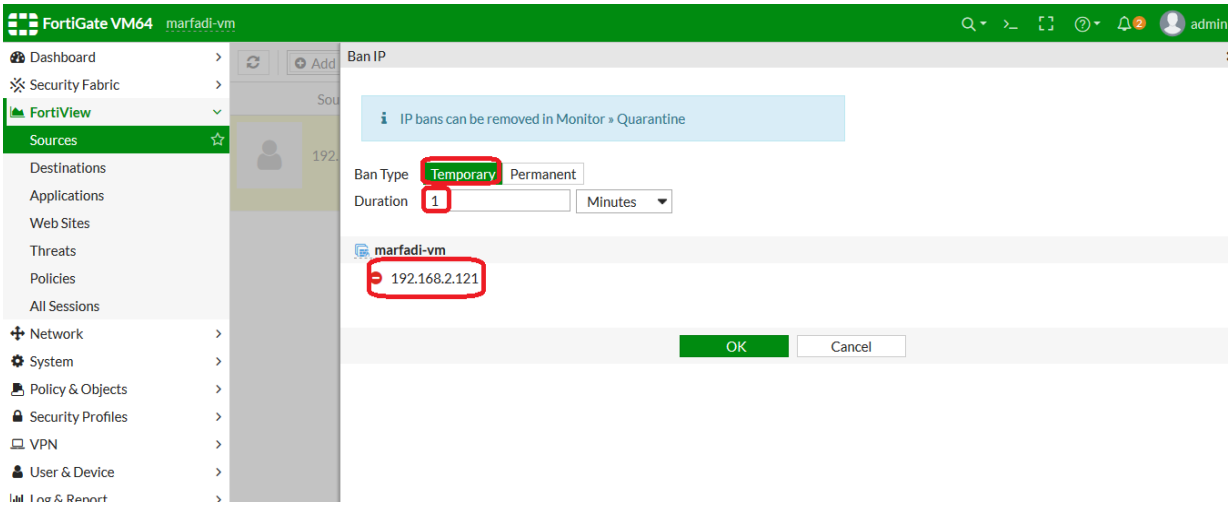
حيث نلاحظ بان الانترنت شغال قبل عمليه الحظر..



الآن سوف نعمل الـban للجهازكما بالخطوات التالية :



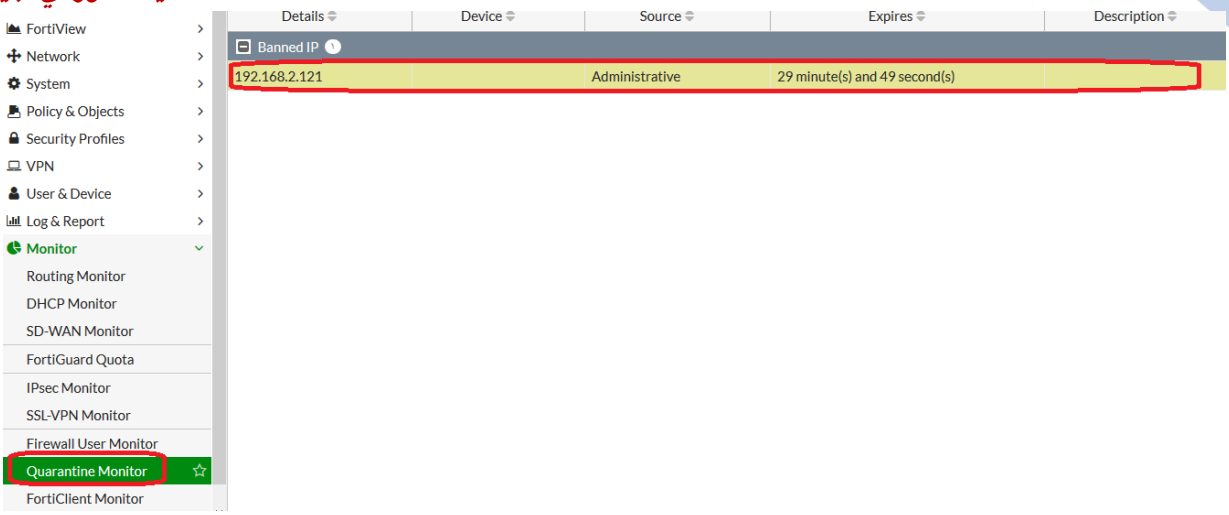


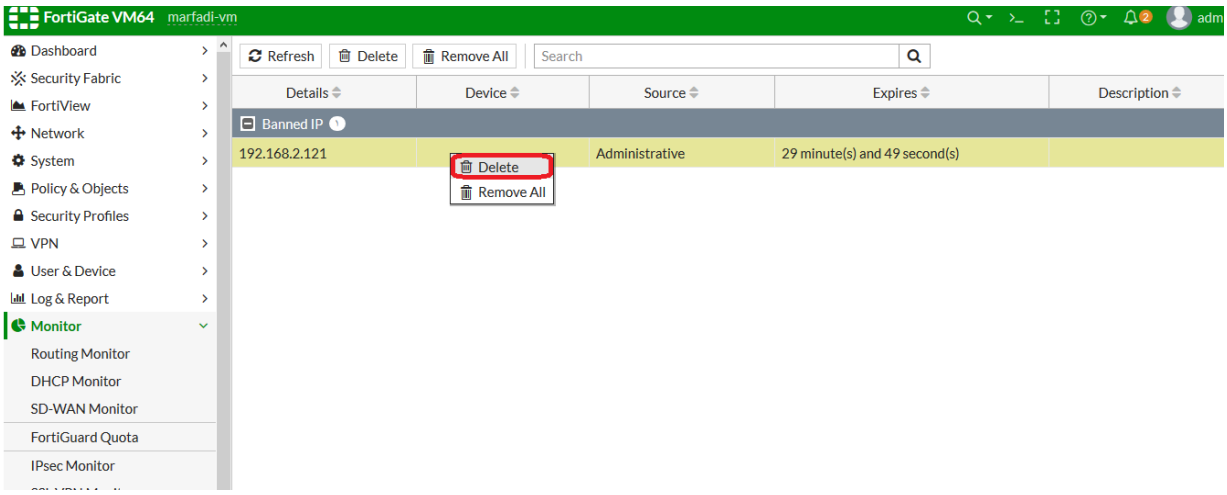


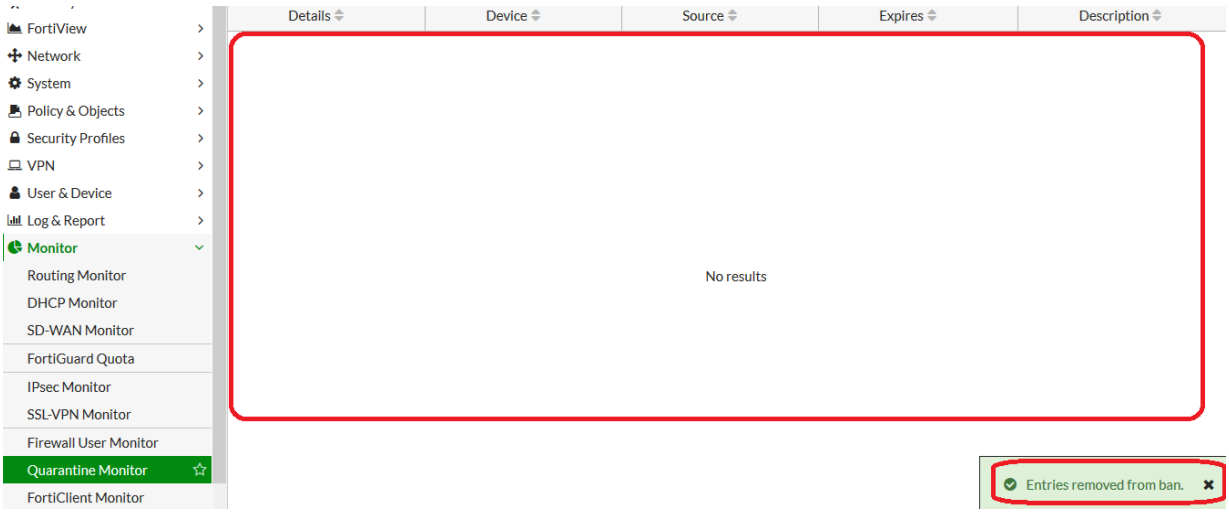
كما بالصورة أعلاه سوف يسالك هل تريد الحظرلهذا الجهاز

Temporary :أي موقت ولفتره زمنيه محدده وليكم دقيقه واحده فقط وبعدها يتم فك الحظربشكل تلقائي .

Permeant :سيتم حظرالايبي (الجهاز)بشكل دائم ولفك الحظرلهذا الجهازيتم الدخول بحسب الخطوات التالية :







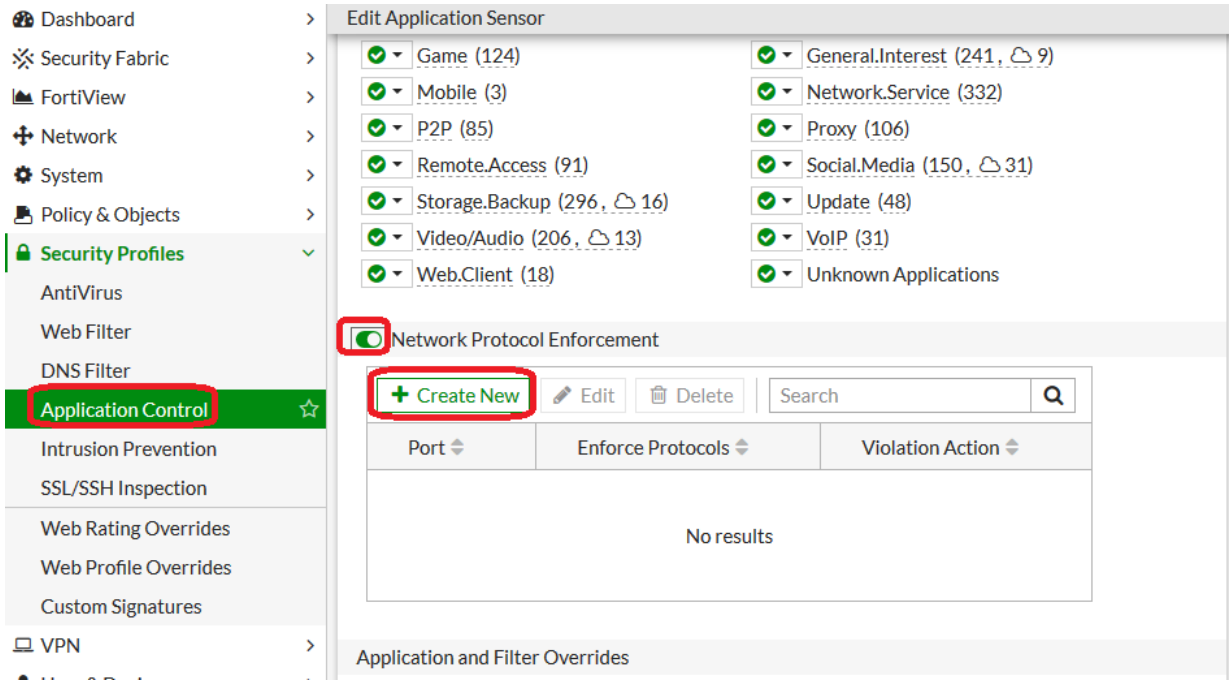
Network Protocol Enforcement :

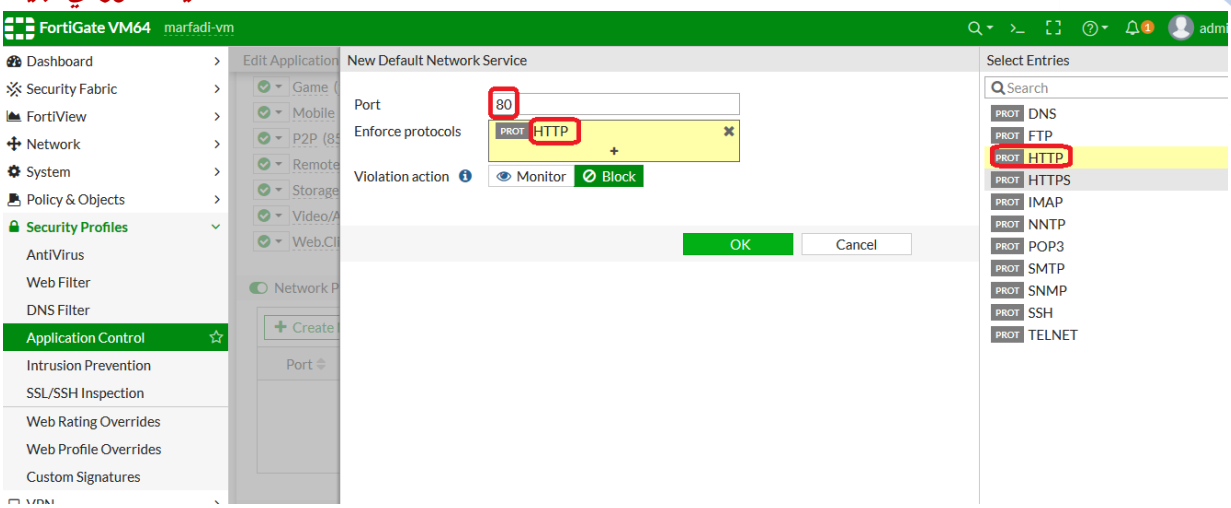
هذه الخاصية موجودة في الـ Application control حيث كما نعلم توجد لكل بروتكول بورت معين بشكل افتراضي كما بالتالي :

Protocol	Default port Number
http	80
https	443
Ssh	22
telnet	23
Dns	53

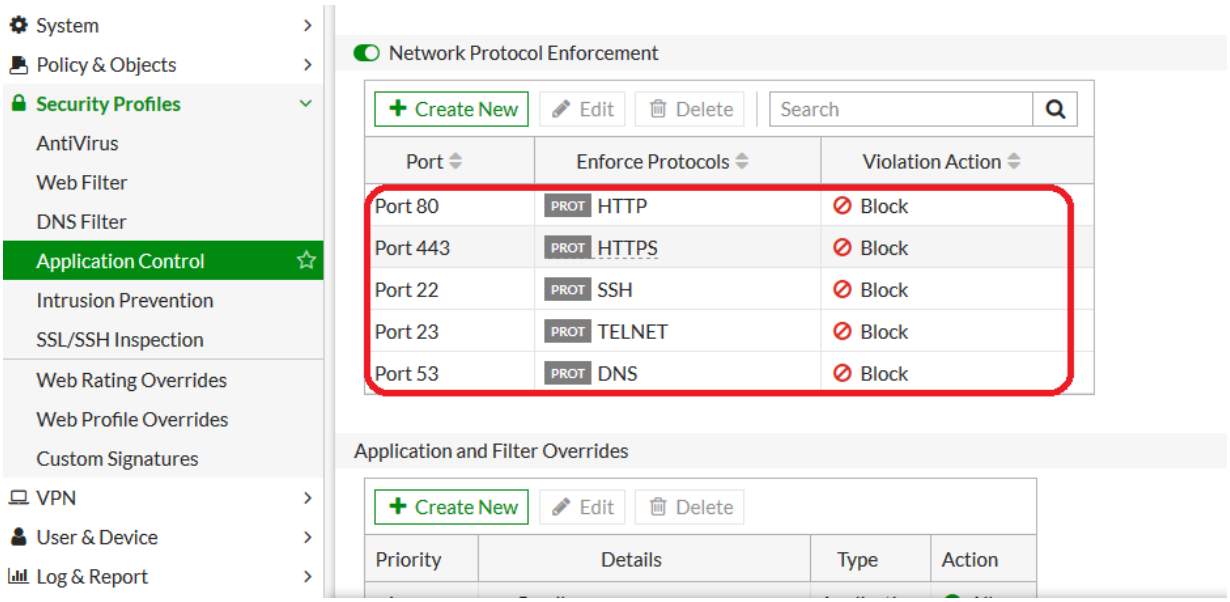
حيث يمكن ان يقوم اليوزر بتغيير رقم الـ port للبروتوكول وبهذا يتم التحايل على الفورتي جيت ..

فيمكن بواسطة الخاصية المذكورة أعلاه بأن امنع عمليه تغيير رقم الـport لبرتوكول معين ..





وهكذا ..



حيث لو حاول احد تغييررقم البورت لأحدى البروتوكولات أعلاه سيتم عمل Block .

❖ Email filter

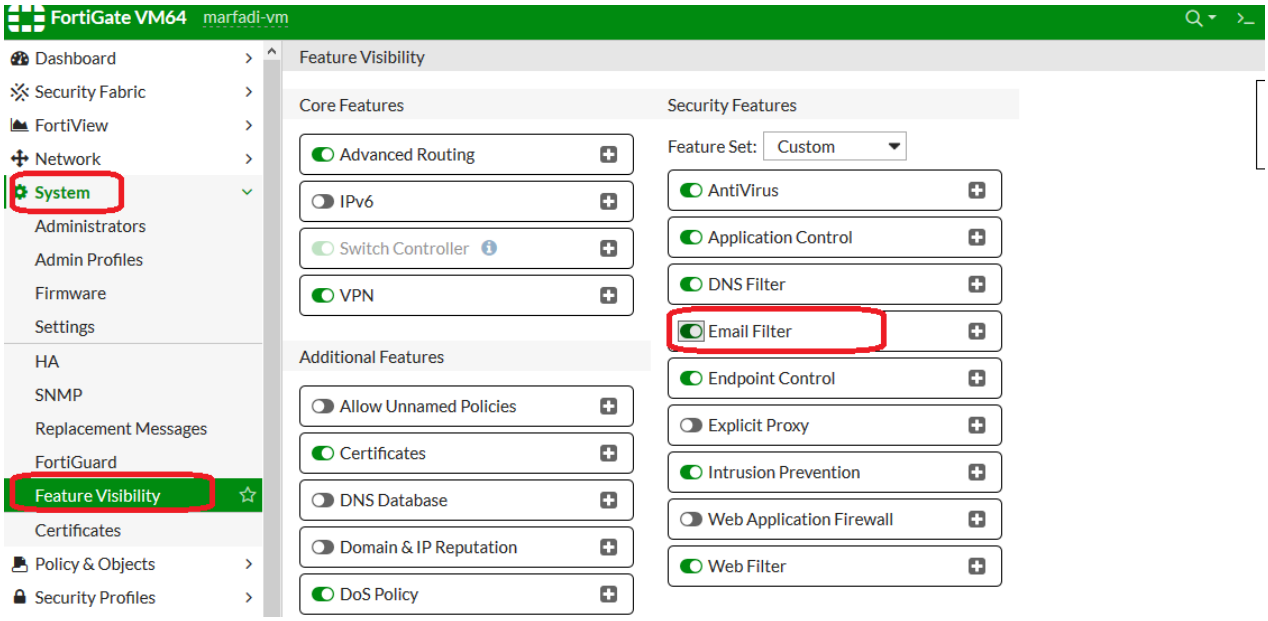
كيفيه فلتره الايميلات على الفورتي جيت ..

أي عمليه اداره الايميلات الغيرمرغوب فيها (spam email)عبرجهازالفورتي جيت سواء وصل الايميل الى الـInbox او الـJunk ..

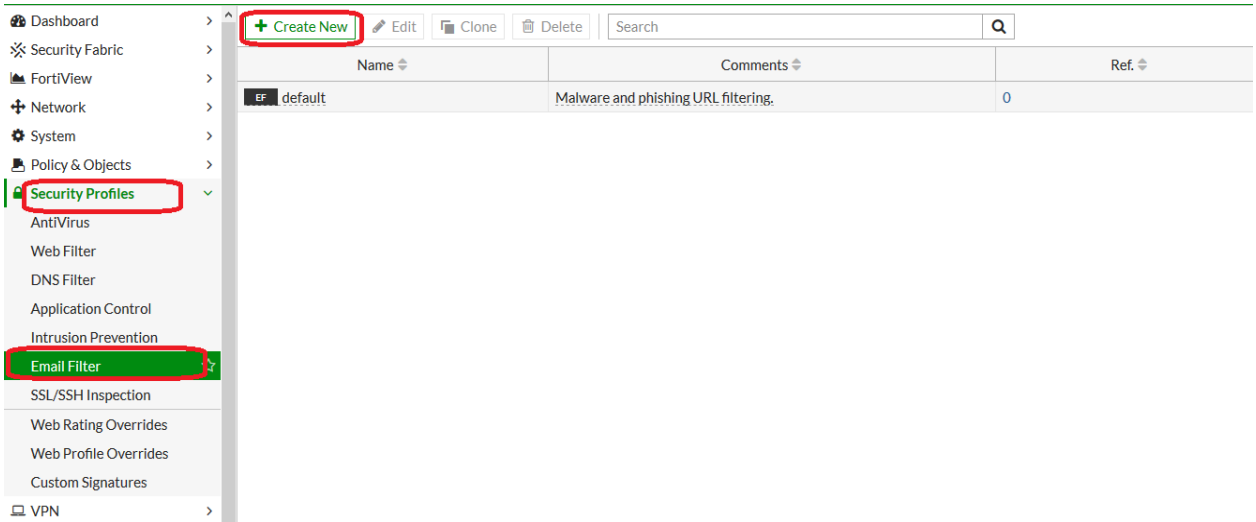
حيث الفورتي جيت معتمد على خدمه من الفورتي جارد اسمها FortiGuard Anti spam services او تسمى Email filtering والتي تحتوي على قاعده بيانات والذي تحدد ما اذا كان الـip او الايميل او URl غير مرغوب ام لا ..

حيث اسم الاشتراك التي يجب ان تشترك بها هو Email filtering ويجب ان يكون معمول له License

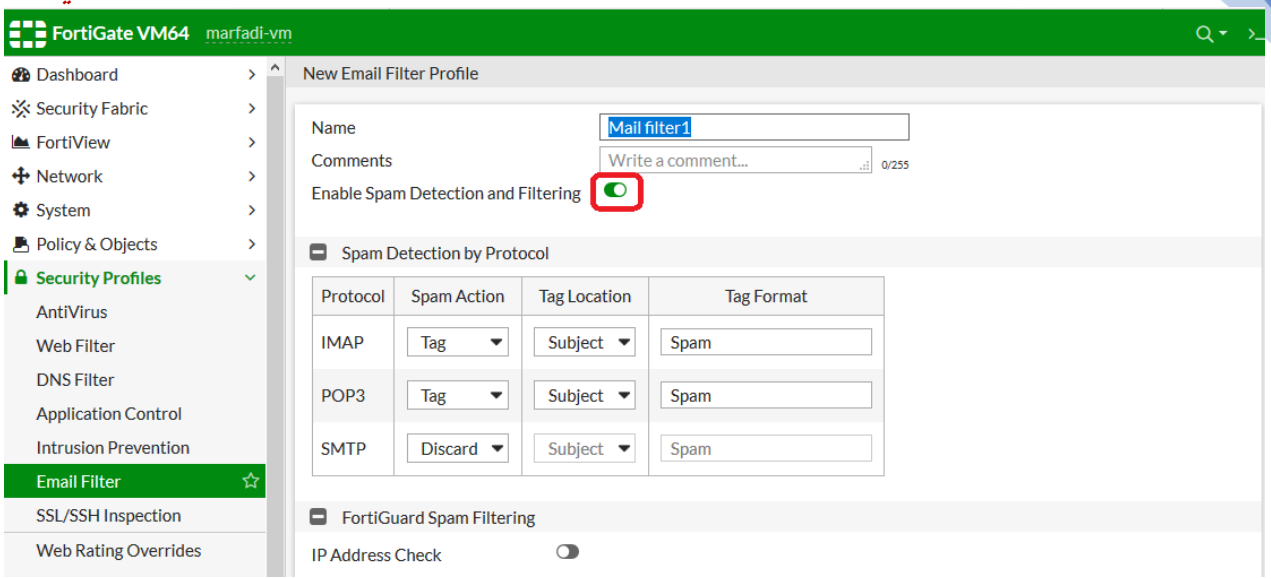
نقوم باظهار خاصيه Email filter كما بالصورة ادناه لكي تظهر في security profiles .



نلاحظ ظهور الخاصية الان ..

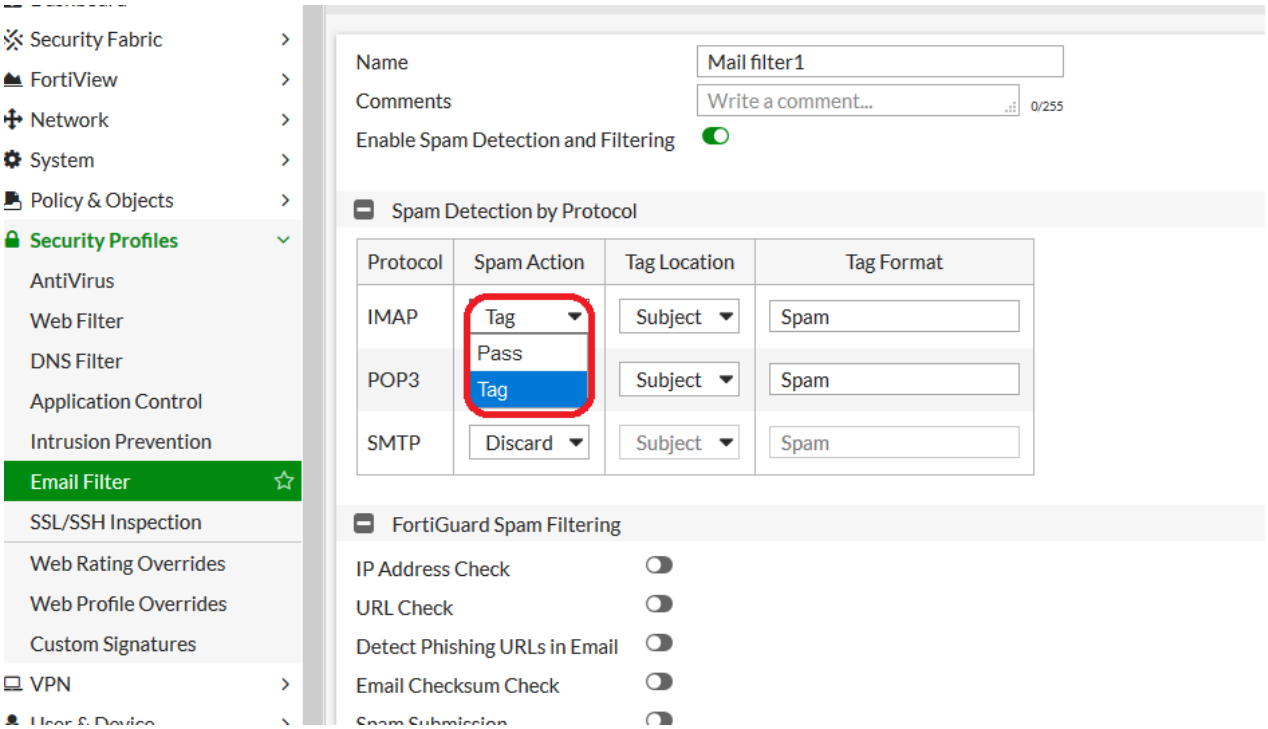


الان يمكنك أضافه بروفايل باسم Mail filter1 وذلك من خلال النقر على الزر Create New



حيث بمجرد تفعيل الخيار Enable Spam Detection and Filtering تظهر لك الجدول المسمى Spam Detection by protocol كما بالصورة أعلاه والذي يقصد به عمليه كشف عن الاسبام ايميل واعمل لها فلتره ..

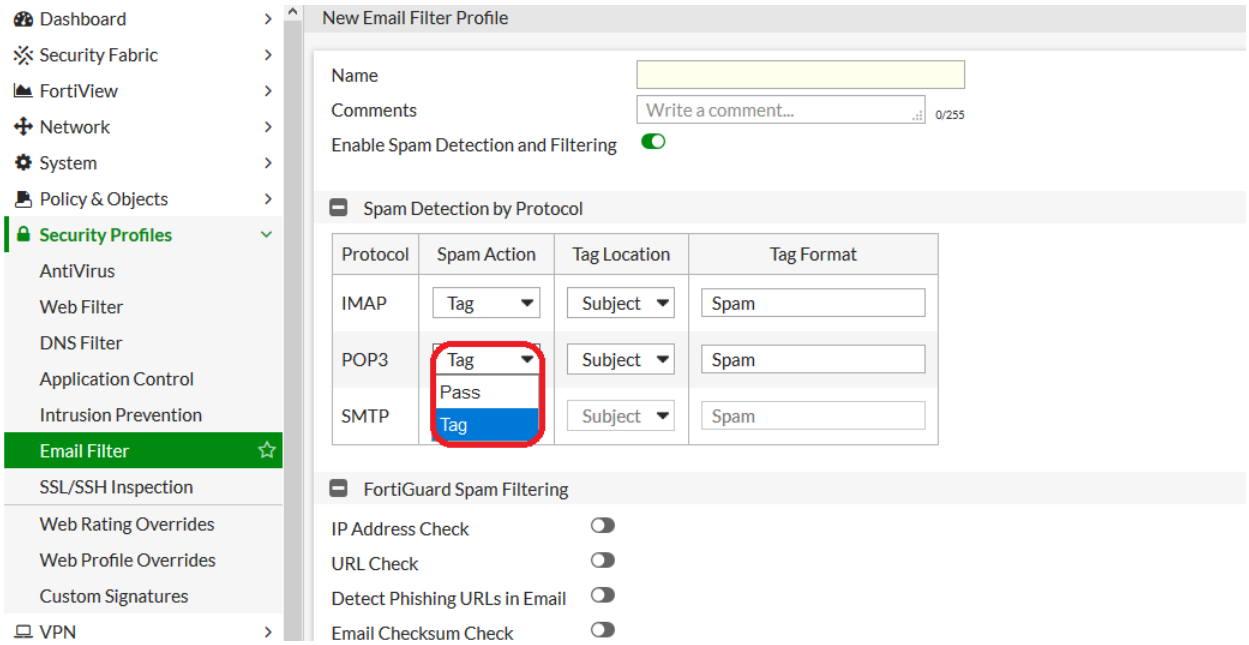
حيث يقصد بالجدول أعلاه بأن أي ايميل بيستخدم ال IMAP او POP3 في الاستلام او يستحدم SMTP في الارسال فأن تم الكشف عليه بأنه spam فأن الـ action الذي ستقوم به في الـimap هو اما Tag او pass



Pass: معناها مرر الايميل بدون ماتعمل له أي action وهذا اجراء غير موصى به .

Tag :أي تعمل علامه على الايميل سواء على Subject الخاص بالايميل او في الـheaders وبهذا سيتم استلامه في الـ spam folder او الـjunk folder وبنفس الوقت معمول له في العنوان او الـheader بانه spam او أي كلمه حددتها في الخانه tag format.

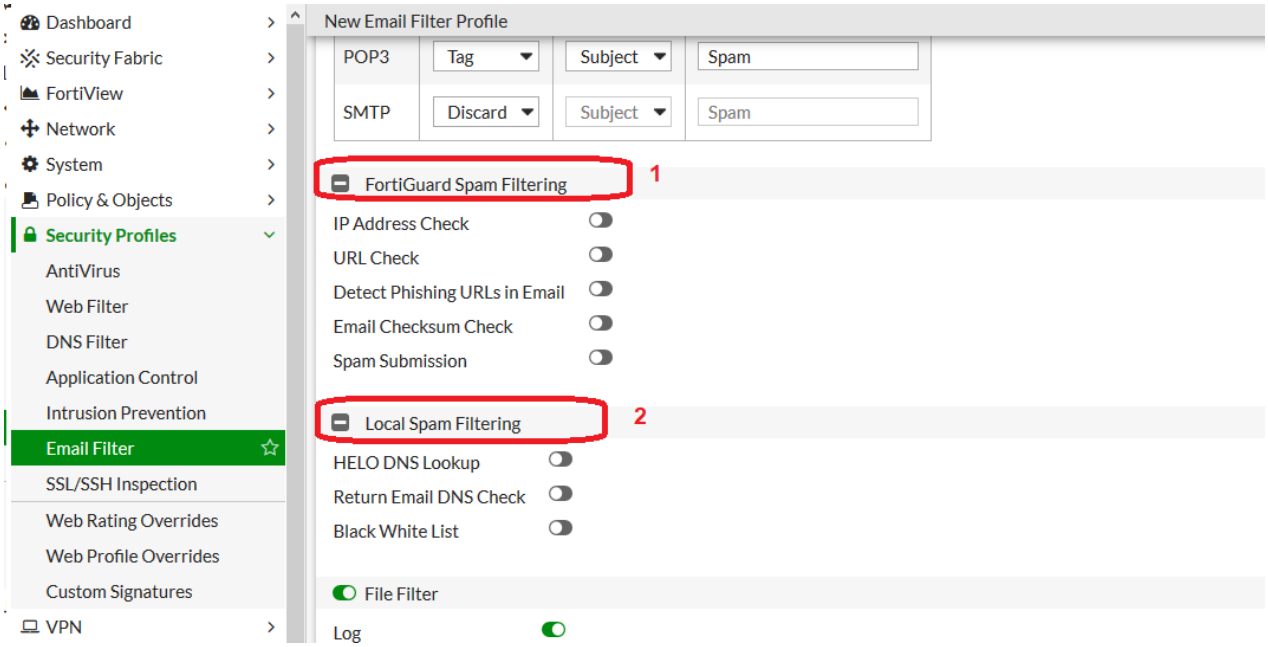
ونفس الكلام مع بروتوكول الاستقبال الـpop3 ...



اما الـsmtp وهو البروتوكول المستخدم لعمليه ارسال الايميل فأن الـ 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 الـHeader بانه spam ..

➢ ماهي الطرق التي يستخدمها الفورتي جيت لكي يساعدك لاكتشاف الاسبام ايميل ؟

يعتمد على احدى الطرق :



A) الاعتماد على الفورتي جارد (fortigurd spam filtering license) :

١. Ip Address check :أي ايميل اورساله تمرعبرجهازالفورتي جيت ستخضع لفحص من خلال الفورتي جارد (سيتم ارسالها الى الفورتي جارد) فلووجد بأن الايبي المرسل منه الايميل موجود بالقائمة السوداء فسيتم عمل اشاره على انه Spam ويتم وضعه في مجلد الاسبام للإيميل اما في حالة كان الايميل سليم فسيتم تمريره الى الهدف بدون أي مشاكل ..

٢. URL Check :أي URL(سواء عنوان البريد او أي رابط في محتوى الرساله نفسها) سيتم فحصه عبر الفورتي 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 .

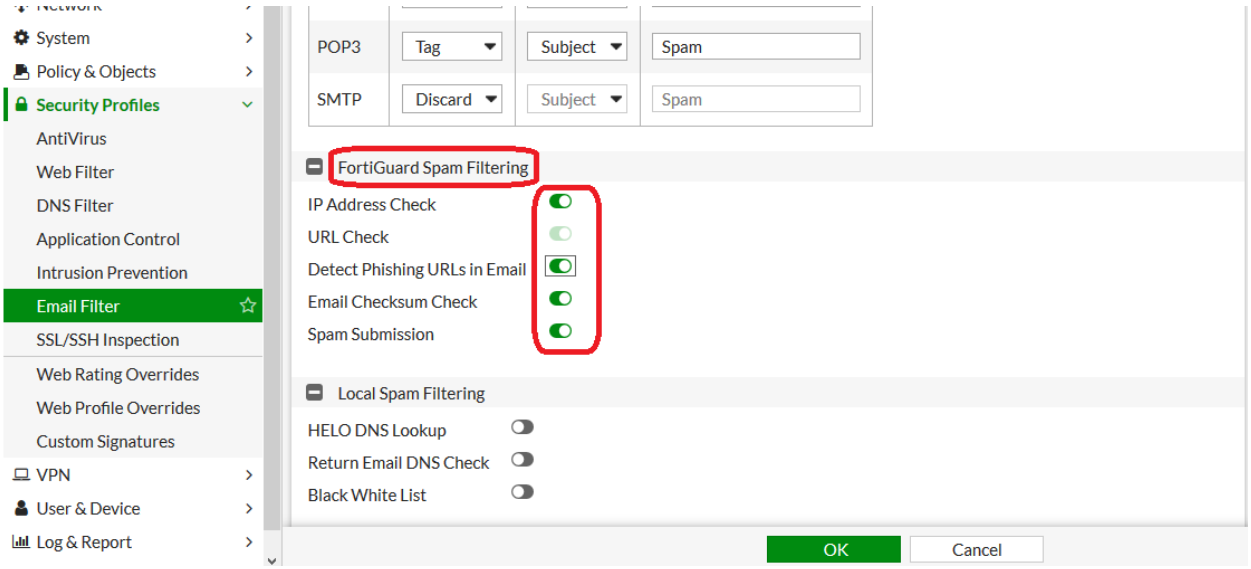
٣. Detect Phising URLs in emils :سيتم الكشف عن روابط التصيد وسيتم اخضاع الروابط(URL) للفحص في URL Phising List فلو وجد هذا الرابط في تلك القائمة فأما سيقوم بحذف الرابط (URL)كاملا او سيترك لك الرابط ولكن سيحذف منه الرابط المشبوه فحتى لو نقرت على الرابط لا يتم تحويلك الى الـphishing URL ..

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 antispm service يعدل الايميل من اسبام الى ايميل عادي ..

حيث لو افترضنا بأن ايميل معين تم تصنيفه من قبل الفورتي جارد عن طريق الخطأ على انه اسبام فلو قمنا بتفعيل هذه الخاصية فأن أي ايميل سيتم وصوله الى الـspam folder فيمكنك تعديله ومعالجته بأن هذا الايميل سليم وليس اسبام وبهذا سيتم ارساله الى الفورتي جارد بحيث مره أخرى سيتم وصوله بشكل طبيعي.

حيث يتم تفعيل كل الخيارات الخمسه أعلاه كما بالصورة التالية :

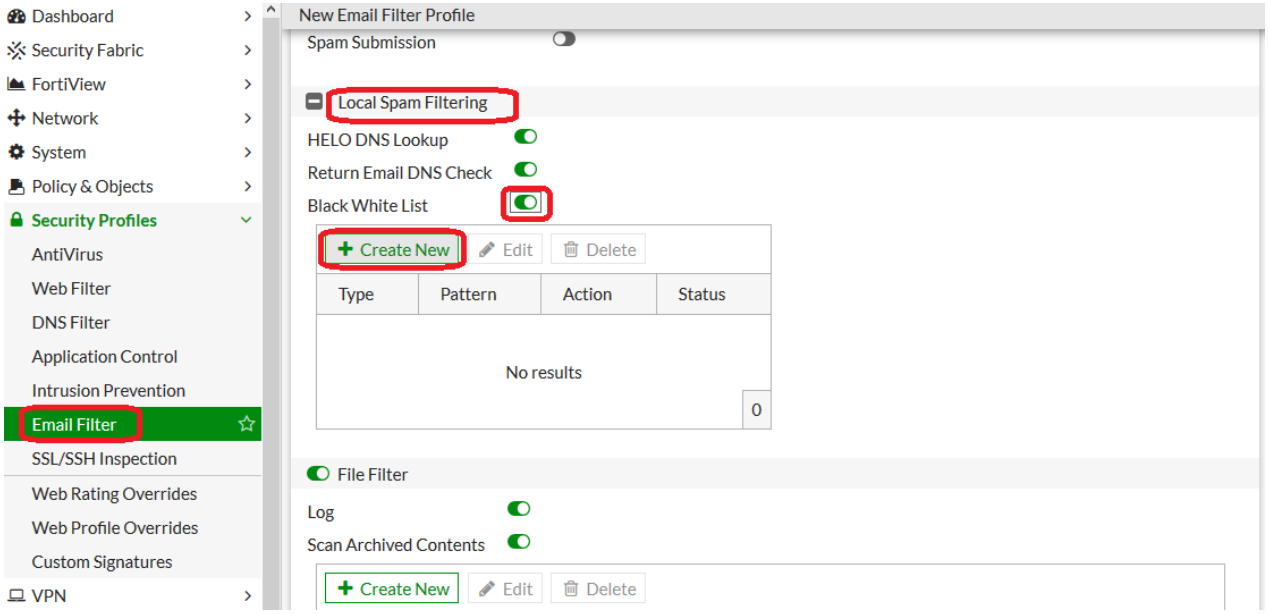


B) الاعتماد على الفورتي جيت نفسه وبدون الحاجه الى لايسنز(Local Spam Filtering) .

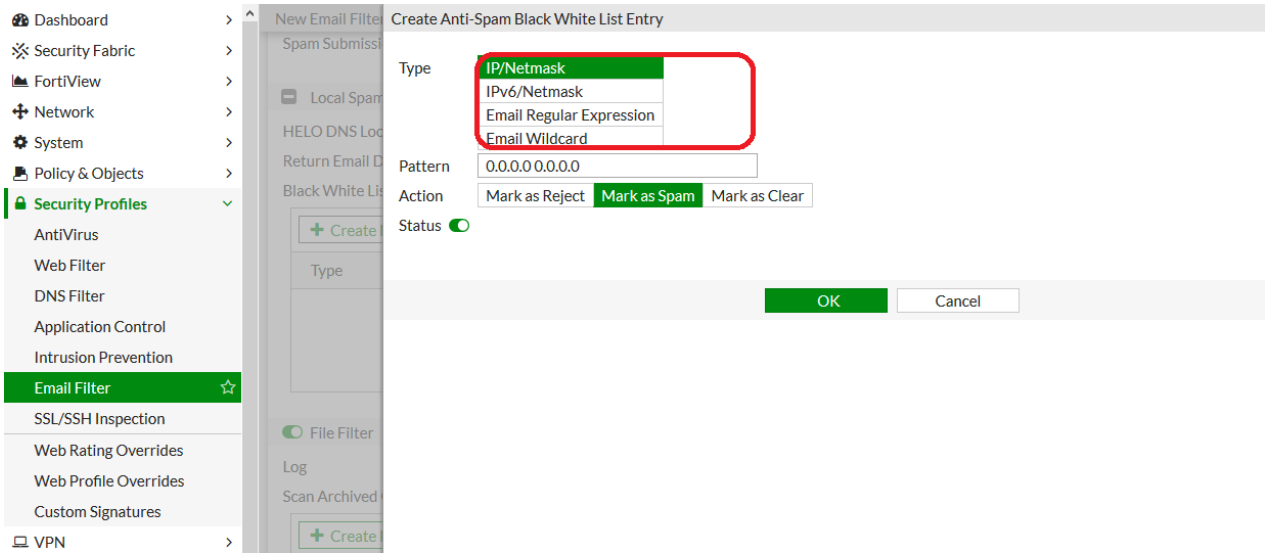
١- Helo DNS Lookup :يتم التأكد هل domin التابع للإيميل موجود في Public DNS فلو لم يكن موجود فسيعتبر هذا الدومين اسبام .

