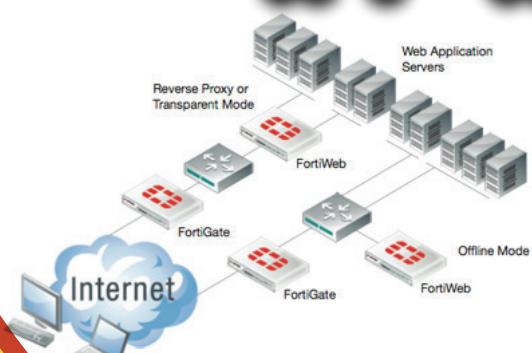




# الفورتي جي

بالعربي



إعداد المهندس

ياسر الزنوني



[www.yaserelzanouny.com](http://www.yaserelzanouny.com)



Yasserelzanouny

Sub:

Date:

## "1" FortiNet Certification

شركة FortiNet تأسست عام 2005 في مجال Security products 22 على مستوى العالم.

FortiCom , Fortianalyzer , Fortimail , Fortigate ;  
FortiDvr , Fortiweb , Fortidatabase.

hardware & Products كانت تعامل بشكل كبيرFortiNet  
Software UTM لكونها تعاونت مع شركة VMware وعليها  
بيانات ووزع سعر الجهاز.

Not Recommended ← Software

### Certification

**FCSNA**

**FCSNP**

"FortiNet Certified Security Network Associate" "FortiNet Certified Security Network Professional"

كانوا شهادتين يحصلوا على Fortigate

**NSE**

غير الاسم

2015 - 6 - 2

Network Security Expert

8 levels

و دول متعددة بالتفصيل



## NSE levels

- ① NSE1 → Network Security technology "Free"  
Fortinet مختبرات الامن
- ② NSE2 → Network Security Solution "Free"
- ③ NSE3 → Advanced Network Security  
• Free for partners or employee on Fortinet
- ④ NSE 4 → FortiGate levels overview "400\$"  
Routing و VPN  
• لا يتطلب امتلاك ميزانية ولوائح قيادة  
FCSNA
- ⑤ NSE 5 → FortiManager + FortiAnalyzer
- ⑥ NSE 6 → FortiMail Or Fortiweb Or  
Forti Dos Or Forti Send Box Or  
Forti wireless  
• لا يتطلب امتلاك ميزانية
- ⑦ NSE 7 → FortiGate → level3 VPN + Routing  
NSE4 مترافق
- ⑧ NSE8 → T-Shooting لحل مشكلات الشبكة



الكورس يتبعنا بزيارة عن

NSE → level 4 + level 7

Dynamic Routing

OSPF

RIP

BGP

Wireless Control

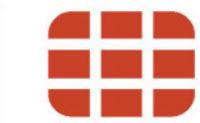
ويمضي الـ

اتنته لوجهها بتراكب على طبق

لوحة تحكم المعاير View N Device

www.FortiGate.Com  
user: demo  
Pass: demo

(x) the session log panel



④ ③

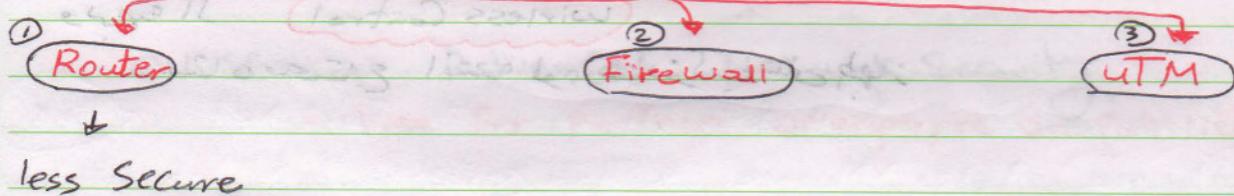
## 2. Introduction

### Network Security Technology

3 Devices <sup>جهاز</sup> يدخلوا <sup>جهاز</sup> Network <sup>جهاز</sup> Secure <sup>جهاز</sup> Less Secure

Network First Devices <sup>جهاز</sup> <sup>جهاز</sup> <sup>جهاز</sup>

خط لفاف داخل رينقسووا (3 اندو)



less Secure

① Router

SubNet A

SubNet B

10.

Router

172.

transmit Data

جيروفا مخلي Subnet ② مخلي

• Disable Interface <sup>مغلق</sup> داخل <sup>جهاز</sup> <sup>جهاز</sup> security <sup>جهاز</sup>

Not Secure ← Router <sup>جهاز</sup>

Packet Filter <sup>او</sup> access Control <sup>او</sup> <sup>جهاز</sup> <sup>جهاز</sup> <sup>جهاز</sup>

Policy <sup>او</sup> NAT <sup>او</sup> VPN <sup>او</sup>

Deny Any Broadcast Traffic

Layer 3

بعد Router <sup>جهاز</sup>

② Firewall

Security + Router <sup>جهاز</sup> Router <sup>جهاز</sup> <sup>جهاز</sup> <sup>جهاز</sup>

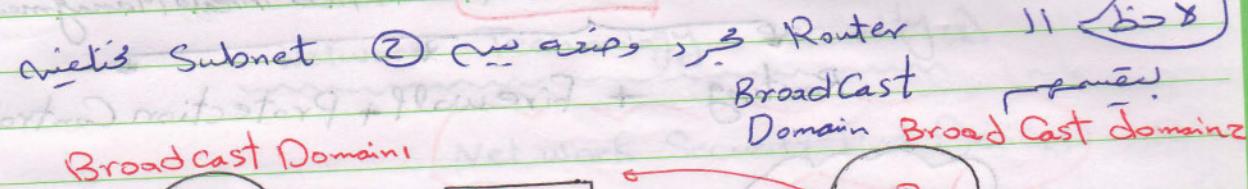
Layer 4 <sup>جهاز</sup> <sup>جهاز</sup> Firewall <sup>جهاز</sup> <sup>جهاز</sup>

Policy <sup>او</sup> Data <sup>وتحل</sup> Packet <sup>جهاز</sup> <sup>جهاز</sup> <sup>جهاز</sup>

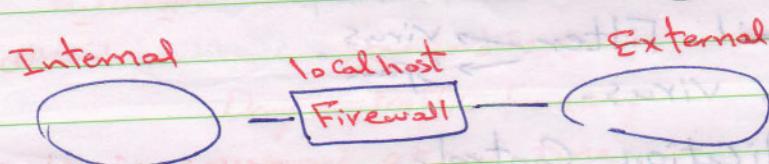
④ Deny Any Traffic From any Network in Any time

Cisco بيع ASA : <sup>جهاز</sup>





Deny any Broadcast traffic Anti Security !!



- 1 - Local (Internal)
  - 2 - External
  - 3 - local Host
  - 4 - VPN → Secu

Interfaces من Router و Firewall میں اسے ادا کرنے والے ہیں  
Enabled ہیکوئے Firewall کا ساتھ میں اسے ادا کرنے والے ہیں  
Disable ہیکوئے Router کا ساتھ میں اسے ادا کرنے والے ہیں

# Unified Threat Management

6

③ **UTM** unified threat Management

Routing + Firewall + Protection Control

Layer 7

يعتبر UTM من الأدوات

UTM Features (Components)

1- Routing.

2- Firewall

3- Email Filter → Virus → Spam

4- Anti virus.

5- Application Control - messages

التحكم في البرامج متعددة الأجهزة سواء موبيل او كمبيوتر

6- Device Control . برامج الكمبيوتر

7- IPS - Intrusion Prevention -

8- Data leak prevention

البيانات التي لا يراد لها خروج من الشبكة

9- End Point Control

FortiClient

10- VPN → IPSEC

→ Site-to-Site

→ SSL

11- Wireless Control

12- High availability

13- Bandwidth Control

External traffic من خارج utm يتحكم utm في Internal traffic

لتحقيق امن اعلى لبيانات العملاء، يجب على utm تحكم في اتجاهات الاتصال

14- Log & Report

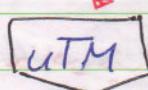
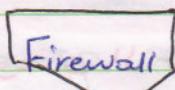
15- web Filtering

Sub:

Date:

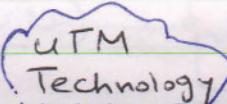
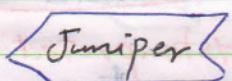
### 3. Introduction to Network Technology Security

#### Net work Security First Devices



- Routing
  - NAT
  - VPN
  - Packet Filter هاتن فيه انت اللى بتعملها
- Routing
  - NAT
  - VPN
  - packet filter موجودة
- Router + Firewall + System Protection

Deny any traffic From any Network at any time



مايكروطق أول شركة اشتغلت بالـ

Open traffic Policy إذا كان يعلم على Firewall لقطة

traffic اللى تابنه على Port معين هيلو 80 يعرف كمال Network

Virus لجه Scan يعلم UTM Scan بنخلاف أى traffic وهواسعى

أى traffic وهواسعى

7 layers لكل سطح Data لكل

1 - application

2 - presentation

3 - Session

4 - Transport → port داتا صوت → 65535

5 - Network

6 - Data link

7 - physical

Source → Destination

mail → 25

HTTP → 80

POP3 → 110

HTTPS → 443

RDP → 3389

٨

لآخر البت  $\rightarrow$  Firewall ونابحتم  $\rightarrow$  Mail  
Port  $\rightarrow$  25  
كنت بفتح فقط

لكن عند استخراج traffic من يمرر UTM  
log, Report, IPS, Anti-Spam, Antivirus  
Bw, DLP

الكتير دا يطبق لو عندى MailServer في الشركة خاصه  
لكن لعامل Hosting بيترا من بعد على دا كله  
Hosting دايم، لشركة اللي عامل عده هيا اللي المفروض  
ديوه UTM يعني الكتير دا.

### UTM Modes

NAT mode  
Full UTM  
Router Firewall

Transparent mode

System protection

Only System protection  
switch Concept

يعنى معنده nothing Firewall  $\times$  NAT  $\times$  Routing

Bur, Report, anti-Spam, anti-Virus

يعنى تركيب Firewall + معاد

Backend

Firewall  $\rightarrow$  BackEnd  $\rightarrow$  FrontEnd

Frontend

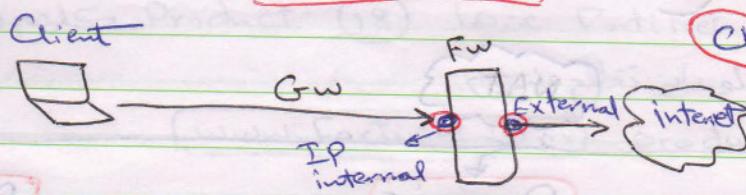
الله دى يستخدمها فقط لو شركه معايزه تركيب وهيا  
البعض منها AsaFirewall منها فحصها التكلفة مش هيسحب  
System Protection قييقلى دور ال Firewall فقط

Not Recommended

Transparent Mode



### NAT Mode



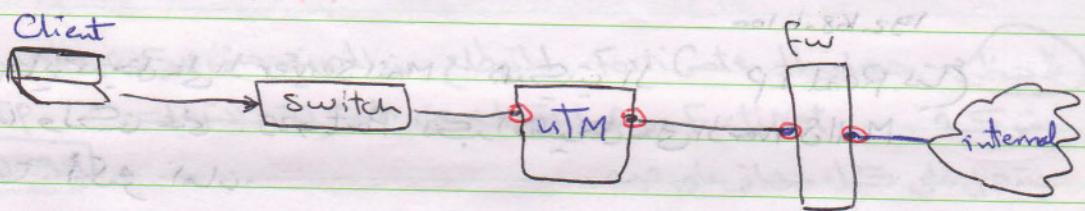
Client || Firewall || Switch على نفس الـ IP

Internal IP ② داخل Firewall  
ويمكن تغييره على IP External  
Firewall ① user Interface Gateway

### Transparent Mode

كل الـ IPs يكونون على نفس الشبكة وسيتم تغيير Management IP فقط

Management IP



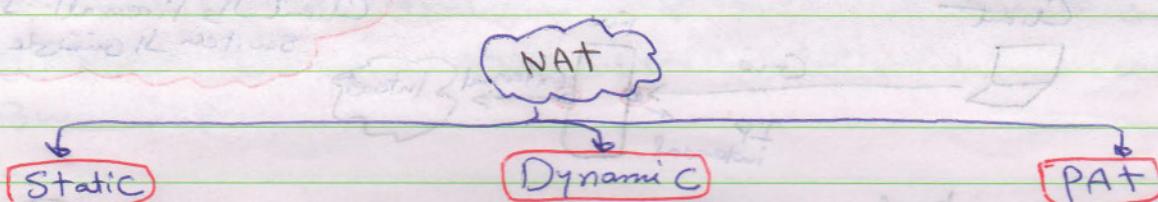
utm ① Client Interface Gateway ②

Firewall ③ من بنية غير لوجيني transparent

للحاجة فيه

الـ box ④ transparent || NATMode  
عنوان حقول من Policy  
ويسمح كل الـ IPs وطبعاً ينطبق Reset  
على المعايير  
Juniper, Sophos, Cyberstrom ← UTM ⑤ كل IP ←

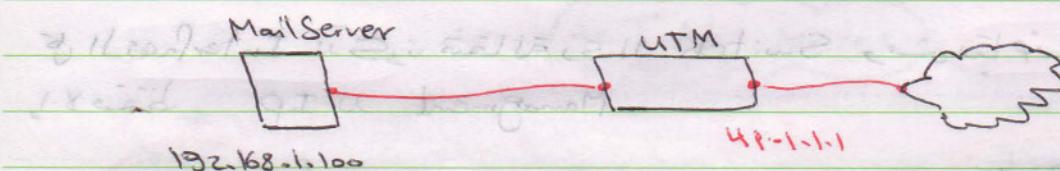
لوهستعمل NAT طبعاً الـ NAT كلن انواع



دابيكوا الاساسى الى شناكل

### ① Static ((Virtual IP))

Assign One public IP to One private IP



ديما اللي عايز يدخل على الا Mail Server هيكتي الا  
 UTN ولڪن على الا Port 25  
 دا طبعاً أكثر امان.

### ② Dynamic NAT ((IP Pool))

Assign Pool public IP to Pool private IP

Or One private IP

لوعاين ابعت 1000  
Dynamic NAT نوع Red IP

IPS Pool من واد نطلع دا  
نامي اخلي الا Mail Server

### ③ PAT

Assign One public IP to Pool private IP

بعن ليكون عينا Public وادر نطلع دا او اول IP  
نامع المسوكه كلها ودار اللي يكون متغير اصل او يستخدمه.

Sub:

Date:

## "4" FortiNet Overview

كلهم يصنعوا Product ⑧ هناك FortiNet شركات

لوعاين تطلع عليهم Security

(www.Fortinet.com) products

③ **Network Security** حلامي الـ

**High-End**

user 1000 ذكر عن

1000 Series

3000 Series

5000 Series

**Mid-Range**

user 200 ذكر عن

100 - 200

300 - 500

600 - 900

**Entry level**

user 1 ذكر عن

30

60 - 90

لaptop جهاز الـ FortiGate للبيع من المصنع من يكون واحد IP

شركة FortiNet وهي بتقطه من الكراين لاستريل

يتحمل على كل جهاز على فيه

Consol or **Https** عن طريق FortiGate management

**Formatos** يستخدم فقط لو اجهزة ملوش ذكر او لو عملت **Consol**

او تكون قسست المسودة بتاخ اجهزة

Formatos que son Configuration format يمكن نقل

\* لوعاين ادخل على الـ Device عن طريق **Https**

**https://192.168.1.99**

user **admin**

Pass

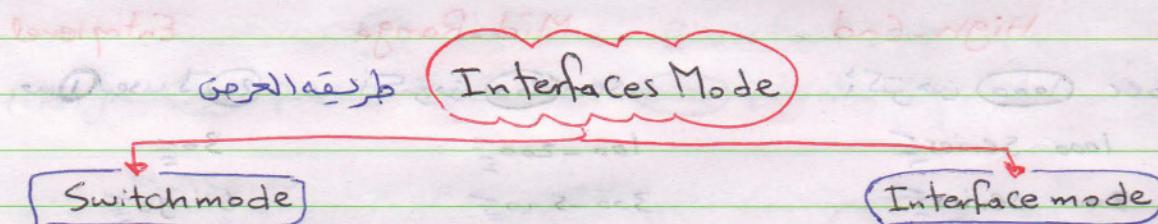


لاحظ الـ Interfaces (جهاز) من أصغر حجم إلى أكبر موديل .