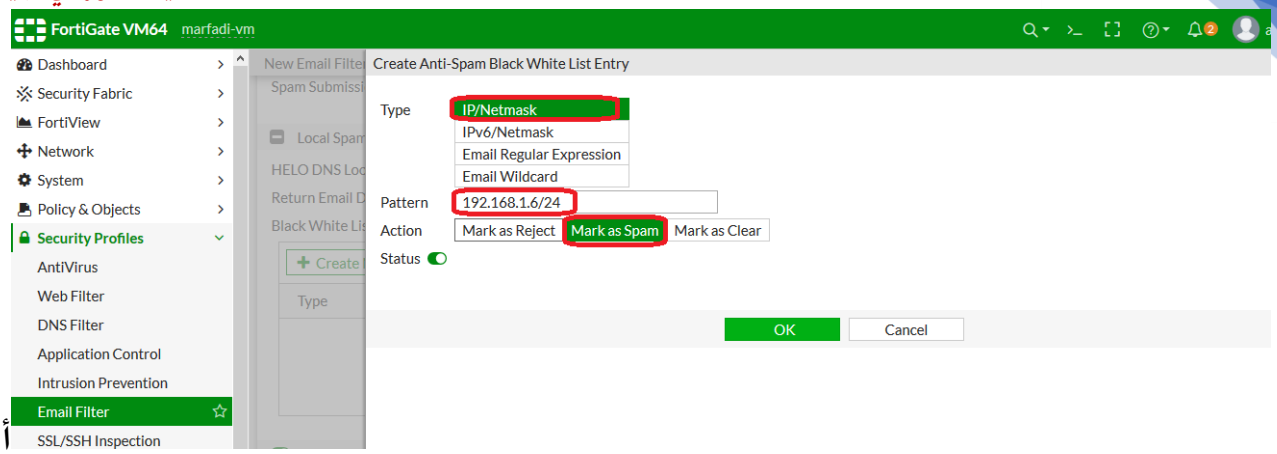
٢- Return Email DNS check

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

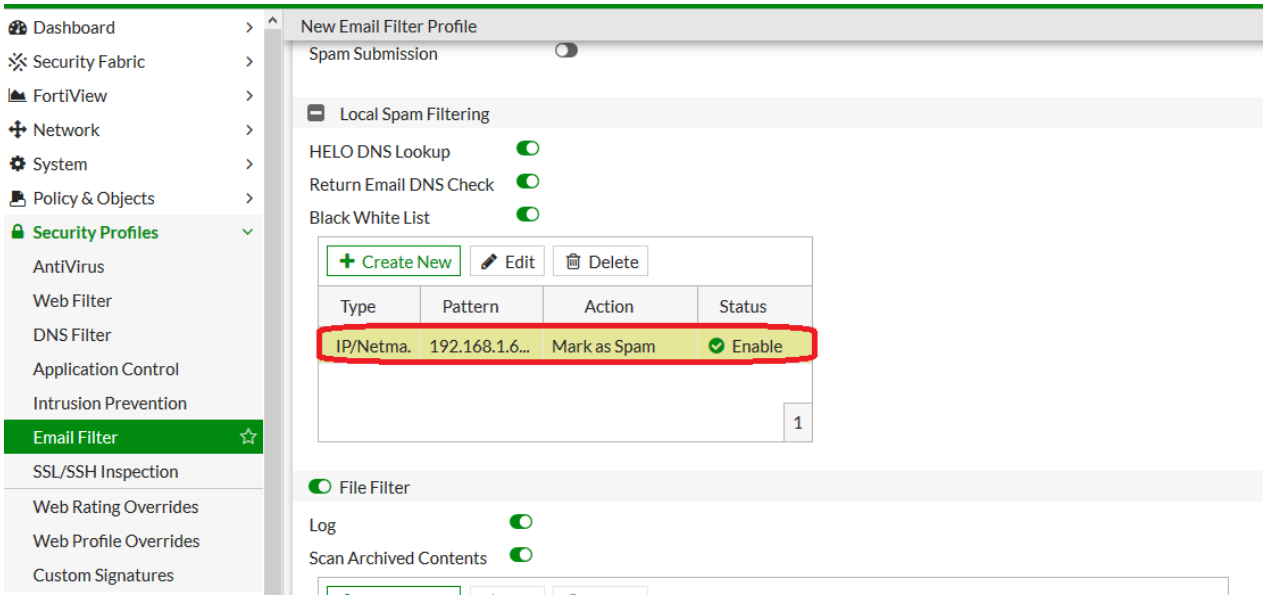




أي

ايميل يأتي من الايبي 24/192.168.1.6 سيتم تطبيق عليه

الـaction=mark as Spam أي علم عليه بأنه اسبام ايميل .



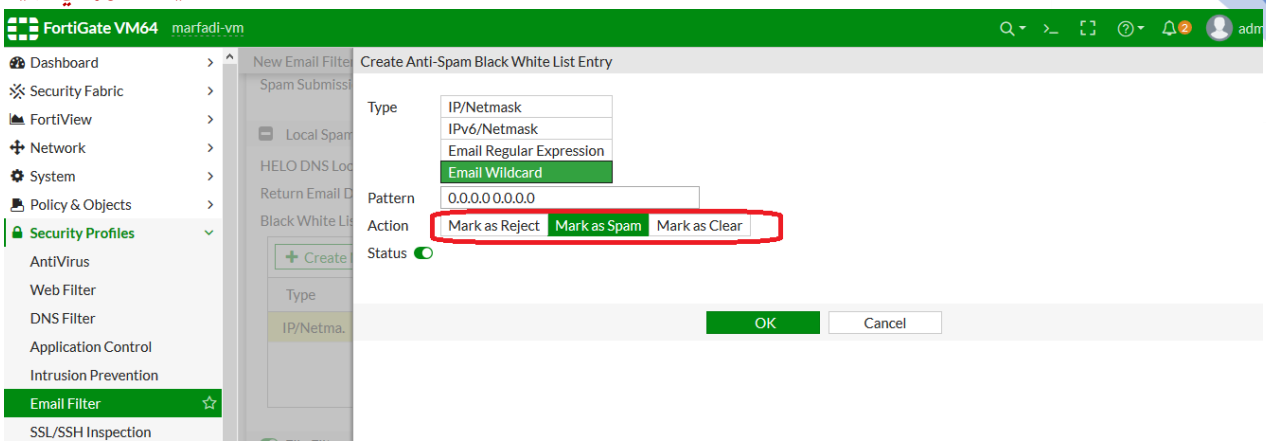
****

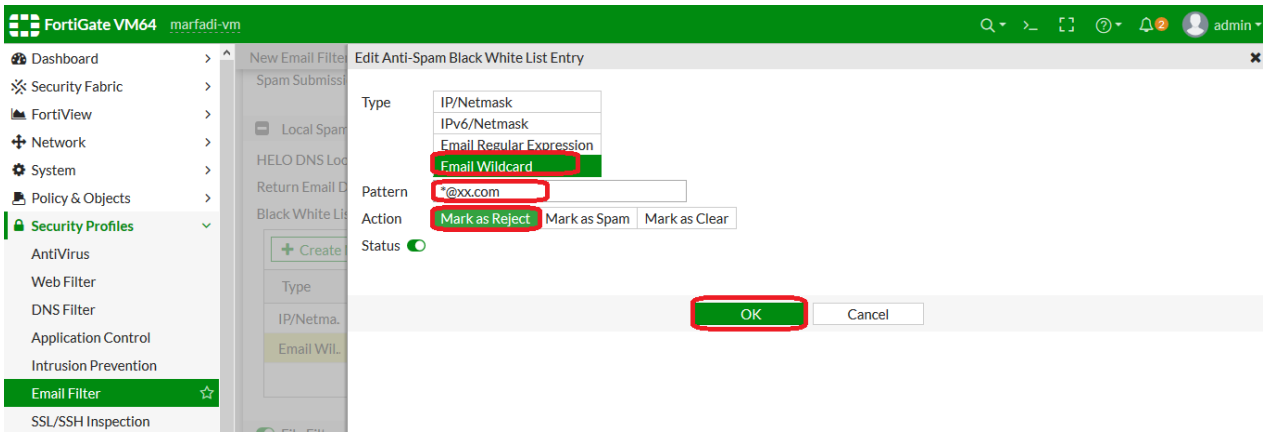
حيث الـ action احدى الخيارات التالية :

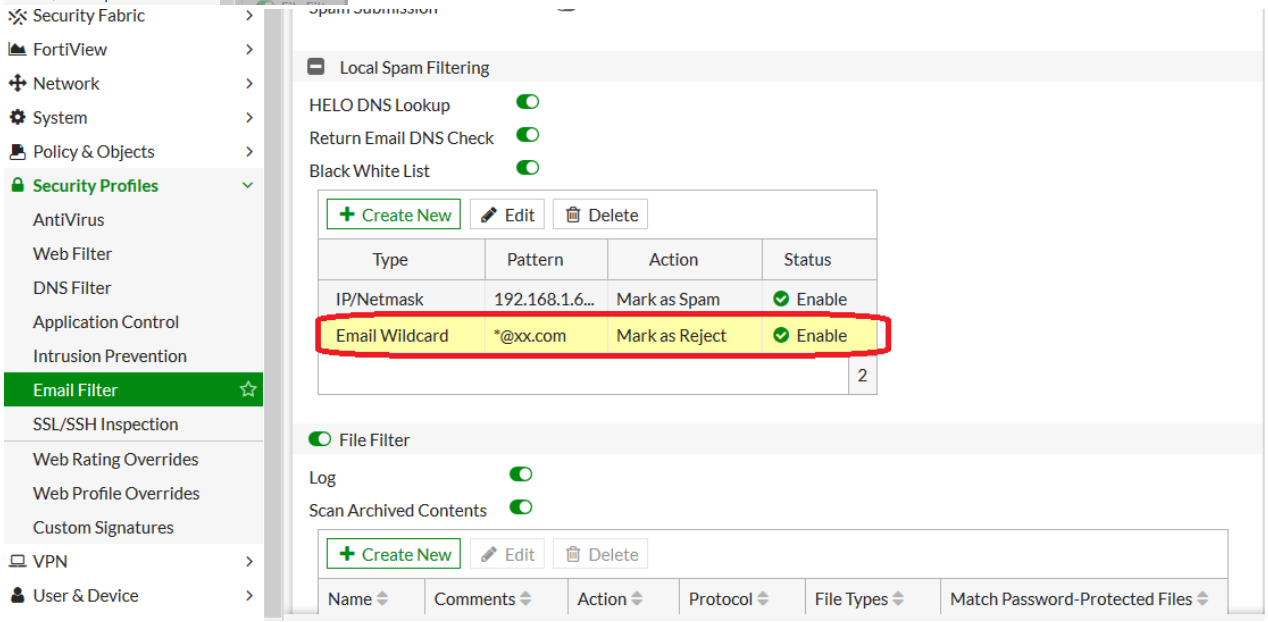
١- Mark as Reject : ارفض الارسال والاستلام من هذا الايميل نهائيا مره أخرى .

٢- Mark as Spam : جعل الايميل ك اسبام

٣- Mark as Clear : مسح الايميل







طريقة الـEmail Wildcard : لو انت تستلم ايميلات مزعجه من دومين معين ايميل محدد فيمكنك استخدام هذه الطريقة حيث هنا يمكن استخدام الرموز مثل * ..

حيث أي ايميل من الدومينXX.COM@* سيتم رفضه ..

طريقة Email Regular Expression :نفس النوع السابق ولكن لا يمكن استخدام الرموز مثل * ..

❖ Logging and monitoring :

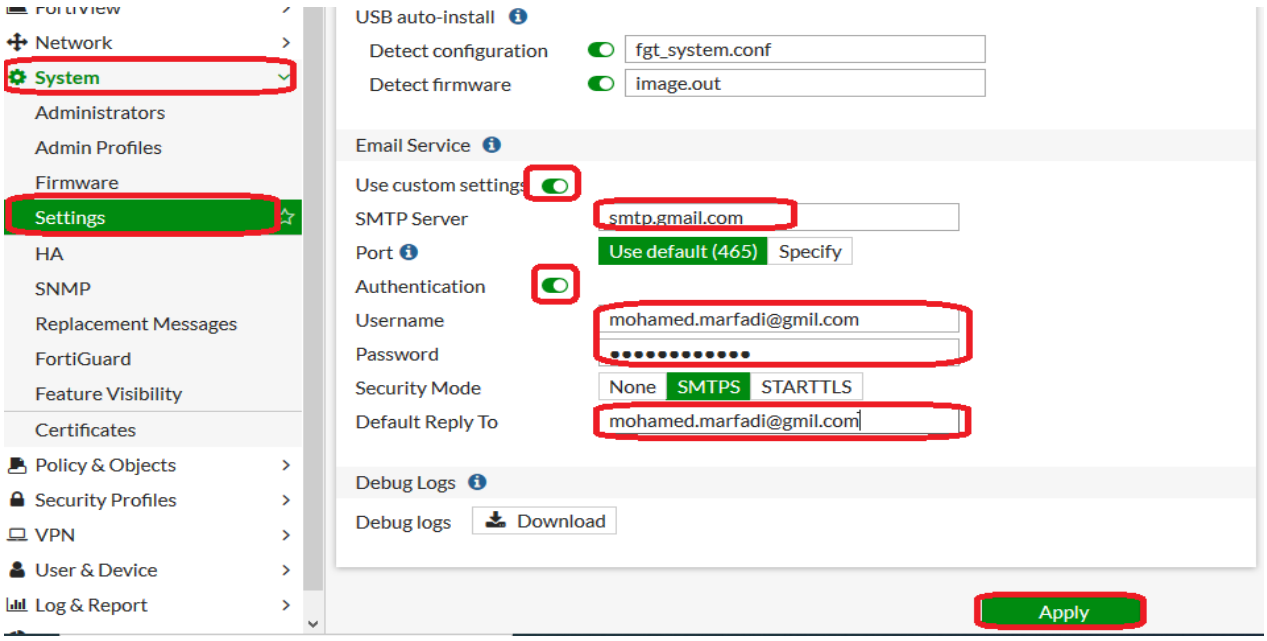
عباره عن ارسال تنبيهات (alert)لمدراء الشبكة الذي يتحكموا بجهاز الفورتي جيت بالأحداث التي بتحدث في الشبكة وذلك كنوع من التحذير والتنبيه والقيام بحدث معين.
حيث في حالة حدوث أي حدث(Event) فأن جهاز الفورتي جيت سوف يقوم بعمليه التنبيه (alert)ولك بالإرسال الى الايميل او الى الموبايل عبر SMS Getaway ..

شروط تنفيذ عمليه logging and monitoring كالتالي :

١. ان يكون الـFortigate device يستطيع الوصول الى الانترنت .
٢. ان يكون لديك SMTP server مثل جوجل او ياهو او أي شركه استضافة مثل blue host او Hostator او غيرها حيث الذي يهمك هو الاعدادات الأساسية لعمليه الارسال مثل رقم المنفذ مثلا smtp =25 ,26,465,587 والإعدادات تختلف من شركه الى أخرى mail.marfadi.com وأيضا تقوم بتحديد الايميل الذي سوف ترسل منه وأيضا الايميل الذي سوف يستقبل رسائل الـalert .
٣. تفعيل عمليه الـevents حيث بشكل افتراضي تكون غير مفعله(deactivate) على الفورتي جيت وأيضا تحدد الاحداث في حالة حدوثها يتم ارسال ايميل (alert) لأيميل يتم تحديده مسبقا ..

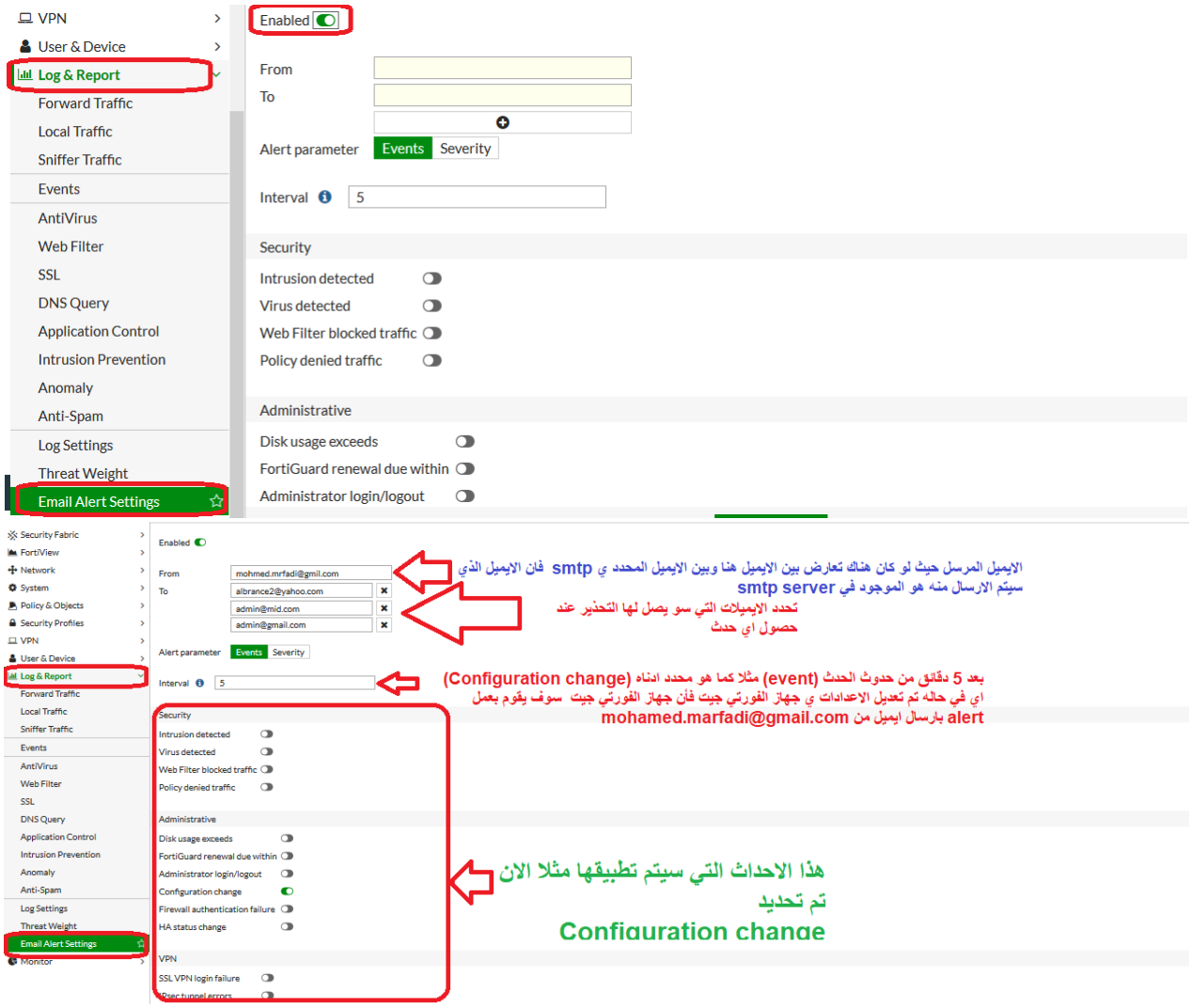
الآن سوف نقوم بتفعيل الـsmtp server على الفورتي جيت مثلا smtp.gmail.com

حيث سيتم الارسال عبر الايميل الخيار *Default Reply To* Mohamed.marfadi@gmil.com



حيث بمجرد تمكين الـ smtp server كما بالصورة أعلاه فأن خيار الـ

Email Alert Settings تظهر لك كما بالصورة ادناه ...



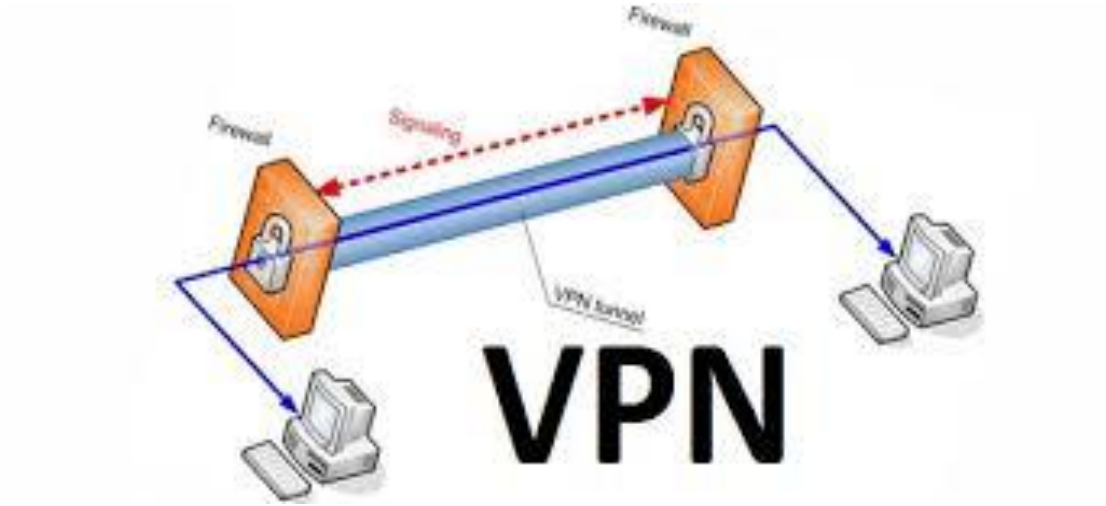
VPN(Virtual private Network)

ما المقصود بVPN ؟

عباره عن شبكة خاصه افتراضيه أي عباره عن تكوين شبكة بين عده اطراف بواسطة الانترنت .

حيث هدف الVPN هو السماح للوصول الى مصادر الشبكة(سيرفرات،طابعات،ملفات،....الخ)عن بعد بواسطة الانترنت حيث تصبح وكأنك موجود داخل الشبكة الداخليه(المحلية).

أي يمكنك عمل شبكة كامله مكونه من عده اجهزه (كمبيوترات،سيرفراتIP 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 الERP من البيت عبر الانترنت .

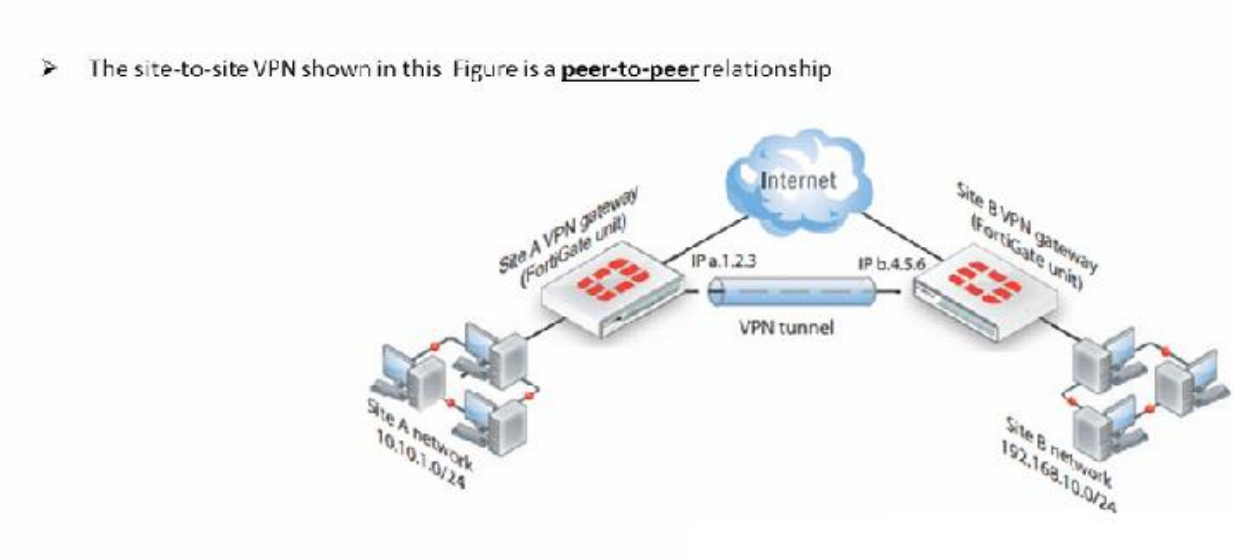


➢ أي بيانات تمر عبر الـVPN تكون آمنه لأنها بتمر ب3 أشياء اساسيه(مميزات) :

١. توفيرقناه (Tunnel) تمرمن خلالها البيانات من المصدرالى الهدف لذا تحقق الموثوقية والأمان .
٢. البيانات بتمربشكل مشفرخلال القناه من المصدرالى الهدف
٣. يكون لها باسورد مشتركه تسمى(pre shared key) ما بين المصدروالهدف .

➢ اشكال الاتصال الـVPN او يسمى (VPN Tunnel designs) :

١. Site-to-site VPN او peer to peer:

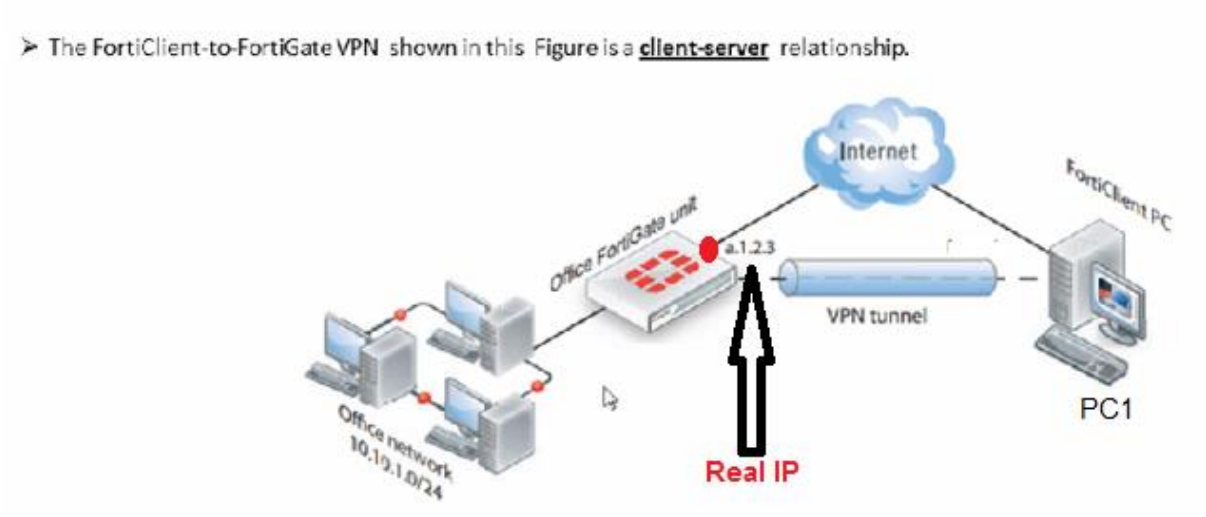


هذا النوع معناه بأن كل طرف لديه جهازفورتي جيت يوجد ما بينهم قناه (tunnel).
حيث كما بالصورة أعلاه يوضح بأنه يجب ان يكون لدى كل جهازفورتي جيت Real ip كما موضح أعلاه الطرف الأول الايبي هو(a.1.2.3) والطرف الاخر(b.4.5.6).

حيث يوجد لدينا كما بالصورة أعلاه 2 فروع (شبكتين محليتين)
24/192.168.10.0 والأخرى 24/10.10.1.0 مع العلم يمكن ان تربط اكثرمن فرع(شبكة)بشرط توفر لديك في كل فرع جهازفورتي جيت وأيضا real ip .

حيث نلاحظ بأن كل شبكة داخليه لها PRIVATE IP مختلف عن الأخرى ولكن عن طريق الـvpn فأن تلك الشبكات المختلفه تتصل مع بعض بشكل طبيعي .

٢. CLIENT-SERVER او يسمى FortiClient-to-Fortigate vpn:



أي ان جهاز pc1 (يجب ان يكون منزل عليه برنامج forticlient) يستطيع الوصول الى الشبكة الداخليه 24/10.10.1.0 وليس العكس .

ملاحظة: pc1 يمكن ان يكون كمبيوتر او موبيل بمختلف انظمه التشغيل .

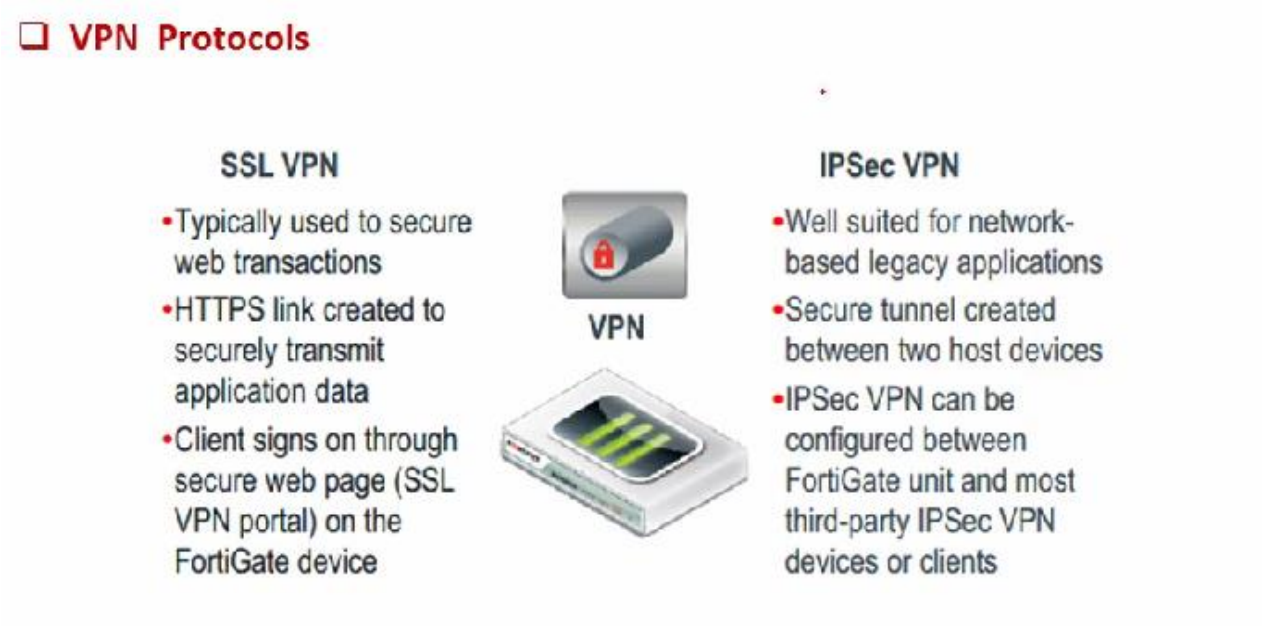
حيث يمكن للجهاز الوصول الى مصادر الشبكة الموجودة على الشبكة 24/10.10.1.0 وكأنك اخذت هذا الجهاز ووصلته بالسويتش الموجود بالفرع البعيد (24/10.10.1.0) .

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 الفورتي جيت والطرف الاخر أي جهاز فايروول يتعامل مع بروتوكولات الـ vpn 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 :



حيث أي فايروول يجب ان يدعم هذه الأنواع من بروتوكولات الـVPN وهما IPSec VPN و SSL VPN

IPSec VPN :تستخدم مع التطبيقات القديمه (windows application)بعكس الـSSL VPN بيعمل ال tunnel مع http link ويستخدم الـ web application مع امكانيته استخدامه مع ال windows application ولكن بشكل نادر..

حيث كليهما يحقق اعلى درجة من الأمان و الموثوقية للبيانات ...

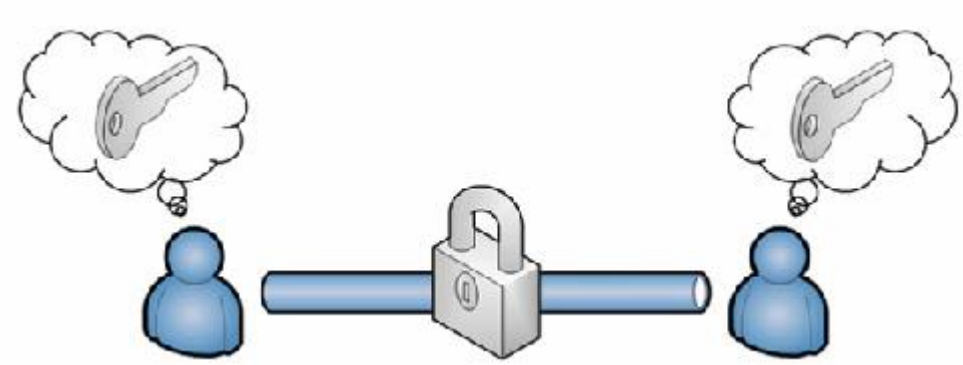
VPN Encryption :

احدى اهم ميزات الـVPN هي عمليه تشفير البيانات التي بتمر من المصدر الى الهدف وذلك لزياده الأمان و الموثوقية .

حيث بتتم عمليه التشفيرفي المصدر(بأحدى خوارزميات التشفير)وعمليه فك التشفيرفي 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



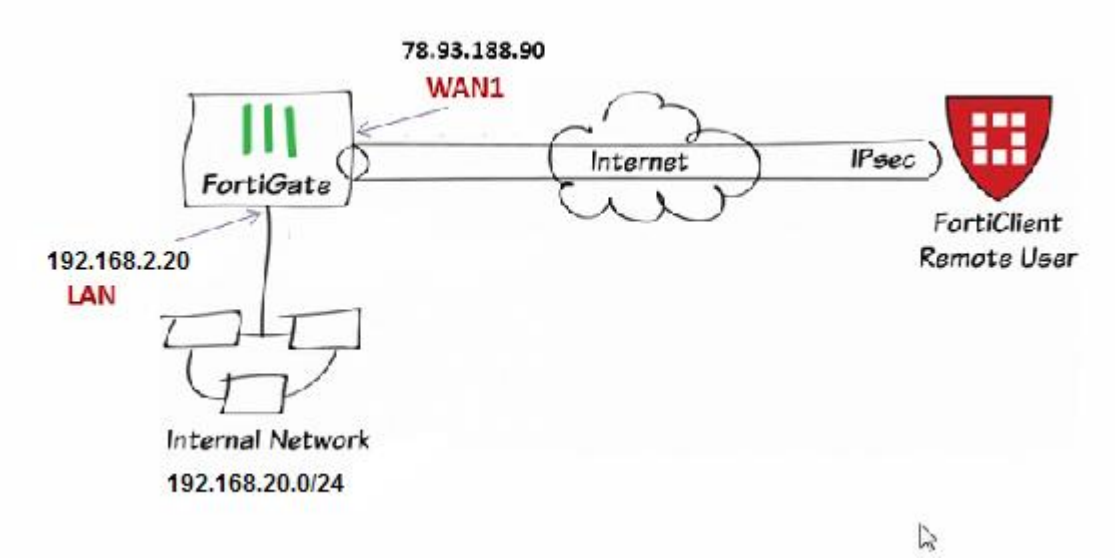
حيث يعتبر الفورتي جيت من اشهر الأشياء التي بتحقق لك VPN server

و الفورتي كلاينت من اشهر الأشياء التي بتحقق لك ان يكون لديك VPN client سواء على اجهزه موبايل اوكمبيوتروبغض النظرعن نوع نظام التشغيل ..

IPSec VPN : يمكن من خلاله ان تقوم بربط فرعين (site to site) او point to site .

SSL vpn :لا يمكن استخدامه للربط بين الفروع بطريقة Site to site بل يستخدم في ربط point to site أي بين جهازكمبيوتر وروتر مثلا يعني لازم تتصل بيوزرنيم وباسورد ..

➢ التطبيق العملي لـ IPSec Client/server :



كما بالصورة أعلاه فأننا سوف نسمح ليوزر(جهاز)بالوصول الى الشبكة الداخيه 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 الموضحه أعلاه .

حيث الجهازسوف يتصل بالايبي 78.93.188.90 عبر برنامج الفورتي كلاينت

. fortiClient

حيث الفكره التي اريد ان احققها هي اني اسمح للجهاز المنزل عليه برنامج الفورتي كلاينت الوصول الى أي جهاز بالشبكة الدخلية وذلك بعد تأسيس الاتصال عبر IPsec بشرط يكون لديه اليوزرنيم والباسورد .

حيث يمكن لعدد كبير من Clients الوصول الى الفورتي جيت بنفس الوقت .

ويمكنك ان تقوم بعمل policy بحيث تحدد الشبكات او الاجهزه المراد الوصول اليها فقط ..

فبهذه الطريقة اصبح الجهاز البعيد(remote user)مثله مثل أي جهاز داخل الشبكة الداخليه ..

ولتطبيق هذا العملية يجب ان تحقق المتطلبات التالية :

١. يكون لدي يوزر محلي على الفورتي جيت (user)حيث هذا اليوزر(الحساب)سوف يتم اعطاءه لليوزر البعيد (remote user)للسماح الاتصال بالفورتي جيت ،كما يمكن انشاء جروبات لتصنيف مثلا جروب للمدراء وجروب للتسويق وجروب للايتي ...الخ حيث ان الجروب ليست شي أساسي ولكن كنوع من التنظيم .
٢. ان يكون لدي عناوين (address) للشبكة الداخليه لتعريف الفورتي جيت بعنوان الشبكة الدخلية لكي اسمح بعد ذلك لأي شخص من خارج الشبكة (remote user) بالوصول اليها .
٣. انشاء IPSec tunnel واحدد فيها preshared key او الشهادة لكي اجعل الاخرين يتصلوا بها .
٤. انشاء بوليسي لكي اسمح للترافيك من الـremote user الى الشبكة الداخليه حيث سيكون لدينا 2 بوليسي

البوليسي الأولى لكي اسمح بالترافيك الوصول من الفورتي جيت الى الشبكة الداخليه وهذه البوليسي يتم انشاءها جهاز الفورتي جيت بشكل اوتوماتيكي بمجرد انشاء الـtunnel

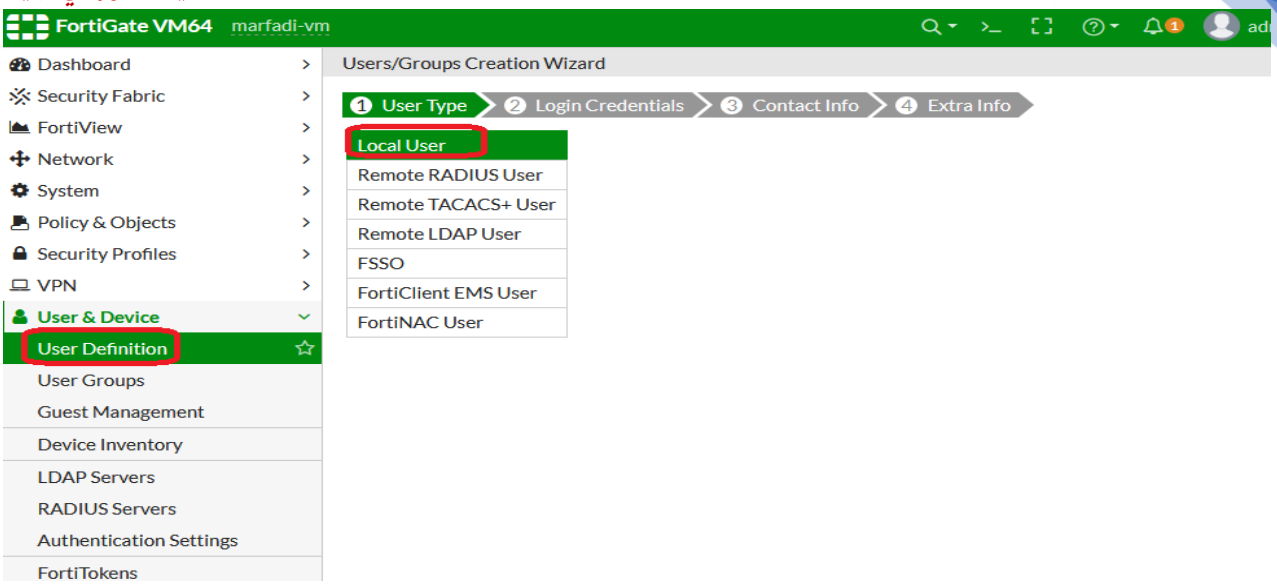
اما البوليسي الثانية سيتم انشاءها بحيث تسمح بوصول الترافيك من جهاز اليوزر(remote user) الى جهاز الفورتي جيت (الى الـwan1 interface)

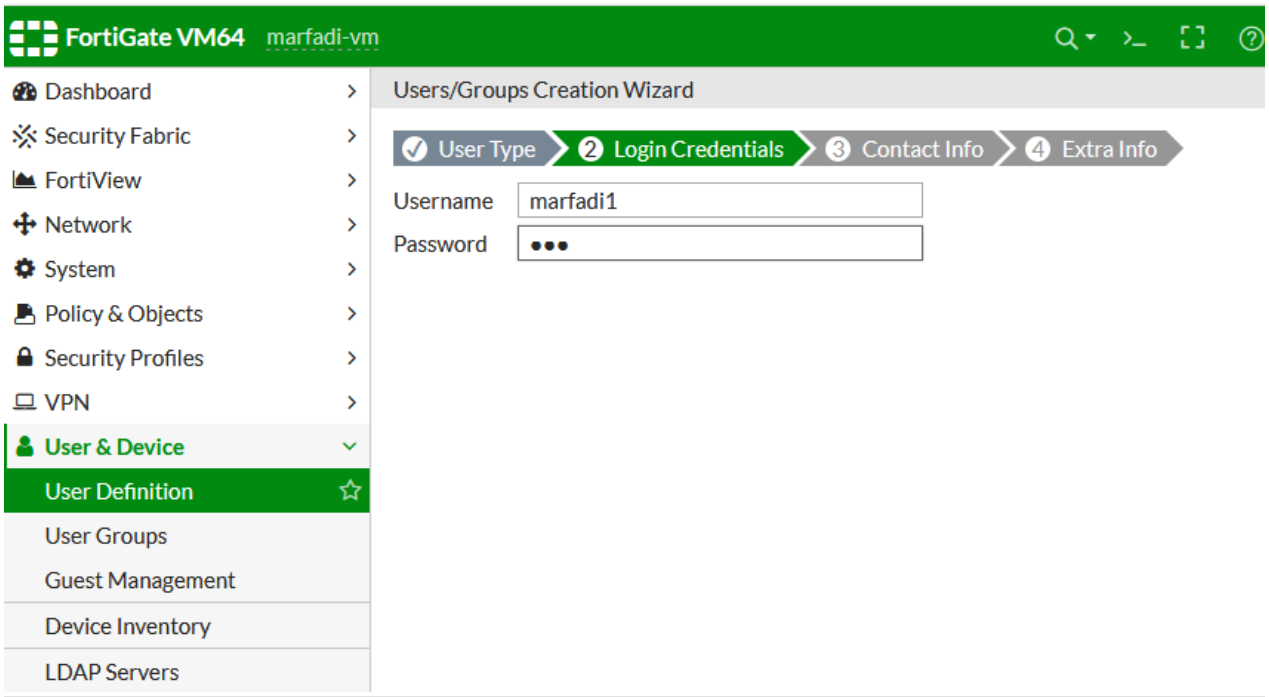
٥. سنقوم بعمل اعدادات معينه لبرنامج الفورتي كلاينت على اجهزه اليوزر(remote user).

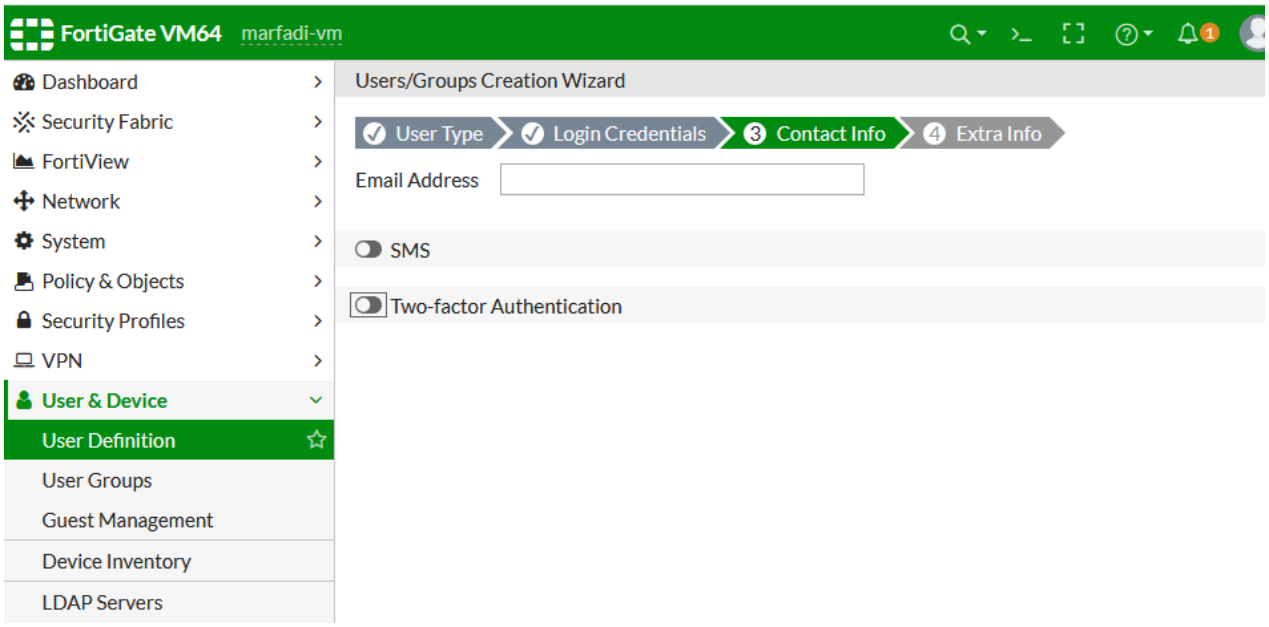
التطبيق العملي :

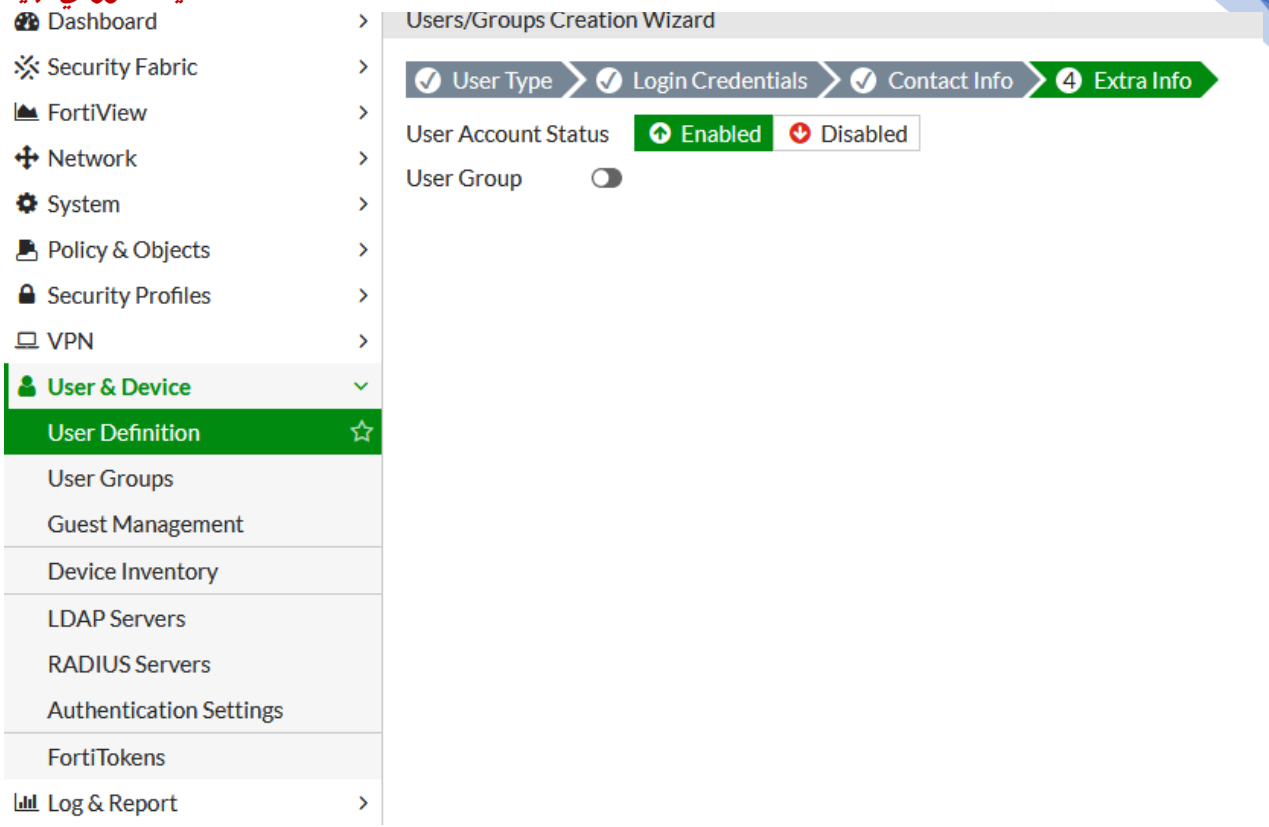
الخطوة الأولى :

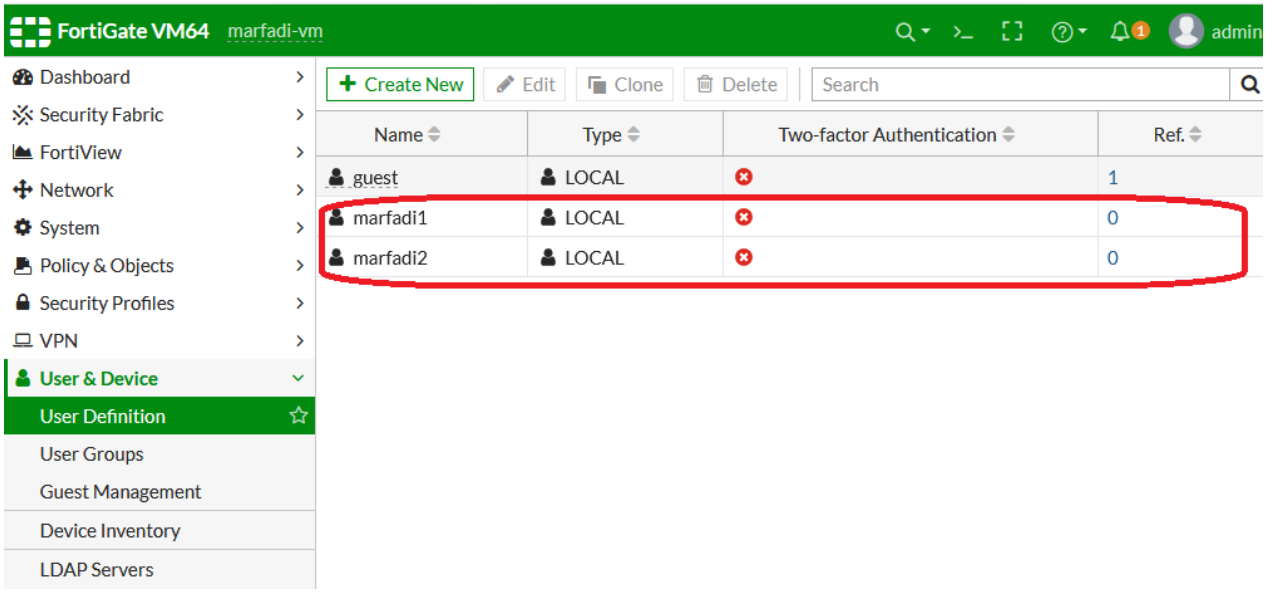
انشاء local user بعدد الأشخاص المراد السماح لهم كما بالتالي :


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
FortiTokens
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


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
Users/Groups Creation Wizard
User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Username
marfadi1
Password

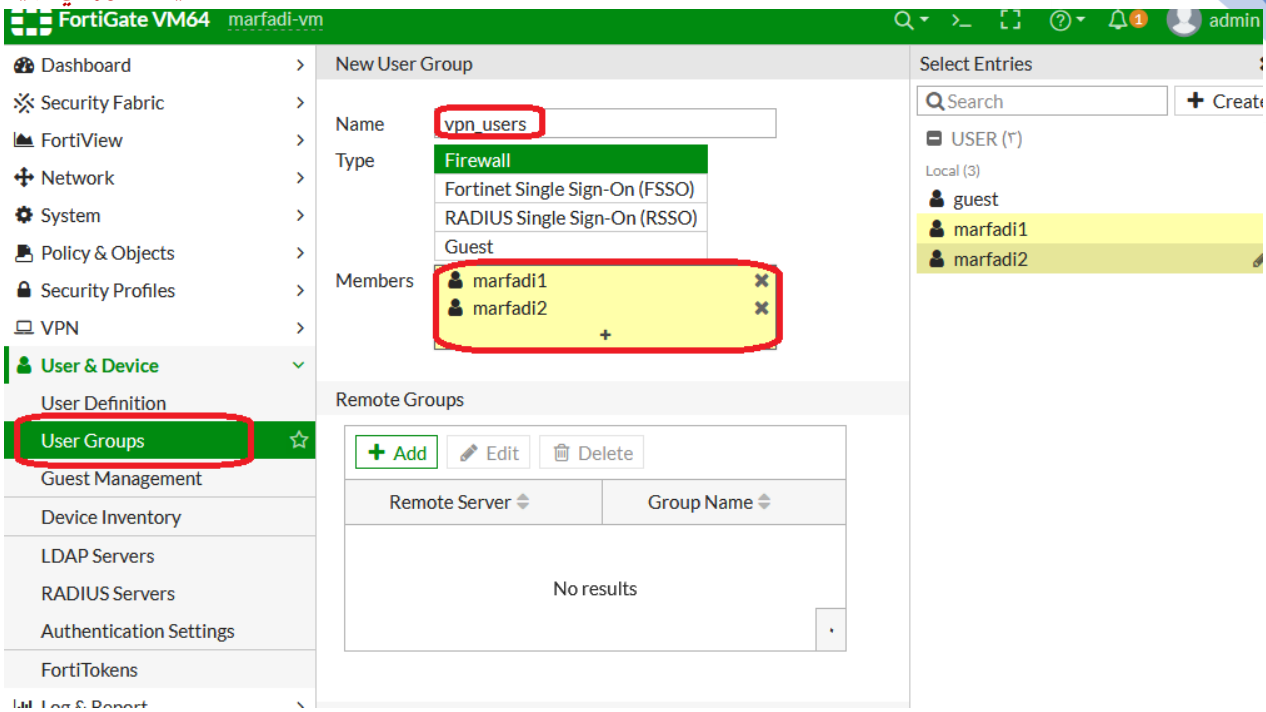

FortiGate VM64
marfadi-vm
Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
Security Profiles
VPN
User & Device
User Definition
User Groups
Guest Management
Device Inventory
LDAP Servers
Users/Groups Creation Wizard
User Type
Login Credentials
3 Contact Info
4 Extra Info
Email Address
SMS
Two-factor Authentication





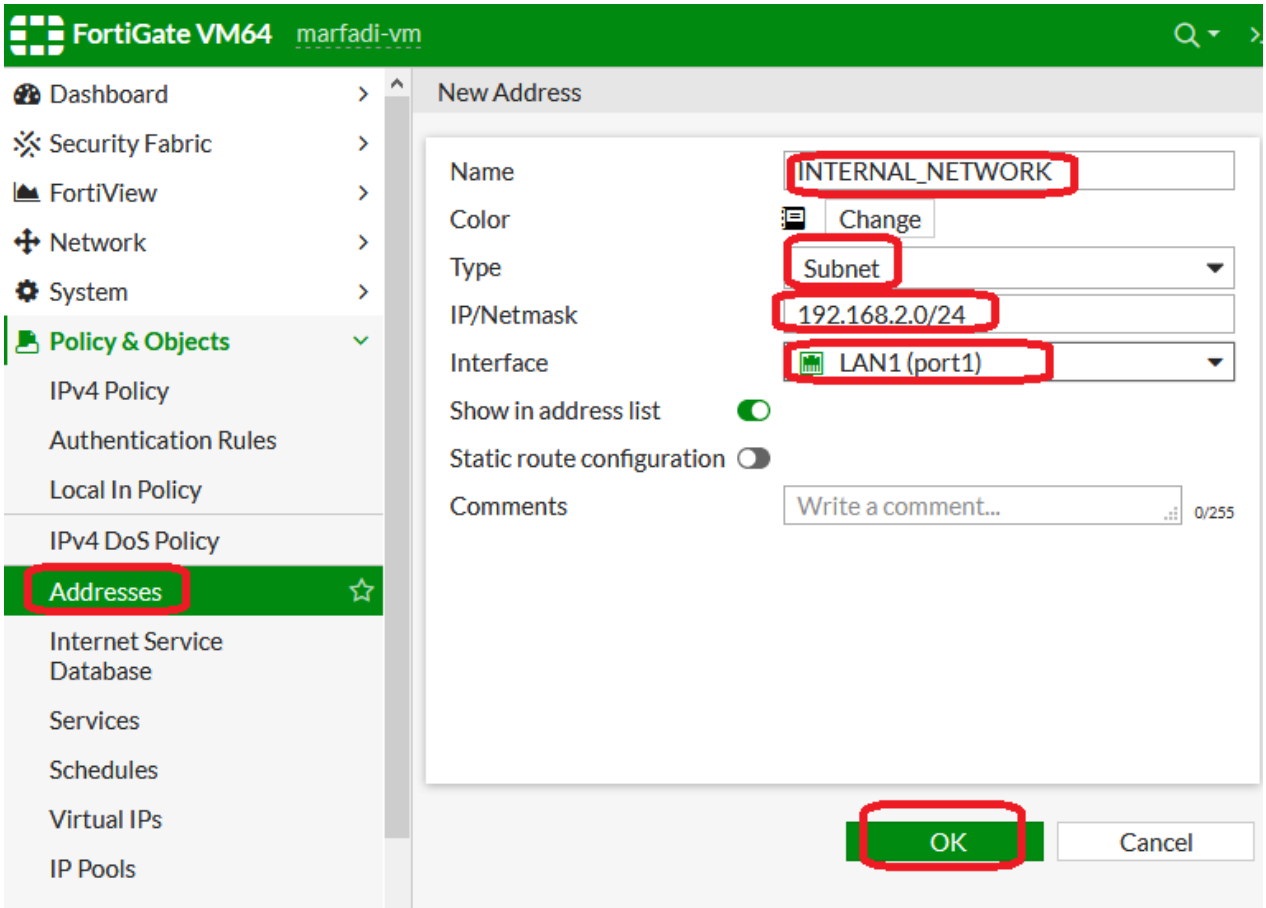
كما بالصورة أعلاه تم انشاء 2 يوزر.

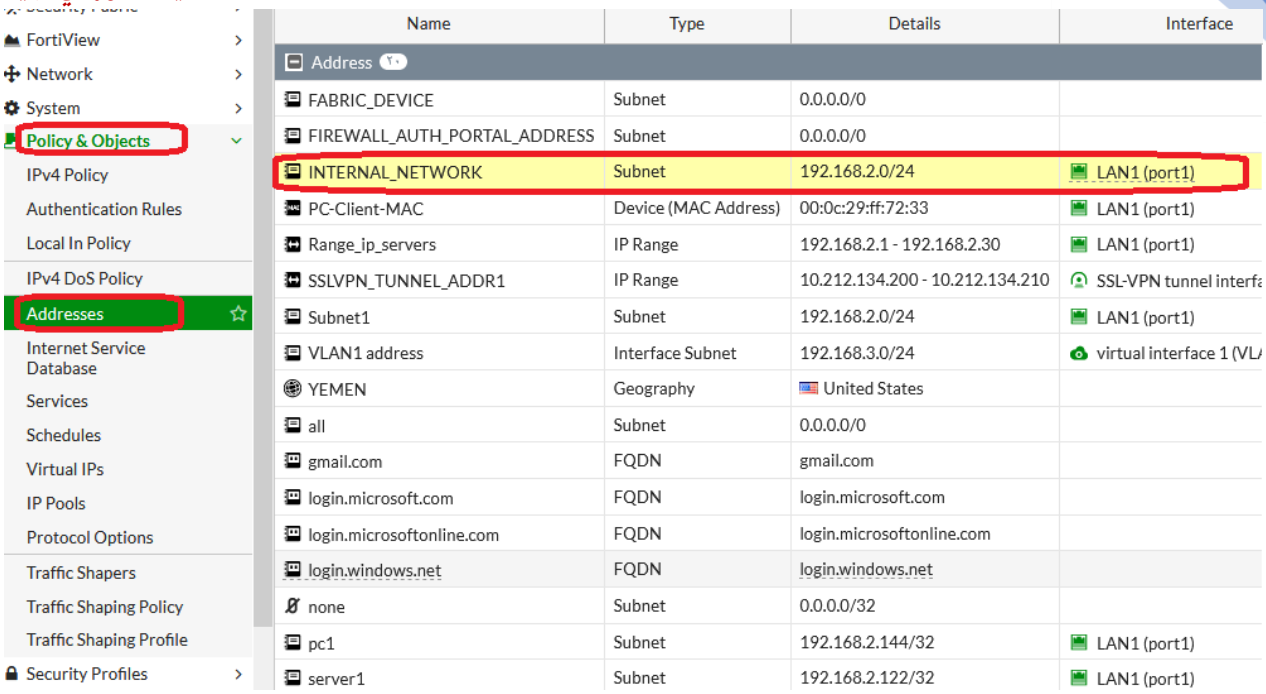
ثم نقوم بإنشاء جروب باسم vpn_users ونضعهما فيه .



الخطوة الثانية :

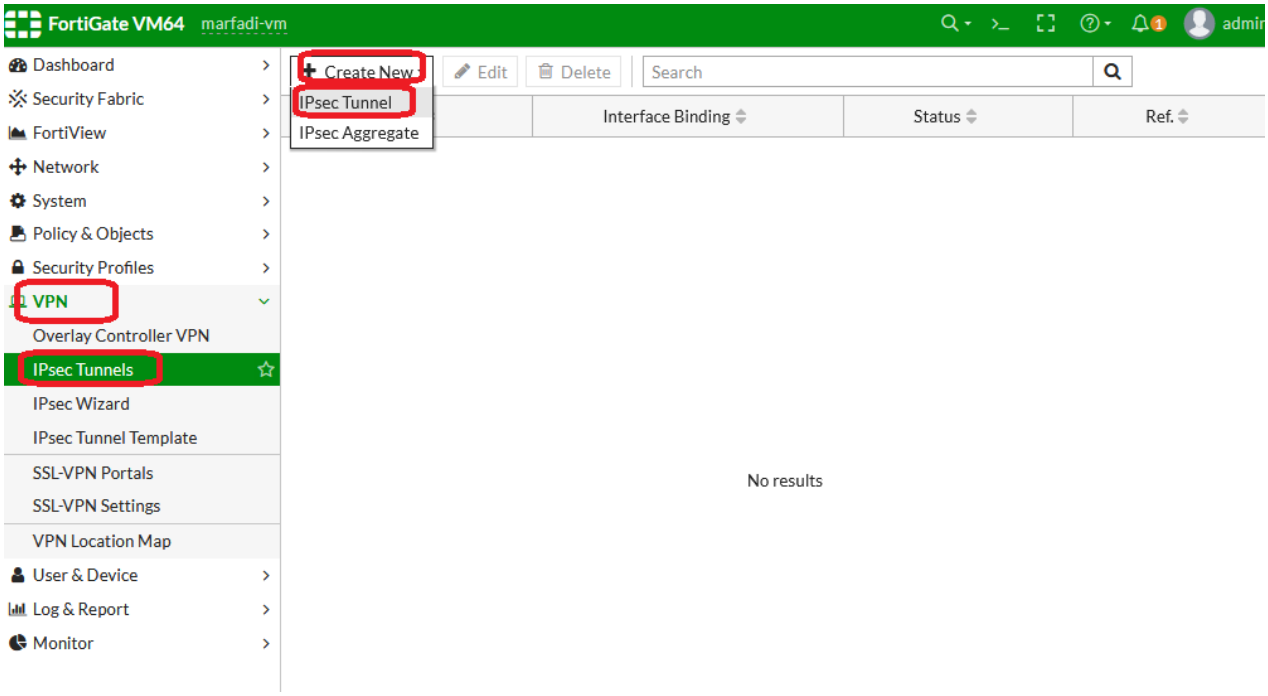
انشاء العناوين للشبكة الداخليه

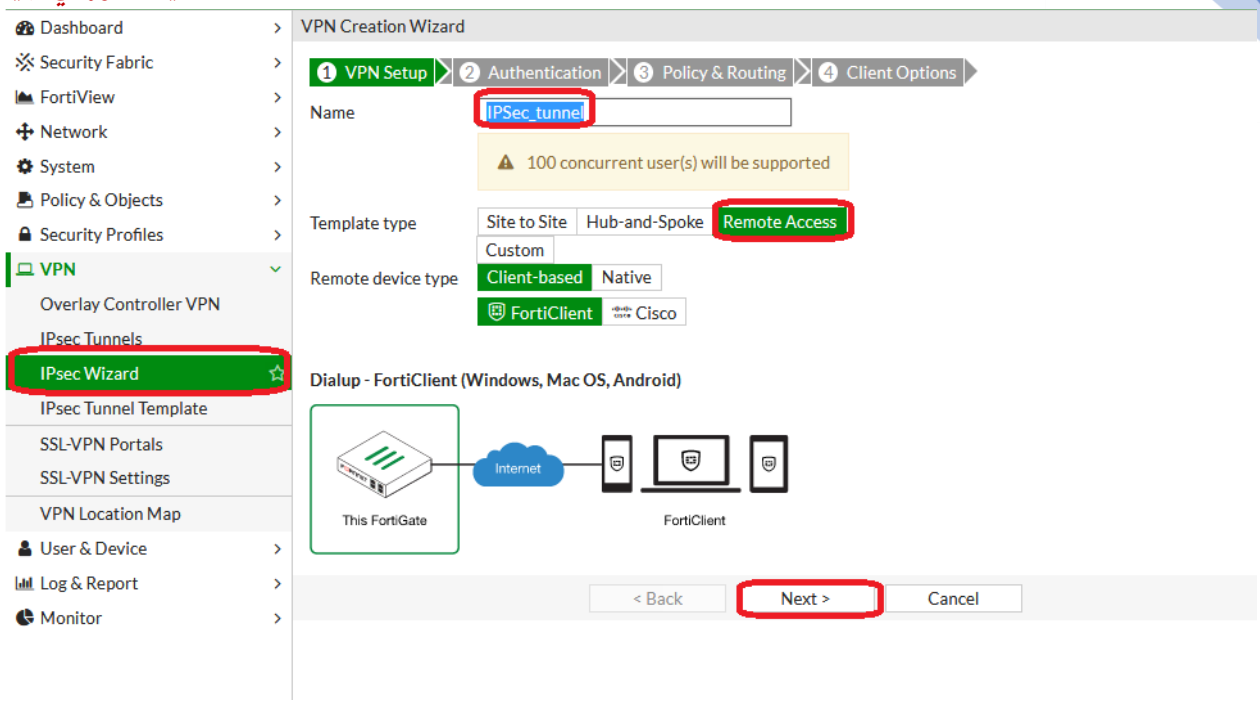




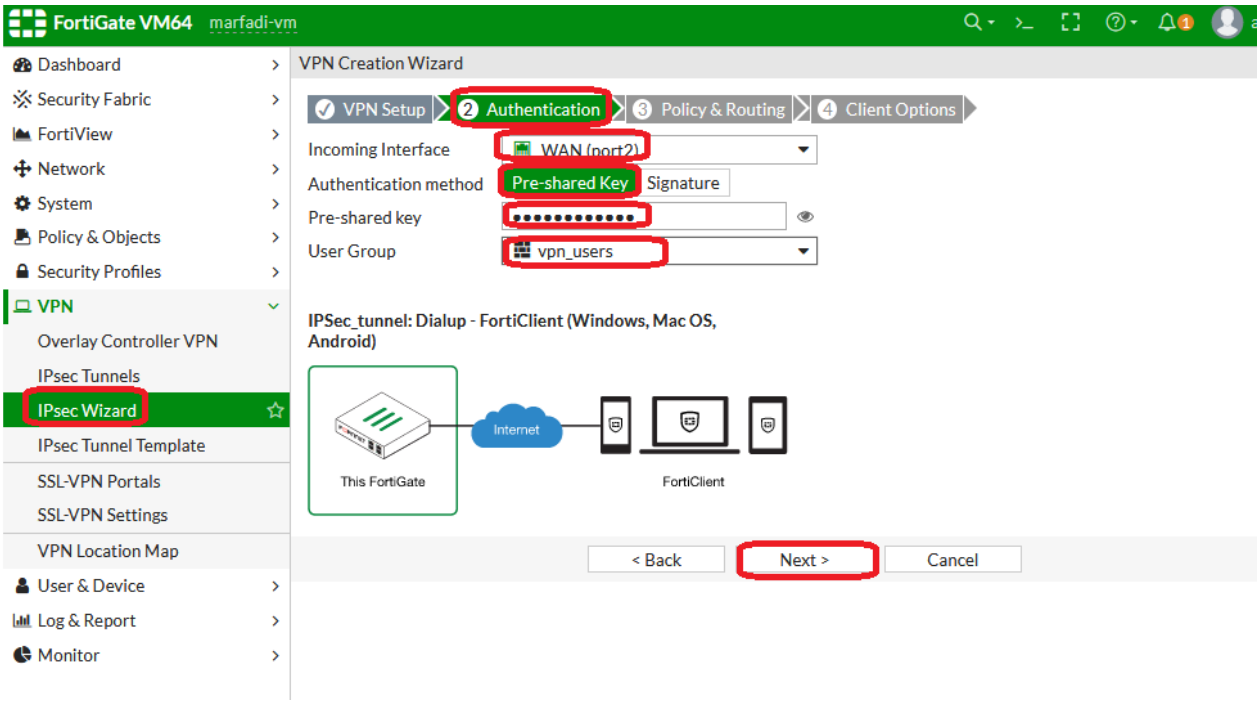
الخطوة الثالثه :

انشاء IPSEC tunnel





حيث تم تحديد اسم للـ tunnel باسم IPSec_tunnel ونوعها Remote Access وكما بالصورة أعلاه فأن اجهزه اليوزر ممكن ان تكون ويندوز او ماك او اندرويد .



كما بالصورة أعلاه تم تحديد نوع الـ incoming interface الذي سيتقبل الاتصال وهو كما شرحنا سابقا سيكون wan1 الذي عليه الـ real ip

وسوف نكتب الـ preshared key التي سيتم إعطاءها للمستخدمين الذي سوف يدخلوا من خارج الشبكة (Remote users)

تم تختار الجروب المسموح لها توصل للـ 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 24/192.168.2.0 .

وتم تحديد الايبيهات التي سوف يحصل عليها اجهزه الـremote users من جهاز الفورتي جيت بمجرد الاتصال بـ vpn وهي 10.10.10.1 الى 10.10.10.5 أي خمسه اجهزه .

وتوجد لدينا خاصيتين :

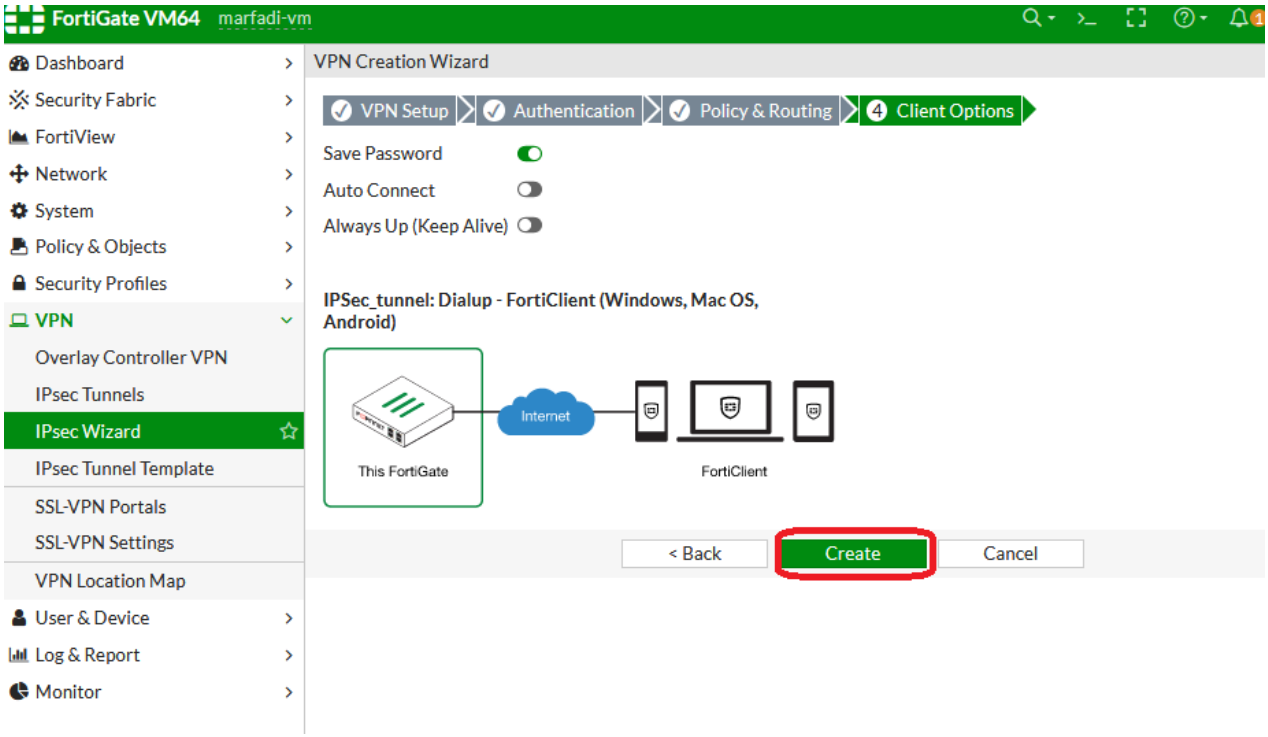
Enable ipv4 SplitTunnel حيث عند تفعيلها فانت تسمح للـremote users بالوصول الى شبكات محدده ..

Allow Endpoint Regsteration عند تفعيها فأنت بذلك تفعل عمليه الـ registration على برنامج forticlient ..

حيث الكلاينت(remote user vpn) يمكن يعمل تسجيل على الفورتي جيت

حيث هذه الخاصية يمكن من خلالها تطبيق بروفايل على هذا اليوزر(الكلاينت)

فبهذا يمكن تطبيق على جهاز اليوزر أي بروفايل (web filter,app control,anti viruse,ips)وكانه جهاز على الشبكة الداخليه وبهذا أصبحت الاجهزه التي تعمل remote vpn مؤمنه أيضا ..



Save Password :

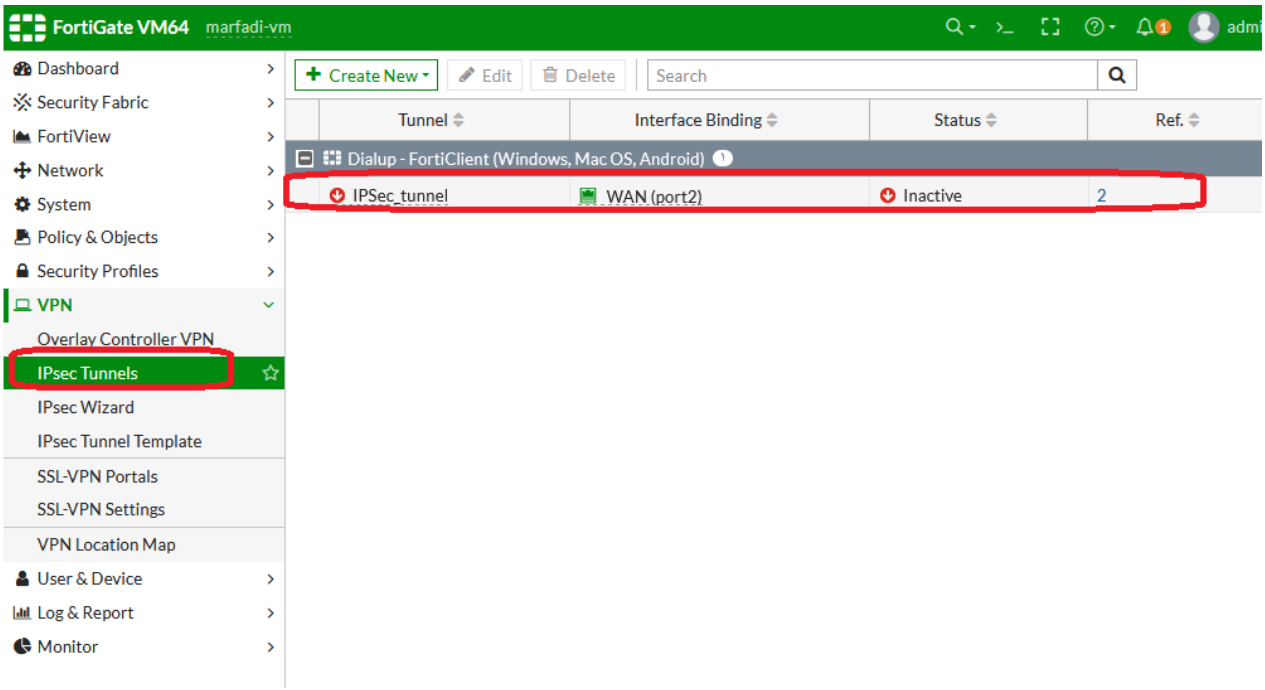
عندما تتم عمليه الاتصال للكلاينت مع الفورتي جيت فهل تريد السماح بعمل save للباسورد على جهازه ام لا !

Auto Connect:

هل تريد بأن تجعل الشخص(Remote user) يعمل Auto connect أي بمجرد ان نظام التشغيل يعمل فانه يتم الاتصال بالفورتي جيت عبر الVPN بواسطة ال forticlient ام لا !!

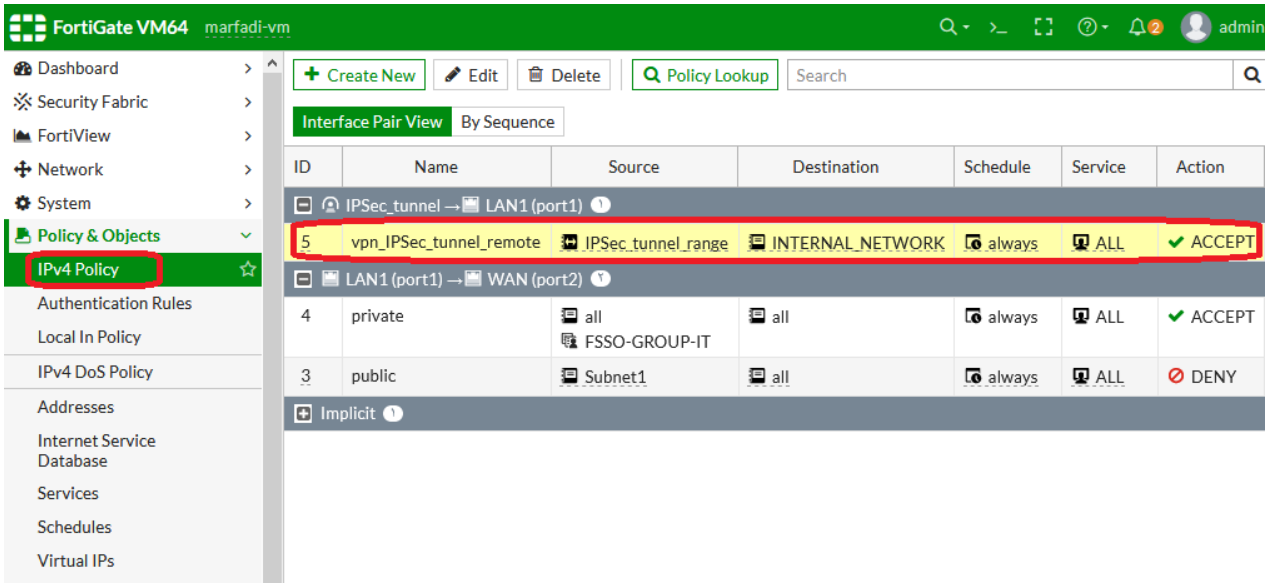
Always Up (Keep Alive) :

جعل الاتصال شغال على طول بحيث لو حصل مشكله او فصل بالإنترنت على جهاز اليوزر فأنه بمجرد ما يعود الانترنت للجهاز تتم عمليه الاتصال مباشره حيث كل 3 دقائق يقوم الفورتي كلاينت بعمل اعاده اتصال ..



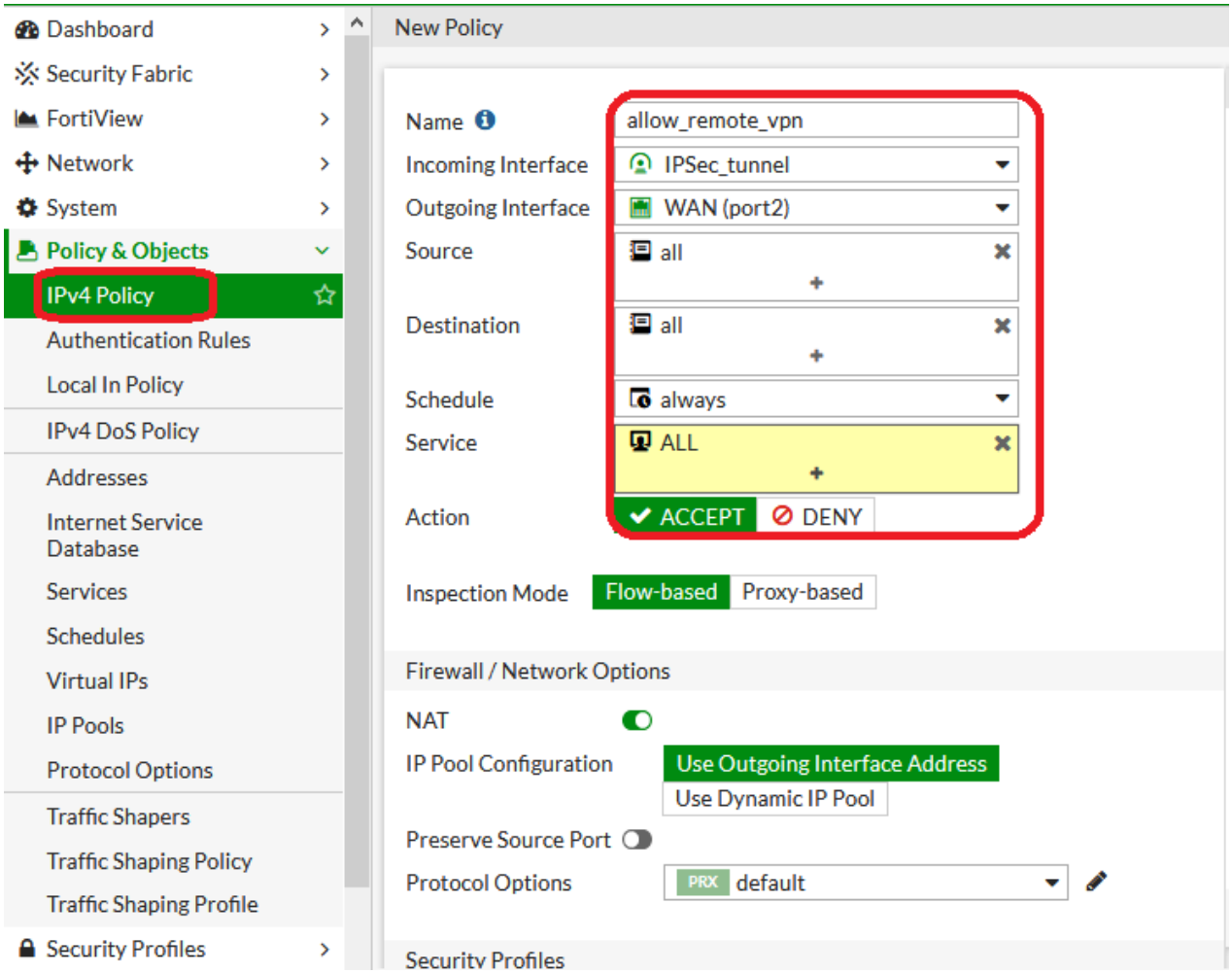
تم انشاء الـvpn tunnel وحالتها Inactive لأن لا يوجد أي اتصال حاليا عليها من أي يوزرفمجرد الاتصال يصبح الحالة active .