لو عايز انتون الـ Interfaces داخلي طهار .

هذا يعني ما ينزل صورة الواجهه System → Network → Interfaces .

وخط الـ mode هيكل كل الـ Interfaces .



احظ الـ Interfaces mode من Switch mode .

الاعنة طريقة الـ Command line .

DMZ , Internal , WAN مكتوب عليها Interfaces mode .  
وليس ترتيب اى استخدم (Interface) يعني الى مكتوب عليها .  
يعني الـ Internal يعني يستعمل WAN .

هذه الـ 11 جهاز الموديلات من سرعة Series .  
الـ 11 يقف عليه بدوريني عدد الدوال او من الـ Concurrent sessions .  
وبيان ينبعى للـ 7500 session الواحد .  
لابيحي نشتري اجهاز .

مثال : 2 million ← Current Session الـ 2 million .  
لو موديل الـ 7500 user يقسمها على 7500 users .  
كل طلع 66.66 .

الـ Session من معناها انه فاعل صفقه ولكن كم Kb من

الصفقه يعنيه session .

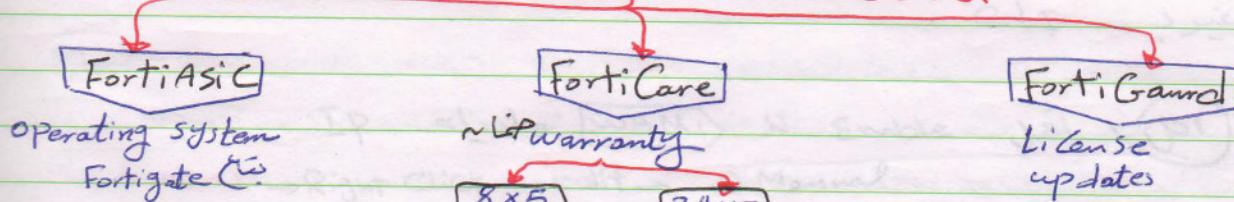
+ معايير الموديلات يمكن تلخيصها في  
 FortiGate 90D or FortiGate/FortiWifi 90D  
 يكون راوتر فاي فاي Wireless Control ويحمل  
 وظيفة انتشري لوحدة التحكم على هوديل  
 ولا يلاحظ انه يفتح انتشري الـ wifi

ما هو؟

فرز من الأسعار من الموديلات (Series) في نفس الدفع  
 لذلك هنا أجزاء انتشري إلكتروني من الموديل  
 مثل 90D و 94D و 95D لكن 100D هي الأكثر كثافة في العمل

+ أهم معايير ونماذج طهار  
 Concurrent session ①  
 Interfaces number ②

### Important definition in Fortigate



شركة Fortinet توفر دعم اجهزة ولكلها تسبيط للطهار  
 FortiCare توفر دعم اجهزة متعدد ودائم وهي الـ

لو اخترت ببايل 8x5 وعندك مشكلة طهار تبيتحت لا تقرب مكتبه  
 يعني بفتح فتح عرض سهلا وينفذ على خوارزمية  
 يعتمد على خوارزمية لحل مشكلة

لو 24x7 مخبر دعائمه بالذكاء يفتح لك اقرب وكيل يركبها، اقدر دريد  
 وسايفون على قيم 700\$



لۇغاتىنىڭ license بىاناتى

Connect Fortigate → Dashboard → status → FortiGuard

- IPS & Application Control
  - optional ↪ • antivirus
  - optional ↪ • Web Filtering
  - optional ↪ • Email Filtering

ـ معاوـدـ الـىـ يـنـرـقـ عـلـيـهـ لـجـرـيدـ سـلـفـيـاـ . فـيـمـاـعـادـوـدـ كـلـ  
ـ اـلـ Featuresـ بـلـامـنـ.

**لروا License** اسہت دیاں اک جگہ سیفیتی دے سکاں طالع نت  
عادی دیکنی میں سعد Scan و لاء antivirus و لاء دی شی  
محبود انہ طالع نت فنتط.

Sub:

Date:

### "5" Convert Interface Mode to Switch mode

للمعاين احول او  $\leftarrow$  transparent Nat or

Dashboard  $\rightarrow$  Status  $\rightarrow$  Operation Mode  $\rightarrow$  Nat (change)

من هنا يتم التحويل ويسعى كل البيانات ولكن هنا يتطلب منه  
Management & IP تدخله

لما يتحول من  $\leftarrow$  Interface mode  
Switch mode

System  $\rightarrow$  Network  $\rightarrow$  Interfaces  $\rightarrow$  dmz  
 $\rightarrow$  internal 192.168.1.99 255.255.255.0

WAN1 0.0.0.0  
 Interface model  
 S1 (is default) دوارة  $\leftarrow$  WAN2 0.0.0.0

لما يتحول من  $\leftarrow$  Interface mode او  $\leftarrow$  Line mode  
 IPs الـ IP مفتوحة على الجهاز  
 mode Connect وسائل متاحة من هنرخ اعمل Internal دوارة  
 CLI غير

لعمل IP واديله WAN1  $\rightarrow$  N Enable

WAN1 Right click  $\rightarrow$  edit  $\rightarrow$  Manual IP 192.168.100.99/24 Range لا زم ريكو  
 مختلف عن internet

Access لفتح دى عنوان تعرف مثل

Administrative Access  HTTPS

WAN2 لدخولها عن طريق CLI

Dashboard  $\rightarrow$  status  $\rightarrow$  CLI Consol #

مثال ⑥ أوامر رئيسية في الجهاز

Config → Configure لغليمه

get → Show عيال

Show → Show اوامر

(diagnose → Fortiguard مع اوامر

execute → Ping من اوامر

exit

Config هنري IP بقى مستخد

FGt80C # Config system interface

FGt80C (interface) # sedit wan2

FG80C (wan2) # Set ip 192.168.200.200 255.255.255.0

FG80C (wan2) # Set first allow access https http

telnet ping

FG80C (wan2) # end

allowaccess IP وادينا IP

ممكن نزوح تاً كمن

system → Network → Interfaces → wan2 → 192.168.200.200

لحوظة لوحظنا او وادينا لجهاز wan1 في Cable من

https://192.168.100.99 Connect ودخل wan1 97 (to Range

https://192.168.100.99

# user admin

Pass

CLI في مرحوم Interface mode لوعانز احوله

# Config system global

(Global) # Set internal-switch-mode interface

# end

Interface Policy مرجع على او Policy Other Error

لارضم ناعتها الاعد Default Policy

② System → Policy & Objects → IP v4 → internal\_wan  
all-all → ~~edit~~ Delete → OK

③ Interface1 mode DHCP N Disable  لازم اجل

System → Network → Interfaces → DHCP Server →  Enable  
OK

وضع يحق عسان نخون الامر  دلوب الامر  mode

# Config system global

(global) # Set internal-Switch-mode interface

# end

# Y

لتحاول وتحتاجها  Restart

Interfaces  افتحها ; استعدي وتحتاجها

System → Network → interfaces → dmz

internal 1 0.0.0.0

internal 2 0.0.0.0

internal 3 10.0.0.0

internal 4 0.0.0.0

internal 5 0.0.0.0

internal 6 0.0.0.0

Wan 1 192.168.100.99 255.255.255.0

Wan 2 192.168.200.200 255.255.255.0

Device  Connect

Local IPs  Local CMC

Local IPs  Local CMC



51

18

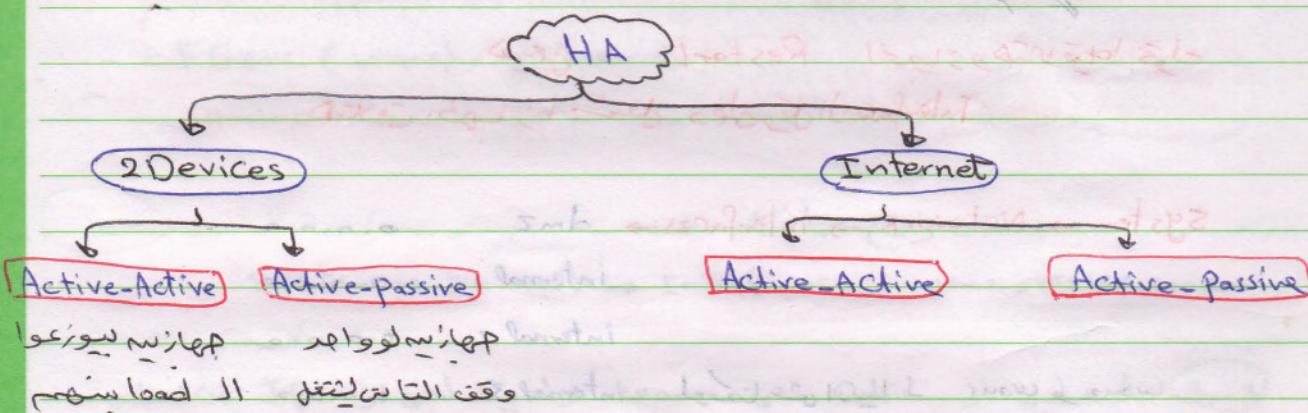
## now - Fortinet - 11.6.1 FortiGate System Information

tools الموجوده في الجهاز يمكنها إنشاء Shortcut  
Dashboard → status → + widget → Shortcut

التي يمكن عملها على USB تكون فيه Fortigate لـ 3G modem Device backup خلاص

نبدأ من شرح بالترتيب  
System → Dashboard → status → system information →  
- HA status

لوحة معلومات

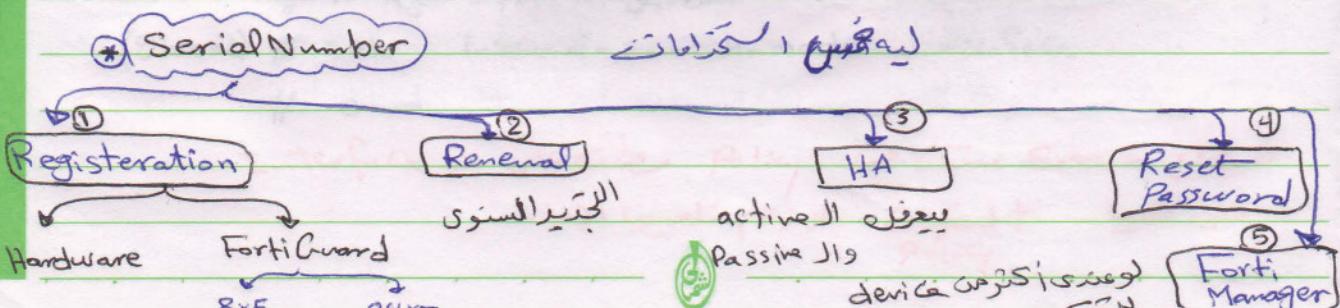


نحو عالي

\*) HA Status → Configure

\*) Host Name → default (غير موصى به) → Change (إذا)

\*) New Name SITE-FG (يطلب باسم الجهاز Report)



ما هوFortiGuard

هذا اسم دماء او Device يدور سطراً يكون الجهاز عبارة عن راوتر قادر على معالجة بيانات او Data و اخراج الانترنت لان العمل فيه إلا الخصائص التالية:

① Firewall

② Routing

③ webfilter manual

هذه المواقع يدوى

SerialNumber → activation

يتعلق لها

FortiGuard

للحظة من اول 100 Model ينفع اخذ license معك اجزاء او EmailFiltering او antivirus فقط او ما يجيء واحد فقط منها

• تشمل او System Information (Features)

Status → ④ Operation Mode Nat Change

④ System time Change لتوسيع الاختير الوقت

يمكن تنفيذها يدوي و يمكن لوميني اخذية ياخذها

Internal Server

External Ntp Pool

NTP Server

موقع مكتوب بالإنجليزية  
Clear

④ Firmware Version v5.2.4 update

updates فيه Version 4.0 او 3.0 او 2.0 ينفع بتنزيل

④ System Configuration Backup Restore Revisions

لعمليات اجل System & Restore او backup

④ Current Administrator admin Change password

④ up time days hours min

يعرفك او box متى كانت قد انتهت؟ قبل ما يطلب اخر مرة



# **"7"**

## **FORTEGATE UPDATE FIRMWARE VERSION**

## "7" FortiGate Update Firmware Version

لو FortiNet نزلت اصدار جديد وتحديث اجل update .FortiNet نزلت الاصدار طبیعی من موقعاً FortiNet .out extension II Firmware .ولاحظ انها يتكون .Features يكتوي بـ PDF release notes .لقد قرأت نشرة ملخص ما تم في كل إصدار

## Point oF update

$$V_2 \rightarrow V_{5,2,4}$$

## النماذج Configuration

سيكون فيه الموديلات التي ينفع ديرل عليها update  
 لكن لو من Configuration من فتحة الـ V6.0.10

Configuration: ~~safe~~ v1 VS. 0.10

اکن لو v2 بیطاح ۱ v4 فر v3 تم ۵-۰-۱۰ تم و طبیع آزم انزل releaseNote دیتاب کار و ادر عستان امرن قیمت

لتحظى بـ Downgrade يمكن امثل بـ upgrade يدل عن المعني ذاتي

Dashboard → Status → System Firmware → update →  
upload Firmware →  Confirm version Downgrade →  
**Downgrade**

\* لوعايرزین بقى جرب الـ Fortigate على Vmware  
١- ننزل الملف بتاتعها من على موقع FortiNet

vm64 -out = DVF

و لاحظ انتهی امدادار 32 او 64

### التطبيق العملي

1- نفك ضغط الملف FGt-vm64.out.ovf

2- فتح VMware workstation

File → Open → FortiGate → FortiGate-VM64 → Open

اخت، المكان الذي ت\_DOWNLOAD فيه → Import → Accept

\* الملف دايمكون له 14 يوم

3- نقل المكينة الى Poweron ← VMware

4- تفتح المكينة بس لاحظ انتها مستبكون و اخده IP ولازم

login: admin

- 5

Password:

# Show system interface

# Config system interface

(interface) # edit port,

(port) # set ip 172.16.1.100 255.255.255.0

# Set allowaccess https http telnet ssh

# end

Ping

Cli → Device Configuration

عنوان مستغل في GwId

6- يفتح جهاز ويندوز على نفس ال Switch وواجهته

Fortigate على نفس ال Switch هو خلاصه على ال Connect



**FORTINET**  
الفورتيت  
بالعربي

22

browser

## ٧ - نَفْتَحُ أَيْ

<https://172.16.1.100>

- ۸ - قید خالص علی اور login مبارکہ ادا Fortigate

user admin

Pass

$$T_{\text{max}} = \frac{\log -I}{\alpha} \in [2.115 \text{ to } 10.16 \text{ s}]$$

• طبع كتب المنهج أو License أو كتاب

## Configuration Modelling

Dashboard → status → HostName → Change SITE

## Interfaces في الـ

Network → Interfaces → Interfaces II

لـنـهـاـيـةـ الـمـوـدـهـ

Firmware N update جاري التحديث

Status → Firmware Version → update → [upgrade file]

• out اخر تاریخ firmware نصب کنید و update کنید

→ open →  Boot New Firmware

Formate Boot Device First

يُتَّسِّلُ الـ OS لِلتَّعْمِيمِ وَرَاسِخٌ بِيُّوكُولُ الـ Configuration

OK

二三八

الموضوع حتى ينام ودلت انت لومي عمل عليه Ping هيقدر اتيه اولاته فقط  
ودا ديل على السرعة .

update Configuration, وتحديث Firmware || update  
• new Features N

23

Sub:

Date:

### 8. Admin Change password &

#### Create profile

firmware اول حاجة بتعملها لتركيب Fortigate admin بعدها تغير ال Password

جامعة ونت تركب او fortigate او Real IP او website او Exchange Conflict معنهاشت غير Real IP ① عياد لو لشركة هحصل هنفهم على نفس آد 443 + Port Exchange ولا fortigate يبي Port Exchange او fortigate آد

#### Admin > Password

Dashboard → status → Current admin → Change password

Administrator admin

Old pass

New pass

Confirm  OK

هيخطاب برو وبحيل او تجربة او Pass user

عيان تغير آد Port من هنا

Dashboard → Status →

System → Admin → Setting →

Http port

Https port 3030 → Port مفتح

telnet

ssh

Idle timeout 60 لومبركتي الموس لمدة كم يخربل برو

Apply

OK

Port 3030

تحريكه ونستوي آد

192.168.100.99 3030

interface # من ويكون ظاهر من ال options داخل telnet  
CLI من هنالك ليه وعند ظهره يكون في Check box

SITE # Config system interface

(interface) # edit wan1

(wan1) # Set static allowaccess http https telnet

# End

دلوت لوبست فورتى options

Network → Interfaces → wan1 → Edit telnet

Connect telnet وبيت اعمل Port لعنيد

C:\> telnet 192.168.100.99 gogo

login:

---> وتحمل

Admin دخول سرع

And System → Admin → Administrators → admin → edit

Connect  Regular  Remote  OPKI  
Remote interface دخول  
---> Connect Remote دخول

Contact Info

Email address

SMS

Reports دخول

يمكنك إدخال رسائل الهواتف عبر USB device

Enable two-factor Authentication

token

fortigate) يرجى تعيين رقم

2 free token دخول ويعبر عن المكونات

Random Password

سلسلة

□ Restrict this administrator login from trusted hosts only

trust Host #1 0.0.0.0

trust Host #2 معرفة معينة لـ IPs

الى ينجزوا المهمات Fortigate N access

External و دولي Internal داخلي

### Admin profiles

Domain 110 Delegate Control 110

لوائح ادارات صلاحيات admin

System → Admin → Admin profiles → Super-admin default 110

new profile 110

+ Create New →

Profile Name Limited access

None

Readonly

Read-write

دي منه محدود

غير المعنون

بعد كلامي عليه

0

0

0

0

0

0

0

0

0

OK

users انشاء Profile بريد لبياناته امنية في

System → Admin → Admin profiles → + Create New →

administrator Mahmoud

Case Sensitive

Regular

Remote

OPE

password

انواع الاعداد

limit access

OK

Mahmoud ← user بال وتدخل بال

صلاحيات التي من هي جعلها None والتي واصح لها

رسوخها بـ Read, write. ie.  حاصل

"9"

## SYSTEM DASHBOARD



### "9" System Dashboard

(26)

للحماية اعمل Shutdown او Restart لجهاز او المحظوظ

System → Dashboard → status → system resources → Reboot

ويمكنك برمته بثوابت RAM و CPU و المحظوظ المفتوحة على الجهاز

لتحذيف لوحة مفاتيح او Power Cable المحظوظ لفتح يبعد

System Check

لعمليات تشغيل المحظوظ التي تستعمله على جهاز من حواسيب الـ UTM

Dashboard → status → features → المحظوظ هنا

ويفتح توقف التي هي خارطة منهم

والمحظوظ ستكون أكتر ممكن من هنا

System → Config → Features → presets Full UTM

والمحظوظ حاجه voip , ssl-vpn , loadbalance , NAT

التي يعاليز تشغيلها لتفعل عليها وتحصل on

لبعد كل ١٣ Dashboard لعمليات تشغيل المحظوظ

Alert Message Console

Logs administration history المحظوظ كل سجلات وتاريخ

للحماية اعمل Dashboard المحظوظ خاصه بي

Dashboard → status → Dashboard → addDashboard →

Columns   Name Ahmed

+ widget المحظوظ في status سداً لتهيئة فيه

لعمليات تشغيل المحظوظ صورة لجهاز unit operation

Scan IT المحظوظ عاليات اقمار عدد Advanced threat protection

لتحذيف المحظوظ



يمكن تنظم المستخل عن طريق إنشاء نجلي Dashboard باسم كل قاعدة

هناك : ١١

Dashboard → status → Dashboard → add → Name [CLI]  
OK

هذا يعنيها خلقت هي اضف القاعدة بتاعتتها.  
ومن widget

دي طبعاً عليه تنظيمية من ذكرا

"10"

## NETWORK INTERFACE



FORTINET.  
الفورتي<sup>ن</sup>  
인터넷  
بالعربية

28

### 10 Network Interface

System → Network → Interfaces

جهاز وطبع مختلف من مهامه للاتصال

لوقت اى وقت وInterface

Interface Name 00:0C:29:BF:7E:4B

Alias internal

Link Status up

الاتصال

Addressing mode

Manual

Dhcp

One arm

Dedicate

Dhcp interface

Filters

Switch ports

Access point

وهي موجهات

wifi

Manual

IP 172.16.1.100/255.255.255.0

FortiGate يحتوي على Management interface لـ Fortimanager،  
logs وFortianalyzer، Device reports،  
بروتوكولات، او راجدات كثيرة،  
يعمل على تحليل كل ما يحصل في الشبكة.

Configuration فيFortianalyzer للوصول

log & Report → log Config → log setting →

Send logs to Fortianalyzer

IP [ ] test

SNMP Simple Network management Protocol

Putty SSH يستخدم لـ Connect على Linux

لتعمل على Linux يجب تفعيلها من هنا

System → Config → SNMP → SNMP agent enable

IP [ ]



Solarwinds

→ Check الأفضل براجوا ↪ ماحظ

Interface ↪ نكمل خصائص ال FCT-Access Connect بمحال الناس يحلوا forticlient بفتح ادار

antivirus → End point Security دا Forti Client ال لاحظ

free users ينزل على اجهزة ال Device ونت پستوريه بيديلك

Detect Register ناكرو من طريقة او لهم : ال Search في forticlient لـ Device لا يسجل نفسه . ولو عايز تستوقي الاجهزه المسجلة من هنا → \* user & Devices → Forti Client profiles → → Monitor → Forti Client Register دفعه هتا اللي معهول لهم

لادظم عياد او Register يتم بيكيل صحيح لازم FCT-Access Interface دا واعلم بره على ال checkbox

Device Management

BroadCast Discovery Messages

بس لو عندك انك تروح كدا ال license هتخسر عساو اد users checkbox كل دا اد يسجل نفسه او ما ليتك في تكون الاوائل استله ال manual واحد عليهم

CAPWAP

نكم خصائص ↪

wifi دا ↪ Control access point wireless access point

Forti access point دا Fortiwifi او بطبعاً يا لما يجيء دا Device او اذ لو مرتب دا

نظام الـ **Features**

- Security Mode **Capitarportal** → wifi برمنجه الـ **wifi**
- Pass → user **user** دخول عندي **user** دخول عندي **user**
- Local External

### ④ Device Management

Detect and Identify Devices

يبحث في طهاز الذي طالع من خلاصه ودبي تقييد وناتج

### ⑤ Network Configuration

Secondary IP Address

لعمائدة على بروتوكول IP

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

### ⑥ Firewall Configuration

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

### ⑦ Policy

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

ابحث في المدخلات والخرجات

### ⑧ Policies

ابحث في المدخلات والخرجات

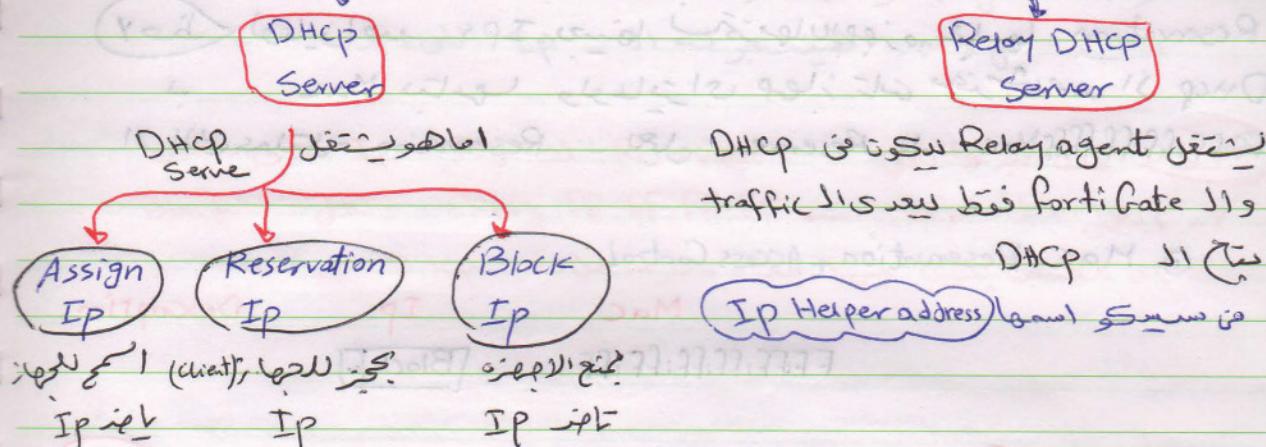


Sub:

Date:

## ١١) FortiGate DHCP Server

FortiGate DHCP ← من مالبسه



التطبيق العملي

system → Network → Interfaces → DHCP Server  Enable

Address Range

\* Start IP  End IP

\* Netmask

\* Default Gateway   
 ○ Same interface  
 ○ Specify

\* DNS   
 ○ Same system DNS  
 ○ Specify

Advanced

\* Mode  Server  Relay →   
 لعامر لـ Relay  
 كـ الـ Forwarding

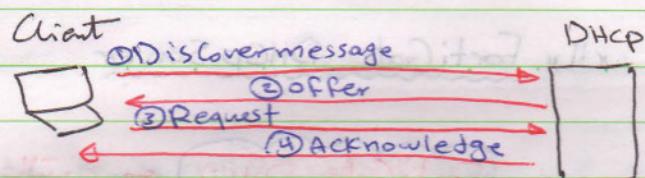
\* Additional Options

⊕ Mac Reservation + Access Control  Create New

Mac Address  او وارد من هنا

Mac	IP	Description
<input type="text"/>	<input type="text"/>	Reserved assigned block





لعماء IPs بعثتها نتائجها للجهزة بعدها DHCP ينبعها ولونياراتي لها IP من المخزن من 11  
FF:FF:FF:FF:FF:FF Mac لـ Reserve نعمل **Reservation** لـ الـ MACs

### ② MAC Reservation + Access Control

Mac	IP	Description
FFFF:FF:FF:FF:FF:FF		Block

لو جهاز دو قطعات على فتحة الـ switch واخترت Fortigate مع

### ③ assign IP automatic

يتم من 11 Mac ونواة DHCP ينبعه حقوله

Reservation → **فريزد**, IP, **فريزد**, **فريزد**

Pass و UserName او دلـ IP مكتوب على Policy 1, **سلوك** دلـ اتصاح.

options دلـ

Type  Regular

IPsec

Client **فريزد** IPsec

فريزد

لعماء IPs عن طريق Clients الى واحدة من 11

System → Monitor → DHCP Monitor

يميل الى Client والـ IP ينبعه ومسنون كل ما تغير في فتحة

وممكن تسميتها من DHCP نقـة الـ IPsec

System → Network → Interfaces → Mac Reservation →

لعماء IPs التي هي في فتحة

الأسهل من اجل اجل Reservation لـ كل واحد اني اعلم

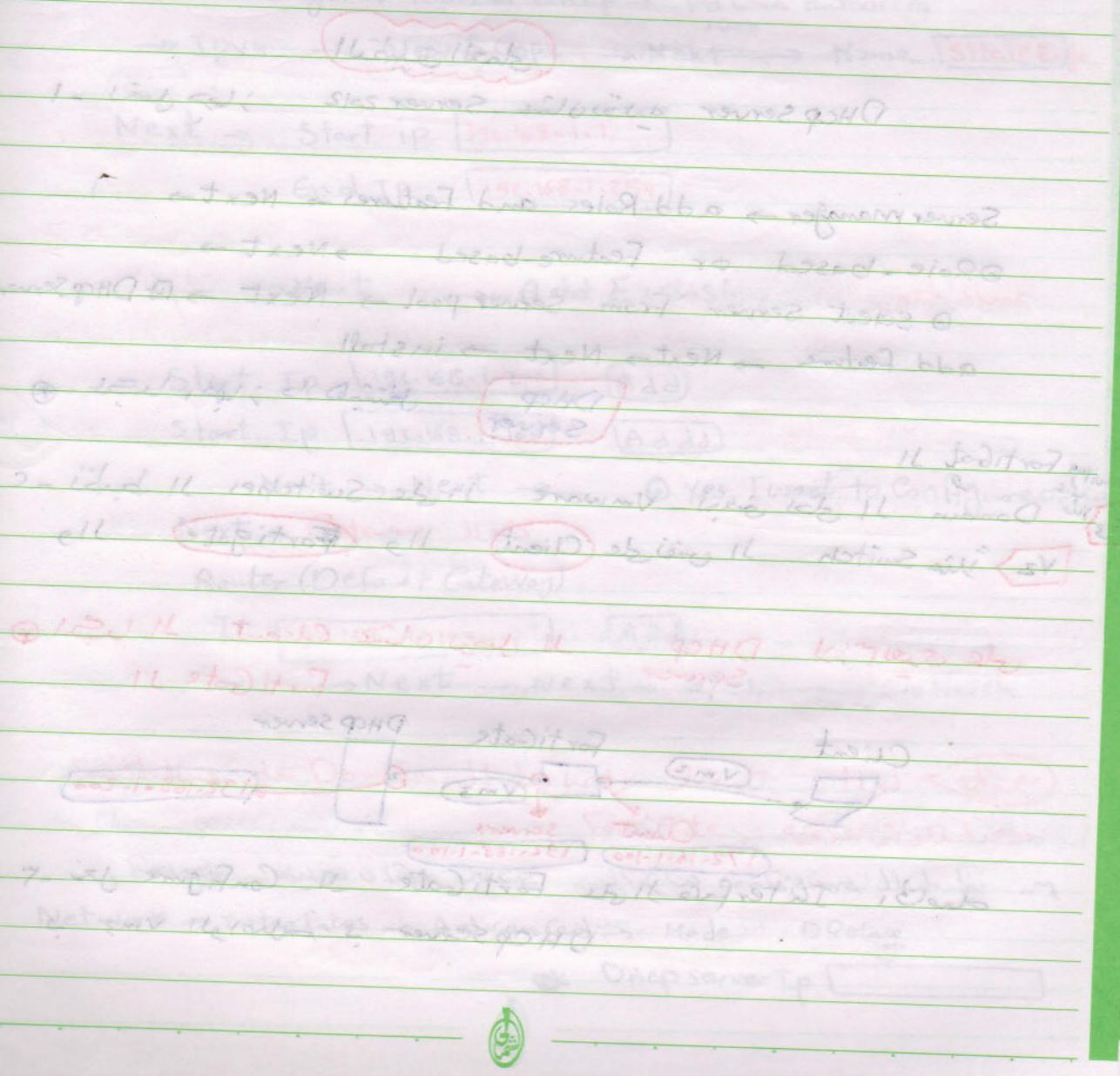
ص ١٢٠ ول assign IP ويعنيه ادخل على

Monitor → DHCP Monitor → Ctrl Ips واعلم على كل Reservation Rightclick وافتار Rightclick بـ ١ كل واحد ضيقجز له او الى الذي اعنه

لخط انته لعمليات Reservation لـ كل او Ips الى عند

Block FF,FF,FF,FF,FF,FF ← Mack يم نعمل ما

DHCP مثمن محض يجب جهاز معاه وسائقه



## ١٢ـ DHCP Relay Server ①

DHcp ٍ fortigate انته ممكن تدخل على Interface ٍ Client ٍ ولكن في المخواط ٍClients ٍ المخواط على Switch لفترة

٦ـ هنجرى الوفع التام ٍ DHCP Relay Server ٍ FortiGate ٍ يجيء من ٍ DHCP Server ٍ من هو ٍ DHCP Server ٍ ولكن في المخواط ينبع ٍ traffic ٍ فقط يجري ٍ traffic ٍ