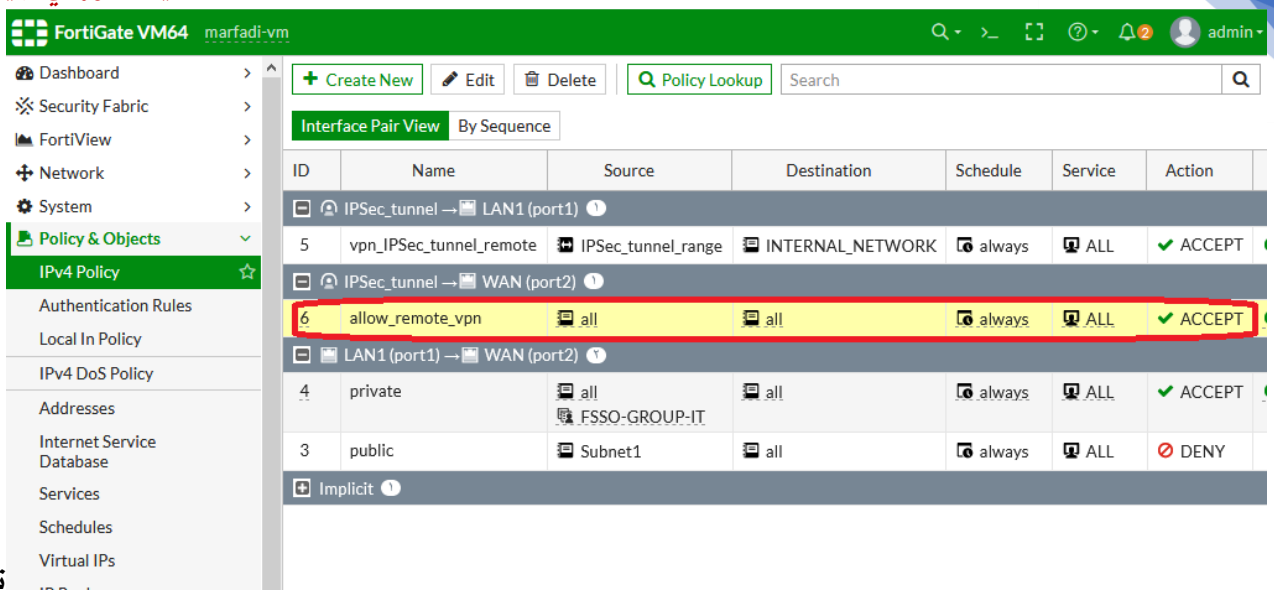
نلاحظ بأنه بمجرد انشاء الـ tunnel تم انشاء بوليسي كما بالصورة ادناه



بعد ذلك يجب ان تقوم بتوجيه الترافيك القادم من الخارج (remote users)الى الفورتي جيت وذلك بإنشاء البوليسي كالتالي :

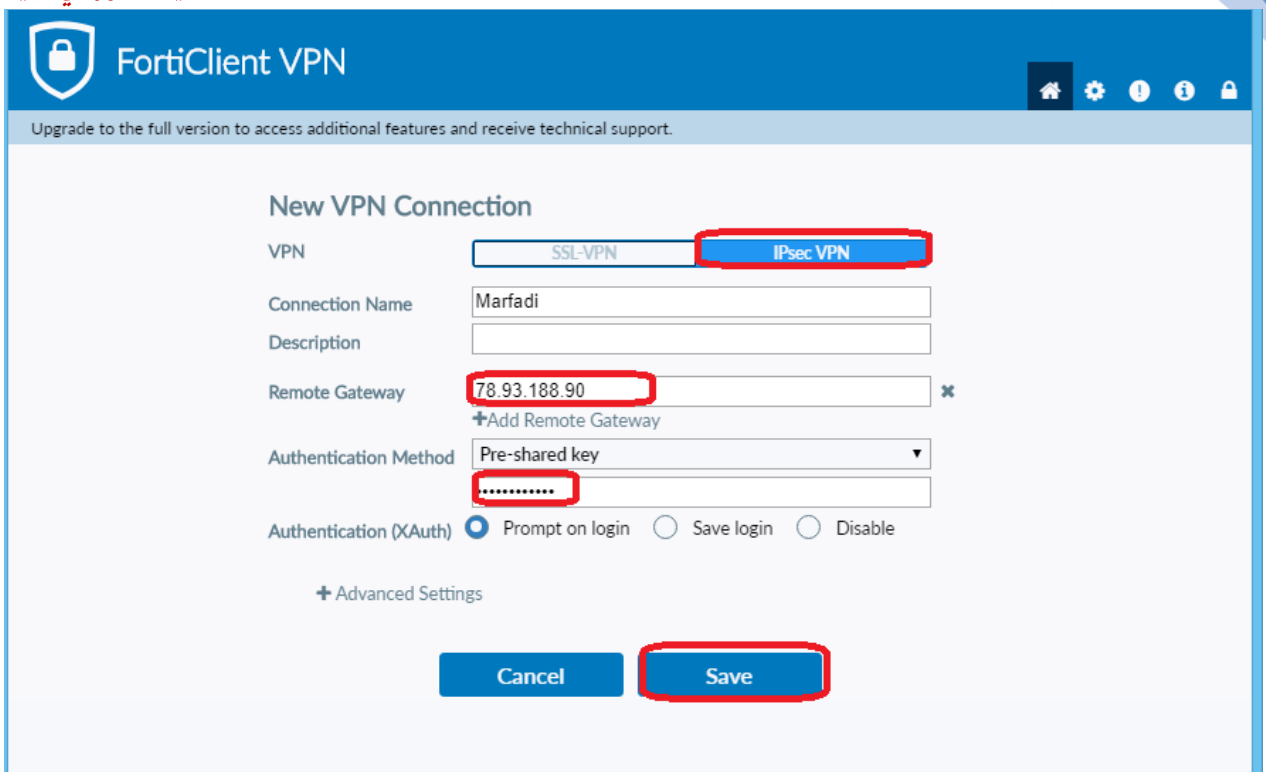
بحيث نقول أي اتصال من ipsec_tunnel وهو الـvirtual interface بأي ايبي سأل على الـWAN1 بأي ايبي اسمح له بالوصول كما بالصورة ادناه





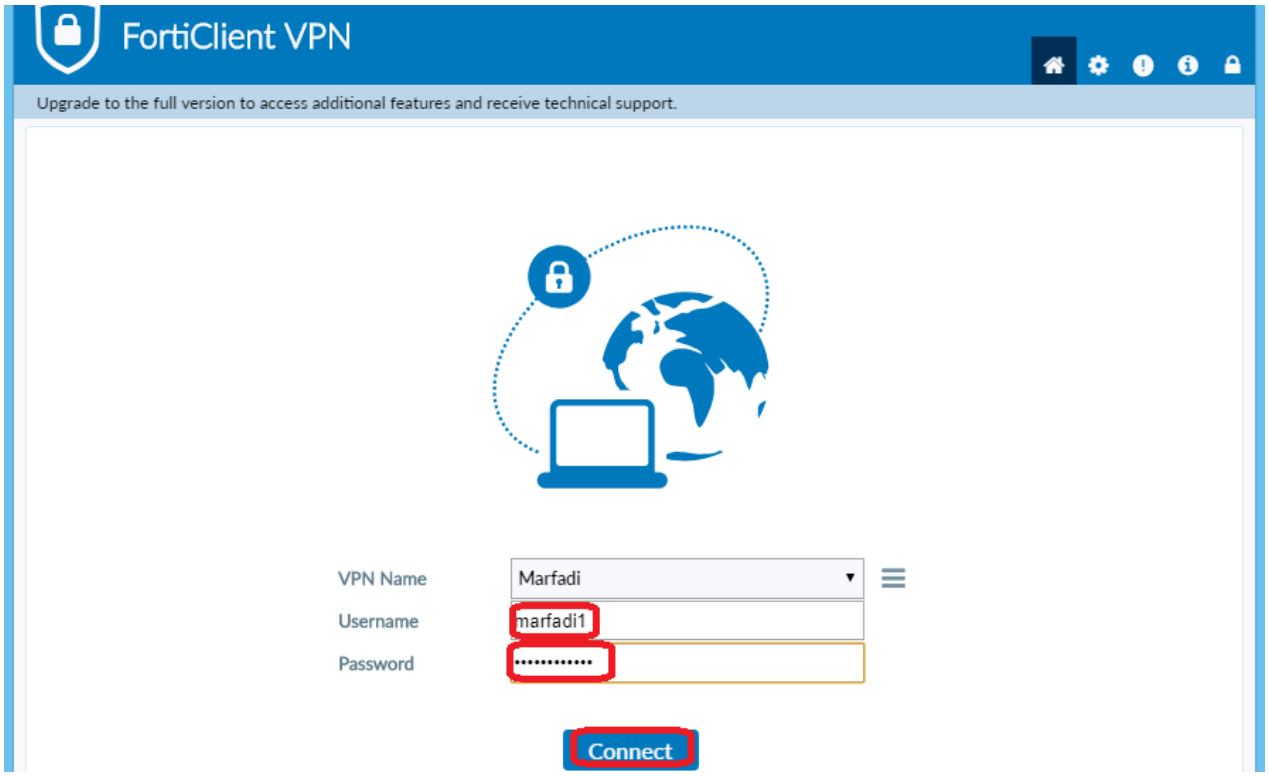
تم انشاء البوليسي وبهذا اصبح جهاز الفورتي جيت اصبح جاهز لاستقبال الاتصال عبر vpn connection

بعد ذلك سوف نقوم بعمل الإعدادات على برنامج الفورتي كلاينت ..

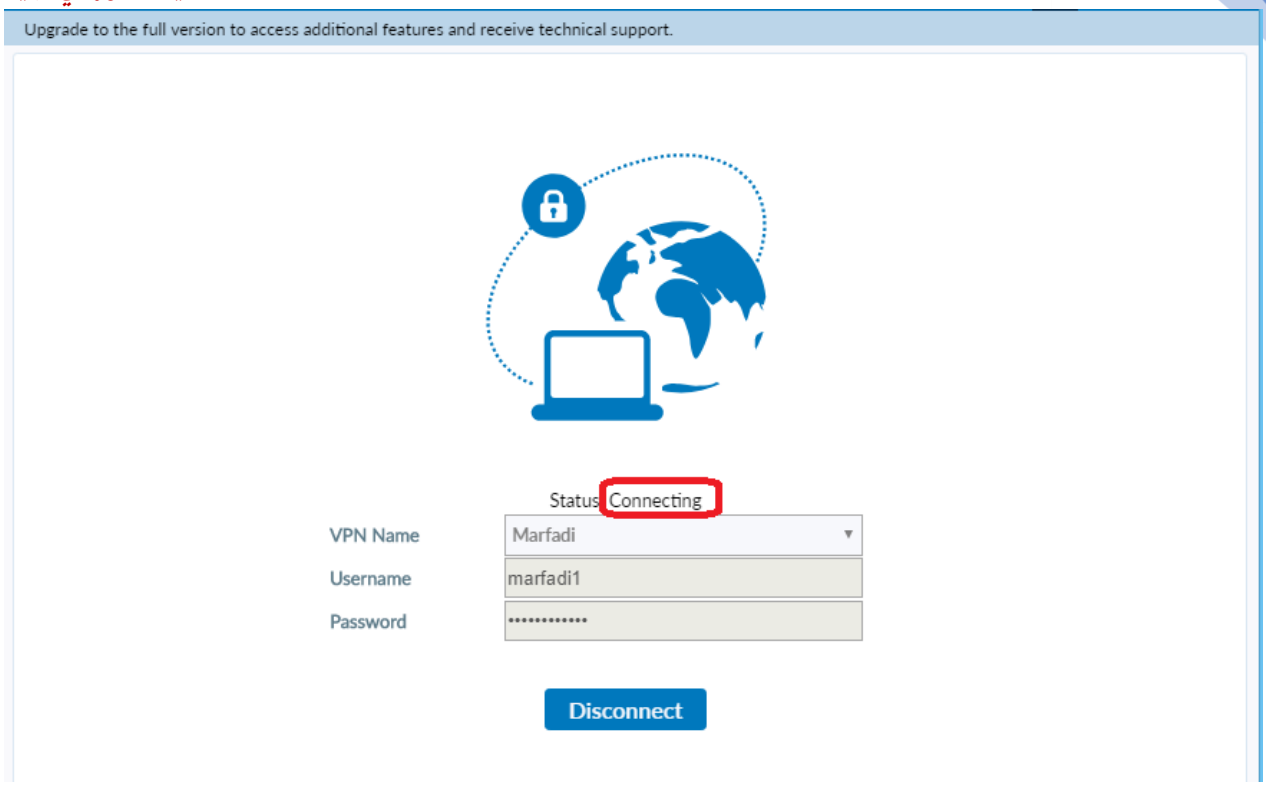


حيث تم تحديد نوع الاتصال هوIPsec VPN ثم أي اسم للاتصال وليكن Marfadi

وremote Getaway هو ايبي WAN1 وهو ل real ip المحدد 78.93.188.90



ثم نقوم بإدخال اليوزرنيم والباسورد لليوزر مثلا marfadi1 والذي قمنا بإنشائه في اول الخطوات ثم نقوم بعمل اتصال ..

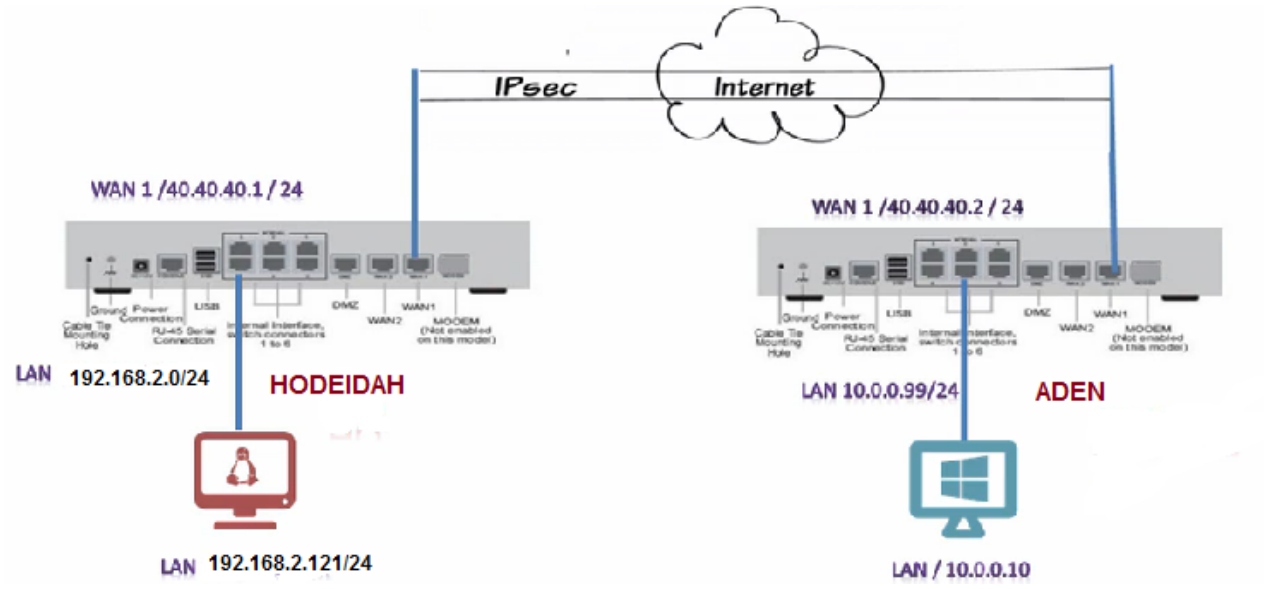


جاااااااااااااري الاتصال ...

للأسف لن تتم عمليه الاتصال لعدم توفر REAL IP لدي ...

IPSec SITE to SITE

ويسمى أيضا PEER to PEER

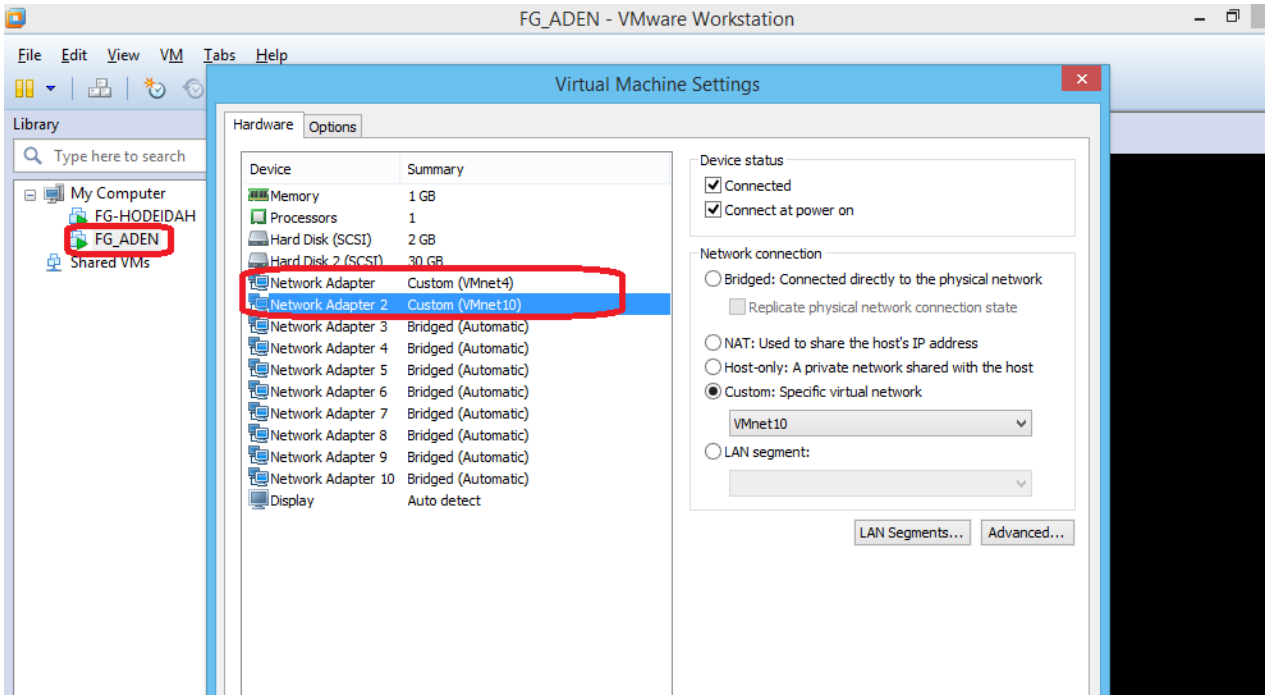


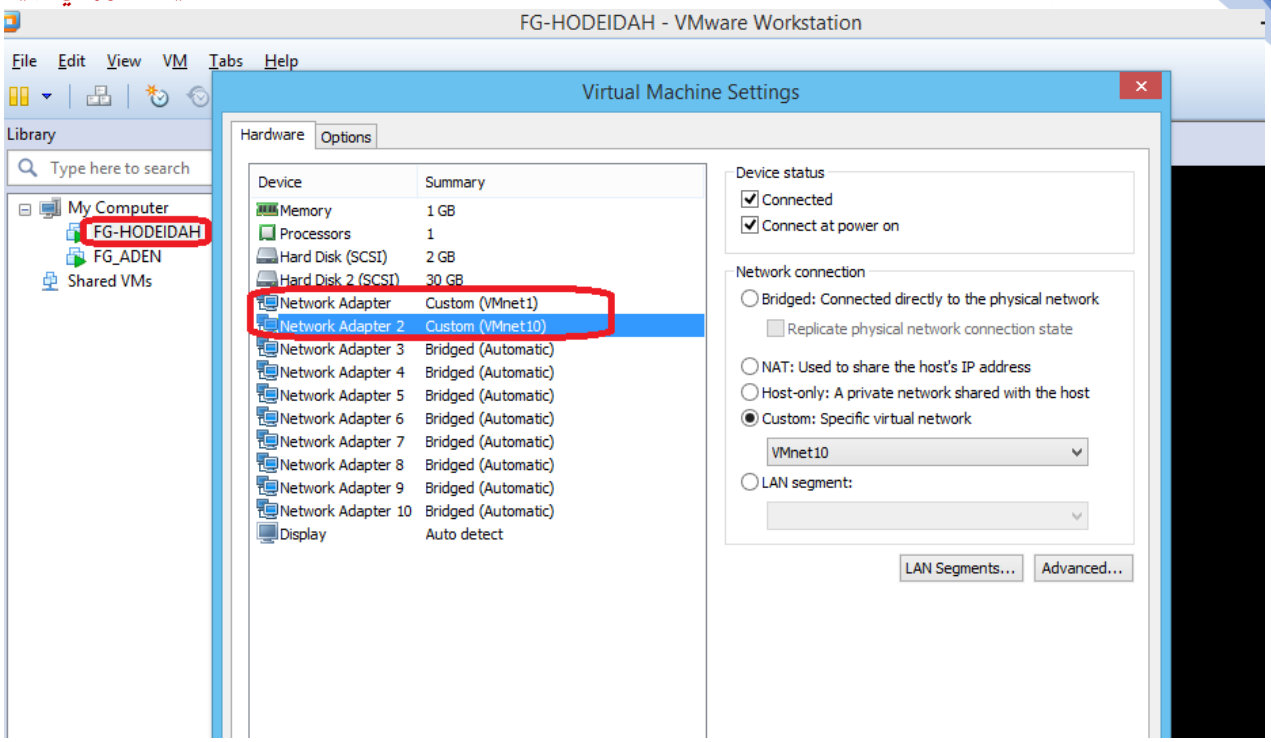
بحسب الصوره أعلاه فأننا سوف نقوم بعمليه ربط فرعين ببعض (الحديده ،عدن)عبر الفورتي جيت بواسطة الانترنت بحيث الجهاز الذي بفرع الحديده يستطيع الوصول بالجهاز الموجود بعدن والعكس ...

نلاحظ بأن هنالك جهاز فورتي جيت في كل فرع وأيضا real ip لكل فرع .

قمنا بأعداد ال vm للفرع ADEN

```
FortiGate-VM64 login:
FortiGate-VM64 login: admn
Password: ***
^C
FortiGate-VM64 login: admin
Password:
You are forced to change your password, please input a new password.
New Password:*****
Confirm Password:*****
Welcome !

FortiGate-VM64 # config system interface

FortiGate-VM64 (interface) # edit port1

FortiGate-VM64 (port1) # set mode static

FortiGate-VM64 (port1) # set ip 10.0.0.99 255.255.255.0

FortiGate-VM64 (port1) # set allowaccess https http ping ssh

FortiGate-VM64 (port1) # end

FortiGate-VM64 # _
```





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 الـVm مربوطين على الانترنت لعمل محاكاه ..

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 .

الـVPN 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 الفورتي جيت تقدم لنا اكثر من طريقة لعمل vpn :

١- vpn over IP SEC

٢- vpn over SSL

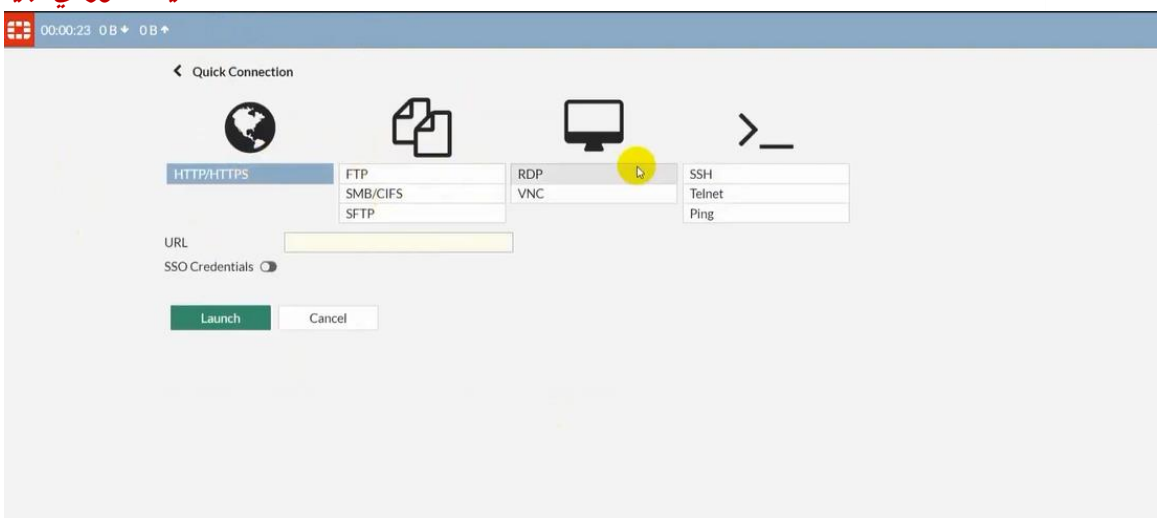
vpn over SSL

حيث الـ vpn/ssl بيتم بطريقتين :

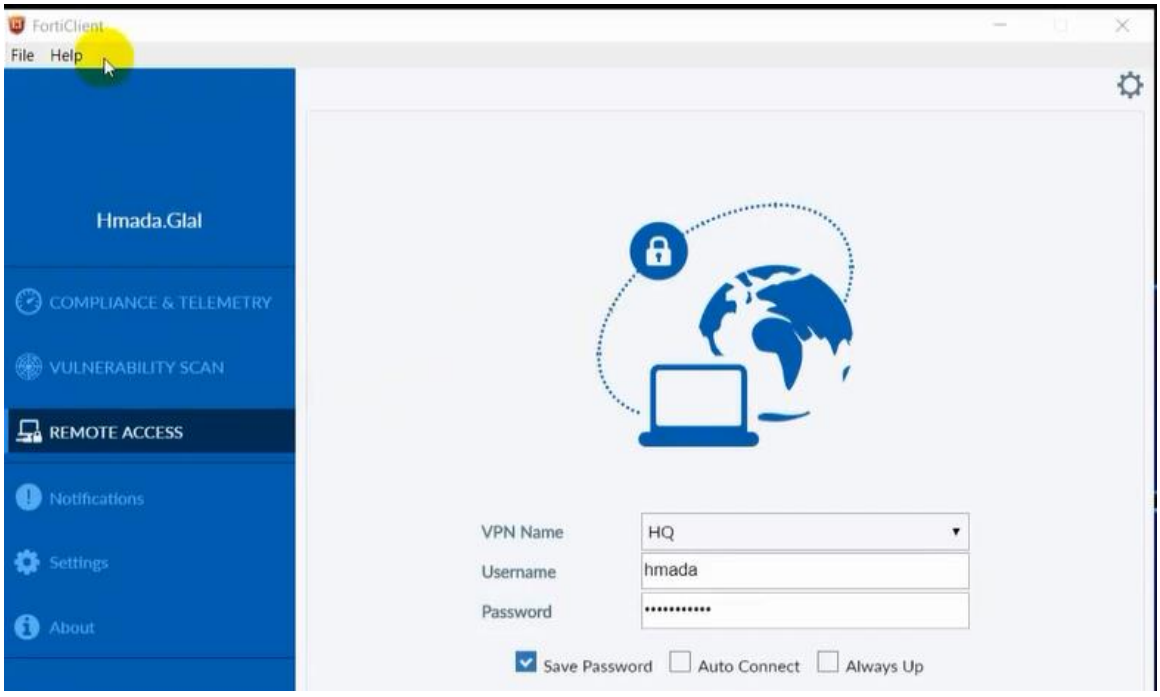
١- ***web mode*** : هي عباره عن صفحة انترنت من خلالها يتم الوصول الى الشبكة الداخليه الخاصة بي واقدر أوصل الى سيرفس معينه انا محددها مسبقا او الى كل الـ services هذا حسب ما تريده وكل هذا بيتم عبر web interface مثلا IE او Mozilla firefox ..الخ

حيث شكل ال web mode كما بالصورة ادناه

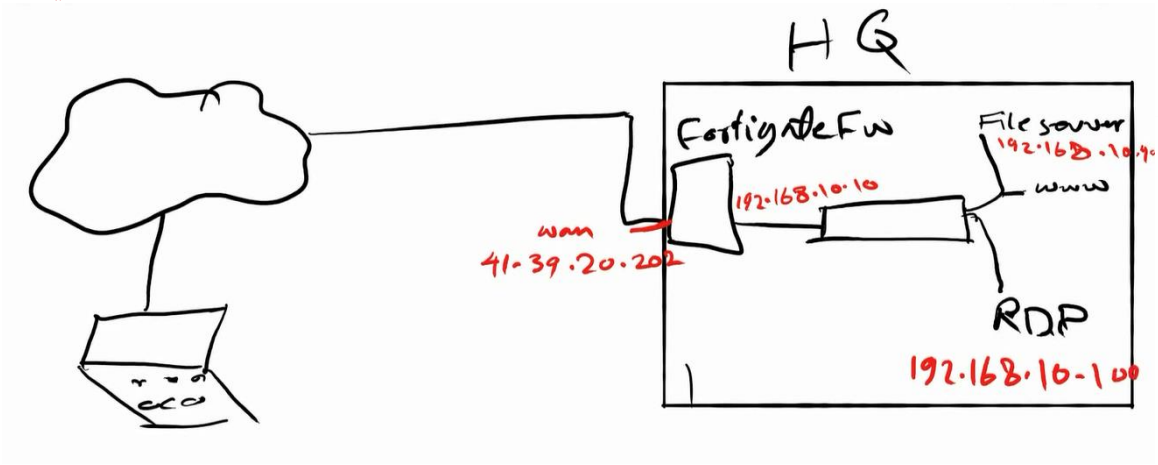
والذي من خلاله يمكنه الوصول الى الـ services كما بالصورة ادناه



٢- *Tunneling mode* : هو الشكل المعتاد الذي من خلاله بعمل vpn حيث فورتي جيت بتستخدم برنامج تابع لها يسمى Forticlient بيتم تنزيله على الويندوز او الماك او اندرويد



كما بالصورة ادناه سوف نقوم بشرح التصميم للـ lab :



حيث نريد الوصول عبر الابتوب الى الفايل سيرفر و باقي السيرفرات الموجودة في الشبكة الداخليه كما بالصورة أعلاه ..

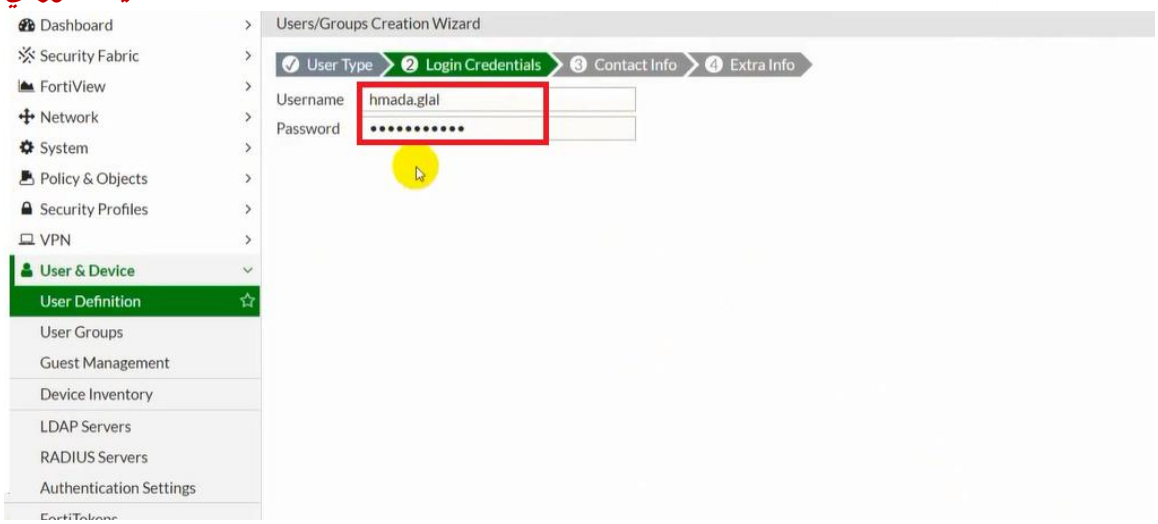
حيث الـ ssl vpn يحتاج بعض الإعدادات على الفورتي جيت لكي يتم تنفيذه :

١- يحتاج الى انشاء local user و local Group لديهم صلاحيه الـ vpn

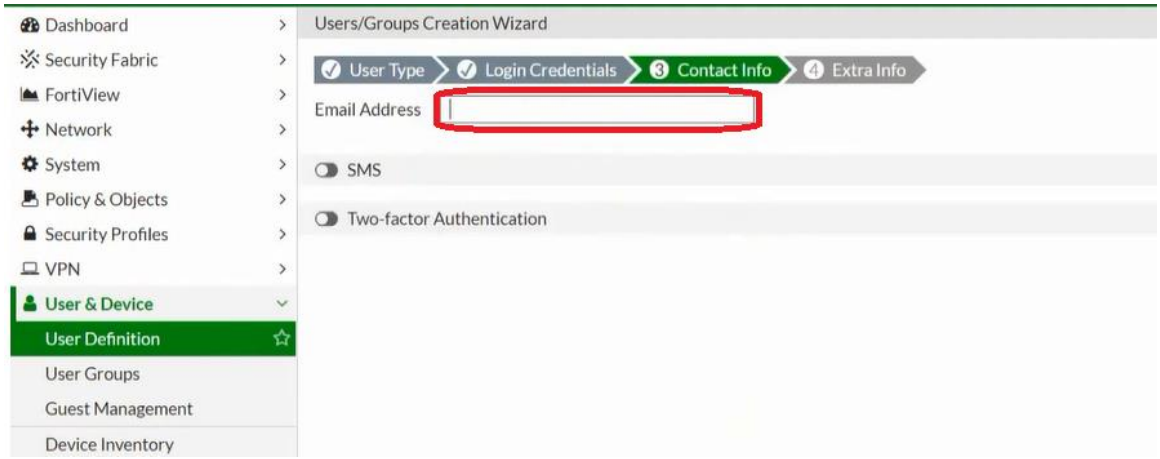
٢- Listen interface وهو الـWAN يكون عليه real ip

٣- Security policy تسمح بمرور الترافيك ما بين الشبكة الداخليه والـvpn وما بين الـvpn والانترنت لو اردت اجعل المستخدمين الي برع الشبكة مثلا جهاز(الابتوب)يستخدم الانترنت من خلال الشبكة الداخليه الخاصة بي .

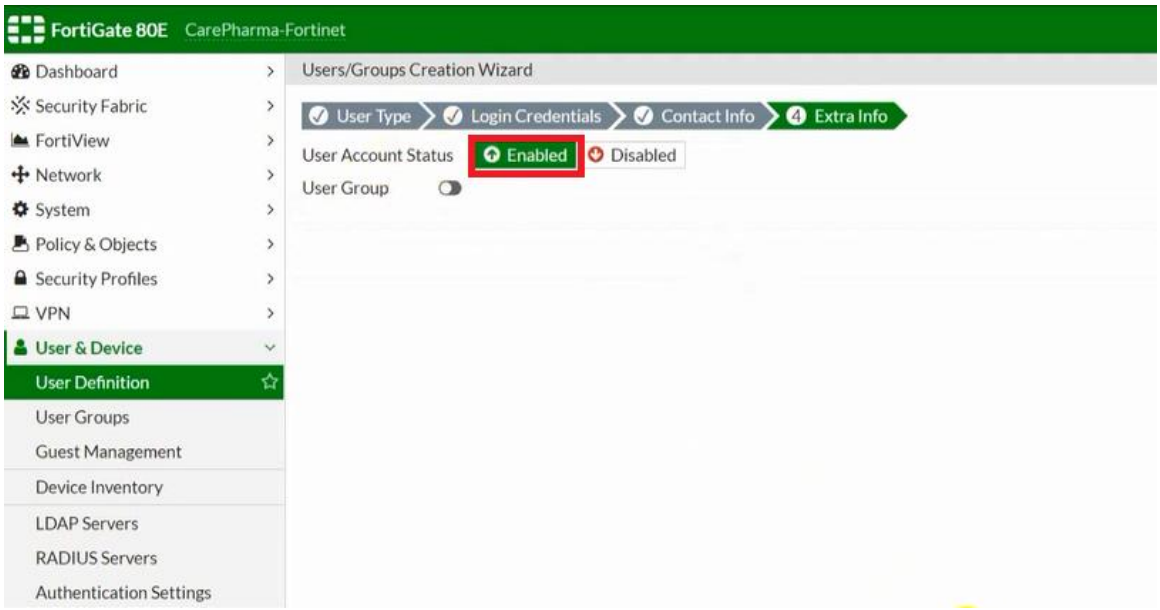
الان سوف نقوم بعمليه التطبيق عمليا :



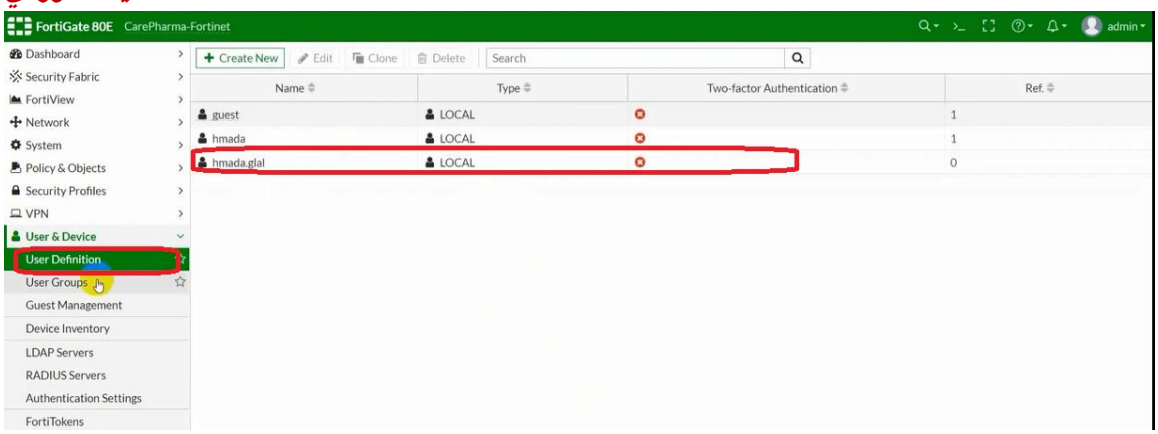
تم انشاء local user باسم hmada.glal



ثم نقوم بكتابه الايميل الخاص بي في حالة تم نسيان الباسورد سيقوم بإرساله الى الايميل في حالة قمت بعمل reset password

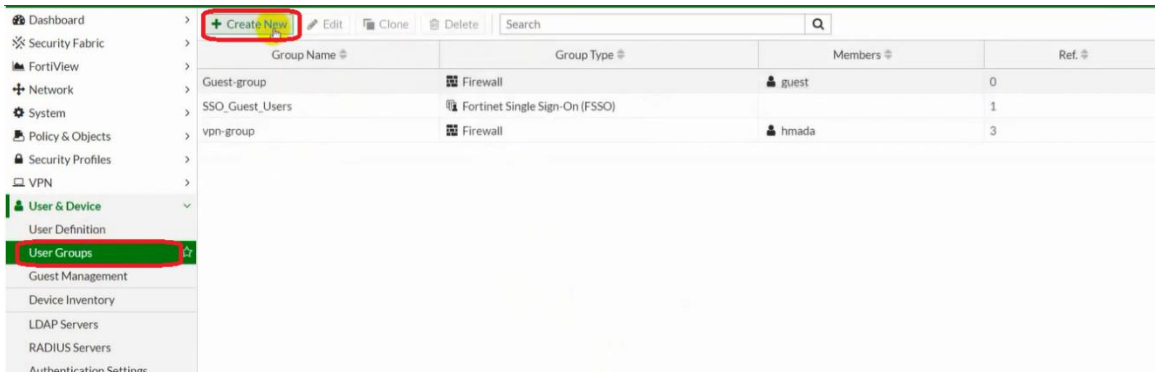


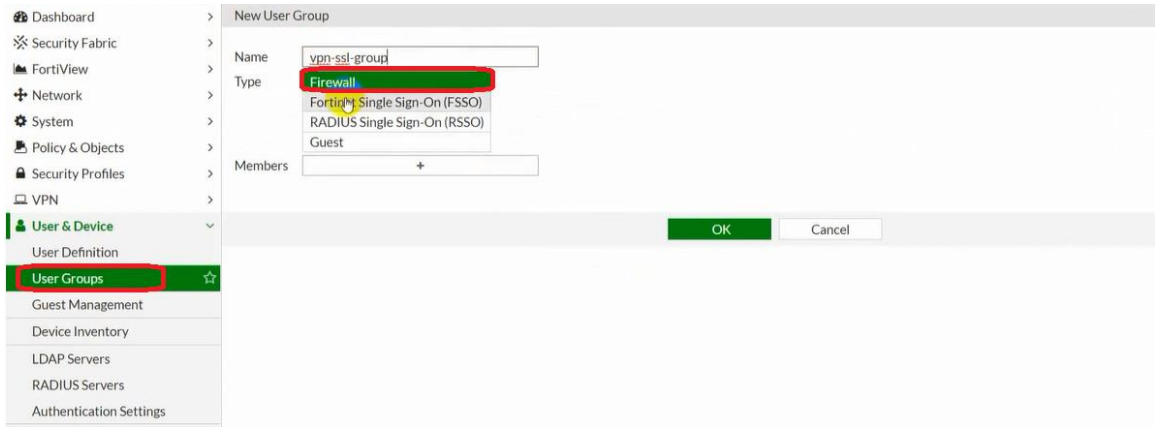
حيث حالة الحساب هي Enabled .



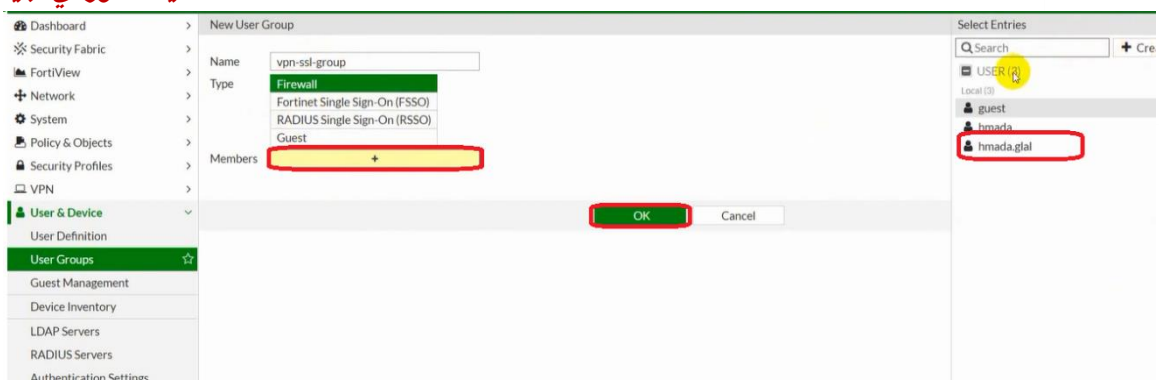
تمت عمليه الانشاء ..

الآن سنقوم بإنشاء group كما بالصورة ادناه

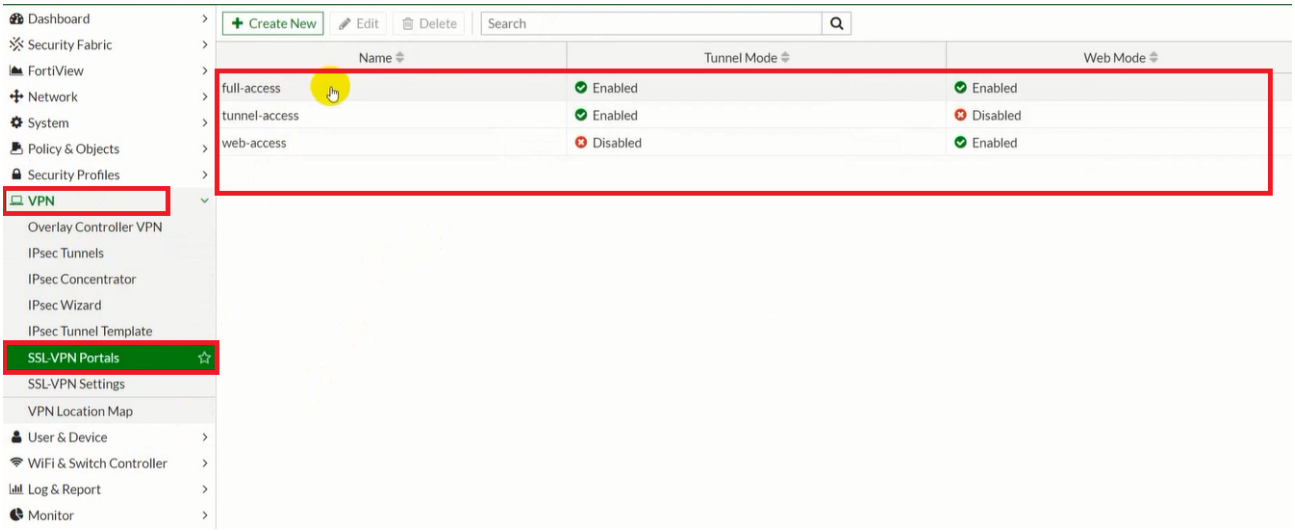




اسمها VPN-SSL-group ونوعها لوكالي (Firewall)



ثم نقوم بأضافه اليوزرات اليها ..