### الخطوة العملية

١ـ نعمل جهاز Server 2012

Server manager → add Roles and Features → Next →

② Role-based or Feature-based → Next →

③ Select Server From Server pool → Next → ④ DHCP Server

add feature → Next → Next → install

DHCP Server

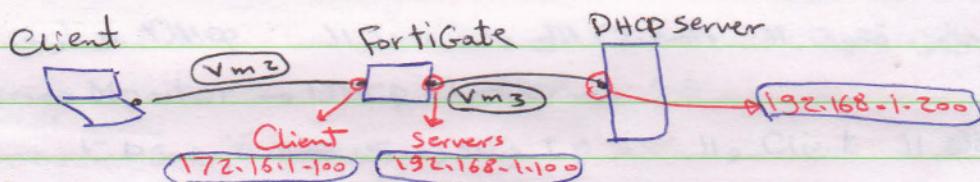
لدينا جهاز ٍ

switch Fortigat ١١

V3 ٍ Domain ٍ لمعنى نحن ٍ VMware ٍ على Switches ٍ نربط ٍ

V2 ٍ Switch ٍ على نفس ٍ Client ٍ والـ Fortigate ٍ

٤ـ نعود على DHCP Server ٍ نعمل ٍ Client ٍ لجهاز ٍ Fortigate ١١



٥ـ نفتح Interface ٍ Fortigate ٍ Configure ٍ

DHCPserver ٍ نوجه ٍ VM3 ٍ



35

Sub:

value

Date:

2020

Servers → dual3, Interface J1\_brid - 2

Alias Servers

IP

192.168.1.100/24

 HTTPS ping HTTP FMG-Access FCT-Access

OK

DHCP → Configure Local Domain J1\_dejais - 0

Servermanager → Tools → DHCP → pdc → Authorize

→ IPv4 → New Scope → Next → Name SiteipRange

Next → Start ip 192.168.1.1

End IP 192.168.1.254

→ Next → Add Exclusion

Start Ip 192.168.1.200 Add

Start Ip 192.168.1.100 Add

Next → Next →

① Yes, I want to Configure options

Next → Gateway Alias

Router (Default Gateway)

IP 192.168.1.100 Add

→ Next → Next → Yes, → Finish

Switch VMs to Domain J1\_zebulon Client لوار (ابدأ)

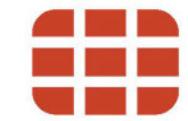
FortiGate → چک علیعه

Relay (اخذ علیعه DHCP ) (To Configure J1\_brid - 7)

Network → Interfaces → Advanced → Mode ST/② Relay

DHcp Server Ip





٣٦

٣. DHCP Range يوزع من IP Scope ليوزع من IP Scope Serve بمعنى انها تعلم IP بتخواصها

192.168.1.1 → 192.168.1.100

متقدمة اعمل Scope جديد من IP

192.168.1.1 → 192.168.1.30

٣٧

لكن ينفع اعملها

172.16.1.1 → 172.16.1.254

FortiGate IP بـ Exclusion واعمل

172.16.1.100

→ Next → Gateway

172.16.1.100

[add]

→ Next → Yes, → finish

٣٨

backdoor في IP

FortiGate كشومل لـ Discover message Client

Firewall و Router يدعى FortiGate IP

Discover message block

FortiGate IP لـ DHCP

Relay DHCP

البيانات تمرر الى Discover message

172.16.1.100 IP → FortiGate IP Client

Discover message IP range من IP

٤ - نزع لـ Client IP automatic و تلقي امن IP Details IP

Domain DHCP

DHCP Server: 192.168.1.200

IP

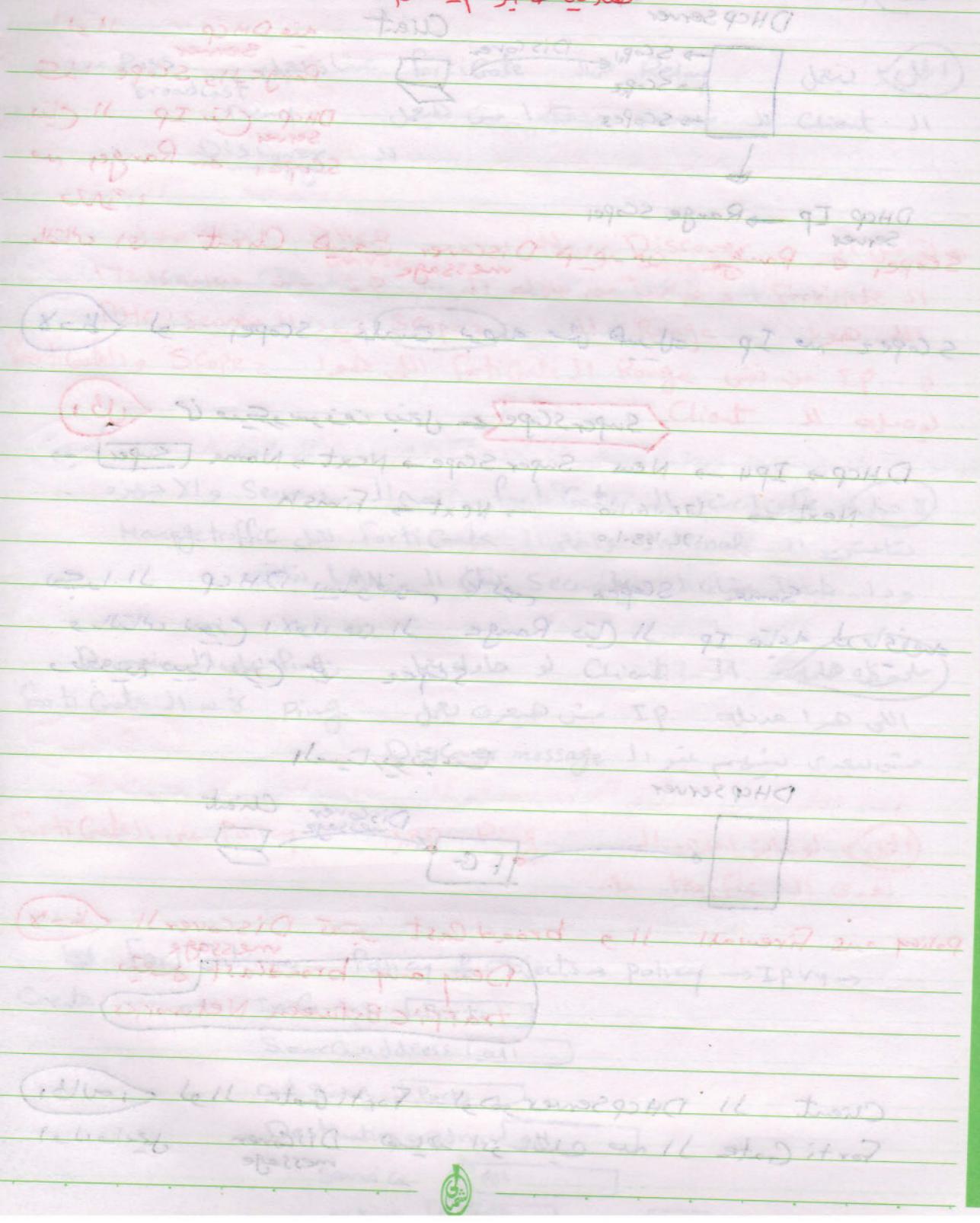
172.16.1.250 →

Range IP  
FortiGate



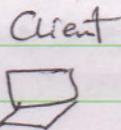
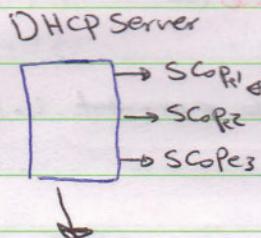


Domain ٩٦٠ ساعٌ DHCP لو سبقت الـ DHCP → PDC → Scope (172.16.1.0) → Address leases → 172.16.1.250 Domain IP ملكية حاصل



38

### "13" DHCP Relay Server 2



لوار  
ـ DHCP Server  
ـ Range Scope  
ـ DHCP IP Server  
ـ Scope1 ← Range no  
ـ ملار :

الاتصالات Client ای دایرکٹ  
ـ Discover message

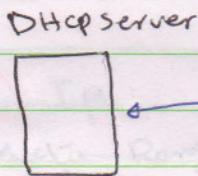
ـ Scope2 no IP ای دایرکٹ من خلاصت برپا کرنے سکتے Scope1 لو

ـ SuperScope ← جائی و سونوچہ بین اول

DHcp → Ip4 → New Super Scope → Next → Name [Super] →  
Next → 172.16.1.0 → Next → Finish  
192.168.1.0

ـ نیکا ای DHCP سیستم کا نہیں  
ـ و بالاتری نیونج ای اول من ای IP دیکھ لے دیا نہیں  
ـ Scope2 سینا نویں من

المستعاریوں پر اتنا



ـ Policy on Firewall و ای broadCast میں Discover message  
ـ Deny any broadcast traffic Between Networks

ـ Client ای DHCP Server لو ای FortiGate

ـ Forti Gate ای no ای میں ای ای میں ای Discover message



(40)

DHCP  
Server

Client .  
لأن من الـ Ping

Reply .  
Ping من المـ IP و هي  
تحتـ Internal

ping to external network

Internal

External

يبـ العمل بـ كلـ users  
حتـ طـ العـ يـ نـ

license

Servers LAN من الـ Policy

وـ العـ يـ سـ لـ

Network Data فيـ الـ

لاحظ سـ رـ سـ لـ

① Requirement of Client

② Requirement of Server

③ Switch

④ Cable

⑤ Traffic

بيانات

كلـ ماـ يـ زـ يـ الـ

Network (Performance) Security

HA



لـ

Deny Discover message من يلعب FortiGate لـ Client Broadcast Client لا يعتبرها

no Pass Deny fortigate Relay Client  
broadcast Deny Server Client

Discover message من يقبل fortigate Client  
DHCP Server IP من يقبل fortigate Client  
Scopez Range Client  
fortigate Scopez Range من نفس IP Client لا يقبل

Management Servers من يقبل fortigate والجهزة  
Manage traffic يقبل fortigate داخل Internal  
و LAN Security Client يقبل

Domain & Ping Client يقبل  
FortiGate & ping من يقبل IP  
Discover message من يقبل

FortiGate على Policy Ping Client  
Louise اعدى traffic

FortiGate → Policy & Objects → policy → IPv4 →

Create New → In Coming Port  
Source address all  
Out going Port  
Destination address all  
Service All  
action accept

OK

١٤٤١

Sub:

Date:

### "14" FortiGate Interface Type

نعمل على دفعات الـ Options

لاحظ يمكن ايجاد مجموعه من الـ Interfaces واسفلهم

System → Network → Interfaces → Create New → **Interface**

Name **Vlan1**

Vlan ID **1**

**Vlan Concept**

لوعندى port و عايز كل Ports **switch traffic** broadCast او سان اقليل او Network

لوعندى **FortiGate** واحد **Vlan 10** يوصلى مجموعات Interfaces تابعه لـ VLANS و دا اللي يجعله

Interfaces → Create New →

Name **Vlan1**

Interface **Port1**

Vlan ID **1**

Manual

IP **192.168.1.10**

OK

Physical Interface Options

Port1 → Interfaces → **Vlan1**

(Port1) → Interface **Vlan1** يفتح اعملاً

طبعاً اهنا يتعين كذا لوا لا switch التي ووصل بـ FortiGate  
Secondary IP ممكن اعمل حل تائج اديله Vlan فيه كذا

النوع الثاني الذي يمكن اعمله على الـ **Interfaces**

type / **802-3ad Aggregate**

دائرياً من الوجهين

Interface ② لديه ميزة أنه **العنوان** له **Interface ①**

الرنجبر بروتوكوله

لوكابيل القاطع كذا كل اتصال من سبأر

التطبيق العملي

Network → Interfaces → Create New → Interface

Interface Name **Team**

Type **802.3ad Aggr**

Physical Interface members

**Port 4**  
**Ports**

② Mammal

IP **192.168.250.1/24**

عنوانه ياتي هنا  
IP

B D C E F G H I

**OK**

Interfaces لوحظت المجموعات كلها من عرض

Aggregate

**team Port 4, Port 5 192.168.250.1**

Interface لاجي اعمل عليها **Policy** كذا

الى كيبيده مع طابعات

Internal بين مخطوطة الـ **HA** ملهاة في ملحوظة ديناصور

النحو الثالث

### Redundant Interface

فهي الـ Concept الى قات مع امتحان انه كابل واحد سئار  
بريله لا يحصل فيه مشكل يعتقد الثاني على ذلك  
هوا يستغل بره Port, سبب الملاط بالـ loadbalance

التطبيق العملي

Name	load
Type	Redundant intef
Physical	[Port 6] [Port 7]
○ Manual	
IP	10.10.10.100/24
□ □ □	

OK

هذا يعني خارج الـ Interface

Redundant

load	Ports, port 7	10.10.10.100
------	---------------	--------------

لاحظ يرحمه لا اجي اجيهم هر فيلم قدام اسم load اللى  
انا عملته لهم من الـ Name

النحو الرابع

### loopback Interface

ـ 1) (عادي هو الـ Routing لويني لكن من Network  
ـ 2) يستقل مع الـ OSPF (Dynamic Protocols)  
ـ 3) يكون موجود من الـ FortiGate  
ـ 4) اعتماده على Port  
ـ 5) يستفاد من جميع الـ Switch trunk Ports  
ـ 6) يستند على الـ VLANs يستند على trunk Port

ـ 7) يحترم الـ Virtual port بين المعني تعمل  
ـ 8) تابعه تطلع منه Net



الفايبر (fiber)  
هناك أنواع من Port وأهمها uplink وlink وlink

### المطبق العملي

Network → Interfaces → Create New → Interface

Name   
Type   
IP   
OK

← خلقت介فيس

loopback

loop 172.16.1.100

Virtual هو يغير Physical interface (اته محجزي ولا يخالط مع كلهم)

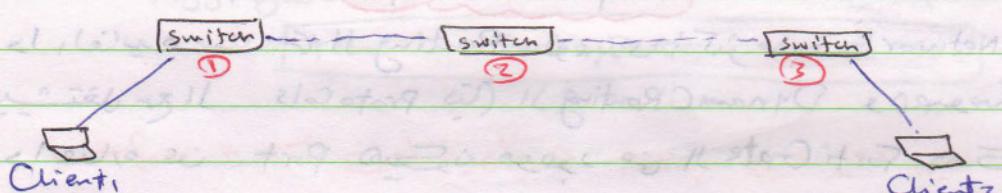
Vlan management , access يعمد فيه

### التوح<sup>فاص</sup>

#### Software Switch

Switch تمتلك Interfaces من الـ

: wireless و Spanning tree Protocol



طبعاً Mac 1 ، switch 1 مستعمل في Client 1 (Mac 1) ، switch 2 مستعمل في Client 2 (Mac 2)

Switch كل Client 1 و Client 2

Delay traffic ، traffic كبير و غير



### Spanning tree الـ (مثل)

ما يقارب مسافة جلوس Switch منهم صنف Root وعارفها Mac

يتابع كل الـ (Root) Network واد (يتم اختياره بناء على احسن Root)

وادي ما يرسل على Mac من ملزمه يسائل الـ (Root) Switch

فطبعاً الـ (Broadcast) ويعمل الـ (Broad Cast) ودى الوظيفة الأولى للـ Spanning tree

### تامن وظيفة

ي يعمل Port fast  
لبيع كل جهاز Client يأخذ 30 ثانية لم يتحقق على الـ switch  
ويسجل في table هو سخليه ليتعرف بسرعه

### وظيفة اخرى

ودى هستخدمها مو الـ FortiGate  
لعموصل ② Switch ② بـ switch  
ليعقل واحد فيه ويشتعمل المفتوح مجرد ما يجيء مثل من اللي ستعمل

### التطبيق العملي

Network → Interface → Create New → Interface →

Name **Switch**

Type **Softwareswitch**

Physical interface

IP **Port 10  
Port 9  
Port 8**

OK

رجيم لوعمل كذا **Spanning tree protocol** الـ (Interfaces) ؟ Switch

كتوريه من خلال عليه

(126)

النوع السادس

Wifi SSID

يجعل wifi N Control بعد ما تركب فيه FortiGate IP و ترتيبها USB

التطبيق العملي

الاول طبعاً ترکب الـ (استناد)

Name [ ]

Type [ Wifi SSID ]

Traffic Mode [ Tunnel wireless Controller ]

IP [ ]

DHCP

wifi N Password على بوك

Security mode [ WPA2 Enterprise ]

Pre-Shared key [ ..... ]

عدد اللي يعانونوا اعملوا  
Connect Maximum Client [ 10 ]

لا تركب الاستناد من يتظاهر كـ Interface ثيرلو مثلك ادخل هنا

الى عذات

النوع (ثانوي)

+ Create New

Zone

عند إنشاء منطقة من نوع Internal أو External، يتم تعيينInterfaces على الموجهة من قبل traffic block. يُمكن إنشاء منطقة من النوع Internal أو External، وتحدد المهمة التي تتم في هذه المنطقة.

التطبيق العملي

System → Network → Interfaces → Create New → Zone →

Zone Name [BlockAll]

[Block intra-zone traffic]

Interface Members

[dmz]

[wan]

[OK]

\* سطح مكتب، ادخل IP سيكون واهذين Zone & Interface

بعد إدخال هاتين المعايير، قم بـ Create Zone

Zone

block all

[dmz]

[wan]

internal (نوع) يسمى policy، كما يدخل من نوع internal وقلنا (نوع) يتبع نفس العكس

Domain Manage Traffic

\* إذا دخلت في Zone، تم تطبيق policy على كل IP

ويمكن إدخال policy، rule، traffic group، ونحو ذلك

لذلك، عند إدخال IP، يتحقق من إعداد Interfaces Configuration

active directory

Resolve DNS من خارج FortiGate أو DNS Server

Clients والـ DNS Server 5.1.1.1 يتحقق هو او DNS Server

لعملاً web filtering

Recommended → FortiNet DNS web Filter

→ System → Network → DNS → Use FortiGuard servers

Primary DNS

208.91.112.53

Secondary DNS

208.91.112.52

apply

لـ DNS استخدم فورتيجي

Service Provider

Specify

Primary DNS

8.8.8.8

Service Provider

Secondary DNS

\_\_\_\_\_

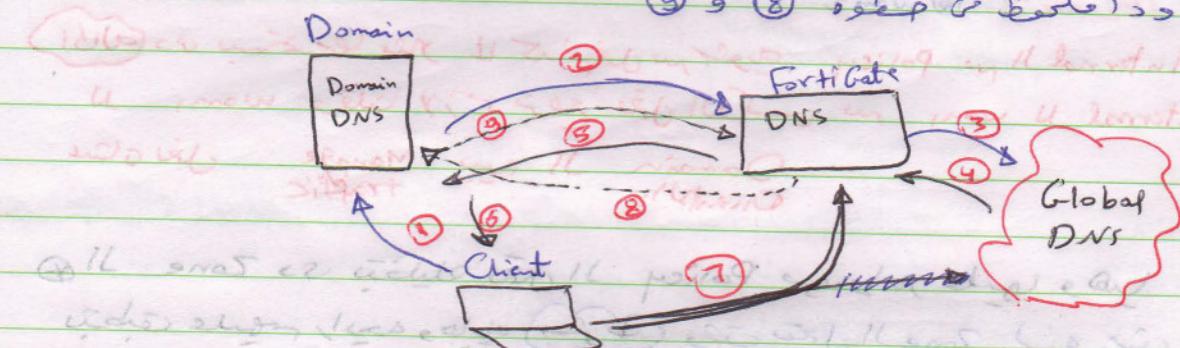
Local Domain Name

site.com

DNS Local

loop دا جياء على سرعة الانترنت طريقة ملحة لا بد

وـ DNS من مكتبه



لـ DNS من مكتبه

لـ DNS من مكتبه

لـ DNS من مكتبه

System → Config → FortiGuard → Web Filtering  
Enable Cache TTL 3600

الى قات دالوار ديع دل fortiGate DNS لـ Resolve

DNS Server

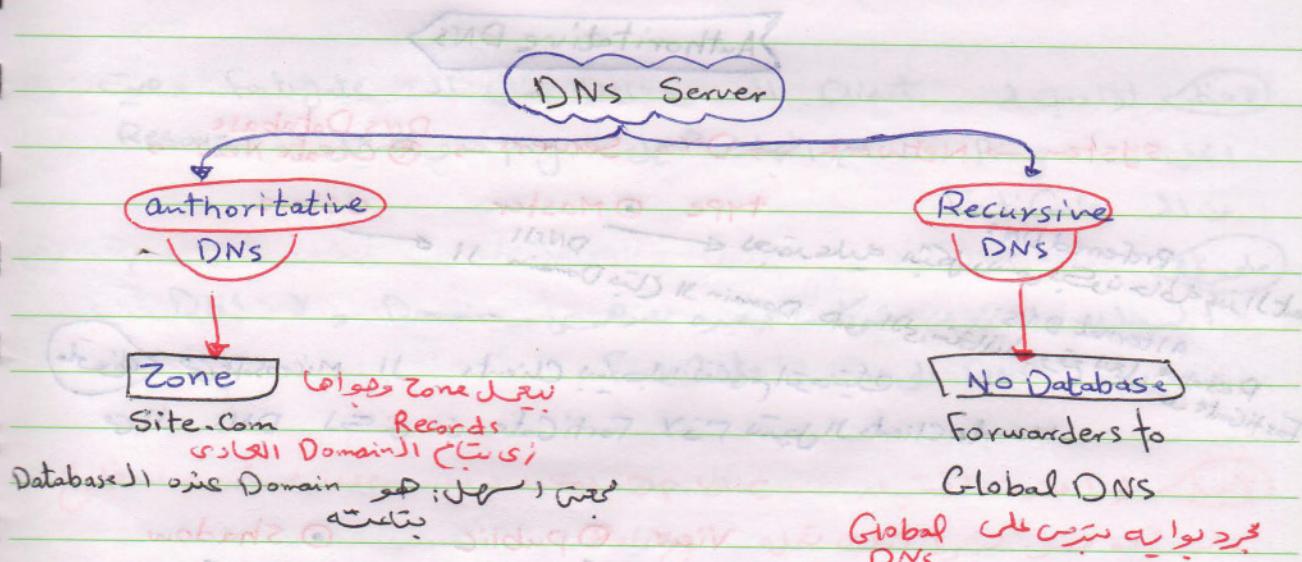
معايير استعمله

التطبيق العملي

① System → Config → Features → Showmore →

DNS ON Database

② DNS Servers Network C5



Recursive Microsoft Concept

① Conditional forwarders : ③ Root Hints :

② Forwarders :

③ Root Hints :

1- Database <sup>Records</sup> يقدر دعوة مرحلة DNS Resolve 11 خاتمة

2- Authoritative → لوحة معلومات Recursive

Microsoft Default Conditional Forwarders Forwarders Root Hints

و دائمه اللي يجيده

(50)

التطبيق الحجمي

Recursive DNS

1- System → Network → DNS Servers → + Create New →

Interface part [ ]

Mode [ Forward to system DNS ]

OK

دالى الاتصال  
Network → DNS من مسوبه

Authoritative DNS

System → Network → DNS Servers → + Create New →

Type [ Master ]

[ Slave ]

Preferred DNS  
Client يختار ديني يكون حاليه عن طريق DNS  
Alternat DNS  
Resolving DNS  
FortiGate IP  
Clients Microsoft  
of real Clients  
FortiGate DNS  
Real IP Client  
Resolving DNS  
External Internal  
استخدامه و لوحة كتبته على مجهز  
الكتاب على المجهز

View [ Public ]

[ Shadow ]

internal IP

برديك لوكال

Recursive  
DNS

DNS Zone [ Site.Com ]

DomainName [ Site.Com ]

Hostname of primary Master

[ dns ]

Contact Email address

[ hostmaster ] hostmaster@site.com

time to leave  
Cache Client

86400

TTL

Authoritative

[ Disable ]

clients من تسجيل  
Recommended Automatic

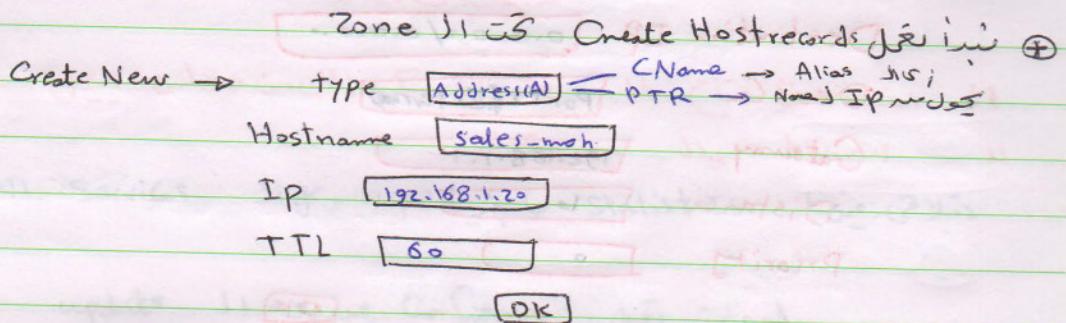
OK





لخط ١١ Create Database من هيئق ايدل

منها تاتي -



في fortigate ١٢ DNS Client لoaded من DNS Client Resove و همزة Ping طلب من FortiGate من ١٢

DNS & Domain المعايير ذات النفع في شركات صغيرة معتمدة على DNS على ١٢

لخط ١٣ لامرت اختبار user يستخدم public Policy السبلة من بروتوكول عمل

Policy & Objects → Policy → Ipv4 → InCom Portz Source all  
 Outgoing Portz Dest all  
 Service DNS Action accept  
 on NAT OK

نعمل مستعار على

Internal ونستوي 172.168.1.100 ← Portz 1 on 1

External ونستوي 192.168.1.250 ← Portz 1 on 2

172.168.1.1 ← VM المهاجر 1.3

4- اطهار رباعي ، كفيف و 192.168.1.10 و 192.168.1.1

o Replicate bridge على Portz 1 على switch

لخط ١٤ لخط ١٤ Ping من 192.168.1.1 FortiGate Reply صنع





~~Static Route~~ يطاعن على FortiGate بـ 192.168.1.1

Router → Static → static Routes → Create new →

Destination IP	0.0.0.0/0.0.0.0
Device	Port2 (External)
Gateway	192.168.1.1
Distance	10
Priority	0
	OK

8.8.8.8 → Ping طالعه و لو كانت FortiGate ردت

Reply رد

ذكر 1 يتحقق اتصال الـ FortiGate بـ Public DNS website او Exchange (يمكن users من Connect) و يمكنه كون عامل في قياس خدمة سين

~~Redirection~~ change setting with security

110 2002 21209 192.168.1.1 port 80 192.168.1.1 port 80 192.168.1.1 port 80

110 480 192.168.1.1 port 80

7002 192.168.1.1 port 80 192.168.1.1 port 80

110 192.168.1.1 port 80 192.168.1.1 port 80



53

Sub:

Date:

## "16" FortiGuard & FortiSandbox & Format Hard

### FortiGuard

Resolve ~~التي من خلالها يعلن~~ FortiGate ~~يأخذ~~ Services ~~anti-Spam و antivirus~~

Services ~~التي متاحة~~ update ~~لبيانات~~ statistics ~~بلامي فيها~~ Licences

update ~~لبيانات~~ Configure ~~لبيانات~~

Update ~~لبيانات~~ ~~مدعى عليه~~ على المونت دفعها من ~~FortiGuard SiteLink~~  allow Push update  Scheduled update [updateNow]  Every  Default  Daily

Services ~~لبيانات~~ update  updateNow ~~لواحدة~~

### FortiSandbox

attack ~~لبيانات~~ License ~~لبيانات~~ Service ~~يرغب~~ ~~فيه~~ ~~لبيانات~~ Report ~~لبيانات~~ Scan ~~لبيانات~~ FortiNet ~~لبيانات~~ Systems Config ~~لبيانات~~ FortiSandbox Device ~~لبيانات~~ واصلاح ~~لبيانات~~

Sandbox Setting  Device ID  IP  [test]

Cloud ~~لبيانات~~ Cloud Sandbox

### Advanced

System → Config → Advanced

Disk management

Hard Disk على هيرمن على Hard Disk

Hard Disk على هيرمن على Hard Disk

أطهار: يجي معاه Default

- 2GB → OS

- 30 GB → logs

لاظهار: و هنا ينطبق على VMware

Hard Disk to format بعمل فيه Command

Hard Disk to format بعمل فيه Command

# get system status

يبيلك معلومات

fixed license to Device

log Hard Disk: Need Format

### Format

Memory to Reports بتنكينا على Command

overwrite Report 97 فلانه منه يتحقق غير بعددين بعمل

# execute Format logdisk

box to Restart كل فحص فرمات

Firmware to upgrade نسخة اخر جامد

لوشنق الهايد ستلاته ظهر

System → Config → Advanced → Disk management

Up to Format لفتح فحص virtual disk

Format Disk

لاظط  $\rightarrow$  انه ممكن تتحقق اذا locap . Hard disk logs على المدى longs

FortiAnalyzer على

لو عايز تعيت الـ Report كليو<sup>ن</sup> Email

$\rightarrow$  System  $\rightarrow$  Config  $\rightarrow$  Advanced  $\rightarrow$  Email Service

Mail Server

192.168.1.100

SMTP Server

Default Reply to

FG@site6.com

Fortigate = باسم Gmail لوصله  $\rightarrow$  Enable

useName

Password

\* SMS Service  $\rightarrow$  SMS Server

Create New  $\rightarrow$

SMS Server

Name Gmail

Domain Gmail.com

SMS Configure دعبرا<sup>ن</sup> OK

بس ازى نطبقها ونضيف الرقم بتات

System  $\rightarrow$  Admin  $\rightarrow$  Administrators  $\rightarrow$  SMS Forticard Custom

Country Egypt

Phone 010235

PhoneNumber 01005522

SMS provider Gmail

ذلك هو  
يمكنها

secretkey سكرته دل كل ما تجيء تعمل login كيطلب منك

دا يستعمله كل مواد على الموارد

Registry  $\rightarrow$  Forticlient

\* FortiClient Endpoint Registration

## "17" Scripts

System → Config → Advanced → Scripts

مخطوطة

لعملات backup لـ FortiGate حيث انتهي  
موبيل موديل معين من الموديل  
موبيل موديل معين من الموديل  
الموديل الموديل

اهمية الـ Scripts

يمكن اخذ اجزاء من المعاينات Configuration  
بيانات Configuration

التطبيق العملي

1- فتح اي موديل من الـ Fortigate ونامزد backup  
FortiNet

System → Status → backup

ونفتح على الـ Desktop

2- فتح الملف بي (Backup) في wordPad → copy  
Config Firewall address

Newtext ( PasteAnd end

3- فتح الموديل والتأكد من الموديل على

System → Config → Advanced → Scripts →

Upload Bulk CLI [Browse] [apply]

Newtext ( المقدمة الى مكتبة مفتوحة

لوحة الـ address → Policy

متوجه الى Configuration

Script History

Script comes from the

IPN install the 3rd after which the **firmware** will be loaded  
 and the system program will be run from the **TFTP Server** or  
 from the **USB** stick from Fortinet's configuration  
 IPN Business Configuration from there

System → Config → advanced → USB Auto-Install

or on system restart

Default Configuration filename **Forti-system.cfg**

or on system restart

Default image name **imageout**

**apply**

58

### "18" Policy Elements (Address Object)

#### Elements of Policy

Objects  
IP Time

Services

Security Profiles

antivirus  
antiSpam  
web filter

#### 1 Objects

Address

IP Or User

Time

IP Range

FQDN

Location

مكتبة ملخص كل الأدوات

لو عايز تدخل في الأدوات

IP

Policy → objects → Address → Create

Name **IT-Mahmoud**

Type **IP/mast**

Interface **192.168.1.1/255.255.255.255**

Show in Addresslist

Interface **internal**

OK

Range

لوج

Start - end

Policy → objects → Address → Create New → Address Group

Name **HR**

Type **IP Range**

IP Range **192.168.1.2 - 192.168.1.20**

Interface **internal**

Show

OK



Sub: \_\_\_\_\_  
Date: \_\_\_\_\_

## Location

Policy → Objects → Address → Create New →

Name  Block from China

Type  Geography

Country  China

External   Interface wan

Show in addresslist

OK

## FQDN

Created

Policy → Objects → Address → Create New →

Name  Yahoo

Type  FQDN

FQDN  yahoo.com

Interface  wan

Show in addresslist

OK

التطبيق العالمي

internet ← clients → Policy → wan

1- Policy & Objects → policy → Ipv4 → Create New

Incoming interface  internal

Source Address  it-manage

لذا نحتاج الى  
الاتصال بال WAN

Outgoing interface  wan

Destination address  all

Schedule  always

Service  All

Action  Accept

Firewall / Network Options

on NAT

Config X





لعملي اجعل Policy IPS حالي لـ block اعمل location مع المصنعين

in Coming interface [wan]

source address [block from China]

out going interface [internal]

DestinationAddress [all]

Schedule [always]

Service [All]

Action [Deny]

[OK]

لاحظ اتنا بعمل او اول حاجة تم بذرة مستخدمها من

- Policy

location, FQDN, Range, IP مع العلامة المعيّنة لجمع او Group ونخدهم في كلهم فيه.