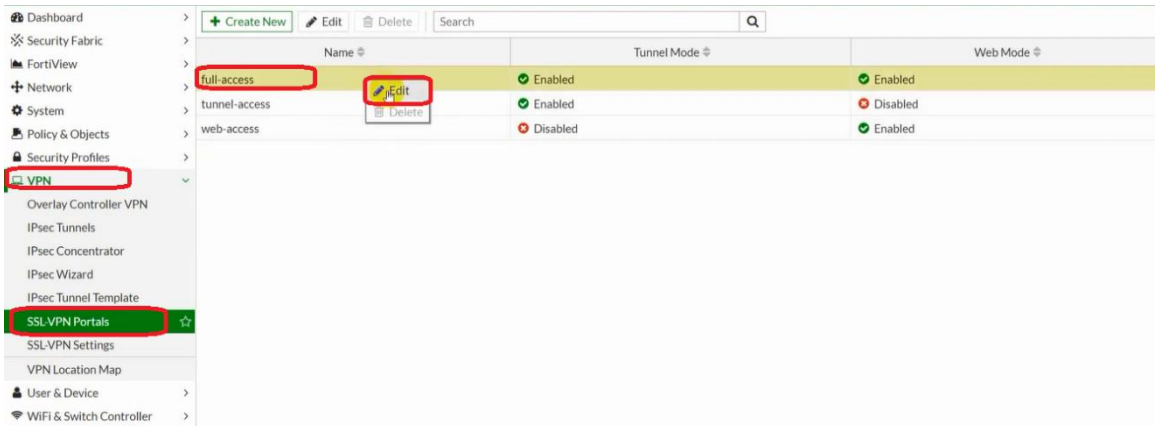
نلاحظ كما بالصورة أعلاه بان الفورتي جيت بشكل افتراضي يوجد بداخله 3 portal كالتالي :

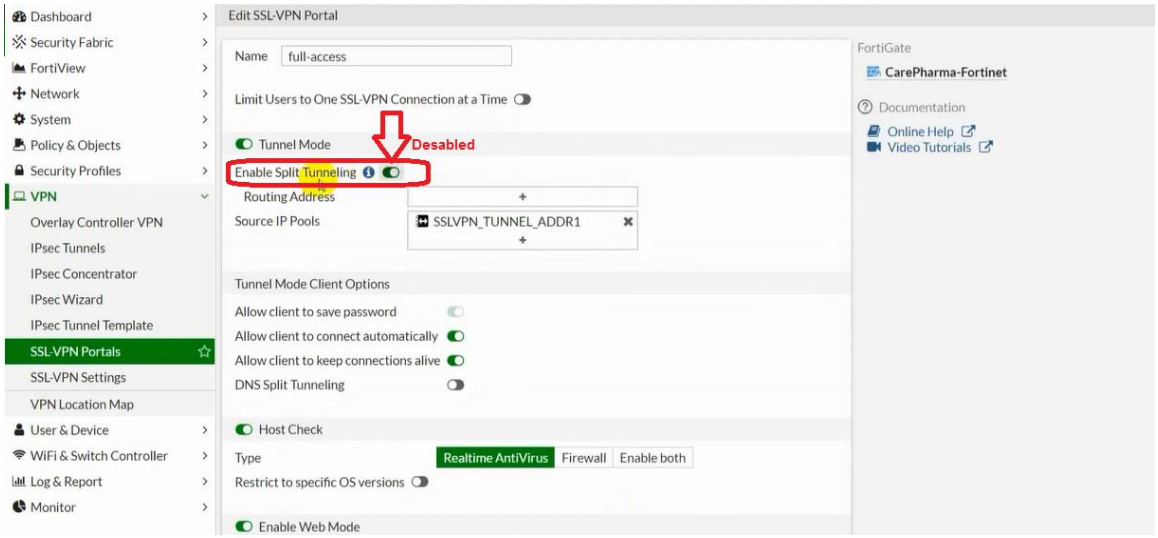
Full-access :هنا لهم صلاحيات بانهم يوصوا الى vpn سواء عبر الtunnel mode او web access

Tunnel-access :هذه صلاحيات خاصه ب tunnel mode

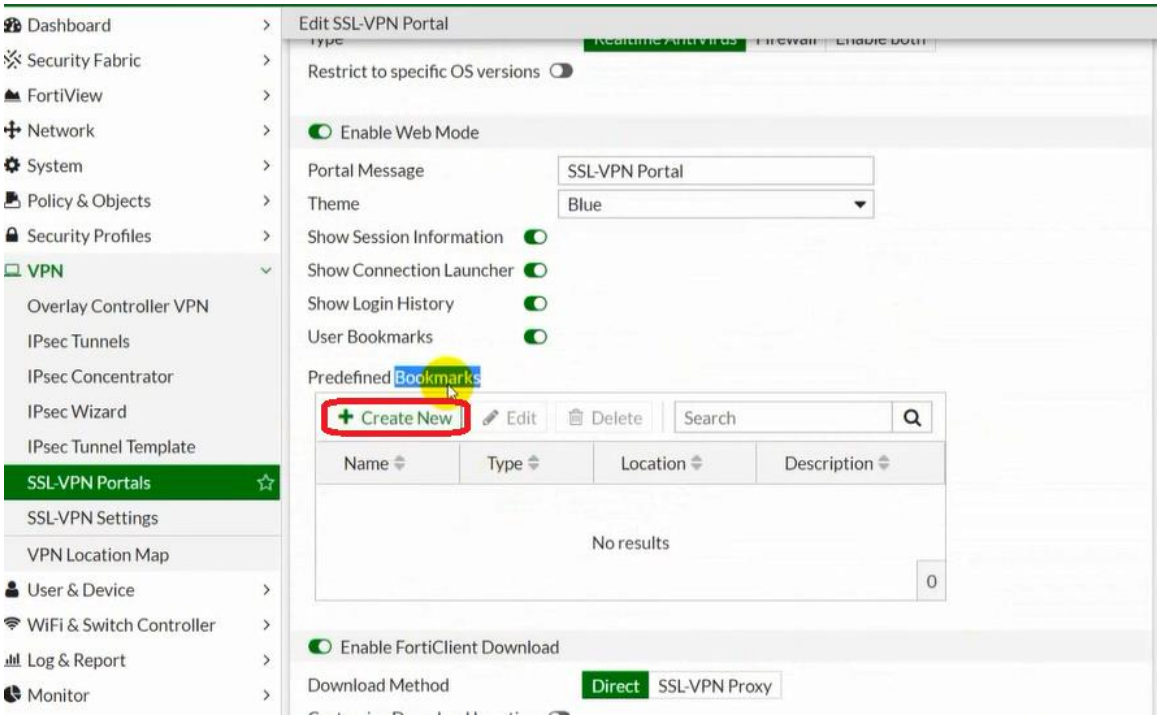
Web-access : هذه خاصه بالويب اكسس حيث اليوزرات التي سوف يتم وضعهم هنا سيتم اعطائهم صلاحيات بأنهم يوصلوا الى vpn عبر الويب مود .

حيث سنقوم بالتعديل على full-access :

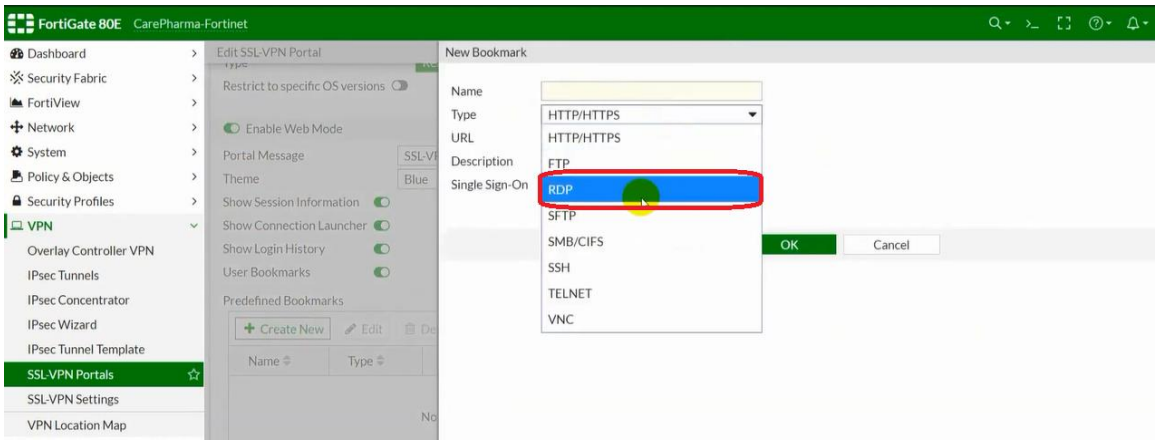


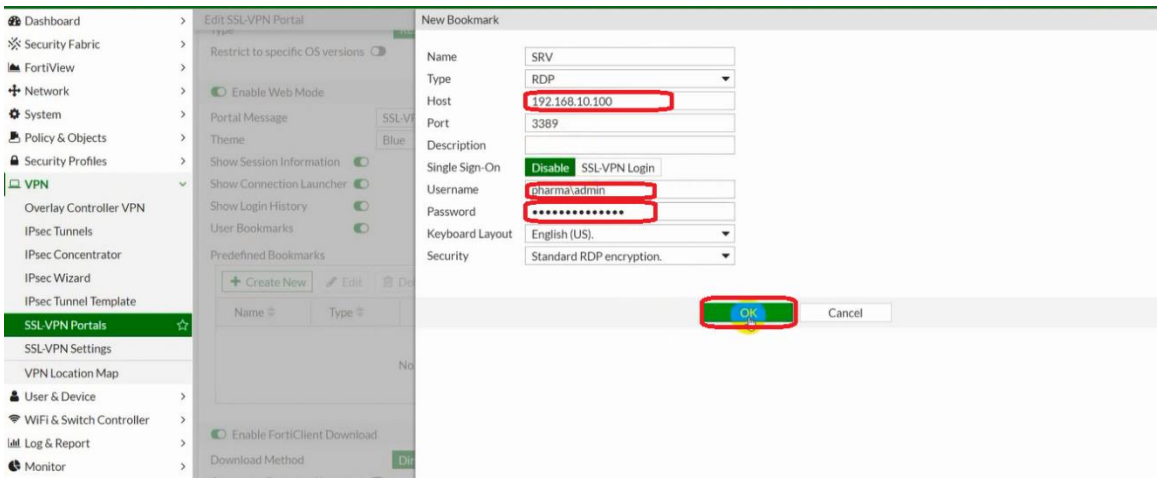


كما بالصورة أعلاه تم اغلاق الخيار Enable Split Tunneling

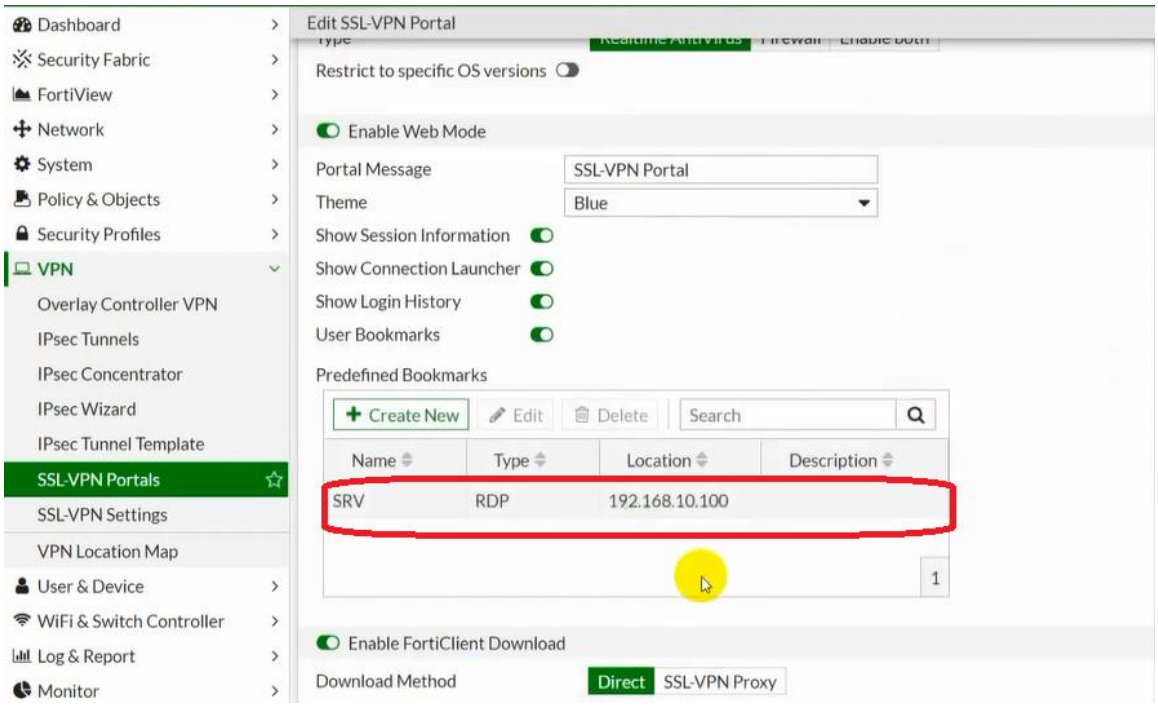


ولو اردت أضافه Bookmarks للـ web access mode

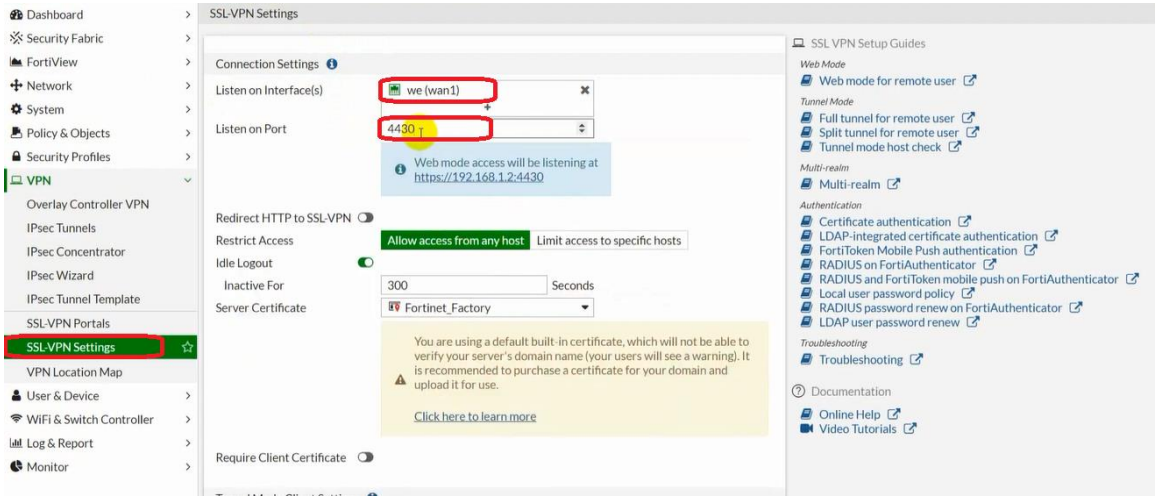




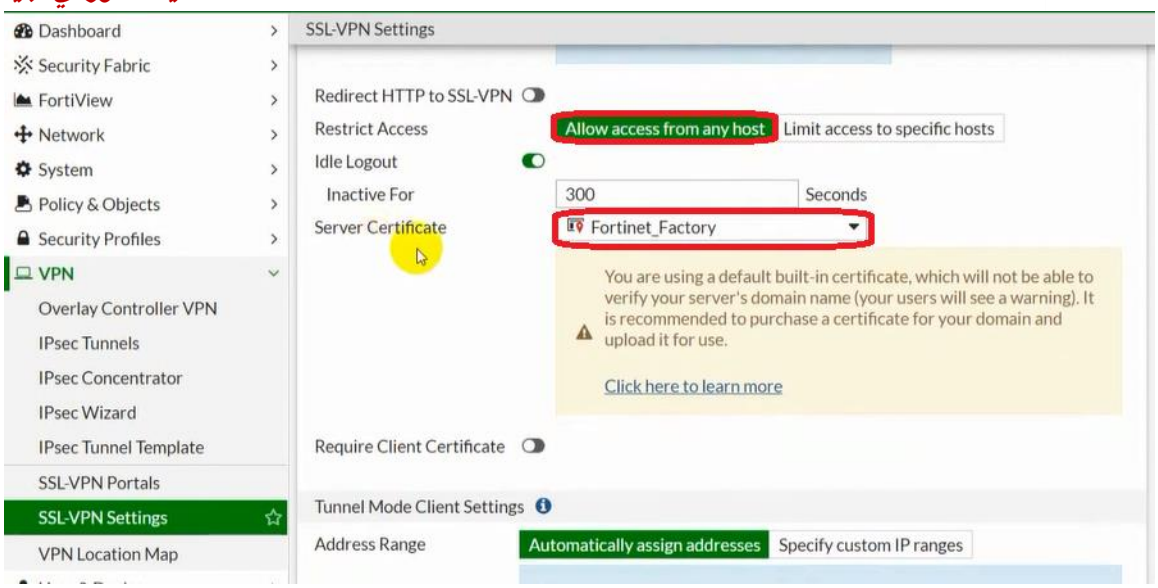
تم أضافه bookmark حيث سيتم الوصول الى السيرفر 192.168.10.100 عبر الـ remote Desktop (RDP)حيث تم كتابه اليوزرنيم والباسورد التابع للسيرفر



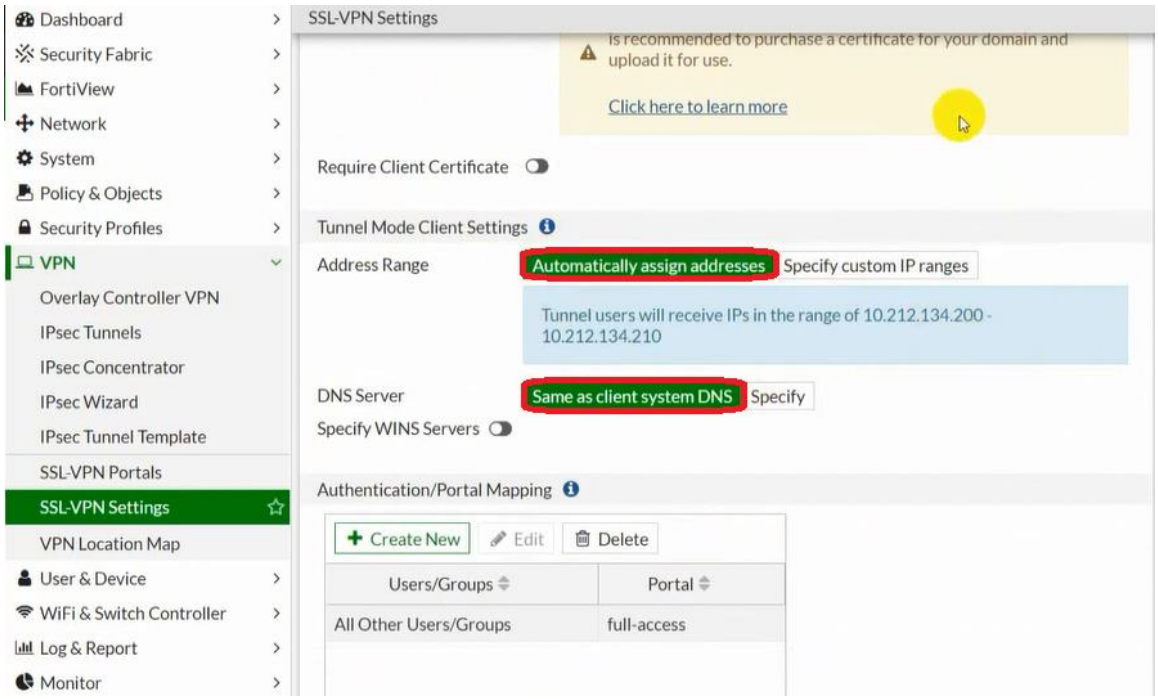
بعد ذلك نقوم بالذهاب الى SSL-VPN-Settings



حيث قمنا بتحديد كرت الـWAN والذي عليه real ip ويفضل تغيير الlistening port from من 443 الى مثلا 4430 بحيث يمكن اداره الفورتي جيت نفسه عبر 443 (https)من خارج الشبكة عبر الانترنت وكما يمكن الوصول الى vpn web mode عبر البورت 4430 .



كما بالصورة أعلاه يمكن الوصول عبر الvpn من أي جهاز وأيضا يفضل لا تقوم بتغير الشهادة واتركها كما هي .



أيضا يتم ترك الاعدادات كما بالصورة أعلاه بحيث الفورتي جيت هو من يقوم بتعين الايبي لليوزرات التابعه للVPN .

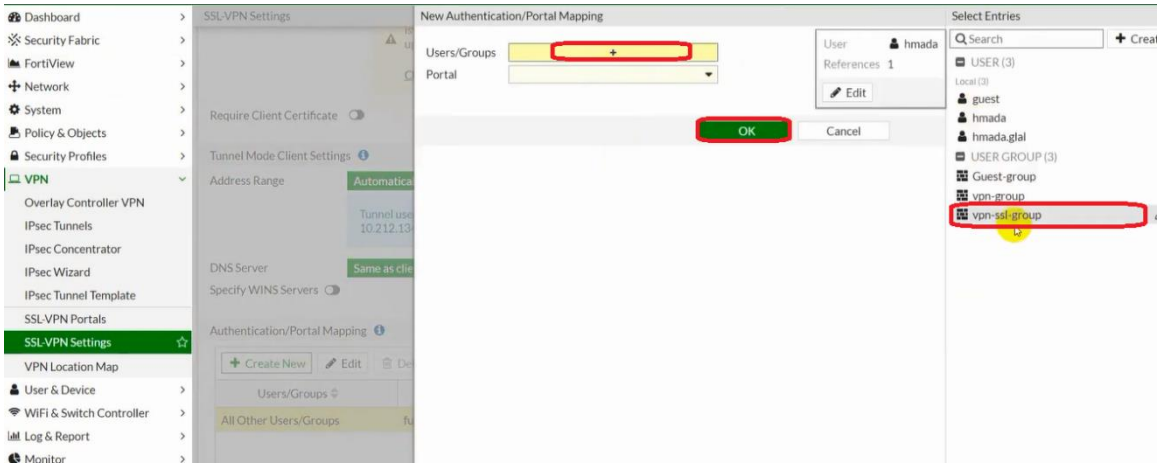
وكما نترك الـ dns server هو نفسه التابع للفورتي جيت .

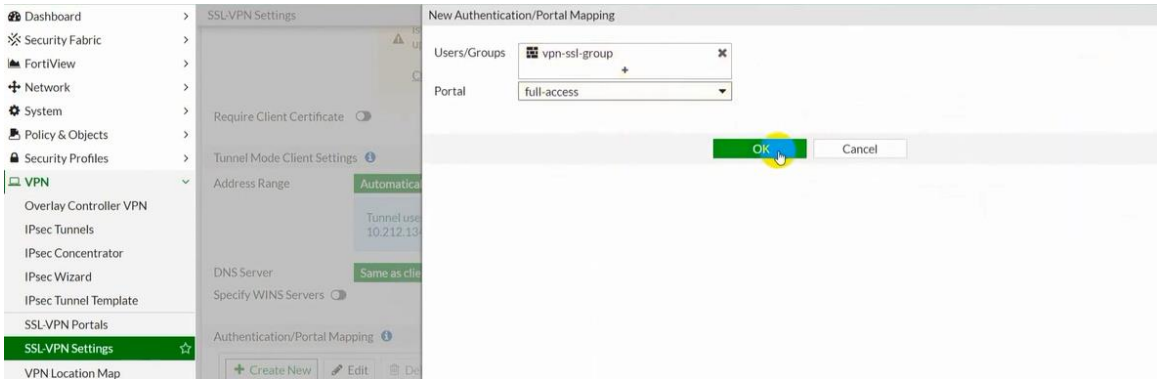
يتم تحديد اليوزرات التي لهم صلاحيات للوصول عبر الVPN للفورتي جيت .

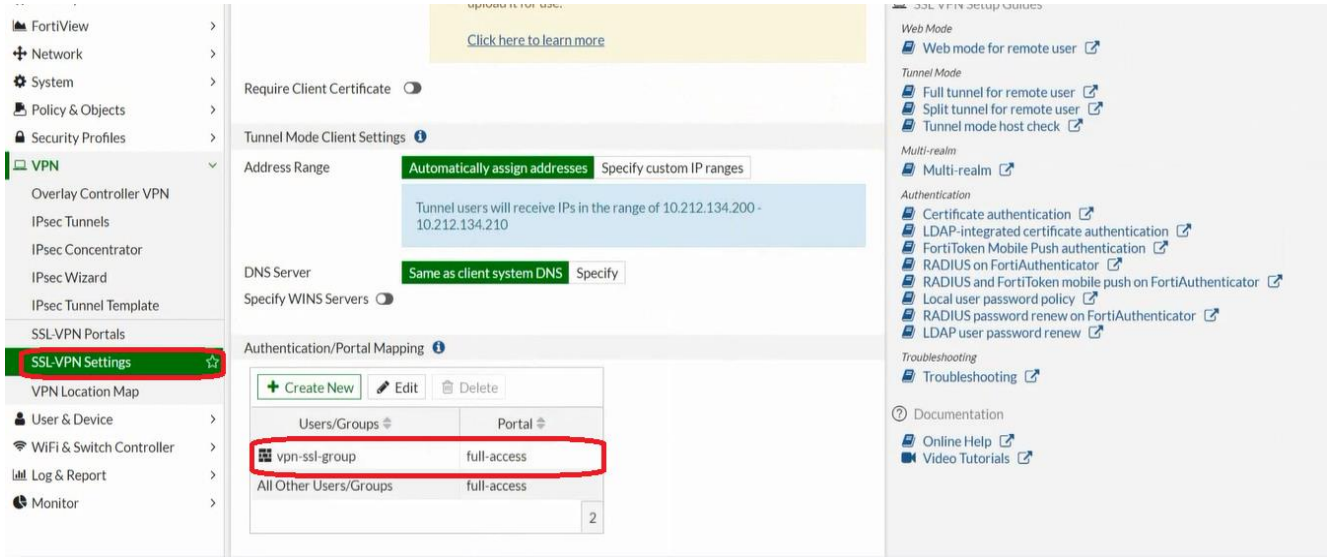
حيث بشكل افتراضي يكون All other users/groups لديها full-access

حيث أي local users بالفورتي جيت له حق الوصول ..

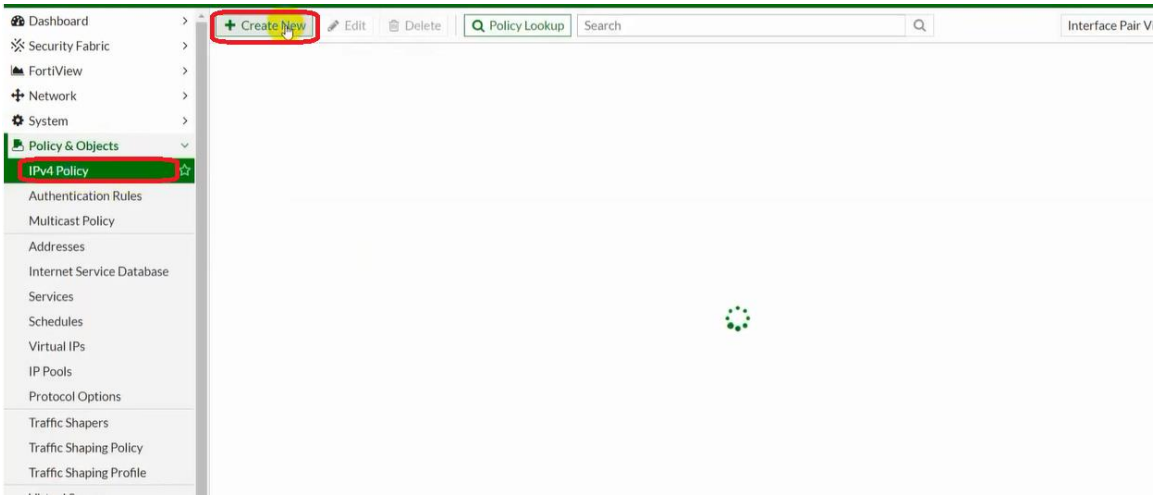
ويمكن تحديد فقط الجروب التي قمنا بإنشائها سابقا كما بالصورة التالية :







اخر الخطوات نقوم بعمل Rule تسمح بمرور الترافيك ما بين الـ vpn و local network وبين الـVPN وبين الانترنت .



قمنا بتسميه الـ rule باسم ssl-vpn-to-localnetwork

ونقوم بتحديد الـ incoming interface حيكون SSL-VPN-tunnel interface(ssl.root)

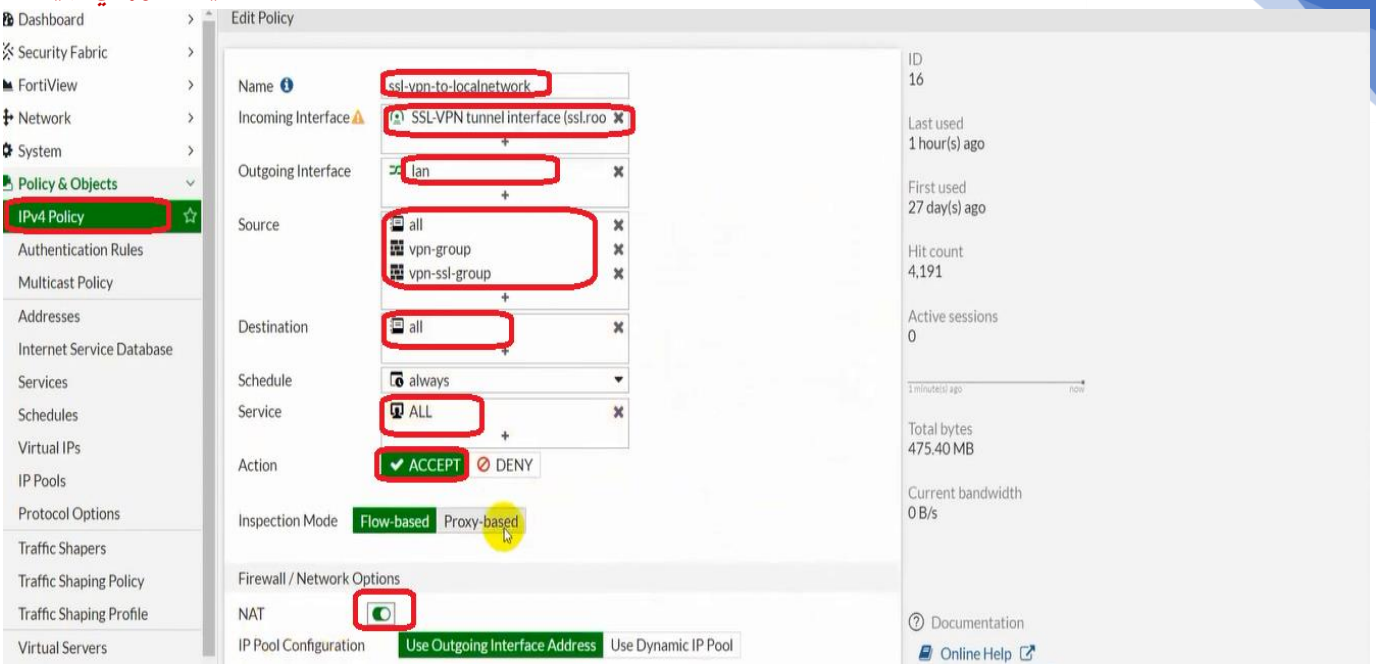
و outgoing interface سيكون lan أي كرت الشبكة الداخليه

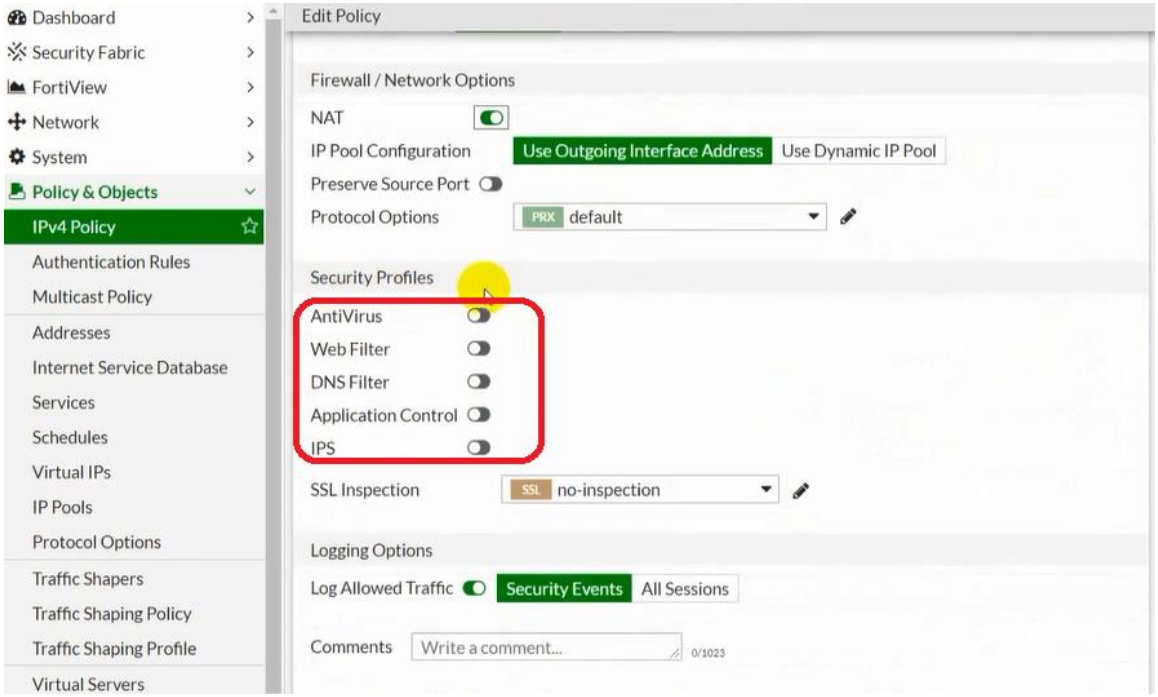
حيث الـ source هم الأشخاص(الجروب)التي تم أنشائها سابقا وهو vpn-ssl-group

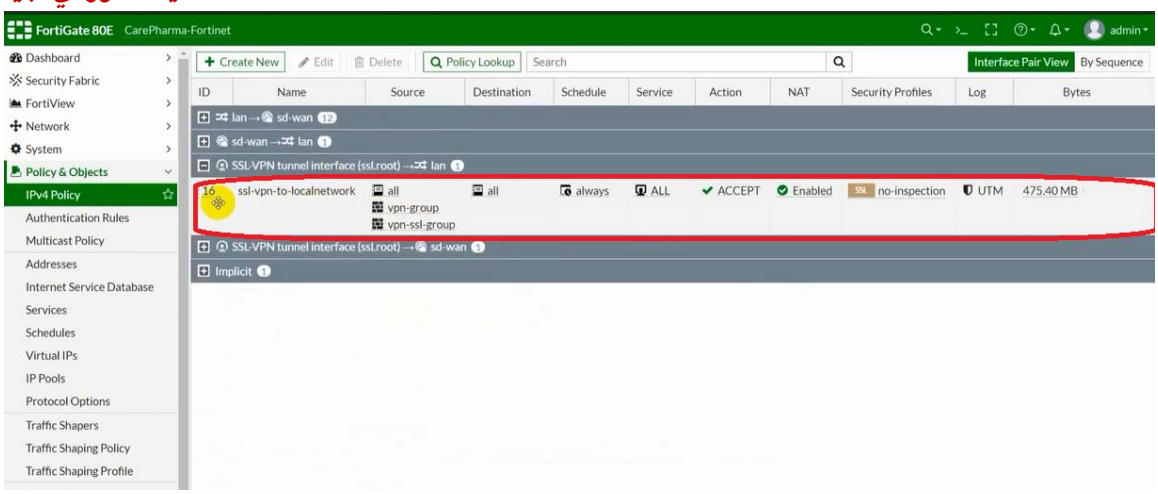
والـ destination سيكون all أي كل اجهزه الشبكة الداخليه ونقوم بتفعيل خيار الـnat

في خيارات الـ security profiles حيث يمكنني تفعيل الـ Antivirusو الـ web filter و الـ Application control وIPS على تلك الـ Rules .

كما بالصور ادناه

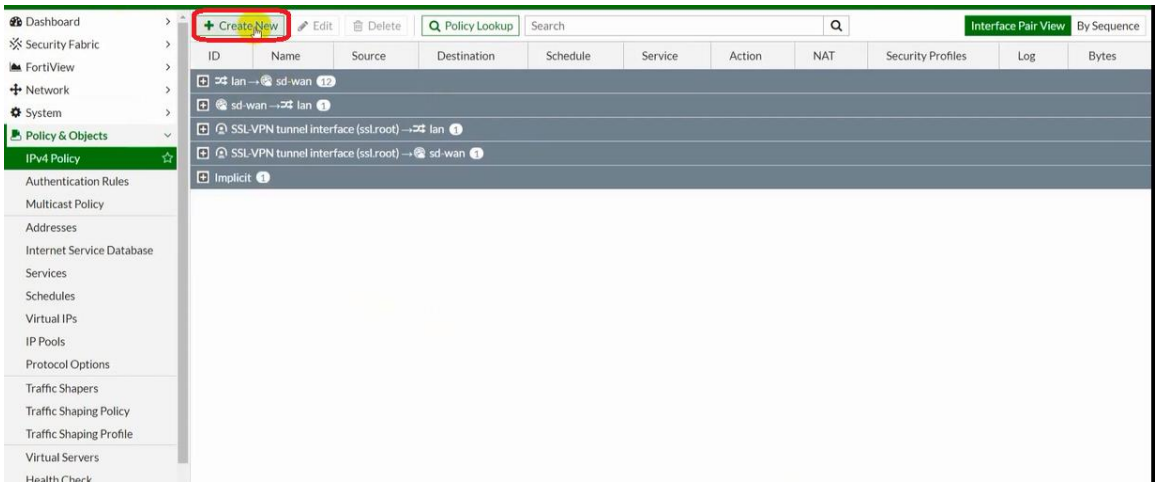

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Authentication Rules
Multicast Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Virtual Servers
Edit Policy
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
DENY
Inspection Mode
Flow-based
Proxy-based
Firewall / Network Options
NAT
IP Pool Configuration
Use Outgoing Interface Address
Use Dynamic IP Pool
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
Online Help

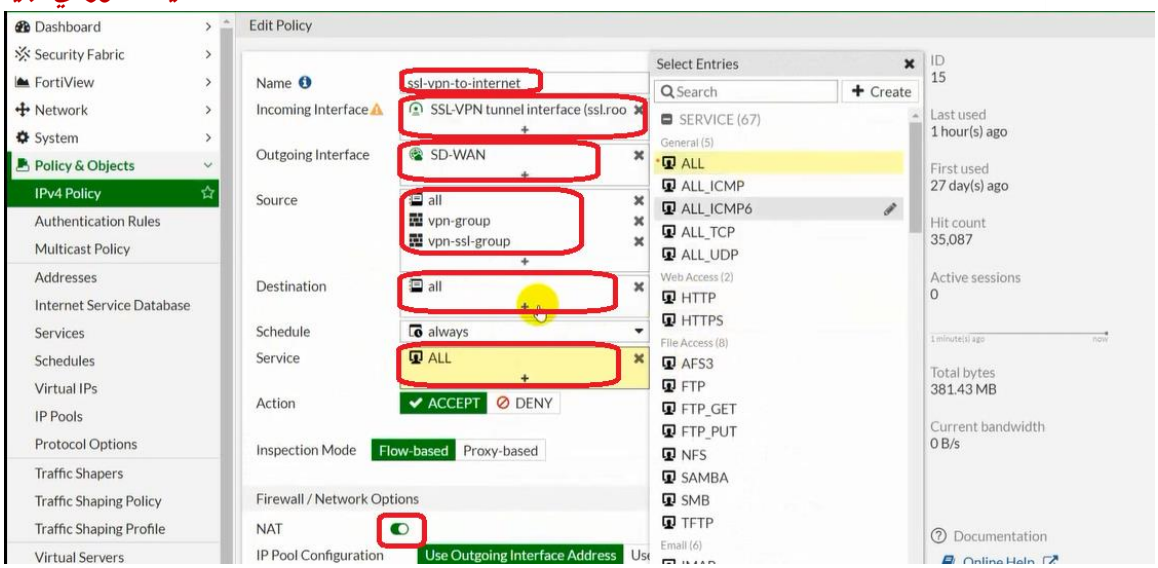

Dashboard
Security Fabric
FortiView
Network
System
Policy & Objects
IPv4 Policy
Authentication Rules
Multicast Policy
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shapers
Traffic Shaping Policy
Traffic Shaping Profile
Virtual Servers
Edit Policy
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
Application Control
IPS
SSL Inspection
SSL no-inspection
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Comments
Write a comment...
0/1023



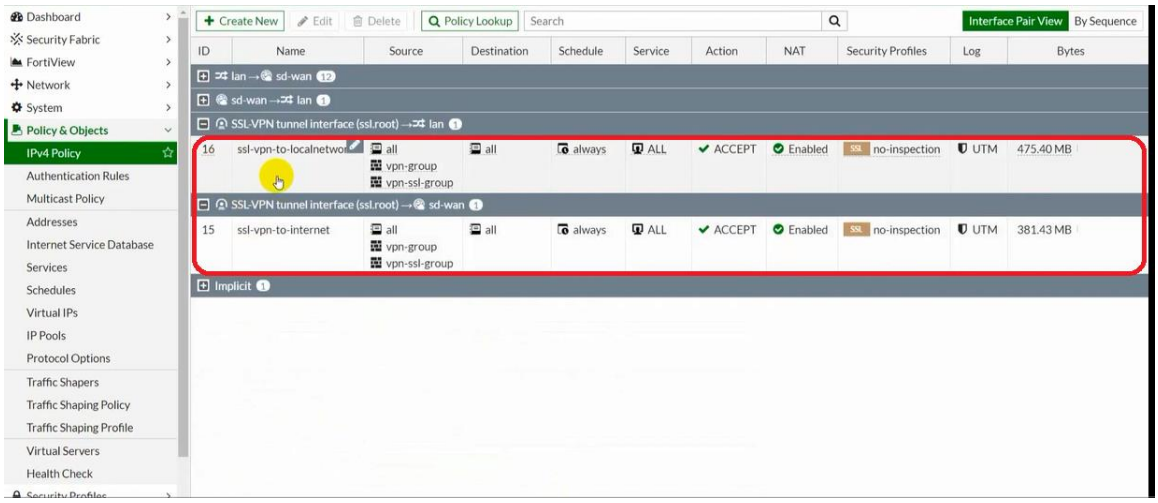
نلاحظ كما بالصورة أعلاه بأنه تم انشاء Rule تسمح بالوصول من خارج الشبكة(عبرVPN) الى الشبكة الداخلية لكن كل اليوزرات التي عبرالVPN لن تستطيع الوصول الى الانترنت ابدا ويجب ان نقوم بإنشاء Rule تسمح للناس بعد ما يقوموا بعمل vpn ان يكون لديهم انترنت عبرHQ أي الشبكة الداخلية حيث سيتعامل معهم الفورتي جيت كproxy server .

الآن سنقوم بعمليه انشاء تلك الRule باسم ssl-vpn-to-internet:





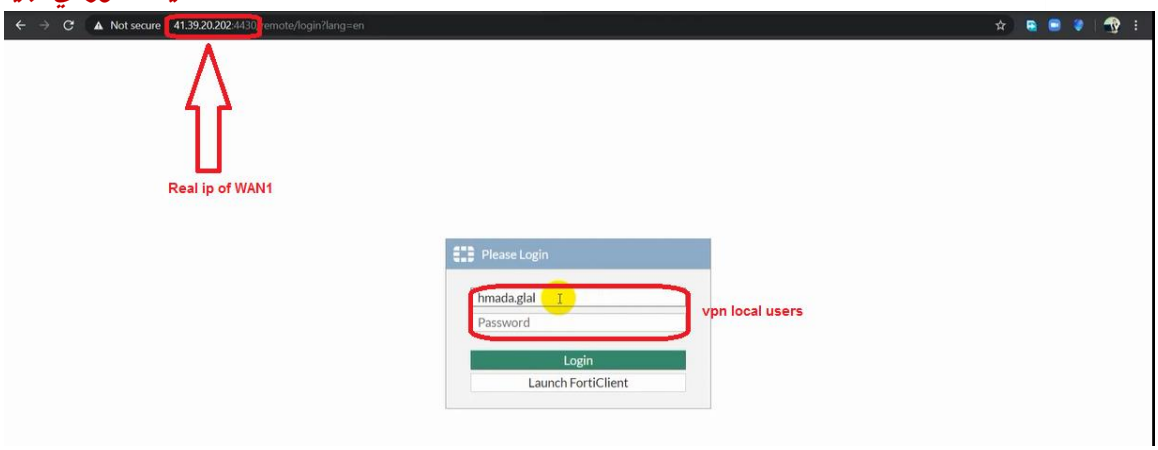
حيث نلاحظ بأن الـSD-Wan= Outgoing interface حيث جهاز الفورتي جيت معمول دمج لأكثر من خط ولذا اليوزرات التابعه لـvpn والتي تم تحديدها بـ source سوف تحصل على الانترنت عبر SD-Wan لجهاز الفورتي جيت .

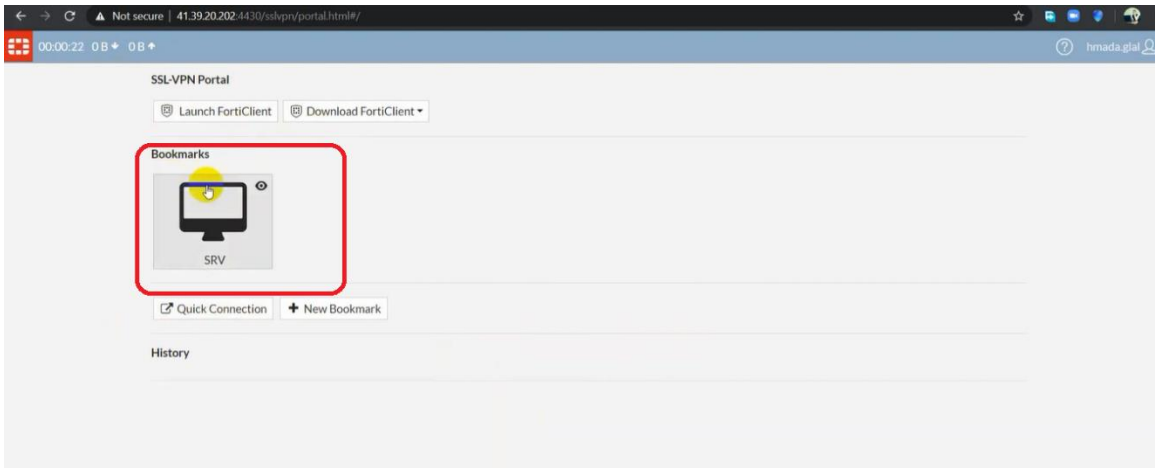


الآن لدي Rule 2 التي تسمح بالترافيك بين الـVPN و LOCAL NETWORK

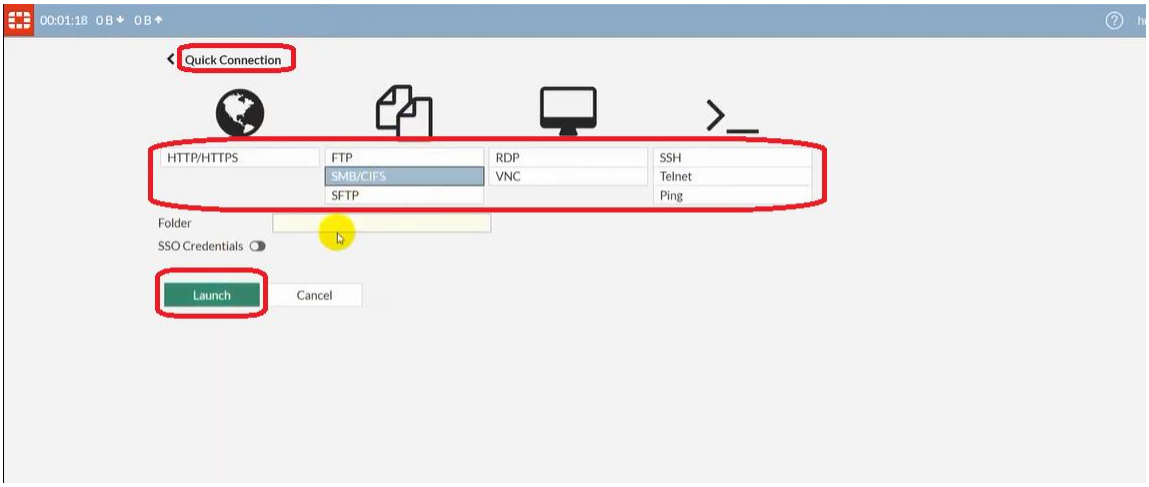
حيث الرابط(URL) التي بواسطته يمكنك الوصول الى الشبكة الداخليه عبر الـ VPN Web mode هو ip wan of fortigate+4430 والذي تم اعداداه سابقا

كما بالصورة التالية :





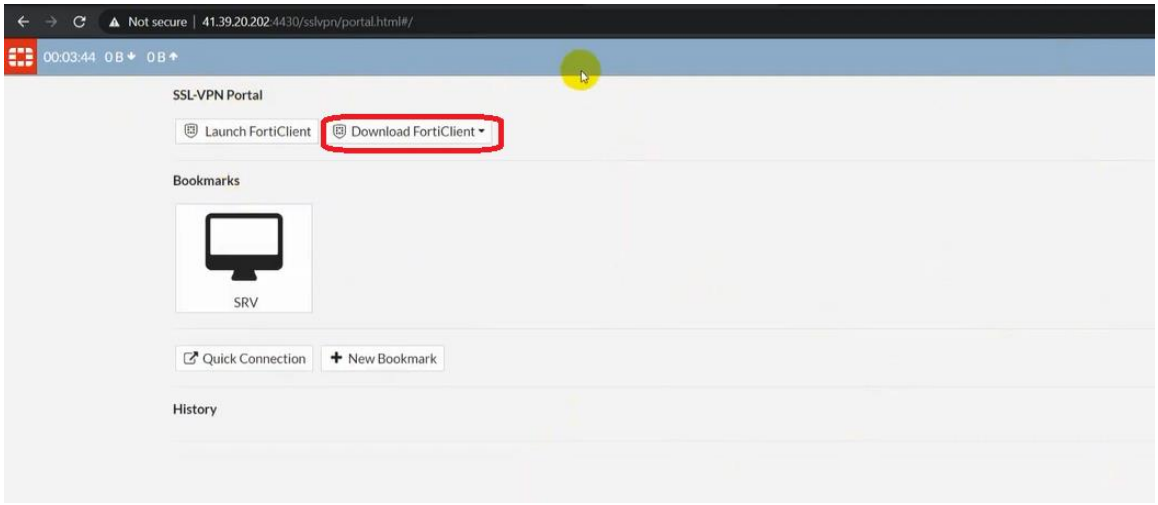
كما بالصورة أعلاه فأن الـ bookmark التي قمنا بأنشائها سابقا باسم SRV موجودة وهو Remote Desktop للسيرفر 192.168.10.100 وبمجرد النقر مرتين عليه يفتح لنا السيرفر...



او يمكنك عبر الـ Quick Connections ان تصل الى أي Service تريدها سواء HTTP/HTTPS RDP SSH Ping..الخ

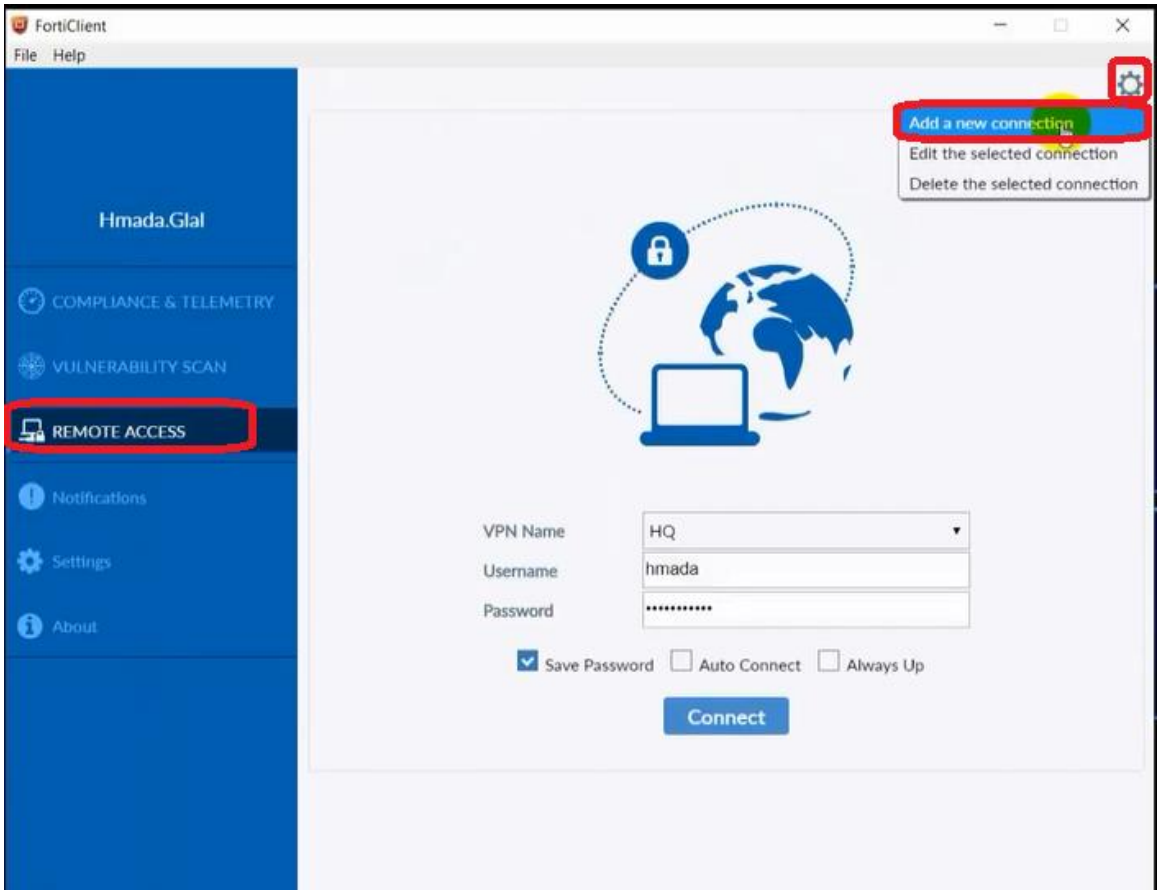
وهذه الطريقة الأولى vpn/ssl عبر web mode

و الطريقة الأخرى عبر الفورتي كلاينت كما بالصورة التالية :



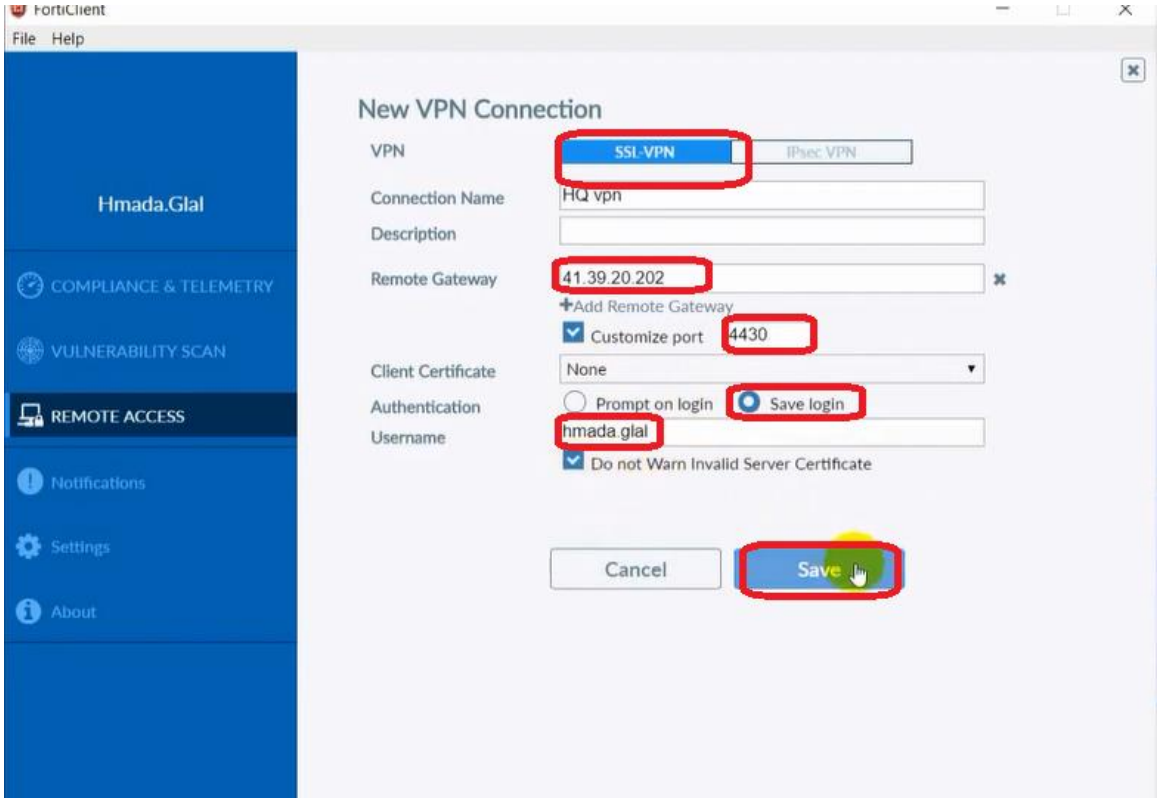
حيث يمكنك تنزيل برنامج الفورتي كلاينت عبر موقع الفورتي جيت نفسه او من الصفحة التابعه لـ web access كما بالصورة أعلاه ...

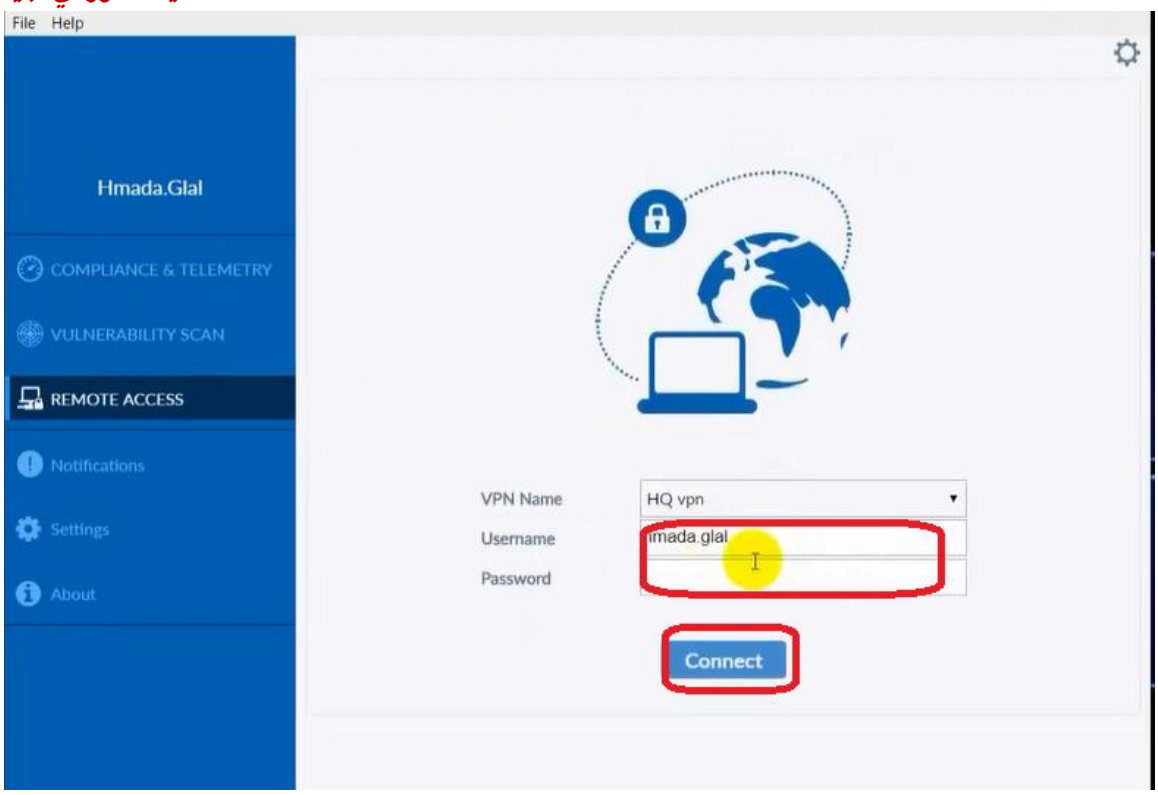
ثم نقوم بعمل install للتطبيق



حيث نوع الاتصال هو SSL-VPN واسمه مثلا HQ-VPN ونضع الايبي للWAN في Remote Gateway ونحدد البورت 4430 ثم نختار Save logging لو تريد الفورتي كلاينت لا يطلب اليوزرنيم كل مره عند تشغيله

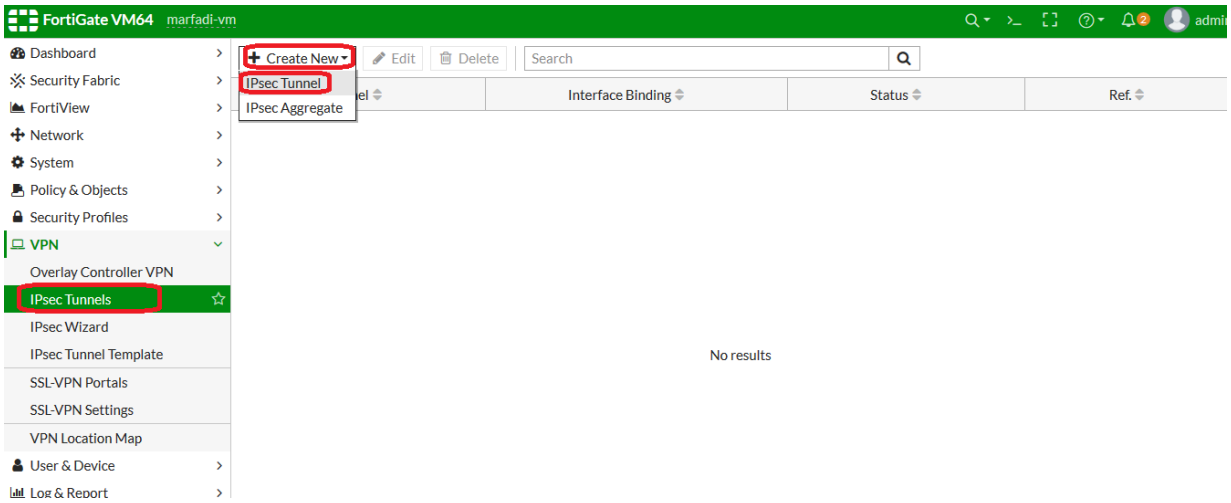
اما انت تريده ان يطالب المستخدم بكتابه اليوزرنيم والباسورد في كل مره فنختار الخيار prompt on login

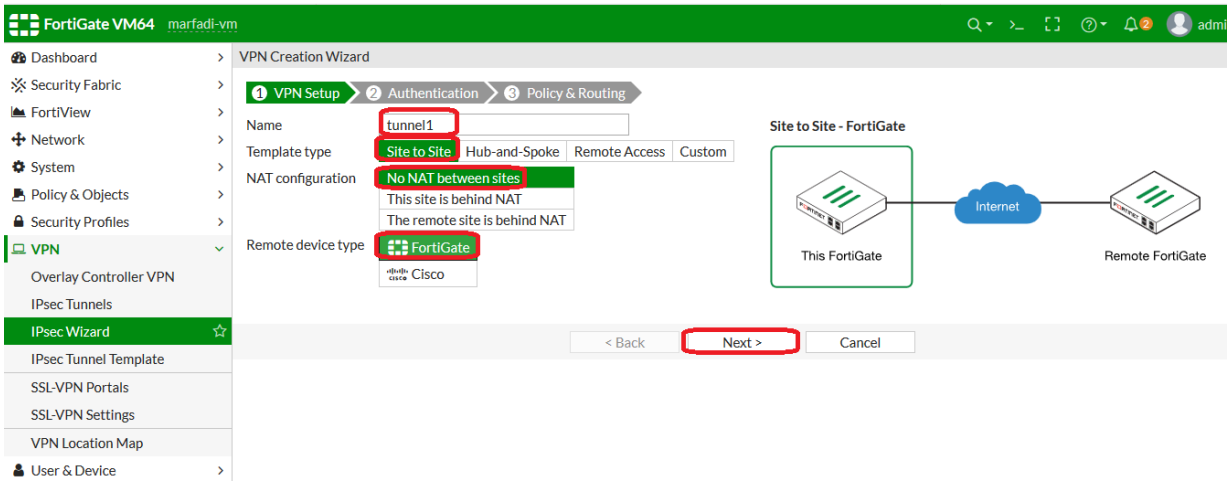




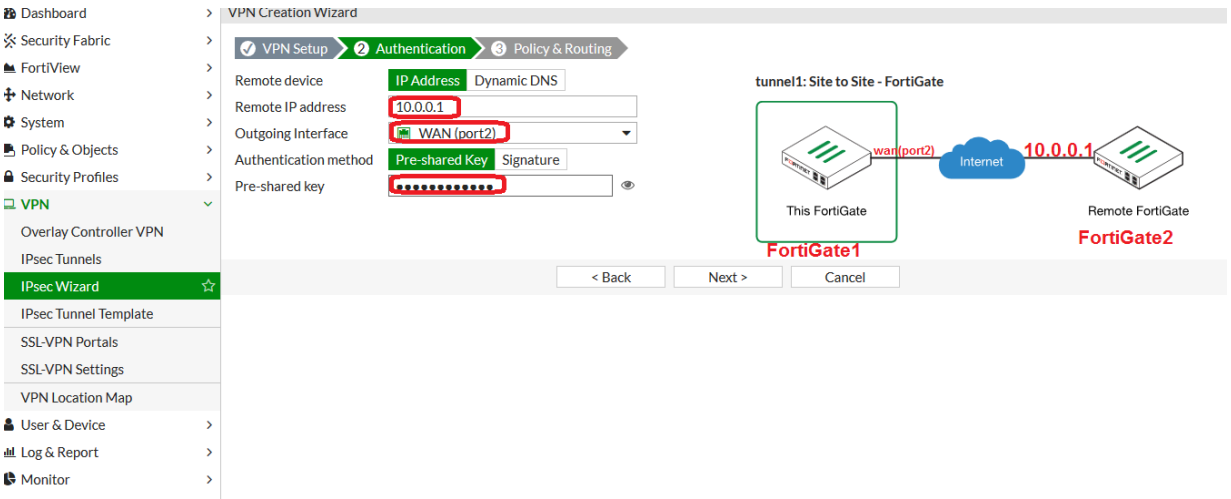
فمجرد ادخال اليوزرنيم والباسورد وعمل connect فانه سوف يتصل ويمكنك بعد ذلك الوصول الى HQ ومنها الى السيرفرات ...

➢ تمرين اخر حول VPN SITE TO SITE:





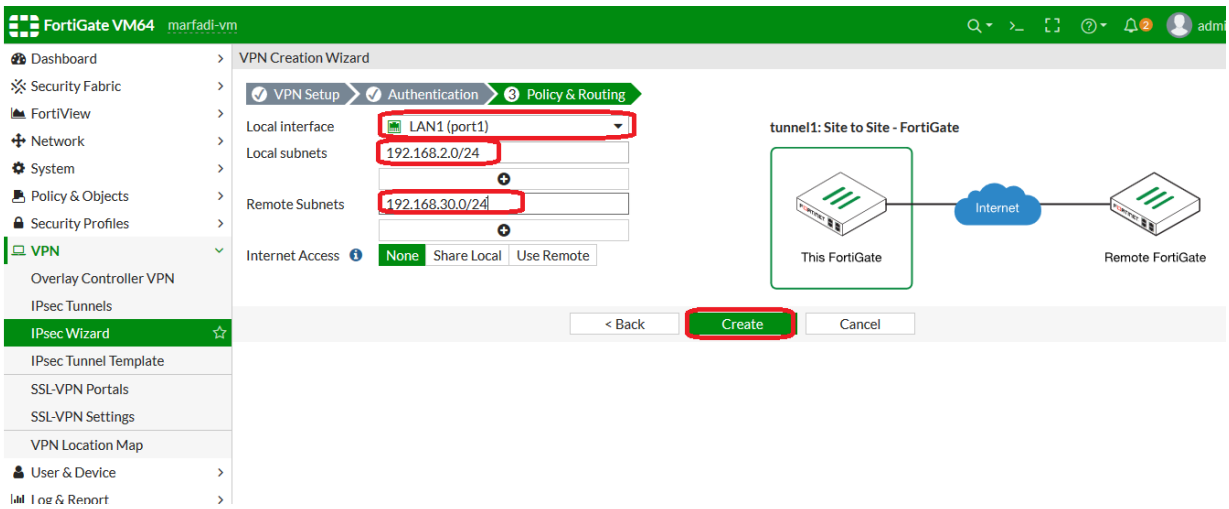
كما بالصورة أعلاه توضح بأن اسم الـ tunnel هو tunnel1 ونوعيه الربط هو site to site حيث تم اختيار الجهاز الموجود بالفرع البعيد هو فورتي جيت2 ..



كما بالصورة أعلاه تبين بأن الايبي لجهاز الفورتي جيت2 الموجود في الـ site البعيد هو 10.0.0.1 وهو الـreal Ip ..

وتختار الـ wan interface للفورتي جيت1 للـsite الذي سوف يخرج منه الى 10.0.0.1 .

ونكتب كلمه السر (pre-shared Key) ..



حيث سنحدد الـ local interface للسايت FortiGate1 وهو الـLAN1

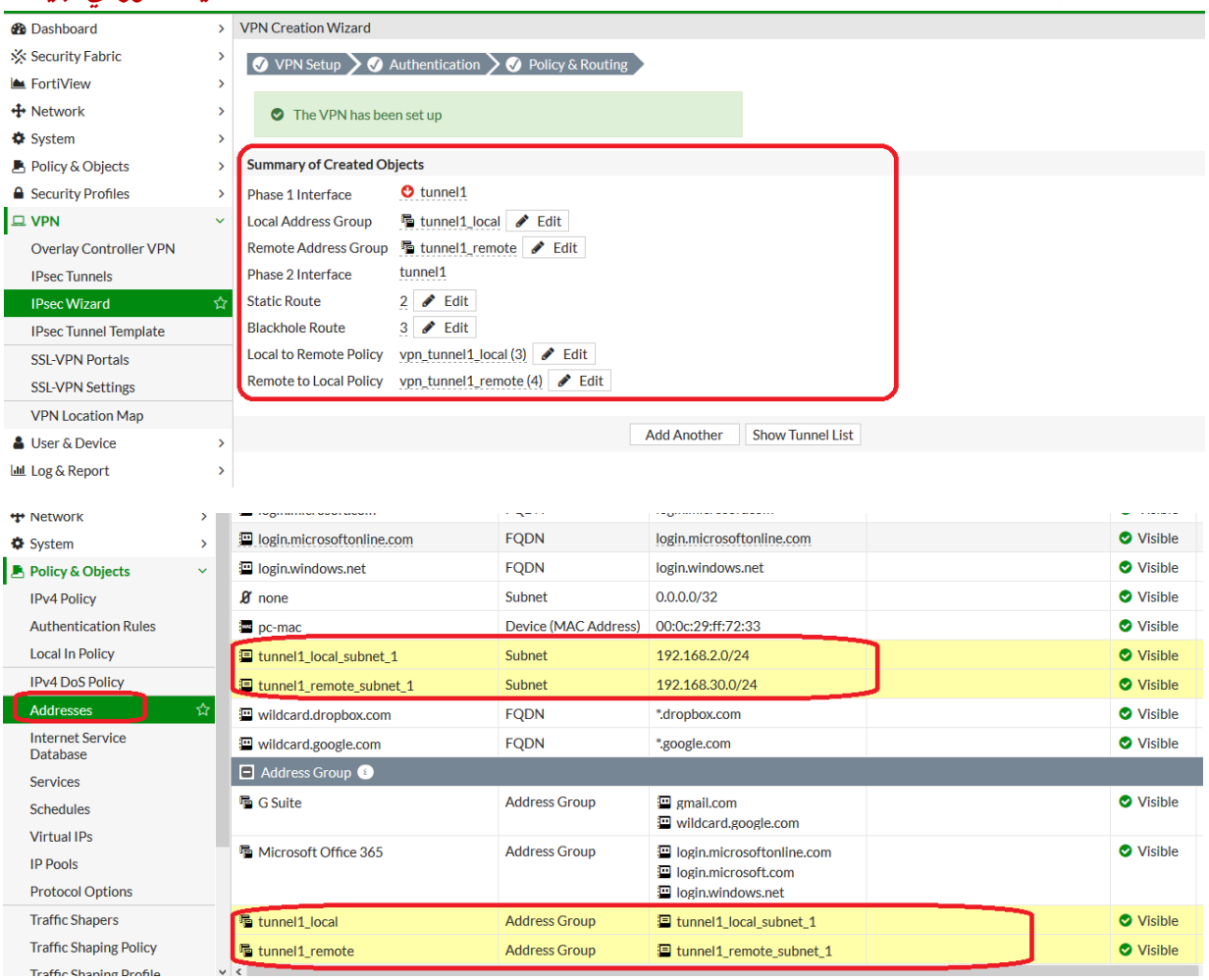
وبشكل تلقائي سوف يتعرف على الشبكة كما بالضورة أعلاه 24/192.168.2.0

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

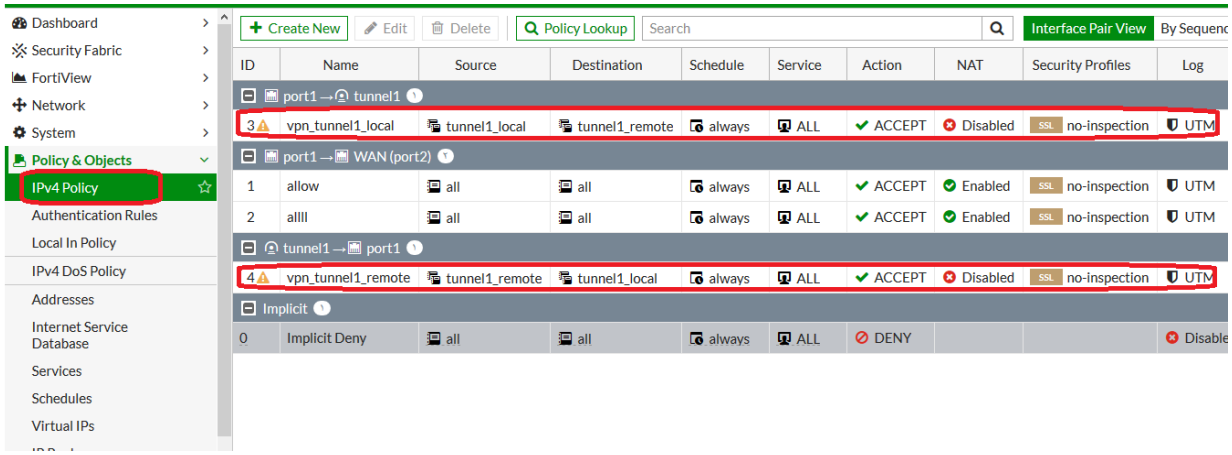
ملاحظة :سيقوم الفورتي جيت بإنشاء Network object لـ 24/192.168.2.0 .

وأيضا لـ 192.168.30.0/24 وهي لـremote subnet كما بالصورة ادناه .



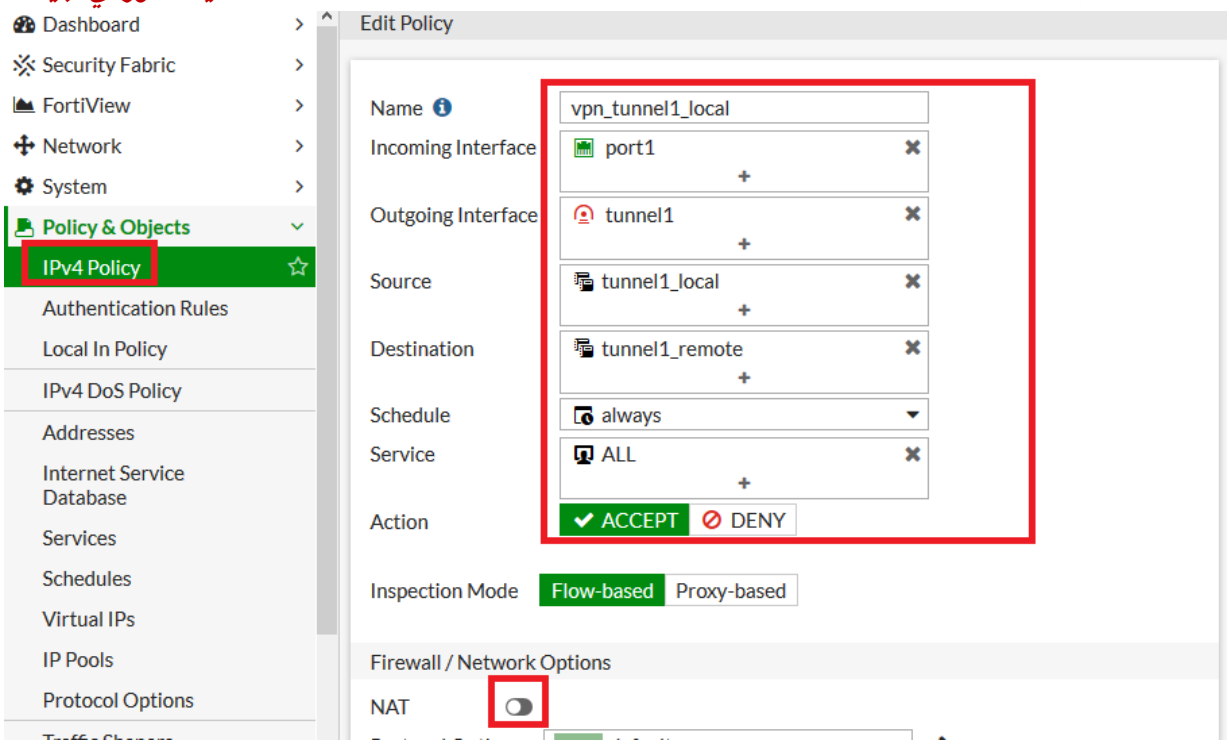
نلاحظ بانه تم انشاء عناوين ومجموعات بشكل تلقائيه كما بالصوه أعلاه ..

وأيضا سيتم انشاء سياستين (two policies) بشكل تلقائي كما بالصورة ادناه

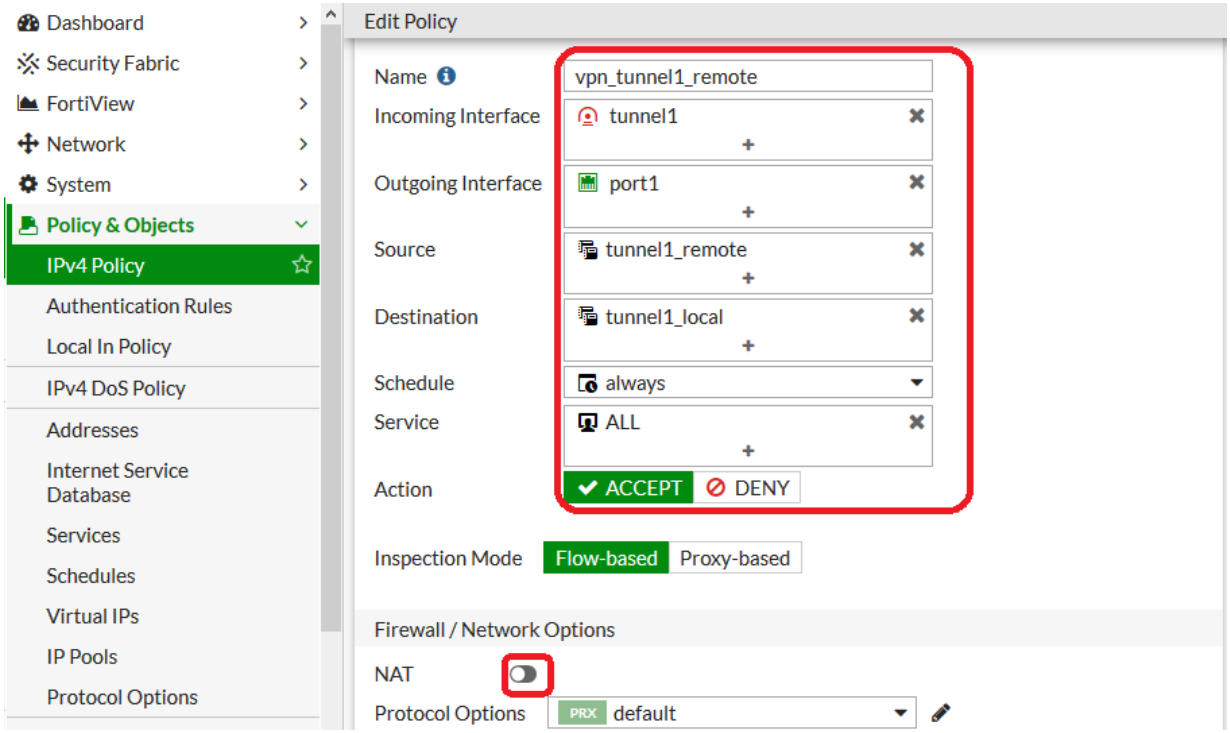


تم انشاء policy 2 كما بالصورة أعلاه ...

1-تسمح للترافيك من الـ local site الى remote site

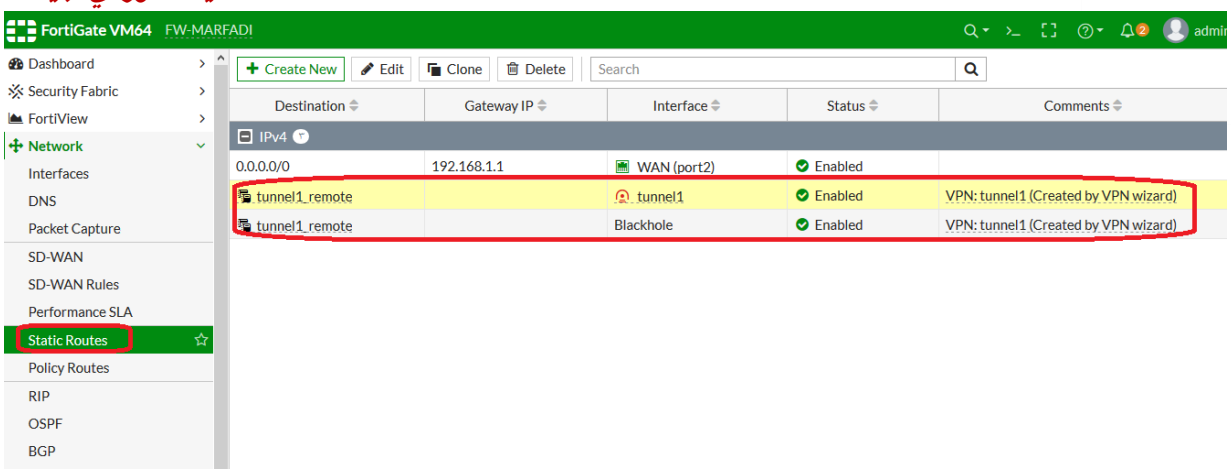


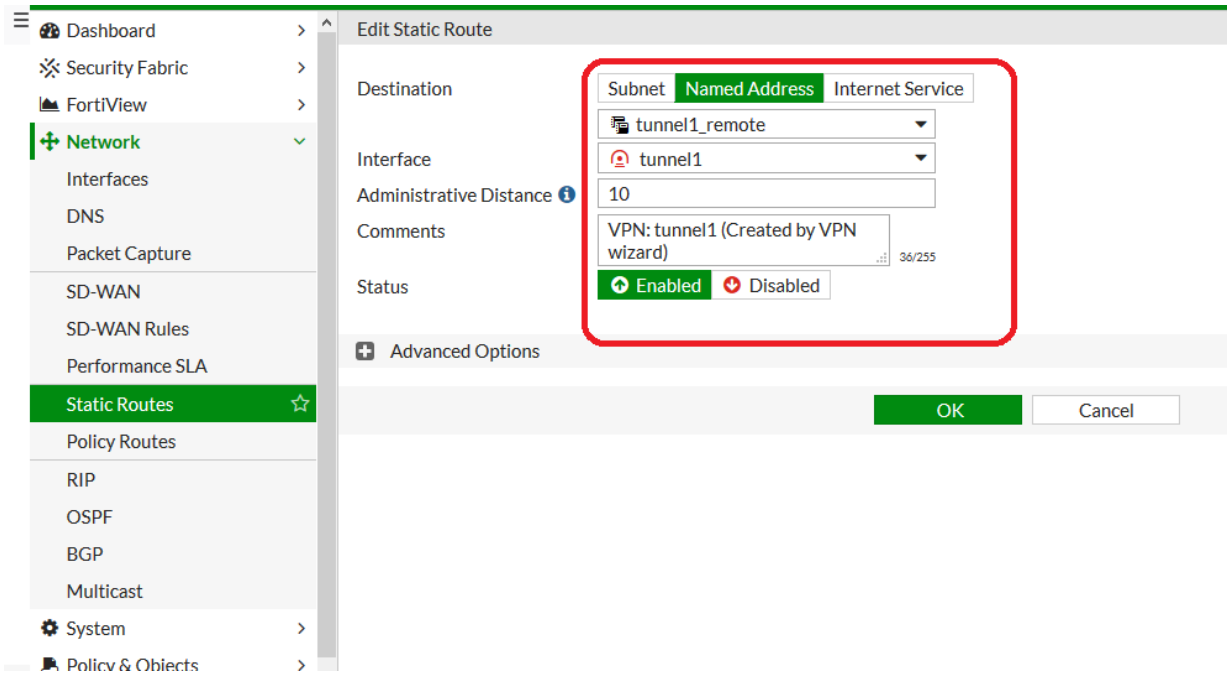
2-تسمح للترافيك من الـremote site الى الـlocal site .



*ملاحظة :لا يتم تفعيل الـNAT ..

أيضا سيتم انشاء static route بشكل تلقائي كما بالصورة ادناه





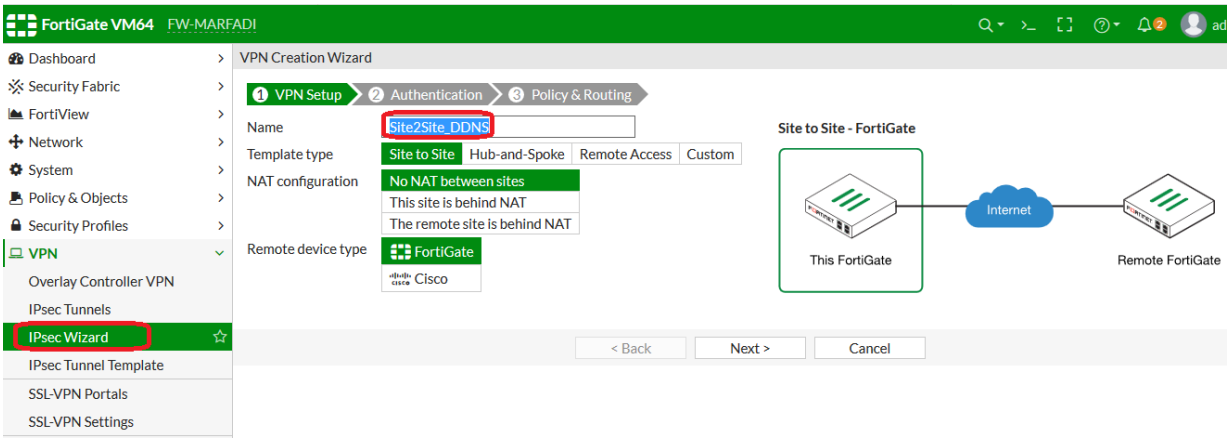
سوف نقوم بتكرار نفس العملية ولكن على الـ Site 2 أي على الفورتي جيت 2...