\* طبعاً اعمل الافضل انتامان فعلش IPS ولكن الممكن Range لكن هتواجهنا من ال Reports من هنبي عارفين اسم كل داير طالع داير كل IP على فيه.

التطبيق العملي لعمل Group

1- نعمل كذا IP ← objects

Objects → Address → Create New → Address Group -2

Group Name [IT]

Show in address [✓]

Members

[it-mahmed] +

[it-mostafa]

و لخبي الداتا الاتالية

[OK]



مع العلم اصلًا في قنابيل الـ Policy ممكن و نابيل

Source Address

اما، ليس object مع تعريف لكن كتنظيم من ذيكر شكل

Policy

لذلك هم كل امثل Group اصحاب الواقع اللي عايز اعتقدوا

احظوا من الـ Members

Policy Groups

Members

Access





## 19 Policy Element (Service Object)

### ② Services

Layer 4 ← Port رقم بروتوكول

Transport

Port

TCP  
0 → 65535

UDP  
0 → 65535

object → Services

هذا يعني أن المجموعة المطبقة على كل بروتوكول

General

All-TCP  
All-UDP

web access

HTTP  
HTTPS

File Access

FTP, FTP-Get

وذلك لأنها تطبق على جميع المجموعات ومهما

هي مجزأة في المجموعات

لذلك يمكن إنشاء templates

حيث يمكن إنشاء قواعد مختلفة

مجزأة في المجموعات

→ E-mail Access

→ Exchange

→ web access

لـ ٤ اصلـ يـنـقـعـ اـعـمـلـ كـيـهـ سـيـرـيـهـ Service ١ Create  
Port Service وـ مـحـتـاجـ اـفـعـ الـ دـرـيـهـ DVR

Policy & objects → Objects → Services → + Create New → Service

Name

Show in Service list

Category

Protocol type

IP/FQDN

Protocol  Low  High

Specify Source Ports

OK

لـ ٥ اـعـمـلـ يـنـقـعـ اـعـمـلـ Services (هـنـاـجـمـهـ) نـزـلـتـ مـعـ اـلـ جـمـيـعـ

Create Service Group

Service → Create New → Service Group →

Group Name

Members

HTTP

HTTPS

POP3

DVR

OK

لـ ٦ كـنـظـيمـ مـمـكـنـ اـعـمـلـ لـكـلـ اـدـارـهـ Services ٣.١ Group

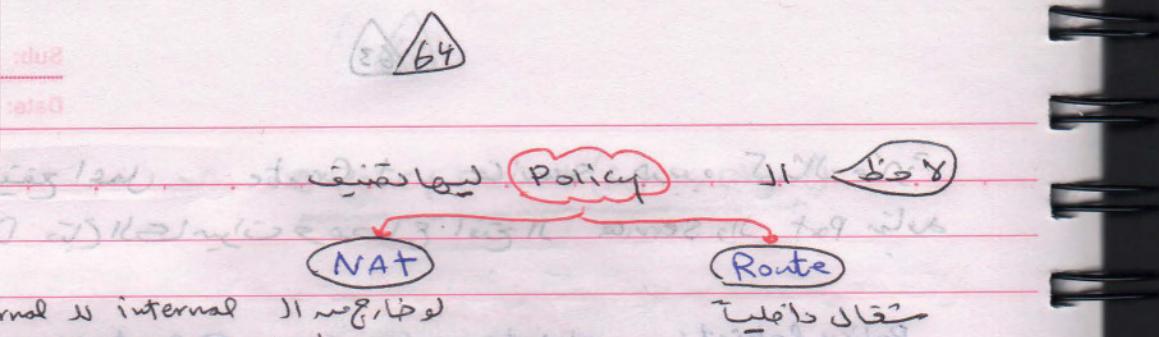
لـ ٧ مـعـنـىـ اـصـلـ اـعـمـلـ خـاصـيـهـ كـيـهـ Category ١ Create

معـ بـعـدـ Cateogry كـيـهـ سـيـرـيـهـ لـ ٨ نـعـلـلـ Create Service of

اـصـلـ الـ هـرـهـ دـيـ اـنـابـلـ بـعـدـ Cateogry

Services مـعـ خـاصـيـهـ مـنـقـتـ حـواـهـ





لقطة يقع امثل برئي عرض الـ Service كعمليه تنظيمية

Object → Services → Category Setting

لوحة اداري سكل العروض اخليه لعمليه  
By Category      Alphabetically

Table      Service

لقطة يقع امثل لـ Delete لكن سطر دفعها من Group او Dent & Delete هي امثلها غيرها من Category

لقطة يقع امثل لـ Delete لكن سطر دفعها من Group او Dent & Delete هي امثلها غيرها من Category

لقطة يقع امثل لـ Delete لكن سطر دفعها من Group او Dent & Delete هي امثلها غيرها من Category



20

# POLICY ELEMENT SCHEDULE (TIME)



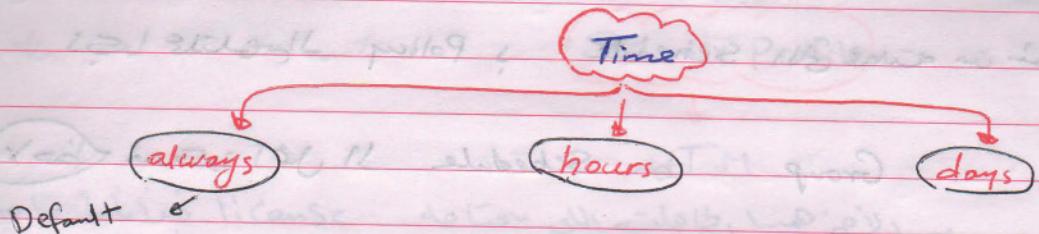
FORTINET.  
الفورتي<sup>ن</sup>  
الجيت  
بالعربية

65

Sub:

Date:

## 20 Policy Elements (Schedule Time)



Policy & Objects → Objects → Schedules → + Create New, Schedule

Type	<input checked="" type="radio"/> Recurring	<input type="radio"/> one-time
Name	Free for meeting	
Start Date	2015/12/9	
End Date	2015/12/9	
Start time	Hour <input type="text" value="8"/>	Minute <input type="text"/>
Stop time	Hour <input type="text" value="15"/>	Minute <input type="text"/>
Pre-expiration event	<input type="checkbox"/> OK	

Type	<input checked="" type="radio"/> Recurring
Name	Facebook
Days	<input checked="" type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday
Start time	Hour <input type="text" value="12"/> Minute <input type="text"/>
Stop time	Hour <input type="text" value="15"/> Minute <input type="text"/>
	OK

لما يفتح الـ Facebook في يوم الجمعة

Policy Element من طبع اتاميل - ١٢:٣٠ طبع

### التطبيق المحمى

Policy → IPv4 → Incoming Interface

Source

outgoing

Desti.



Schedule

Service

Freeformet

websaca

تحت المعنون



Accept

التي تحدد من شروط Schedule  $\rightarrow$  Policy

Group  $\leftarrow$  Schedule لخط ممكن فعل لا

Objects  $\rightarrow$  Schedules  $\rightarrow$  Create New  $\rightarrow$  Group  $\rightarrow$

Name [1-3, 5-6]

Members [1-3]  $\oplus$   
5-6

دالى مستخدمة هنا لمعايير افتح من 1  $\leftarrow$  3

3  $\leftarrow$  1 no Schedule Element 1- فعل

6  $\leftarrow$  5 no Schedule element 2- فعل

3 - جمجمة Group

$\rightarrow$  time settings

polynomial polynomial polynomial weight

[ ] start [ ] end with time

[ ] start ( ) end with date

70

بروتوكول التحكم في الموارد  
is defined as transport layer 17 port

Network Control

[ ] start [ ] end weight

[ ] start

[ ] end

start [ ] end

start [ ] end



Sub:

Date:

## 21 Security profile (Antivirus)

Security Profile

لأنه يعتمد على license طابعات التي تحتاجها

Antivirus

Virus

Trojan

Spyware

Security profiles → Antivirus

web filter

Application Control

enable او disable

System → Config → Features → Security features → presets [Full]

Security profile ظهر حمايات

Create Profile أعمل Antivirus

System → Config → Features → Multiple security profiles

Create security profile Antivirus بعد ما تدخل في زر New على [apply]

Security profiles → Antivirus → Edit Antivirus → [Add] +

Name IT

Comment

—

OK

اهمية Customized Security Profile لكي نعمل على Scan

الى Scans التي نجتى من هذين Scans التي نستخدمها

على كل حماجه ولكن على حمايات معينة

912089

Policy هي الأدوات التي يظهر في Create profile بعد ما نعمل

وتحاكيها

Features in Security Profile ومنها ي العمل

Security profiles → Anti Virus → +

Name IT

Customize  
هذا، الحالات التي نعمل  
Scan على

web traffic emails قالب اسفله على او  
رسائل البريد الإلكتروني

Inspection Mode Flow-based

Proxy

virus class من هنا يتم  
 Blocking العناصر التي تم

Detect virus Block

Monitor

Send file to FortiSandbox

لوحة الفيروسات  
لقطة شاشة

Config إلى المعرفة

Cloud معرفة

Detect Connections to Botnet C&C

Cloud & C2I  
servers

Block

Monitor

Cloud & C2I  
servers

Block

Cloud & C2I  
servers

Apply

FortiGuard - FortiGuard Antivirus

System → Config → FortiGuard → ATPservices

Antivirus

IP Class Monitor يتحقق من هنا

User & Device → Monitor → user Quarantine

default يتحقق هنا

Comd لعمليات المروج

System → Dashboard → Status → CLI Consol

ممكن ندخل خصم الـ Dashboard

Telnet و يمكن ندخل  
Interface على telnet تغيير

C:\>telnet 192.168.1.99

login: admin

Pass :

```
# Config antivirus setting
(Setting) # Set default-db extended
# end
```

Mode الـ دينا غيرت الـ

Mode ② يعتمد على Antivirus ①

Normal

يعتمد على Db

FortiGuard

Default

Cmd (غيرها)

Extended Recommended

يعتمد على معايير انتي فيرس

license informs لبيانات الترخيص

\_db

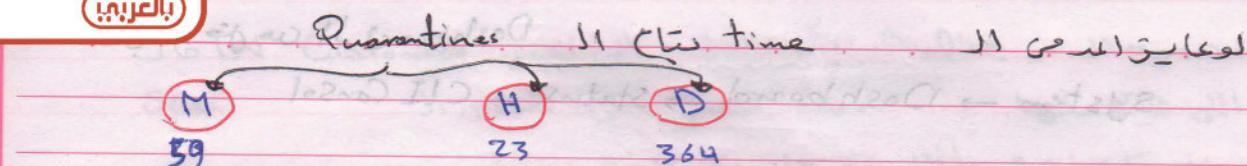
FortiGuard المزود

وتحتاج

لوباءز اغل Virus Scan Enable Grayware

```
# Config antivirus settings
(setting) # Set grayware enable
```

10



اد اعد من القديم → Create profile ممكن ان

# Config antivirus profile / tomist</>

(Profile) # edit HR كـ (الملف المعرف)

(HR) # Config nac-quar

network access Control

# Set infected quar-src-ip

# Set expiry 5gm or 23h

# end

GUI طابط الى علت هادر

ما ينفعه

ذلك زر دخلي

### \* Creat Av profile

1- Config antivirus profile

2- edit Profile Name ()

### \* Enable grayware enable

1- Config antivirus settings

2- set grayware enable

### \* Enable Nac

1- Config nac-quar

2- Set infected Quar-Src-IP

3- Set expiry 5gm

لـ **Copy (do)** و **Profile** لـ **Security Profiles** اـ **Antivirus** **71**

Security Profiles → Antivirus →   

list view **list** **عرضهم**

لـ **Scan** تـ **Antivirus** **71** **ماكمات** اـ **Scan** الملفات أـ **كبيرة** طـ **large** اـ **viruses** اـ **known** اـ **new** اـ **unknown** اـ **new**

System → Config → Features → local In policy **on**

Vulnerability Scan **on**

Apply

لـ **Policy** **هـ** **لـ** **objects** **هـ** **لـ** **Policy** **هـ** **لـ** **objects** **هـ**

Policy & Objects → policy → ~~Proxy options~~

Common options

Block oversized file/email 

MB **10**

داعـ **Protocols** **لـ** **الـ** **محـ** **منـ** **فـ** **وـ** **فـ**

email **HTTP** **FTP** **SSH** **telnet** **SNMP** **ICMP** **ARP**

"22" TRAFFIC Shapers (objects)
Objects
Traffic Shapers

التحكم في الـ Bandwidth user او تقسيم وتوزيع السرعات

ويمكن امره website معين لنقل سرعة المتصفح بناءً

مع ملاحظة يمكن احتل الا 256 ← browsing

512 ← Download

انواع Traffic shapers
Shared Traffic
Per Policy

نوع واحد Policy لـ مجموعه

Policy على مجموعة traffic الشaper bandwidth المتصفح

traffic shaper لـ Policy

لـ IP

Priority
traffic shaper
High
medium
low

Policy & Objects → Objects → Traffic shappers →

نوع المجموعات

512 ← Policies type ○ Shared

○ Per-IP

512 || Layer 7 Policy || ↳  
IP-Range

### التصنيف العملي

Address ← objects ② ١- نعمل  
 IT-mahmoud 192.168.1.2  
 IT-Ahmed 192.168.1.3

### Traffic Shaper ٤١ - ٢

Policy & objects → Objects → Traffic shapers →

Type  Shared

Name  ١M Perpolicy

Apply  per policy

Max Bandwidth ١٠٢٤ اقصى سرعة

Guaranteed Bandwidth ١٥٢٤ اقصى سرعة

OK

٣- نعمل على تعيين الطرق و لكن بخلافها Traffic Shapers

Apply  All Policies

T.S II Create policy ٤- خارج

Policy & Objects → Policy → Ipv4 → inCom

Source

outgoing

Destin

Action

### Traffic Shapping

SharedShaper

٥- نعمل على تعيين policy لـ user (IT-mostaf)

← T.S درجة حرارة

6- دينار على user كفالة policy ② بحسب خط اتصاله  
 - دخل مقطوع بـ 1mb لوحدة -

1mb ← T.S دينار على درجة حرارة Range IP list - 7  
 Per-policy درجة حرارة

1mb كفالة مقطوع بـ Range ①

لوضع خارج All policy الى Per-policy T.S  
 على كل ثلاثة policies المقابلة  
 1mb كفالة مقطوعة كلهم بـ Policy ③

ديرا خارجنا الـ All policy او Per policy سواء Shared

\* بحسب النوع الثاني

Policy & Objects → Objects → Traffic shapers →

Per-IP

Name [HR 1mb PerIP]

Apply [Per policy] 8ARP policy

Traffic priority [1024]

Max bandwidth [1024]

Guaranteed bandwidth [ ]

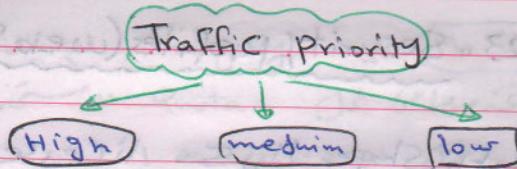
OK

لوضع اطبع كفالة policy de T.S معينة دلوقت

user كفالة HR دينار بـ Range IP وحدة

Recommended line [500] 1mb مقطوع بـ HR كفالة

175



Policy ② ينستخدما لـ T.S ②

Priority high 4.1mb ← T.S ① لـ علـا

Priority low 8.mb ← T.S ②

لـ الـ وـ اـهـ ① تـ سـبـ الـ مـ بـ دـيـ اـهـ وـ مـ هـ بـ اـهـ

Download T.S ② دـيـ لـ عـلـاـهـ

افـيـ اـتـ traffic shaper مـ حـلـقـةـ

- Shared Shaper → Download
- Reverse Shaper → Upload
- Per-Ip Shaper → Range الـ مـ بـ وـ مـ هـ بـ اـهـ