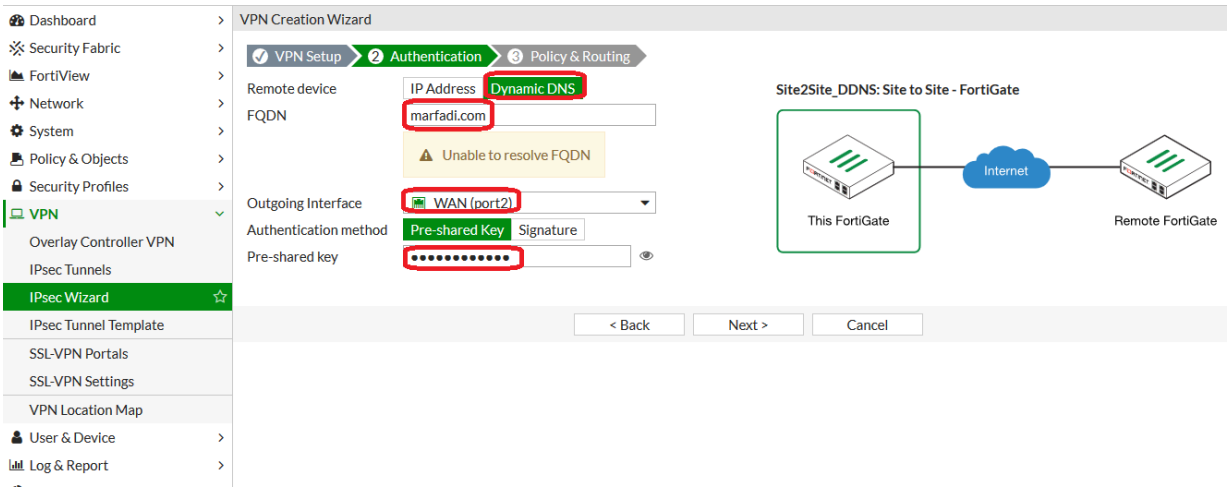
VPN SITE TO SITE DYNAMIC DNS(DDNS) :

ربط فرعين بواسطة فورتي جيت عبر الDDNS وليس عبر الـ static ip

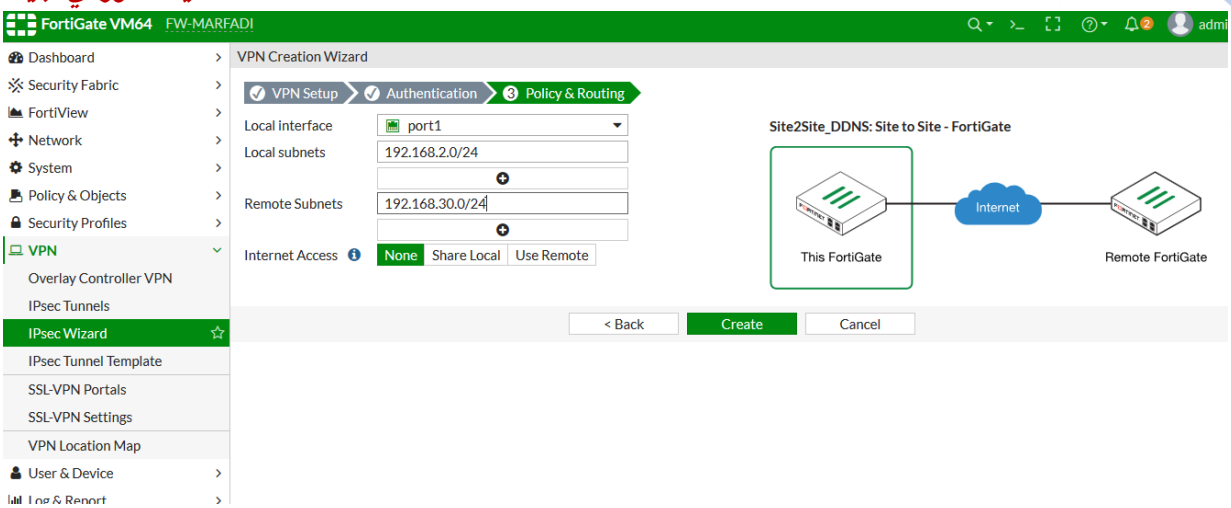
حيث توجد مواقع كثيره تستطيع بواسطتها انشاء DDNS مثل موقع no-ip.com

حيث نفترض بأن الـ site 1 لديه Static IP والـ site 2 لديه DDNS .

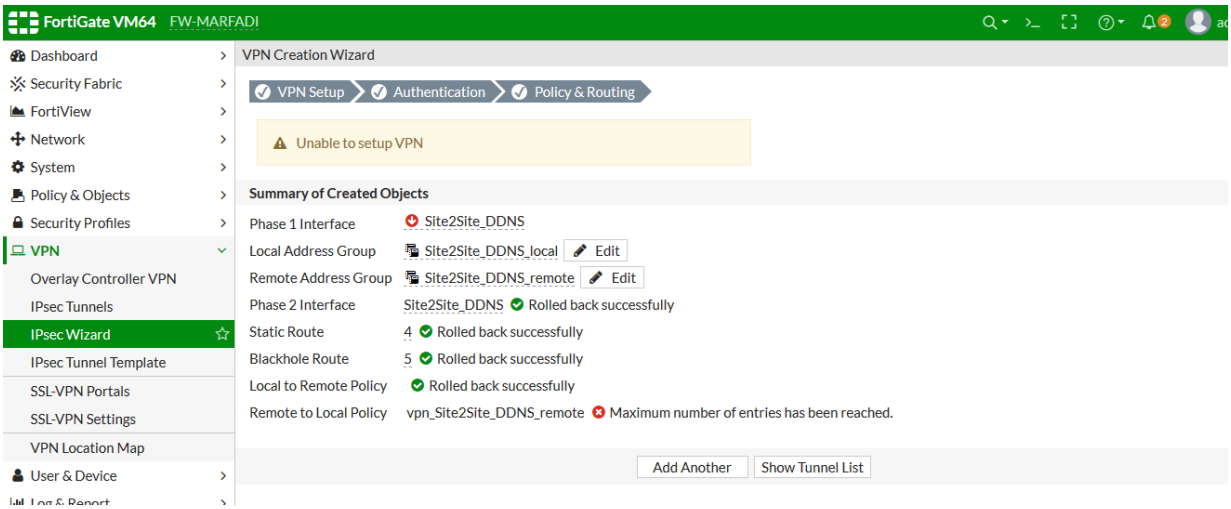




لنفترض بأن الDDNS للsite البعيد هو marfadi.com كما بالصورة أعلاه ..



كما بالصورة أعلاه . كم تم بالإعدادات الـ vpn site to site سابقا

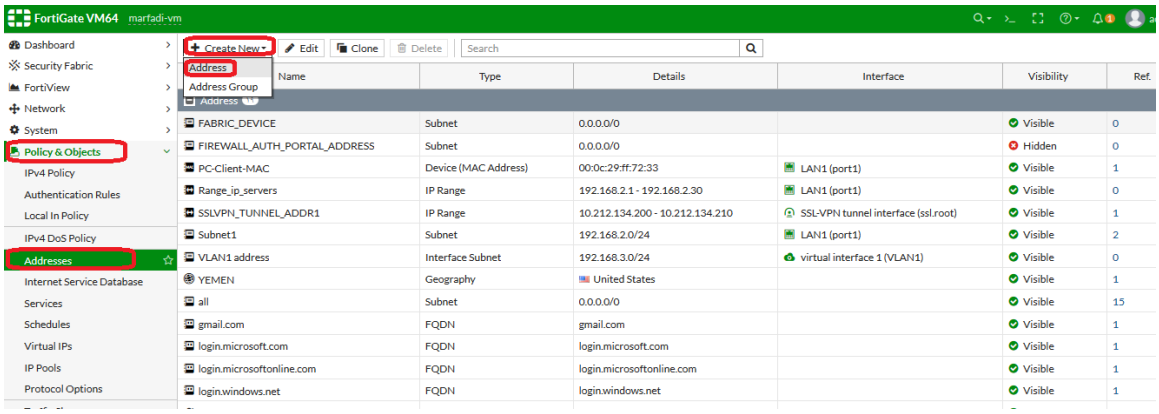


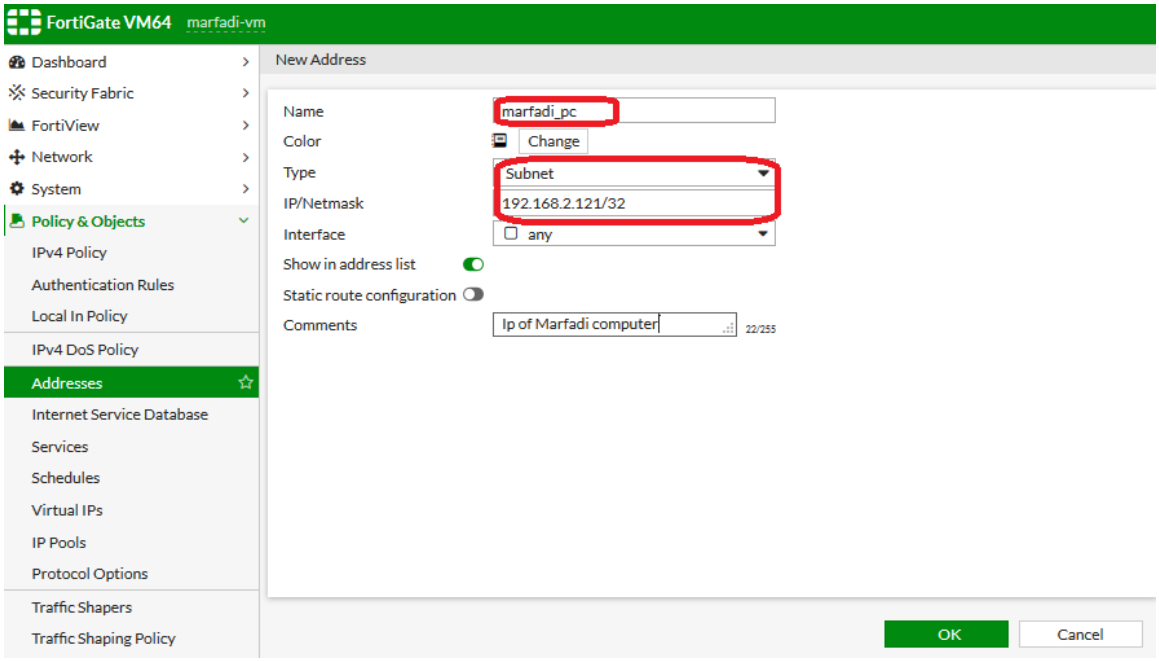
تمت العملية على الـsite1 وسوف نكرر نفس العملية على الـ site 2

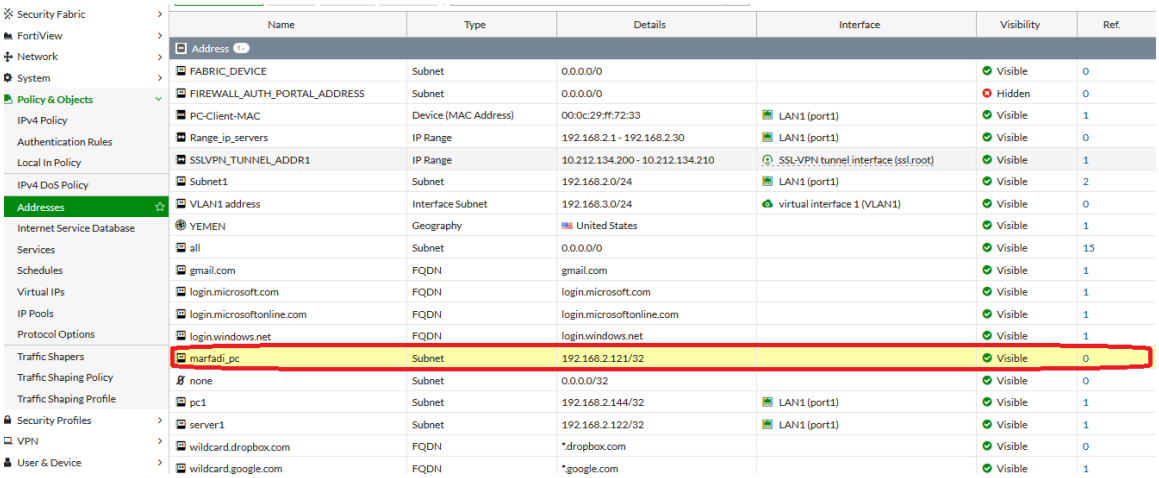
لكن في حال الـsite1 لديه static ip فاني سوف أقوم باستخدامه ...

: Network address

طريقة انشاء عناوين بالفورتي جيت







تم انشاء عنوان باسم marfadi_pc وتم تخصيص ايبي له 192.168.2.121

Traffic shaper :

هي عمليه تخصيص سرعه معينه سواء لـ 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 الفورتي جيت هي 200 كيلو بايت بالثانية سواء لعمليه الـ download او الـ Upload .

Maximum Bandwidth : اقصى سرعه هي 400 كيلو بايت بالثانية سواء لعمليه الـ download او الـ Upload .

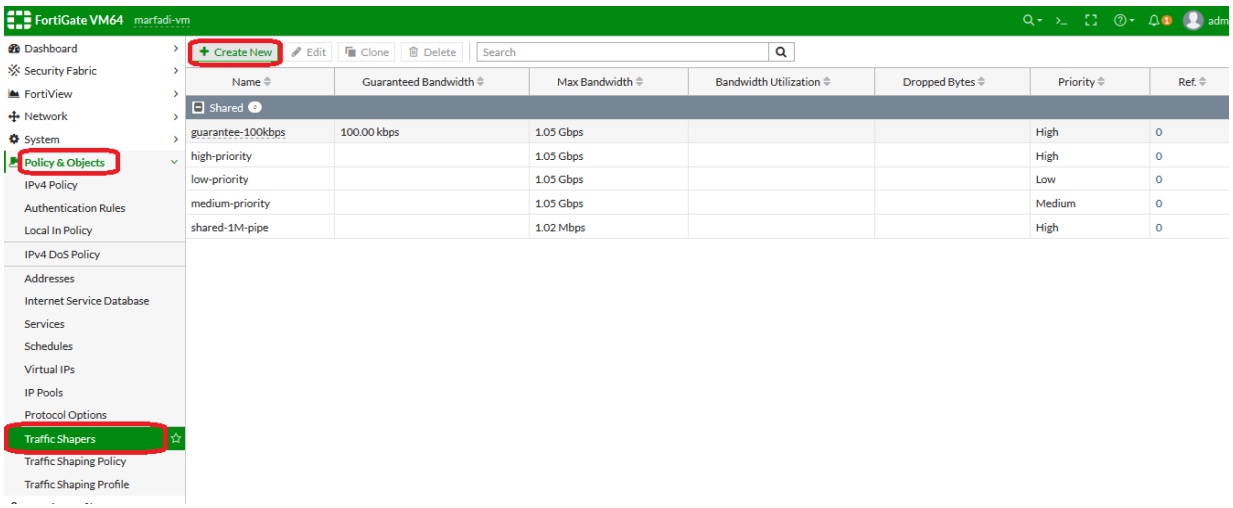
ملاحظة:

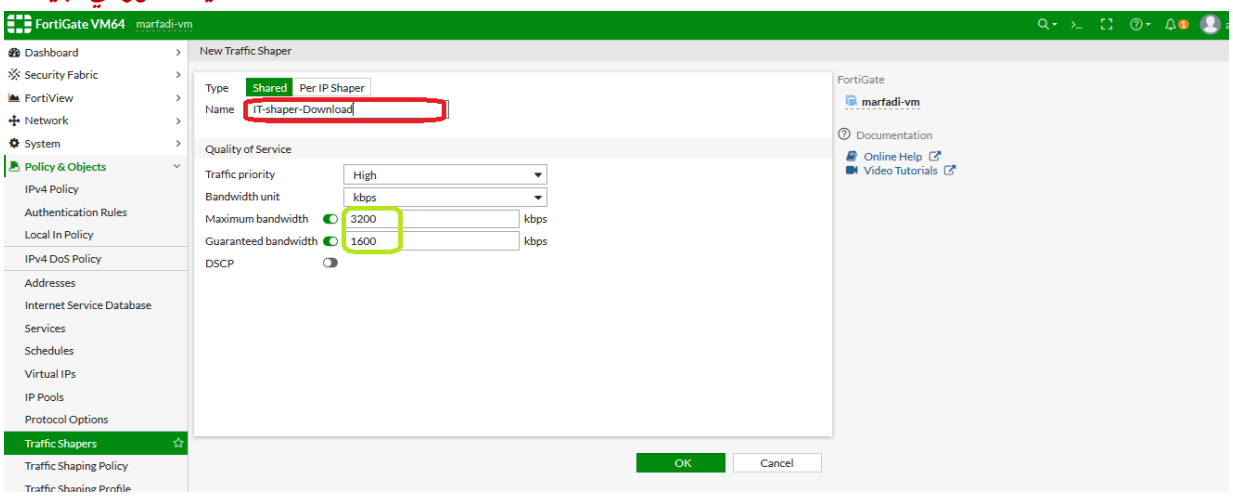
KBps :كيلو بايت بالثانية

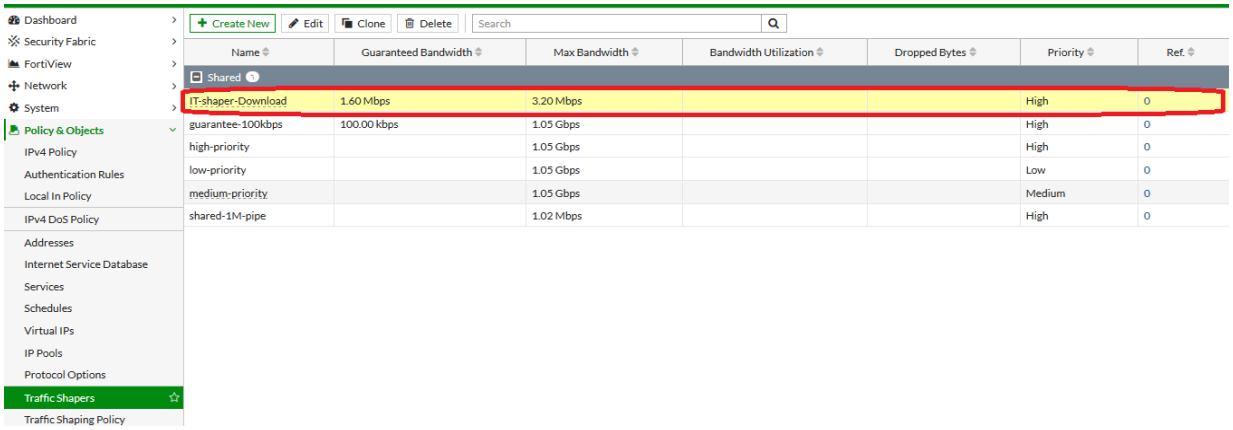
Kbps : كيلو بت بالثانية

KBPS=8 Kbps

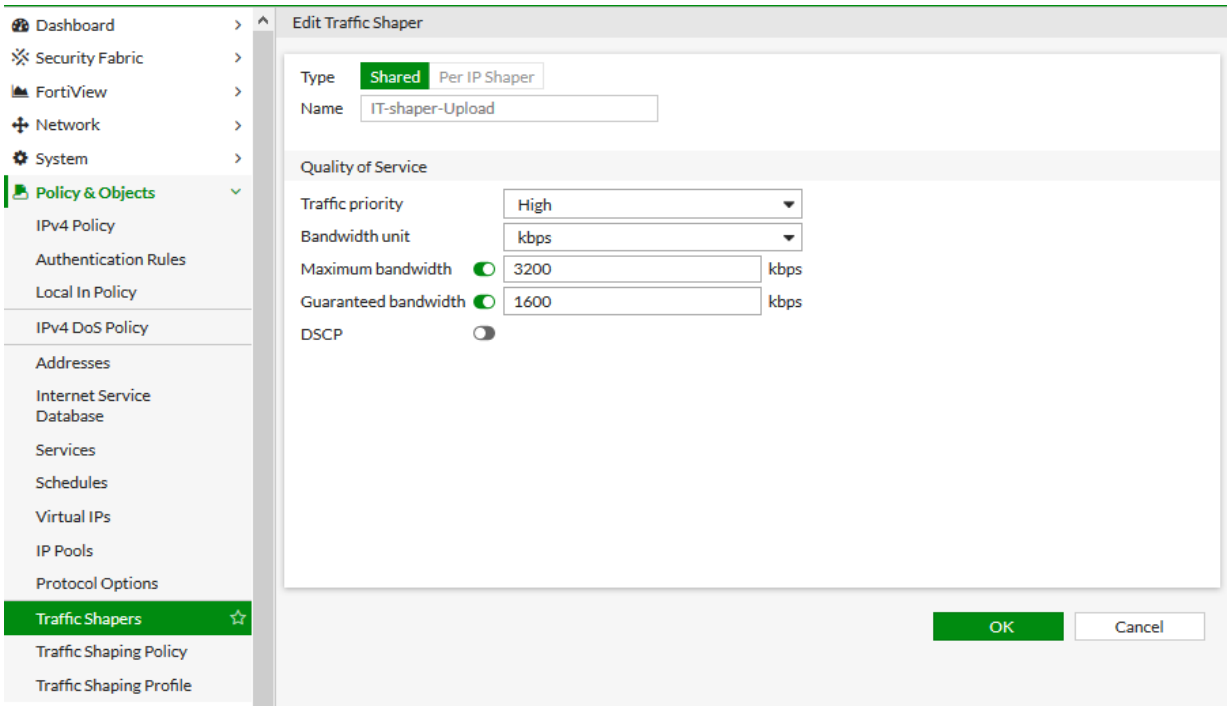
حيث سوف نقوم بإنشاء Traffic shaper كما بالخطوات التالية:

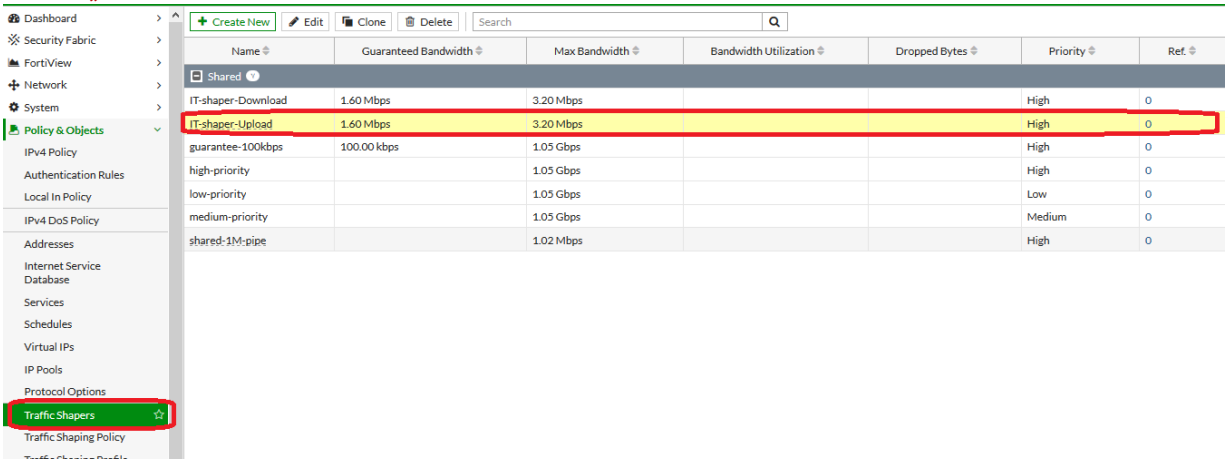






الان سوف نقوم بإنشاء traffic shaper for upload للـIT مثلا





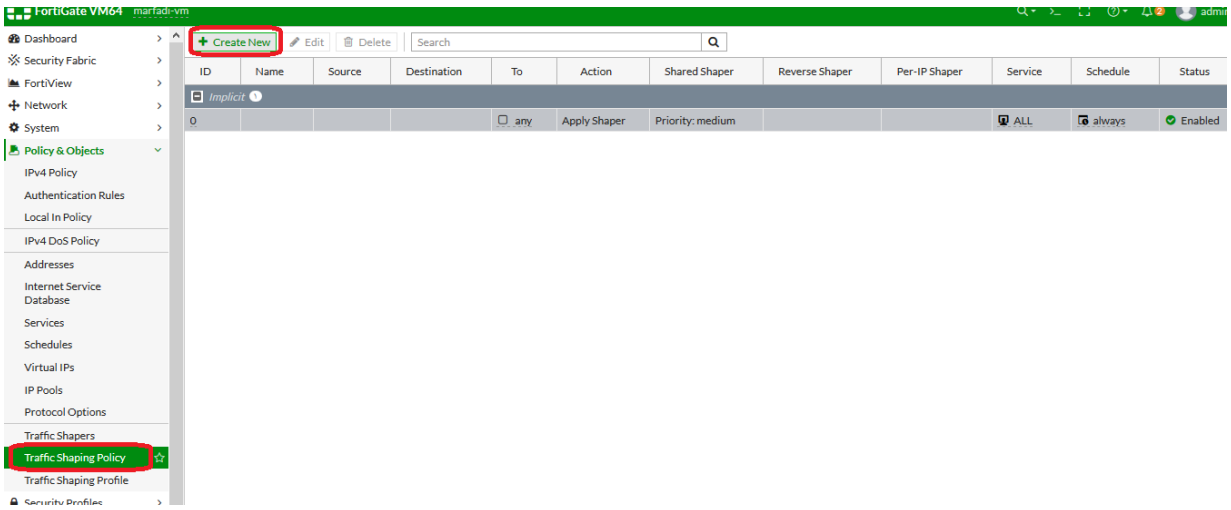
Traffic priority : وظيفتها إعطاء اولويه من يأخذ سرعات حيث الذي لديه priority اعلى هو من يكون له الأولوية في السرعات .

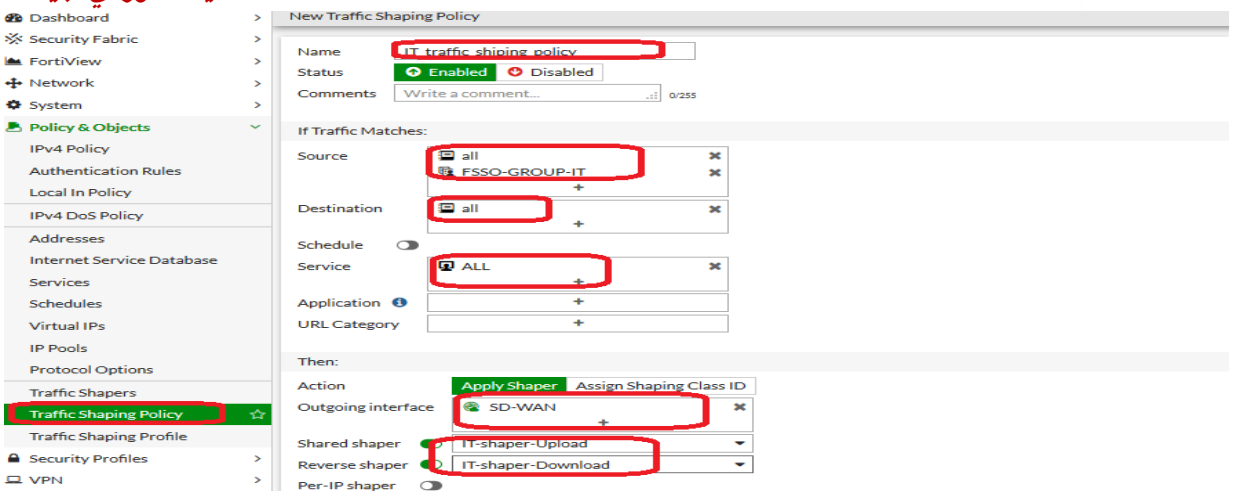
انوع الـtraffic shaper :

Shared :يتم تقاسم الـ traffic shaper حيث 400 كيلو سوف تقسم على عدد الأشخاص .

Per ip : يتم تخصيص traffic shaper لكل ايبي أي سيتم تخصيص 400 كيلو لكل شخص .

طريقة انشاء Traffic shaping policy :



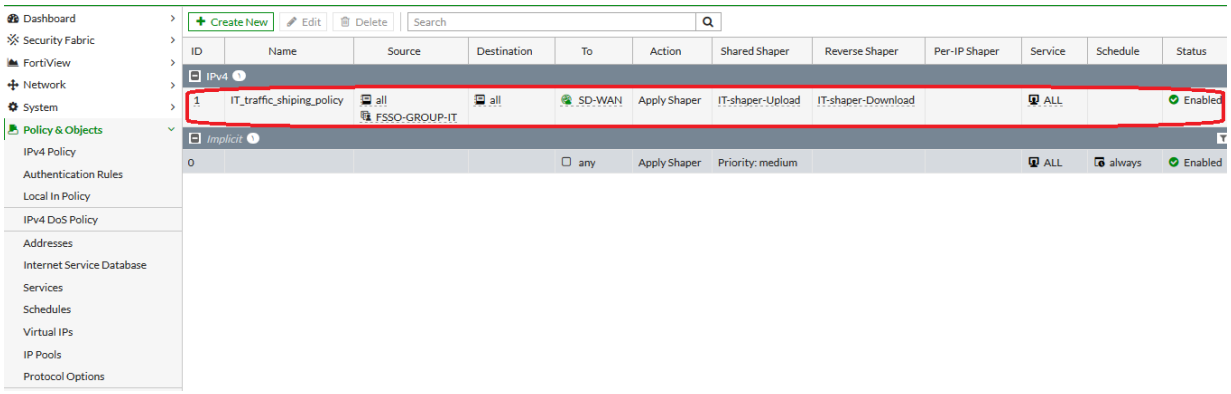


تم انشاء بوليسي لموظفي الايتي(FSSo-Group-IT)حيث

Shared shaper يقصد بها الـUpload

Reverse shaper يقصد بها الـ download حيث تم تحديد الـ traffic shaperالذي قمنا بإنشائها سابقا باسم IT-shaper-Download و IT-shaper-Upload

وبهذا أي يوزرضمن الجروب FSSO-GROUP-IT سوف يطبق عليها سياسه traffic shaping كما بالصورة ادناه ...



ملاحظة هامه :

أي بوليسي موجودة في قائمه الـIPv4 Policy فانه سوف يتم المرورعلى ال traffic shaping policy كما بالصورة أعلاه سيتم المرورعلى البوليسي المسماة IT_traffic_shiping_policy فان لم تطابق السياسة فأنه يمرعلى البوليسي المسماة Implicit والذي معناه لا تطبق traffic shaping على هذا البوليسي ...

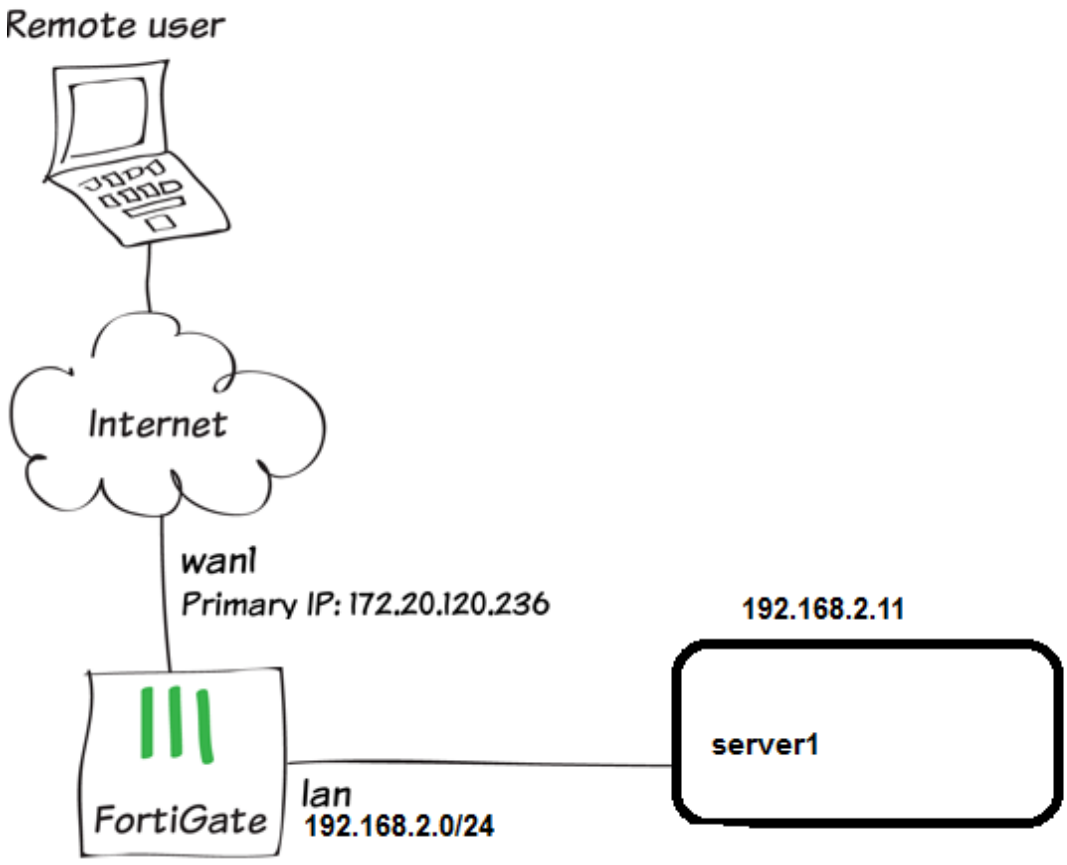
أي لو كانت الـ rule لا تطبق عليها احدى traffic shaping policy فأنها تمر على السياسة المسماة Implicit وهي موجودة بشكل افتراضي .. والتي تعني لا تطبق على هذه السياسة أي traffic shaping policy ...

Virtual IP : عمليه الوصول من برع الشبكة الى جهاز معين في الشبكة الداخلية.

مثلا :الوصول الي سيرفر موجود بالشبكة الداخليه عم طريق الremote desktop protocol او ما يسمى (RDP) ويسمى بعمليه الـ publishing .

او تريد مثلا عمل publish لـweb server الموجود بالشركة وتريد الوصول اليه من خارج الشركة..

حيث أقول للفورتي جيت لو وصل لك اتصال عبر بورت معين قم بإدخاله الى السيرفر الفلاني ..

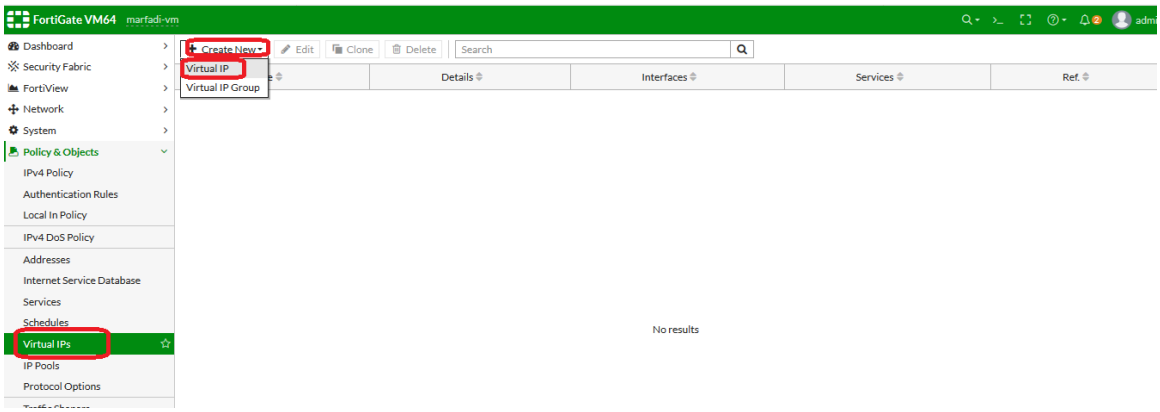


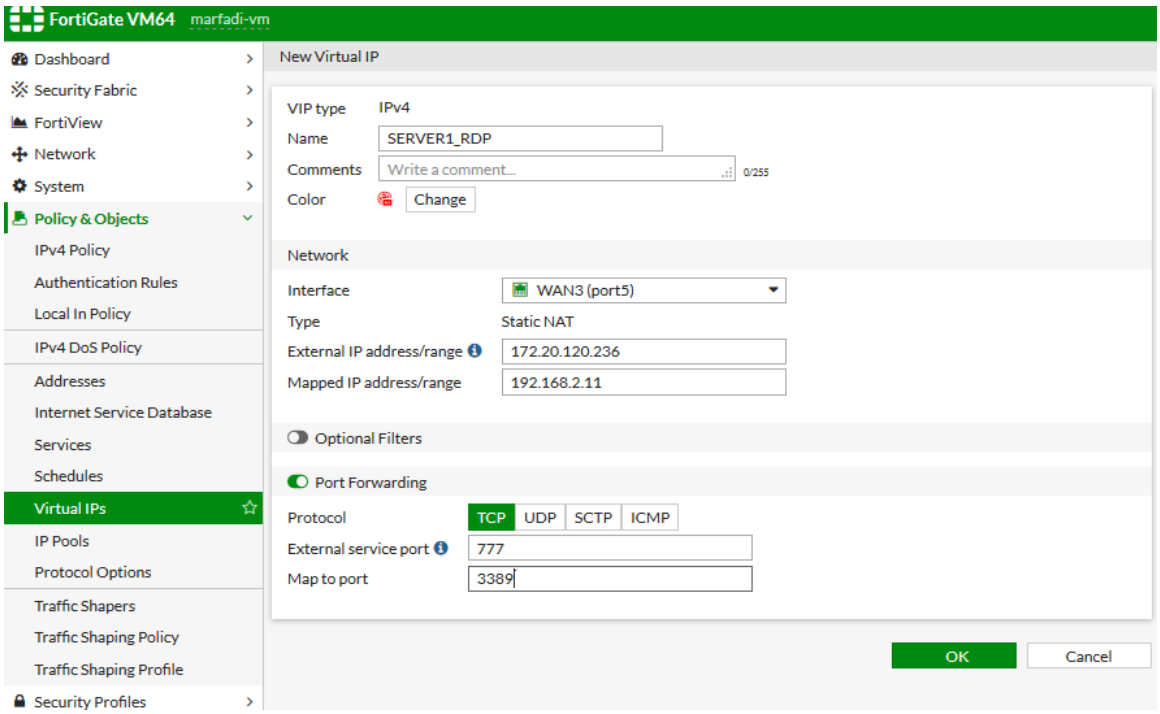
حيث wan1=172.20.120.236 هو public ip ..

فلو وصل لك أي اتصال الى المنفذ wan1 عبر الـport مثلا 777 فقم بتحويله الى الايبي التابع للسيرفر 192.168.2.11 عبر الـport 3389 وهو البورت الافتراضي لـRDP .

حيث قمنا بتغيير البورت الافتراضي لـrdp الى 777 كنوع من الأمان وتجنبا من فايروس التشفير(الفديه) ....

➢ طريقة انشاء Virtual ip :





حيث interface :wan3 وهو البورت الي موصل عليه الـ static ip وهو 172.20.120.236

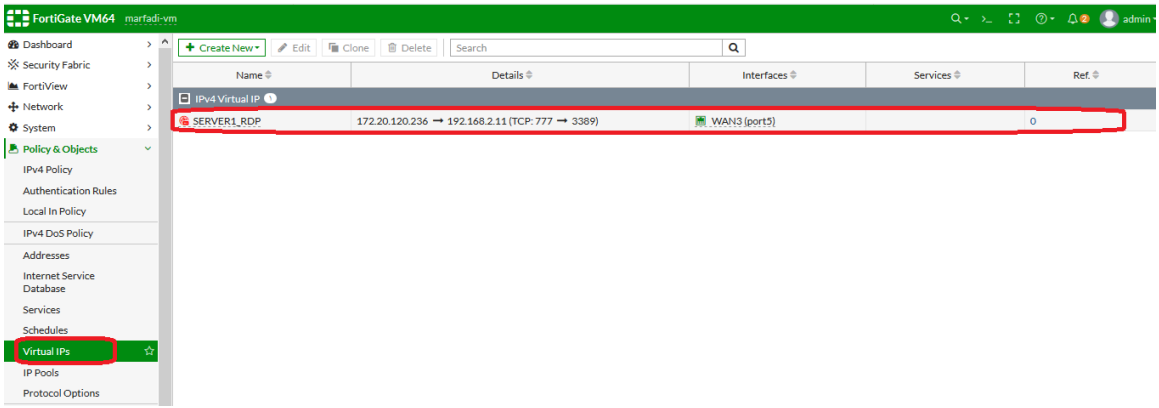
External IP address : هو الايبي الـ static الذي سيستقبل الـ connection

Mapped IP address : هو الايبي ال private وهو ايبي السيرفر server1 وهو 192.168.2.11 .

حيث سنقوم بتمكين الخيار port forwarding

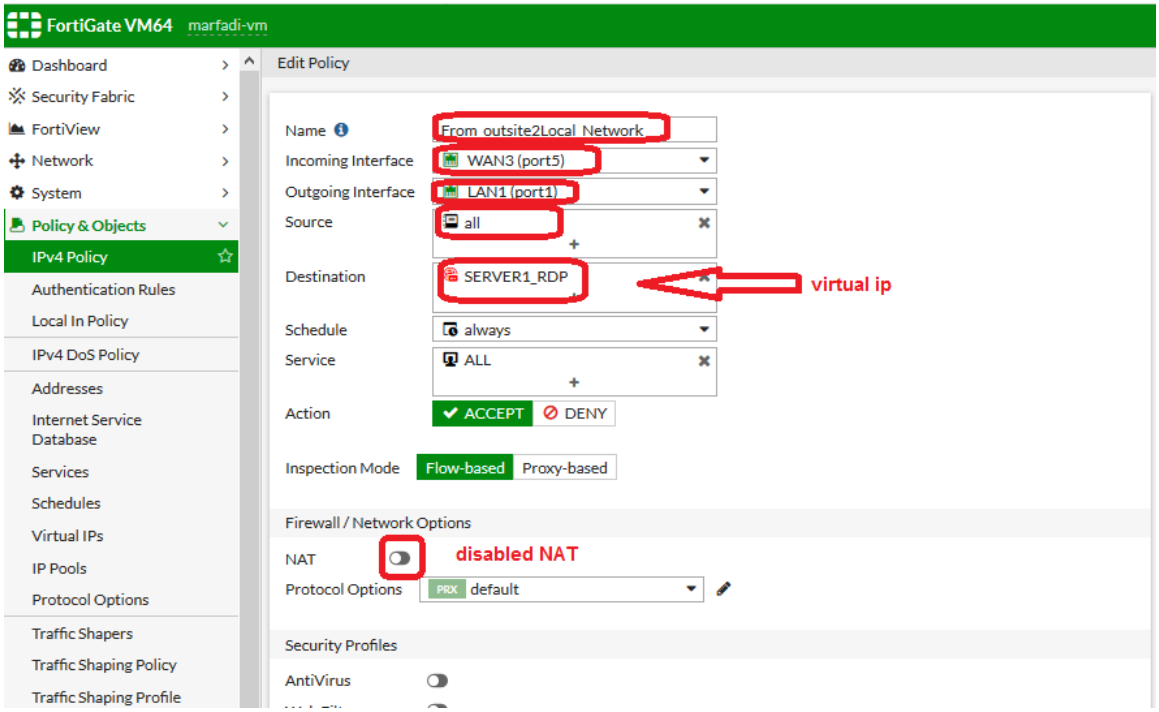
ونضع البورت 777= external والmap to port= 3389

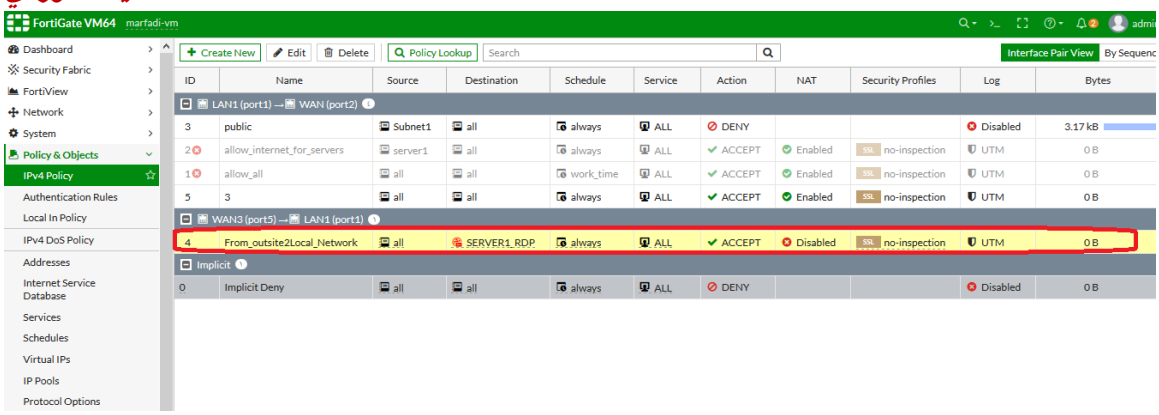
حيث اللي واصل لك عبر البورت 777 قم بتحويله الى البورت 3389 .



فبعد ذلك يجب ان أنشئ بوليسي تسمح بالاتصال من خارج الشبكة الى داخل الشبكة

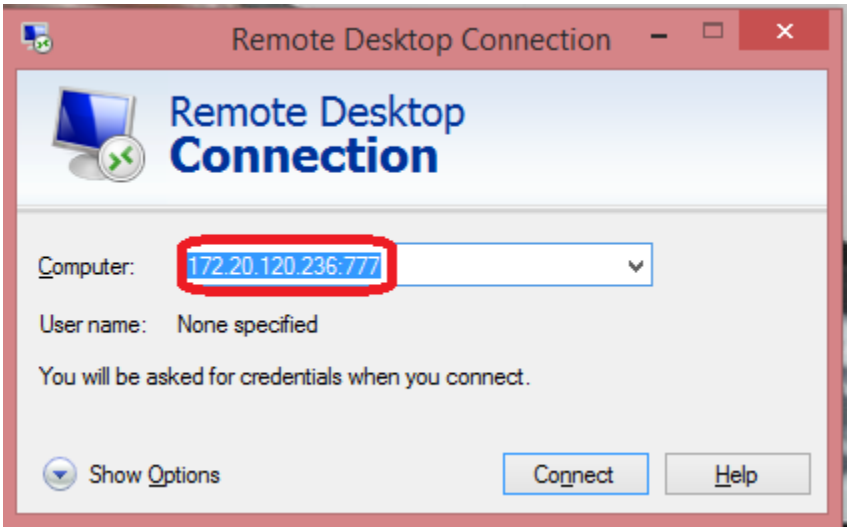
(internet الى local network).





تم انشاء البوليسي ....

الآن سنقوم بتجربة الوصول الى السيرفر server1 وذلك كالتالي

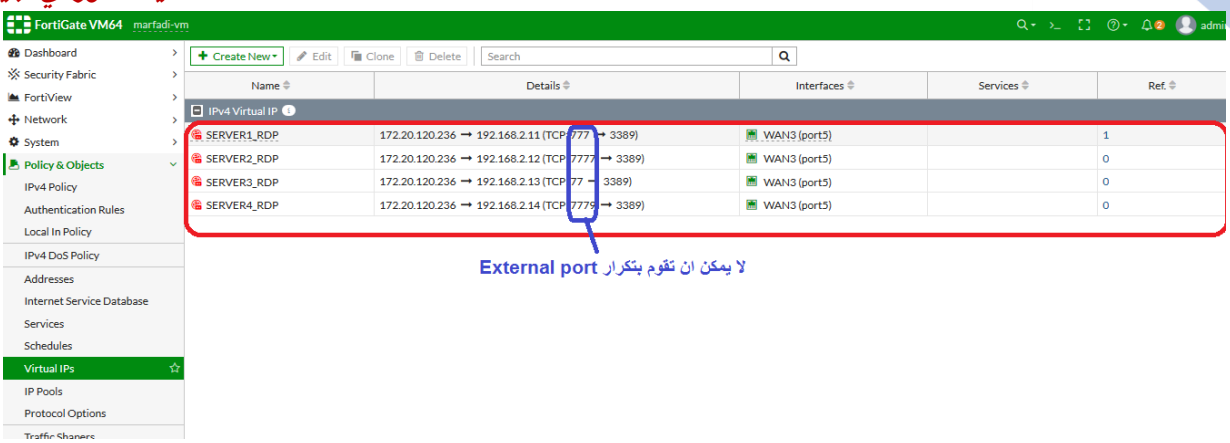


حيث بمجرد الدخول الى 172.20.120.236:777 سوف يتم تحويلك الى السيرفر 192.168.2.11 مباشره.

Virtual group :

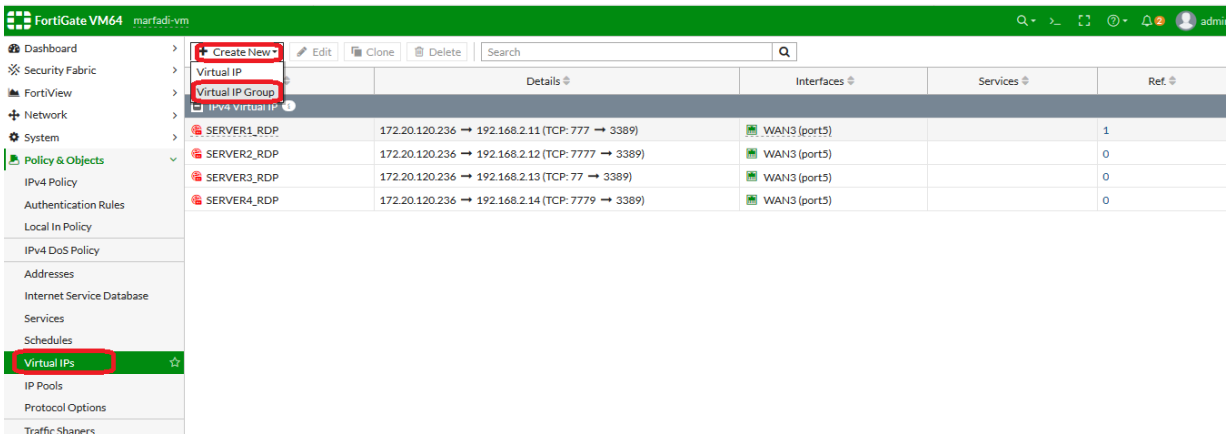
نفترض لدينا 4 سيرفرات معمول لهم 4 virtual ip

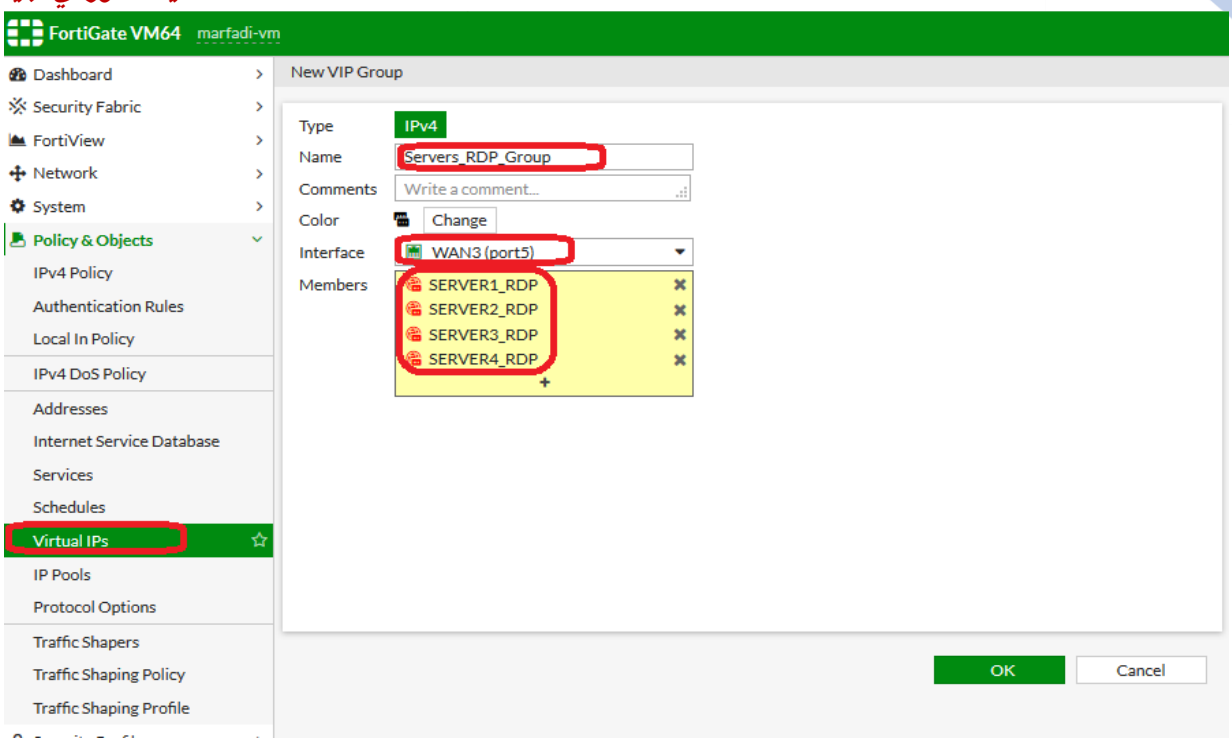
مثلا server1_RDP ، server2_RDP، server3_RDP ، server4_RDP كما بالصورة ادناه ..

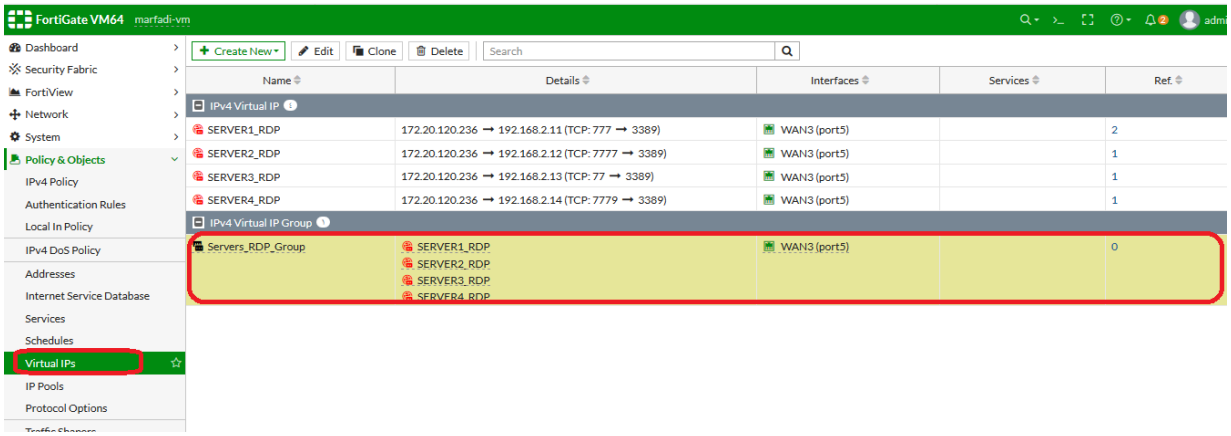


يجب External port يختلف من virtual ip لآخر...

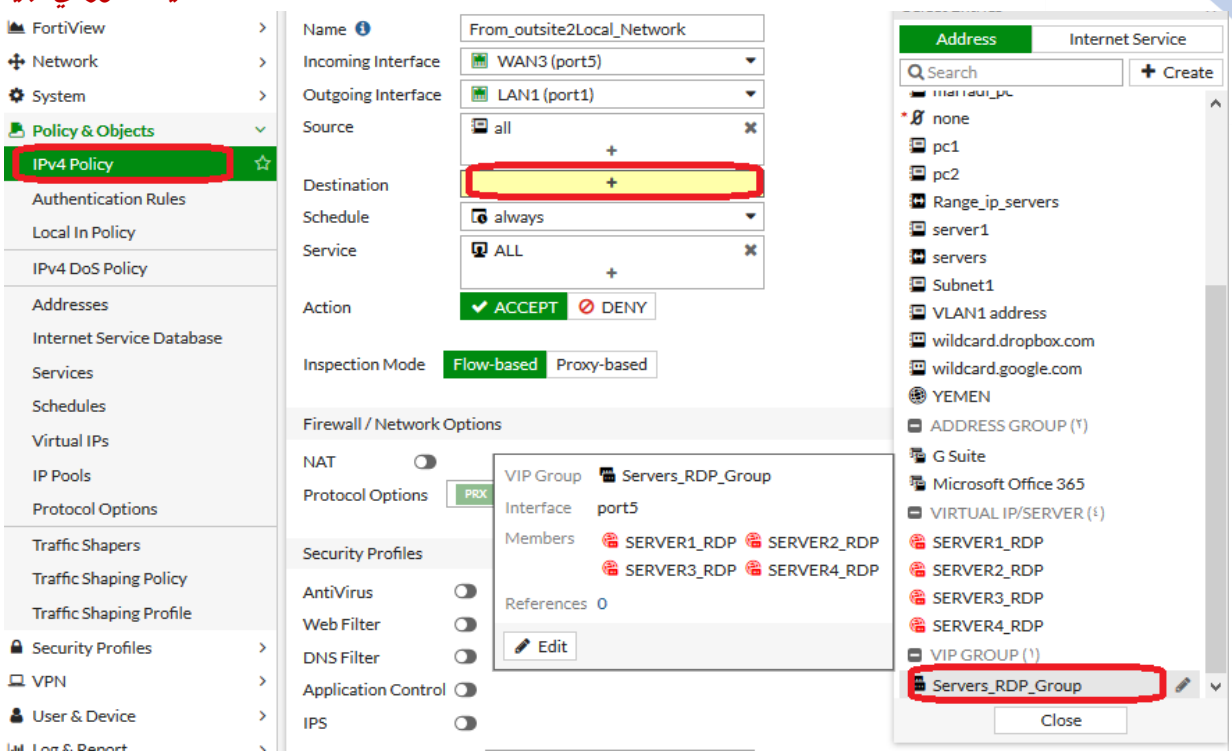
➢ **طريقة انشاء virtual group بحيث أقوم بضم الـ4 virtual ip's بداخلها ..**





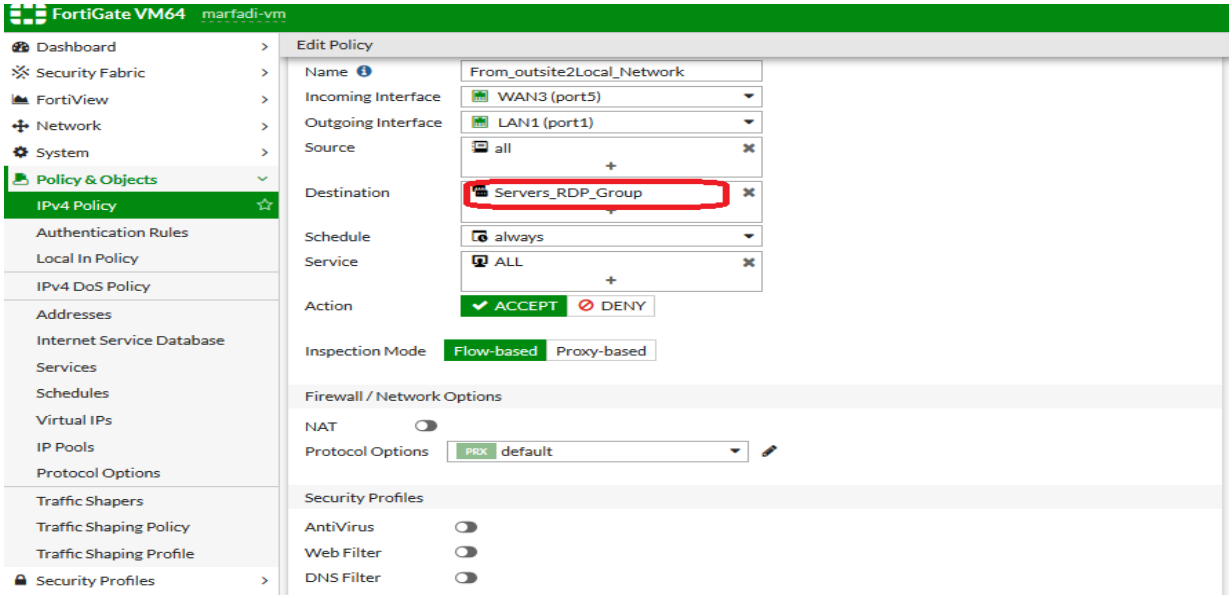


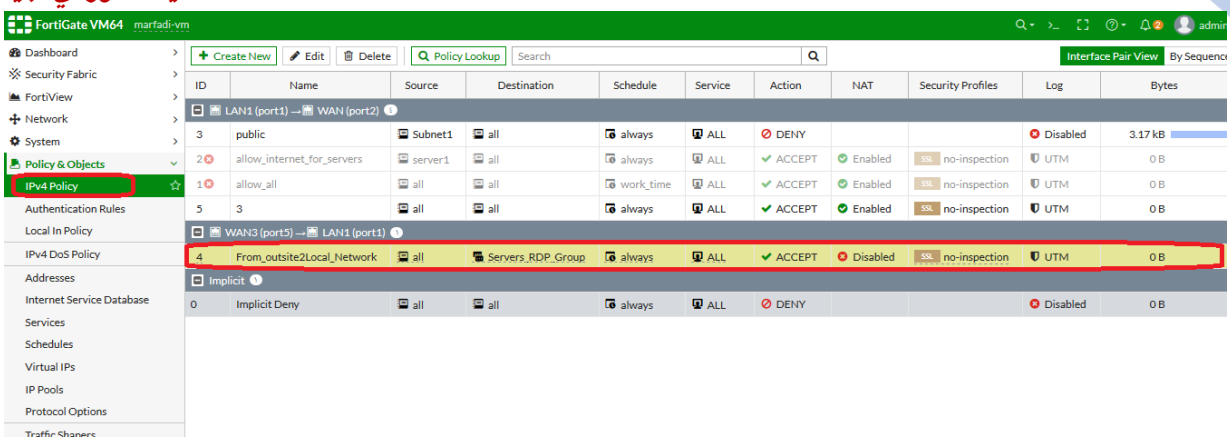
سنقوم بإعداد البوليسي التي تسمح بالاتصال من خارج الشبكة الى الشبكة الداخليه



كما بالصورة أعلاه تم تحديد الـdestination = Servers_RDP_Group

فبدلا من أضافه الـ4 virtual ip's فقط نقوم باختيار virtual group .





➢ IPV4 DOS policy configuration :

الـ TCP Connection عموما بيتم ارسال SYN من قبل المرسل ويتم الرد عليك من قبل المستلم بـACK ,SYN بأن الـ port مفتوح و جاهز للاستلام ومن بعد ذلك تبدا عمليه الارسال وتبدا الجلسة بينهما ...

فأحيانا تحصل هجمات تسمى DOS حيث بيتم ارسال كميه طلبات كثيره جدا على خدمه معينه من اجل ايقافها ...

مثلا سيرفر عليه remote desktop connection بيستلم الاتصال عبر البورت 3389 ،

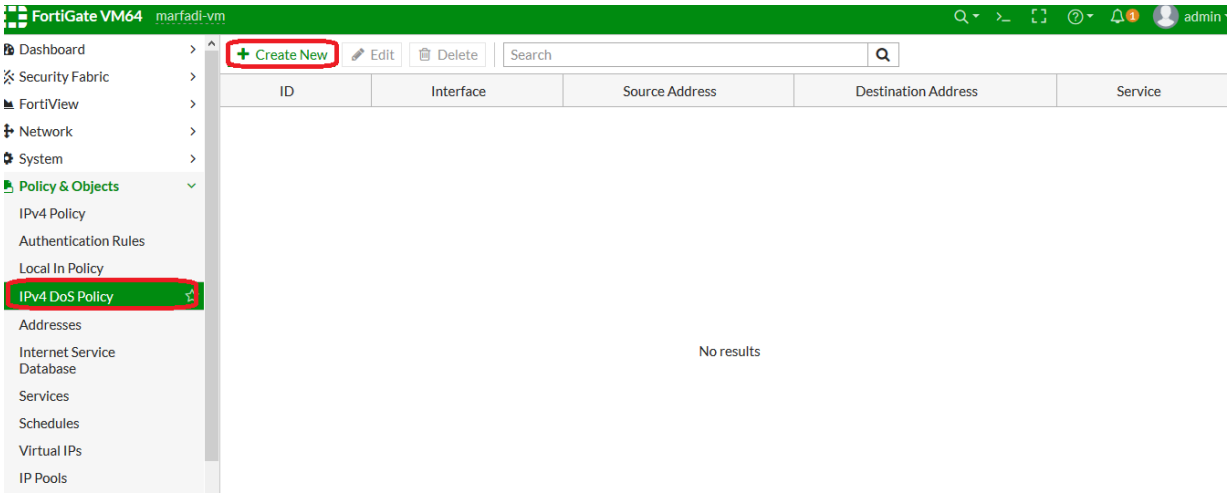
حيث ممكن استغلال هذا البورت المفتوح بحيث أقوم انا كا هاكر بارسال SYN و السيرفر سوف يرد بـACK ,SYN و تتكر العملية بيني وبين السيرفر الى ان تتم عمليه إيقاف الخدمة (RDP)لأن هناك أدوات وبرامج تقوم بعمليه ارسال ملائين من SYN في توزيعه كالي لينكس ..

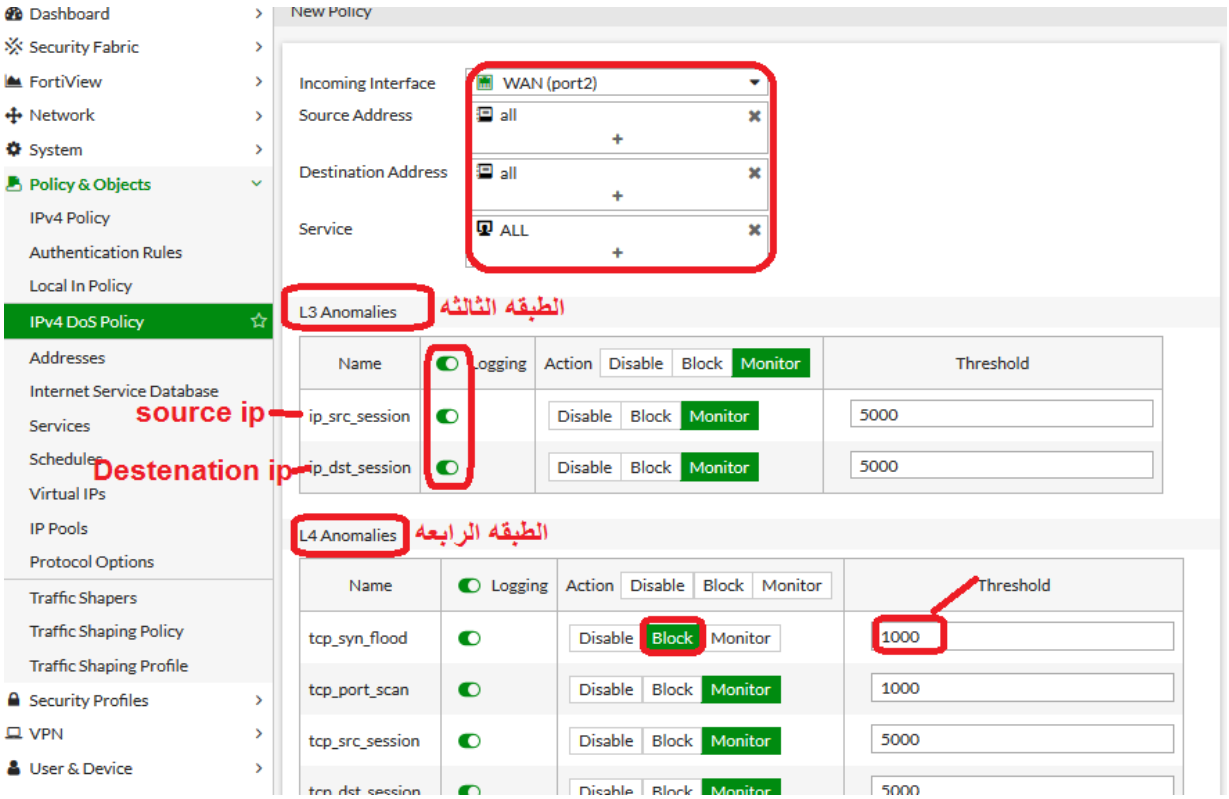
وهذا يسبب بأن الخدمة التابعة لـ RDP الموجودة في السيرفر تصبح Down وتسمى هذا العملية TCP syn flooding attack وتعتبر نوع من أنواع الـDOS attack .

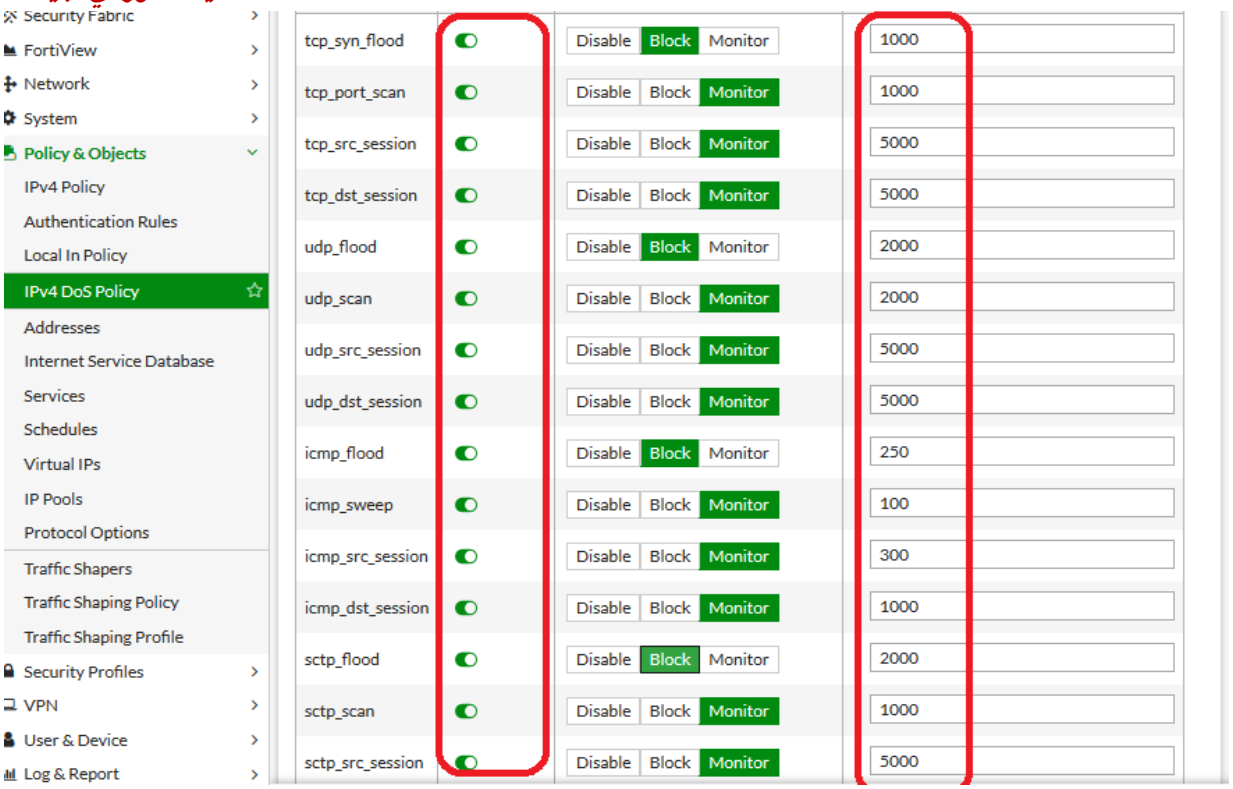
يوجد أيضا هجمات أخرى مثل الـ ICMP syn flooding attack و UDP flooding وغيرها وكلها تندرج تحت الـDOS attack .

فالفورتي جيت عنده خاصيه جميله اسمها IPV4 Dos policy حيث تستخدم هذه الميزه من اجل منع والتحكم بهذا النوع من الهجمات ..

الآن سنقوم بإنشاء policy تمنع هذه النوعيه من الهجمات من برع الشبكة(من الانترنت)

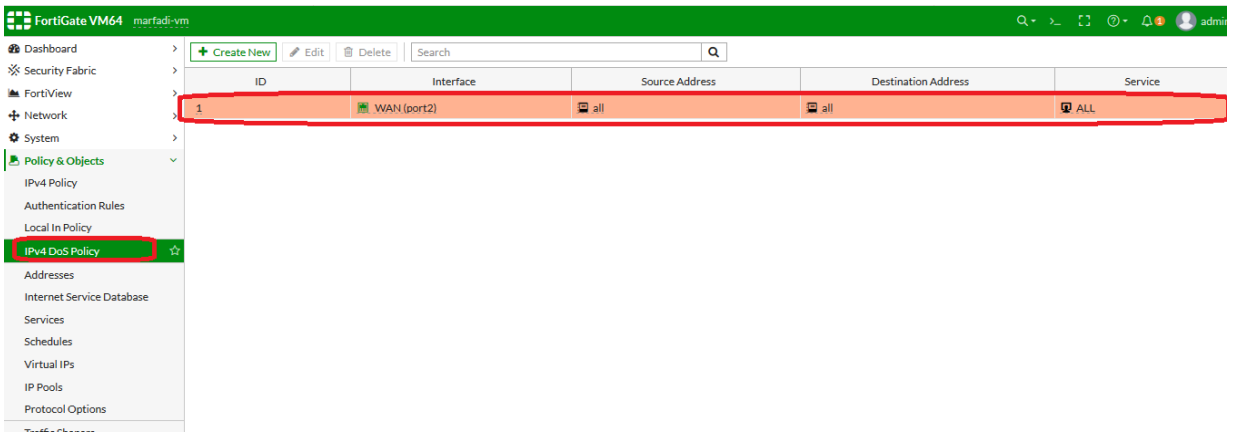






الصور أعلاه توضح بان عمليه الفحص والتحكم بالـ connection القادم الى الـ wan interface حيث سيتم عمل log للاتصال القادم من او الى source ip و Destination ip وتعدى الـ5000 .

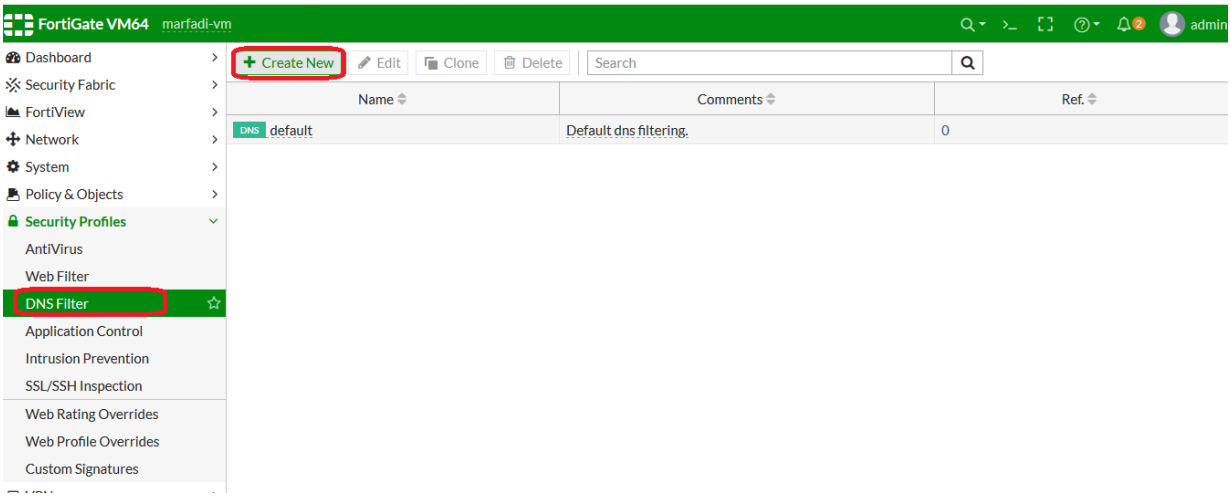
أيضا يتم عمل Block لـtcp_syn_flood لو وصل عدد الجلسات عن 1000 لبورت معين ..وهكذا

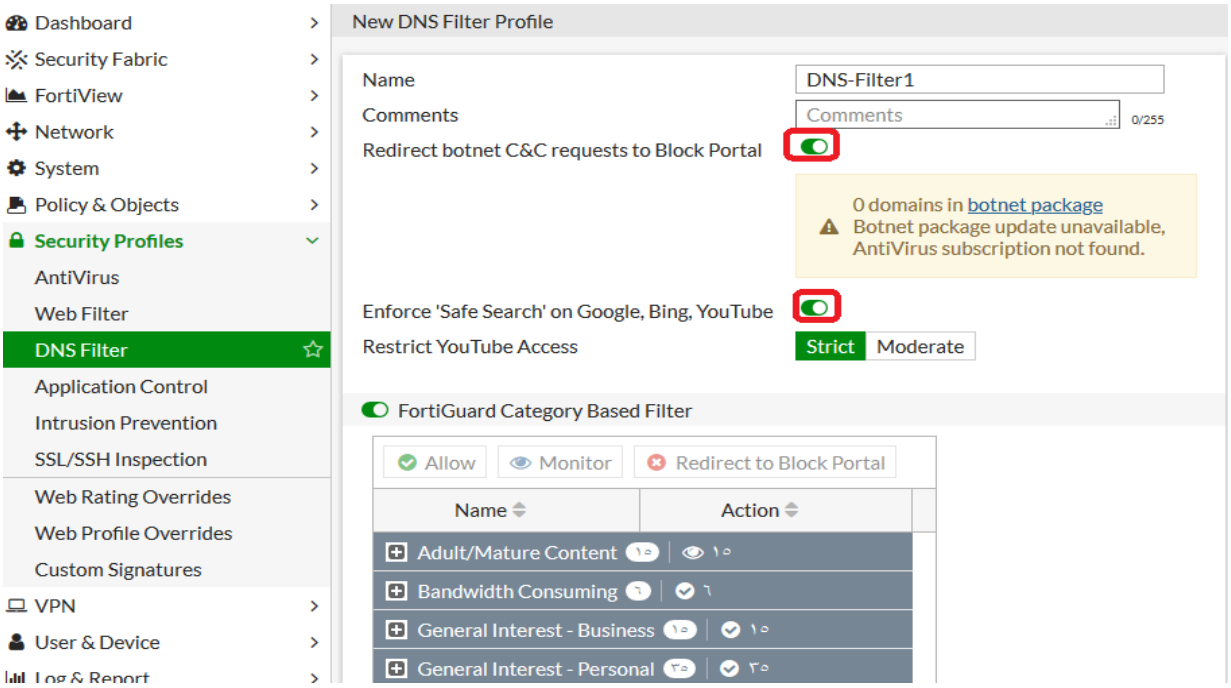


بهذا انا قمت بتأمين الترافيك الذي يأتي عبر الـwan interface سواء على شكل tcp او udp او icmp من هجمات الـDOS .

➢ DNS Filtering :

عباره عن خاصيه بالفورتي جيت استطيع ان اعمل بها web filtering بواسطة الDNS





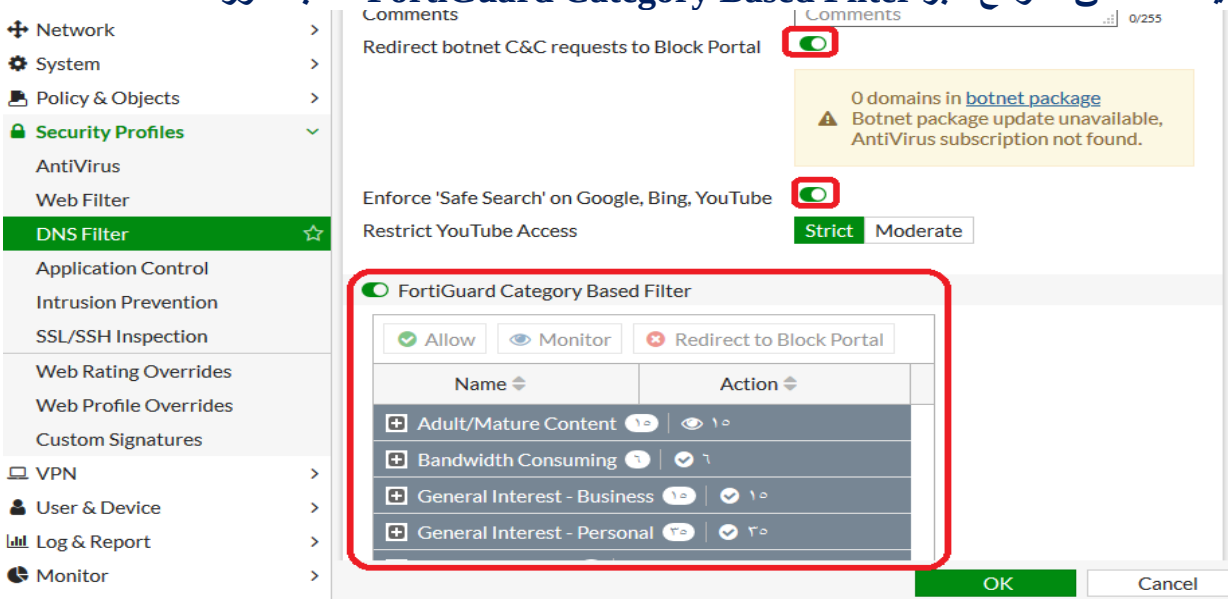
: Redirect botnet C&C requests to Block Portal

الفورتي جيت سوف يقوم بإغلاق الوصول لأي Domains خاص بالـBotnet ..

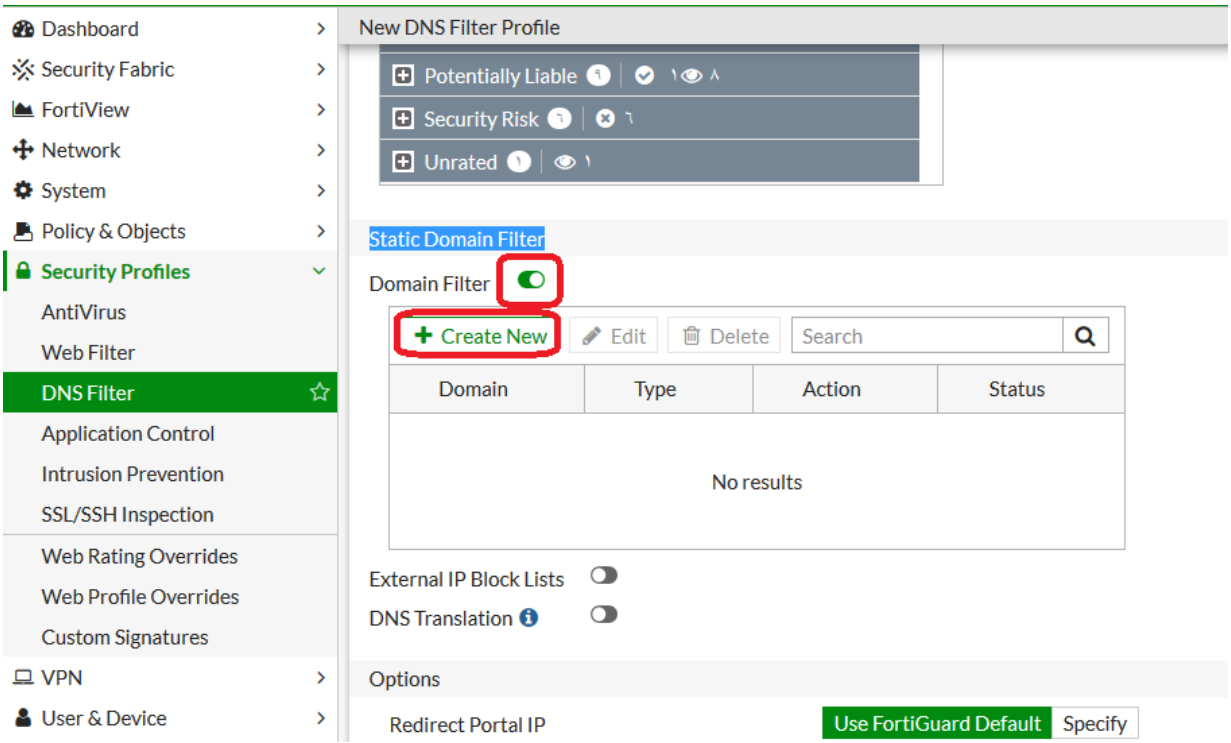
: Enforce 'Safe Search' on Google, Bing, YouTube

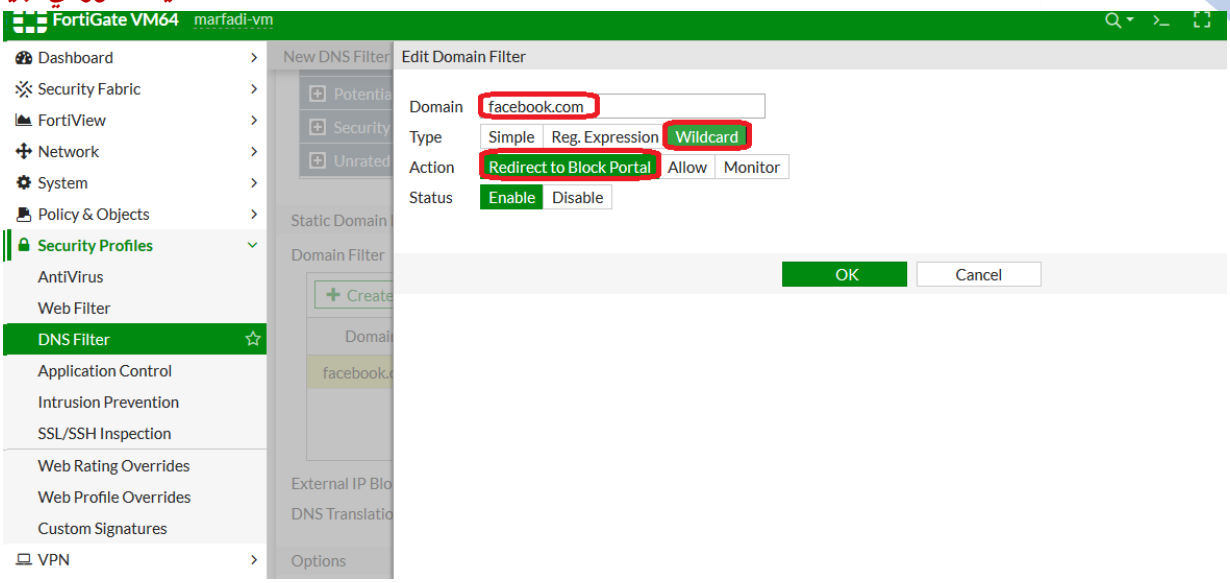
عند تفعيل هذه الخاصية فان عمليه البحث ستكون أمنه ويتم استخدام هذا الخيار خصوصا في المدارس ،حيث سيمنع الوصول او البحث عن أي موقع محضور او غير مناسب فلو قام اليوزر البحث مثلا عن مواقع اباحيه او مواقع تجاره الأسلحة ..الخ سيتم منعه وعمل له .

كما يمكننا اغلاق المواقع عبر FortiGuard Category Based Filter كما بالصورة ادناه



استخدام Static Domain Filter لأغلاق المواقع :





عمل Block لموقع الفيسبوك ...

➢ الفرق بين ال web filter And dns filter :

الويب فلتر يعمل Block للموقع عبر الـURL

يعني ممكن تقفل الـwww.marfadi.com/test و بنفس الوقت تكون سامح ان المستخدمين يفتحوا Www.Marfadi.com/users

لكن الـDNS filter بيقفل عبر الـ DNS Queries من البداية أصلا ..
يعني لا يعمل resolve لـwww.marfadi.com أصلا ..

الخاتمة

الحمد لله تعالى الذي وفقنا في تقديم هذا الكتاب، وها هي القطرات الأخيرة في مشوار هذا الكتاب، وقد كان الكتاب يتكلم عن فورتي 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 أرتقت بدرجات العقل الفكر، حيث لم يكن هذا الجهد بالجهد اليسير حيث استغرق تقريبا 8 اشهر من الاستماع لفيديوهات مختلفة والبحث في الفورتي جيت من مصادر مختلفة، ونحن لا ندعى الكمال فإن الكمال لله عزوجل فقط وانا أصلا شخص مبتدأ في الفورتي 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، واخيراً نرجو أن يكون هذا الكتاب قد نال إعجابكم. وصل اللهم وسلم وبارك تسليما كثيراً على معلمنا الأول وحبيبنا 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