وـ دـاـ طـبـعـاـ

traffic shaper الـ مـ حـلـقـةـ options

DSCP

diferentiated session user الـ مـ حـلـقـةـ sessions

bandwidth الـ مـ بـ وـ مـ هـ بـ اـهـ

Session طـبـعـاـ الـ مـ بـ وـ مـ هـ بـ اـهـ

Not Recommended





## ٢٣ "Security Profiles (web filter)"

لائحة انتهاء محتوى trafficShaper لا تملك license لـ trafficShaper

### Web Filtering

#### FortiGuard

#### Manual

license لم يتم شراؤها yet  
website 47 million منها FortiNet website موجودة في Database

Antivirus profile | المترافق مع web filter || داخلي

#### المُطبق الحال

Name

Inspection mode

Proxy

Flow-based

DNS

جاء من http:// browser side

Fortigate لـ trafficShaper

نقطة إنترنت  
التصفح من category

#### FortiGuard Categories

Custom | Local Categories

أصناف كبيرة | Potential liability →  
Allow Block Right Click

user يمكنه تنفيذ actions في Block | دخلي

System → Config → Replacement Messages →

FortiGuard Block Page

وينقع لغتها من دخلي



لادن يمكن نعمل رساله على اطارات Category Monitor الى **Monitor** التي يفتحها كل 15 ثانية عمل Quota لوضع بعض Schedule كاملاً ام درس 1-4 يفتحوا Facebook لكن Monitor امرده ساعه يفتح فيها Facebook في دعائنه سنه

Social Networking → Monitor → Quota → Create New →

General interest-personal

Social Networking

Quota **5** minutes

**OK**

site كل ما يدخل على **warning** حذف كل اجل illegal بطبعه رساله اند على موقع Category تحريم او warning و لكن كذا الوقت اللي يظهر فيه

~~System → Config → Replacement messages~~

website كل معناها كل حاجي ليت **Authenticates** يمكن اعمل معين يطلب هن Password و userName و يمكن استخدم فيها اى مفتاح على اداره Facebook N Policy و لكن يعرقش يدخل عن طريق **Active directory** الي او بي ان

Category **Allow Blocked override** **Policy** نعمل

Apply to Group **Group** ماتغير

Assign to profile **Profile**

Scope **Scope**

Duration Mode **Duration**

### ① Search Engines

- Enable Safe search
- Search Engine Safe search
- YouTube Safe search
- YouTube Education filter
- Log All Search keywords
- Search logs
- Search by keyword
- Search by URL

### ② Static URL Filter

- Block invalid URLs
- Enable URL Filter
- Enable web Content Filter

### ③ Rating option

- Allow websites when Rating occurs
- Rate URLs by Domain and IP
- Rate images by URL (Blocked images Replace)
- Block HTTP Redirect by Rating

### ④ Proxy options

- Restrict Google Account usage
- web Resume Download Block
- Provide Details For blocked HTTP 4xx and 5xx Errors
- Block User Error as website
- HTTP Post Action
- Remove Java applet filter
- Remove ActiveX
- Remove Cookie

### Local Categories

ماهتم بالـ Local Categories لـ موقع ما معنـى  
او، (Local Categories) لـ موقع ما معنـى

Security & profile → Advanced → web Rating overrides →

Custom Categories → + Create New →  URL (www.facebook.com)  
 Custom Category  Category rating  Allow  Block URL

Advanced → web profile overrides →

Create New → User Usergroup  SourceIP

الى Custom Categories

لـ اصحاب تفـقـد

Policy & Objects → Security profiles → web filter →

FortiGuard Categories → Local Categories

Allow  
Block

لـ اصحاب

Category  Related  URL  لـ اصحاب تفـقـد

System → Config → FortiGuard →  URL's category rating → Click here

URL

Verify

Submit

Category  حسـمـة

by this Path  اقتـنـى لـ اقتـنـى  (اقـتـنـى الـ قـيـمـةـ)  Local

Category



180

## 24. Web Filter

URL filtering (فیلترینگ) فیلتر ناشر (FortiGuard) (web filter) ایجاد کردن

URL 5000 (کد فایل) (Web license)

Security & Profile → web filter →  Enable URL Filter

+ Create New →

URL: www.Yahoo.Com

Type:  Simple  Reg. Expression  Wild Card

بیکنل نظریه ای URL فقط که ای لینک  
و آن اوتکاره بیکنن مادری

برای ای URL و ای مادی بیکنن  
DomainName  
www.Yahoo\*.Com/\* ویلیا www.\*.Yahoo\*/\*

Action:  Exempt  Block  Allow  Monitor

Scan Virus  Filter URL  محدود کردن  
که فیلتر شود  محدود کردن  
که فیلتر شود  محدود کردن  
که فیلتر شود  محدود کردن

Status:  Enable →

تغییر کردن  
که فیلتر شود

OK

## 25. Content Feature

Security & profile → web filter →  Enable web Content Filter

فیلتر ایمیل (Custom Extension) (که فیلتر شود)

Create New → Pattern type:  Wild Card  Reg. Expression

Pattern: \*.\*.exe  
\*sex\*

Language:

Action:

Status:  Enable

OK



181

Sub:

Date:

### 25 Application Control

خط ترتيبها من 11 view الدخاله مع اهم التطبيق العملى هو الاولى

- Policy ↴ ترتيب التطبيق
- ① Antivirus ↴ العملى
- ② Application Control
- ③ web Filter

التطبيق العملى

1- Security & Profile → Application Control → + → Name **HR**

Categories

view Right click Botnet  
 Signatures Apps Socialmedia  
 قصرين المجموعات  
 face اقسام

Signature ↴ add ممكن نعمل خط

+ Application override

+ Add Signatures → وتصنيف

خط مكتوب على Categories si

Allows	
Monitor	
Block	ممكن نعمل مكتوب هنا
Reset	
TrafficShapping	ممكن نعمل شاپر

خط مكتوب على Network Service Category

خدمات DHCP و DNS و Network مكتوب على

Options

- (on) Deep inspection of Cloud application
- (on) Allow and log DNS traffic
- (on) Replacement Messages For Http-based

Options مكتوب على

نوع اتصال فايبر او بروتوكول امن اتصال  
 Connector مكتوب على

whatsapp الجماعة في البروتوکول لفتحه على http

OK



Policy نطبقها على من اد Application Control

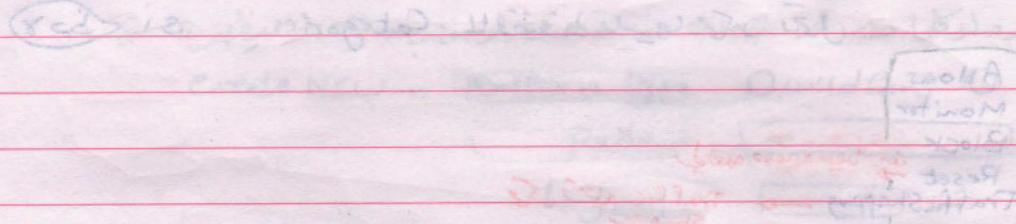
Policy & Object → Policy → Ipv4 →  Application Control

SSL Inspection (يعني تفاصيل Youtube والـ Facebook) المواقع التي

Policy → SSL Inspection →  →  profile

Policy II (عندما نطبقها على المواقع)

SSL Inspection



Project 403 II (متى نطبقها على المواقع)

Ex 1 (ما هي)

fastest download speed with high bandwidth utilization quota @  
lowest latency and high bandwidth utilization quota @

latency



bandwidth utilization quota @

latency quota @

"26" Instruction Protection System

Templates (ما يطلق عليه Fortigate) Hacking (التجسس والهacking) ← دراسة الجيسم والهacking

Customize (تعديل) (ما يطلق عليه customization) حماية وتعديل امني

with configuration

Security & profile → Intrusion protection → Note: [ ]

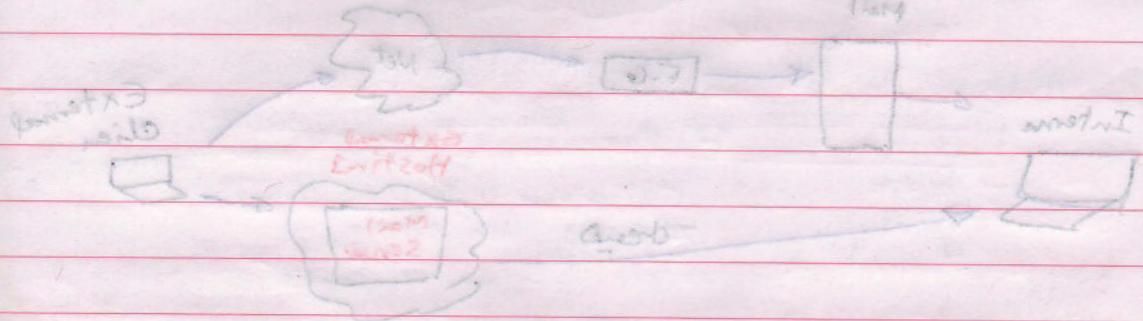
لوحة تحكم بابا يار

③ Application Sensor Client → Create New  
 target (الهدف) OS (النظام) Sensor Type (نوع المترقب) Filter Based (متعدد) Specify Signature (تحديد التوقيع)  
 Filter Options (متعدد) Options (الخيارات) Basic (Основные) Advanced (متقدمة)

Action (عملية) Signature Default (افتراضي) Monitor All (مراقبة كل) Block All (منع كل) Reset (إعادة تعيين) Quarantine (العزل)

Default (افتراضي) أو Custom (مخصص) templates (ال��ل) (ما يطلق عليه Templates) الاختيار طبقاً لاحتياجاتك

IPS (ON) (فتح) Policy (سياسة) وتحت سطح IPS (فتح) ويعبر ماء العذبة (فتح) (فتح)



Red dots indicate monitoring points or sensors placed throughout the network. Labels include 'Cloud', 'Client A', 'Client B', 'Router', 'Switch', 'Monitor 1', and 'Monitor 2'.



### 27 Email Filter

الآن ندخل في بحث Anti-Spam على هذا  
level (12) نجد FortiMail لكن المنتج المتقدم (1)

Create profile (ج) AntiSpam (ج) AntiSpam

Security & Profile → Email Filter → +

+ Name HR  
Mode  proxy  flowbased

Enable Anti-Spam detection

IMAP action

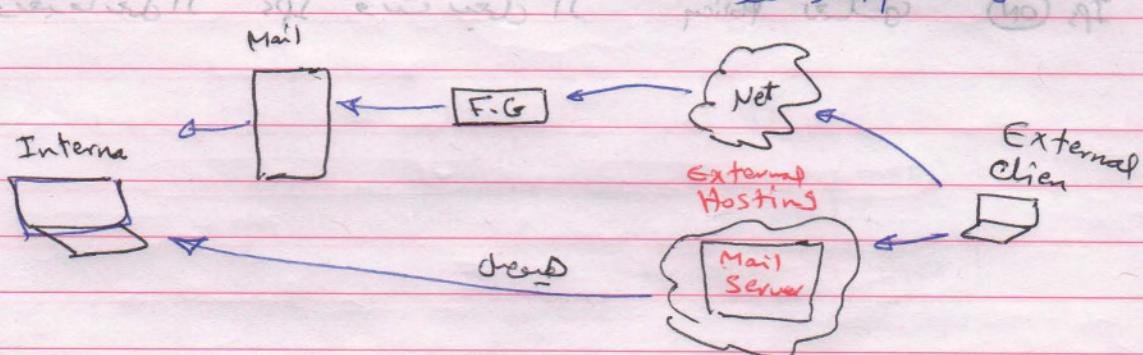
Pass tag

Exchange (ج) ← SMTP subject (ج)

smtp bie & tag Pass Discard

### Anti-Spam

خط ارسال Mail Server → Internal → Discard (ج) مفاجئ



Mail Server (ج) يأخذ من إعدادات غير لو (ج) باقى (ج)  
Internal.

لهم يرسل موقع قاتل mail (ج) URL

- ④ FortiGuard Span Filtering
  - IP Address Check
  - URL Check
  - Detect phishing URLs in Email
  - Email Checksum
  - Spam Submission

① Local Spam Filtering

BH610 DNS lookup

Return Email DNS Check

② Black white list

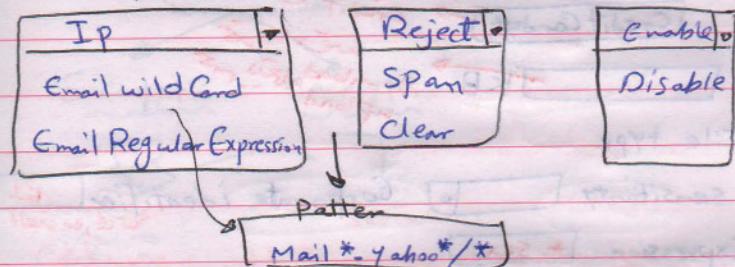
→ blacklist ~~and~~ Domains ~~white~~  
whitelist ~~و~~

③ Create New

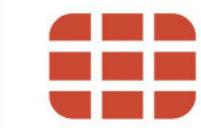
Type

Action

Status



Internal ← Mail Server ~~لـ~~ دعـم مـنـظـرـة Options ~~لـ~~ ~~لـ~~ ~~لـ~~ ~~لـ~~



180

### "28" Data leak Prevention

"DLP"

مَانِعُ تَسْرِيْبِ الْمُدَّىَّاتِ ("لِجَسْدِ الْمُدَّىَّاتِ")

Security profiles → Data leak prevention → Create New →

① message      ② files

③ Containing

CreditCard#

مُكَوَّنُ بِكَارِدِ الائتمانِ

④ File size

JKB

كِيلُوبَايتٍ

Download

Upload

extension

مُنْسَخَةٌ مُعَادِنَةٌ

Specify file type

Down

load

Watermark sensitivity

Corporate identifier

load

Down

Regular Expression

\*.sex

load

Down

Encrypted

Examine Following Services

Service 1, is

webaccess

التي هي بطيءة على 1, الـ

Email

—

—

others

—

—

#### Action

NON

For

Minutes

logs view

Block log

CLI

بالنهاية لـ DLP

Default

logs view

Quarantine

# Config dlp sensor

sensor (W)

# edit sales

# Set nac-quar-log enable

Default or Clone

أو حفظ الملف

Policy and Objects to DLP

options

Policy & Objects

→ Policy → IPv4

→

ON DLP Sensor

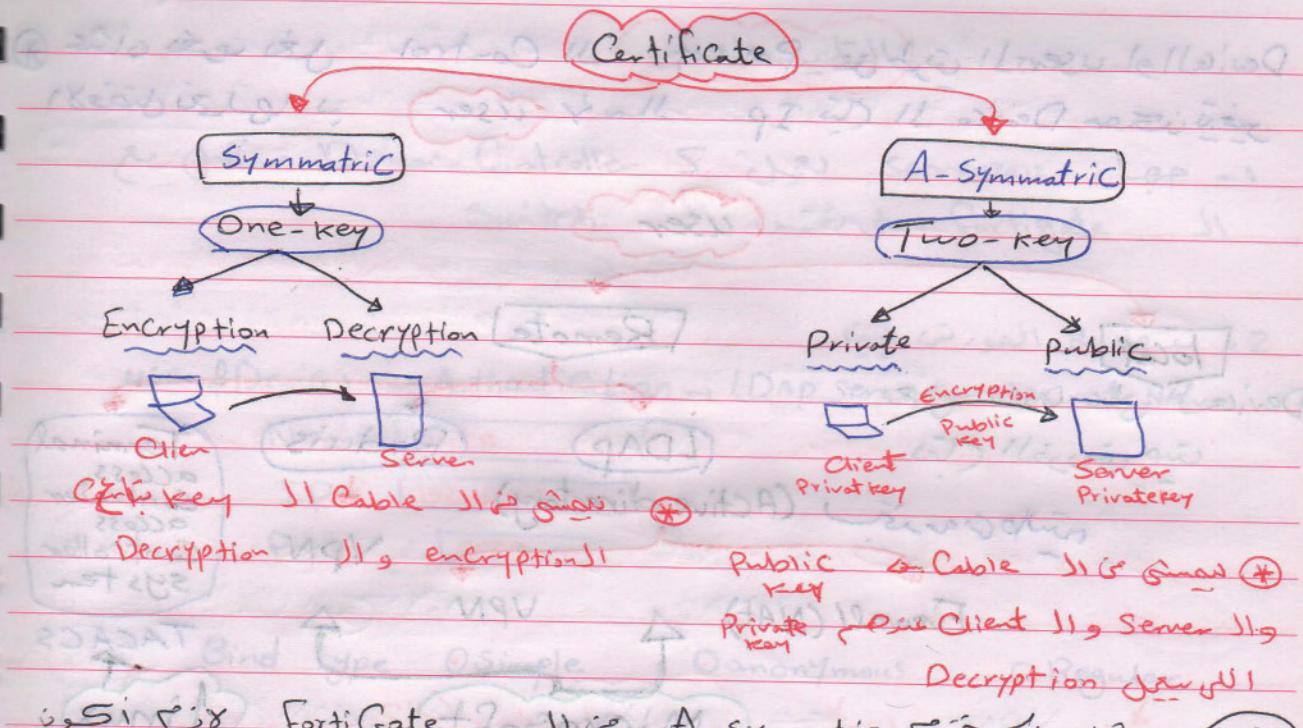
→

Profile

المكتوب



Encryption و Certificate II مع الجوز  $\rightarrow$

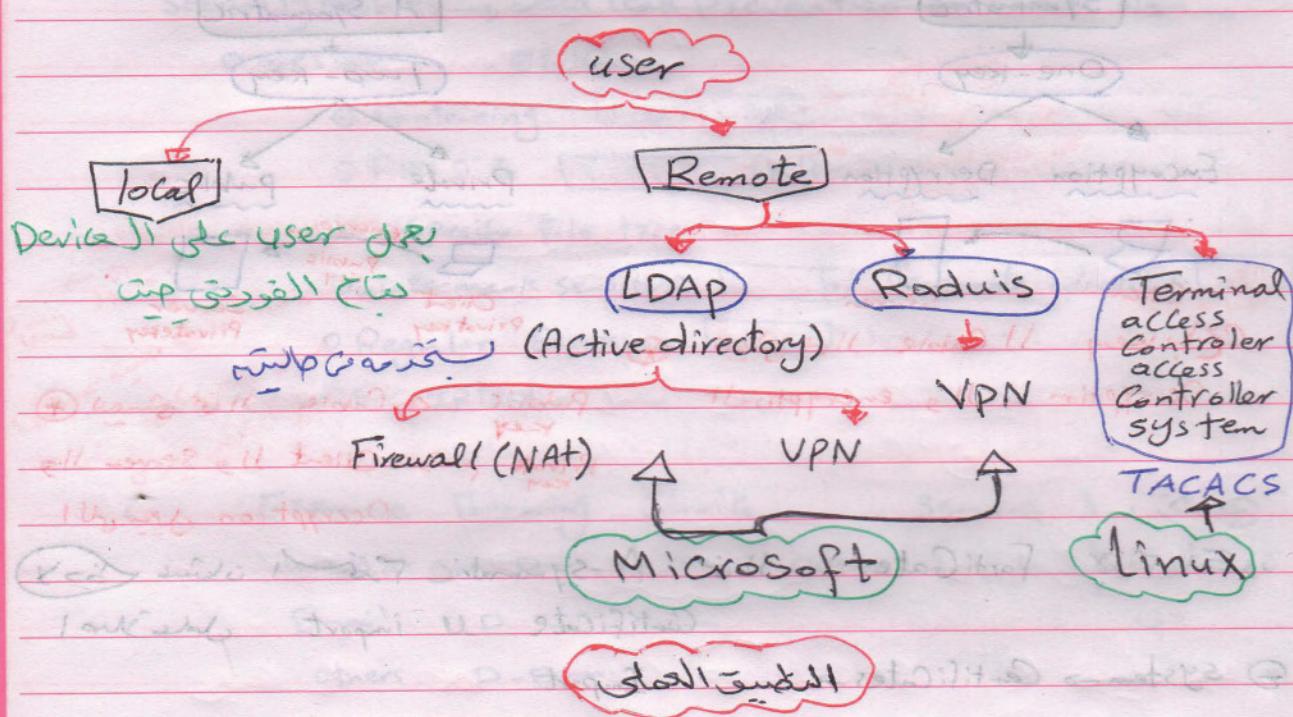


FortiGate 47 من A-Symmetric في حين  $\rightarrow$  Certificate II import

④ System → Certificates → Import

## 29 Users (Local & LDAP users)

عندما نعرف بعمل Policy أو Control  
عن طريق ما يملك Device IP ينادي user  
الأفضل استخدامها



### Local user

- 1- users & Devices → user → user Definition → Create user
- 2- Local user → userName [Ali] → Next → Password [aaaa]

Email Address

→ Next

Enable

two-factor authentication token

SMS

Create

users (أيضاً) ونسميها user  
users & Device → user → user Definition → Ali local

٨٩ - LDAP اول نوع ال Remote user

### التصنيف العملي

- ١ - نعمل مع جهاز Domain Controller 5 بعمل 5 Server2012 ; لـ LDAP  
Switch على نفس IP على fortigate

- ٢ - ندخل على الفورت بمعرفة

user & Devices → Authentication → LDAP servers → + Create New

Name Site

IP 192.168.1.200

Port 389

Bind type  Simple  Anonymous  Regular

Ex: Site\mahmod

نحوه

child, tree

نحوه

automatic Detect

Pass دار

وكلما يجيء

٩٠ - Distinguished Name (العنوان المميز) لـ Regular

Domain → Active directory users and Computers → users

administrator → Right click → properties → Attribute Editor →

distinguishedName → CN=administrator,CN=users,DC=SITE,DC=Com

Copy نسخه

وندخل على الفورت بمعرفة

Bind Type

Regular

user DN Past

Password

test

نجل

٩١ - Domain Certificate (جواز التحالف) لـ Secure Connection

Secure Connection

نجد ما عرفناه في Fortigate هو Domain LDAP

4 - User & Devices → User → User Definition →

⇒ Remote LDAP user → Next → Choose Existing

1 - اختر الموقع الذي ينتمي اليه حسابه من سطوة site

2 - اختر Next → Ou=IT

Ou=Computer لـ user المعماري

Ou=users → ahmed → add selected →

[Create] → OK

users Fortigate هو انجاز جيد

ولا يقتصر على اضافة Group كامل منه سبط و افراد user

نجد اطبقنا النوع الاول الـ LDAP

VPN

← RADIUS

تطبيق النوع الثاني الـ RADIUS

نجد تطبيق الـ LDAP في انجاز

حيث ندخل على موقعه فنحصل على pass و userName

ولو ما استخلص على المتصفح (5) دقائق المتصفح و يمكن تزويدها من Monitor

والعاشر تكررها

لوباء ازدحام المتصفح

User & Devices → authentication → Setting → Authentication Timeout

لتغييرها

الـ Default

المشكلة ان طرد ما بعد انجاز

الاستونت يعني حفظ قابل للتغير

لوعاير تعامل لو عايز تعامل users نخصية فيها group

User & Device → user → user Groups → Name **IT**

Type  firewall

Members **10**

**OK**

login يتعامل في الـ FortiGate II **لوكاين**  
وليس الـ login Name وليس الـ DisplayName

user & device

user & device

user & device

**10**

user & device

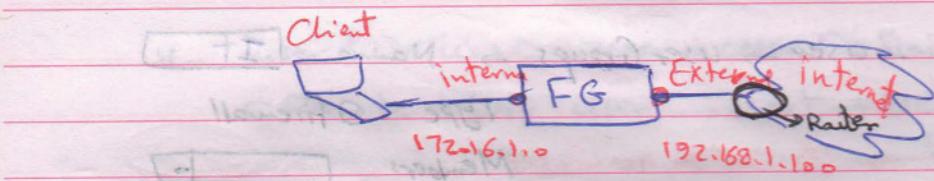
**10**

user & device



92

### 30 Configured IDAP Server



التطبيق العملي

Default Routing ونعمل على Net خارج Fortigate ١٩٢.١٦٨.١.١٠

Router → Static Routes → Destination IP [0.0.0.0/0.0.0.0]

Device [Port2 External]

Router خارج Router Gateway [192.168.1.1]

OK

Internet على Fortigate على Ping .  
زنـ 2 زنـ 3

internet N Client طلـ ١٧٥ Policy

Policy & Objects → Policy → Ipv4 → Incoming interface [Port1 (internal)]

Source [All]

Outgoing interface [Port2 (External)]

Destination [All]

Schedule [Always]

Service [Allows]

Action [Accept]

On NAT

OK

internet N Internal على طلـ ١٧٥ Policy مـ ١٣٥ \*



المثال اللي قات دا كان عن طريقه اشتا حددنا IP معين و دا لا يعنى

عن طبيعة الاعتنى يكوى عن طريقه الـ user

group

Source users HR

\* بقى بلاحظ لو طبقتها طريقة الـ user اللي بيطلع في كرتيل user Pass

userName AhmedAli

Pass

لاظ

Display Name

logon Name

لوعايز نشوى الـ users اللي طبعهم

user & Device → Monitor → Firewall → AhmedAli

\* هيسجله اللي دا فاسم على الـ الت دلوقت

الـ secret

user name

password

secret

"31"

## CONFIGURED RADIUS Server



### 1.31 Configured Radius Server

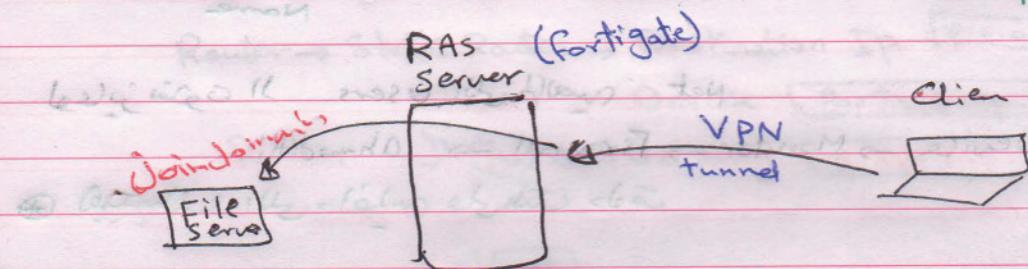
#### Radius Authentication

2003 Win Server  
IAs internet authentication Service

2008, 2012 NPS Network Policy Server

Radius (fortigate)  
File Server

خطاطي اعل LDAP SIE



جي دي في Network ١١٠ Client FG على local able دايماراد Pass user يدخل Network ١١٠ users لـ RAS او افعه الـ Authentication

join domain <--> Server ١١٠ RADIUS Server  
Domain ١١٠ Authentication <--> Fileserver ١١٠

#### الخطوات

Domain او Fileserver ١١٠ win 2012 > let - 1  
Server manager → add roles and features → Next → Next →  
File and Storage

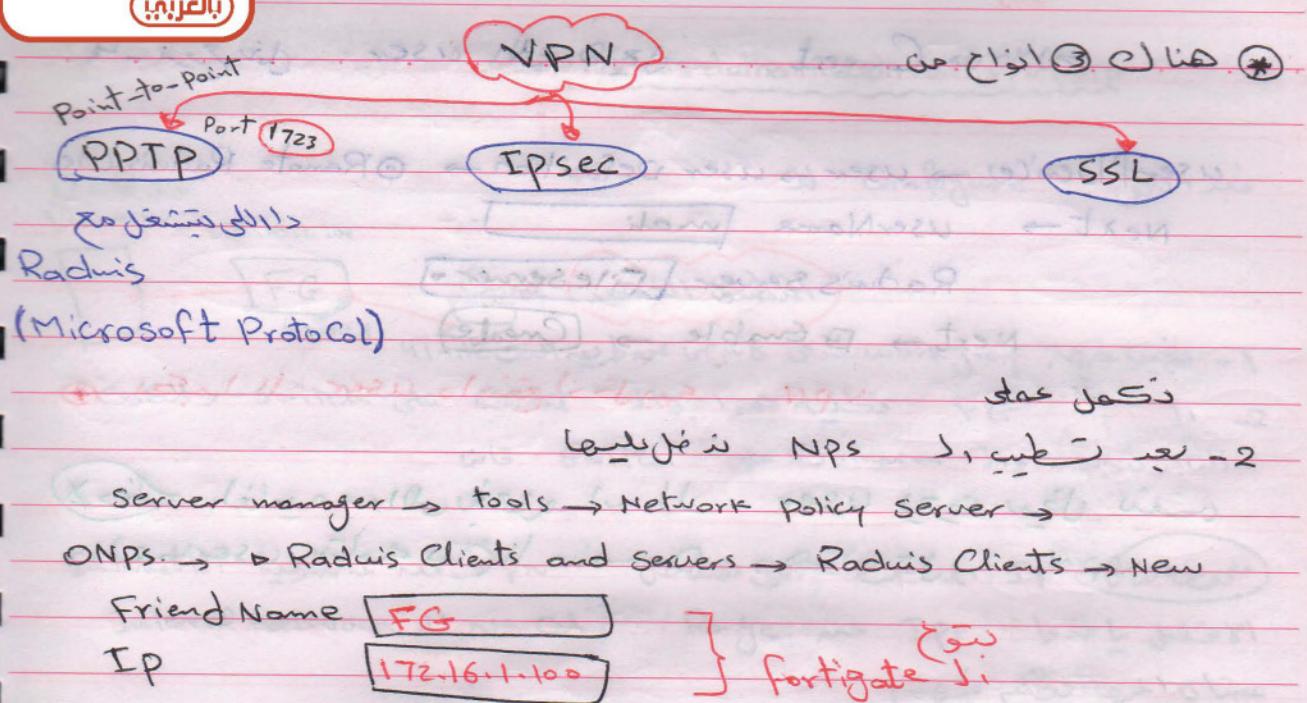
Network policy and Access services

[add features]

Next → Next → Network Policy Server

Next → [Install]





Shared Secret .....  
Confirm .....

FortiGate نزع علا - 3

User & Devices → Authentication → MS-CHAP Servers → Radius

Name File Server

IP 172.16.1.100 NPS

Primary Secret

.....

الكلمة السرية

test

test will do it

Success User, Client, Pass

Authentication

Default

Specify

Method

MS-CHAP-v2  
MS-CHAP  
CHAP  
PAP

تحتاج إلى صيغة فقط  
Product id

OK

حالات Connect

الى قيم user المزمع

userDevices → user → user Definition → Remote Radius User

Next → userName mali

Radius Server FileServer

Next →  Enable → Create

VPN دينج داخلية

لما يدخل الـ user يجري سفل بعده

يتم إنشاء مسماح الـ Domain userNamed

user [ 27 ] small business

user [ 28 ] small business

[ 29 ] small business

[ 30 ] small business

[ 31 ] small business

[ 32 ] small business

[ 33 ] small business

[ 34 ] small business

[ 35 ] small business

[ 36 ] small business

[ 37 ] small business

[ 38 ] small business

[ 39 ] small business

[ 40 ] small business

[ 41 ] small business

[ 42 ] small business

[ 43 ] small business

[ 44 ] small business

[ 45 ] small business

[ 46 ] small business

[ 47 ] small business

[ 48 ] small business

[ 49 ] small business



"32" Radius Authentication with VPN PPTP

172.16.1.0

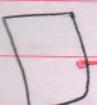
Domain

172.16.1.100

VPN

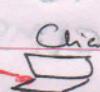
Configure

نبدأ بـ



FG

41.1.1.1



Client

التطبيق الحاسوبي

1- نبيح جهاز FG كأنه جزء من مجموعة العمل

2- نبيح جهاز FG كنútنة لها IP 172.16.1.100 ونبيح جهاز switch كنútنة لها IP 41.1.1.1

التابع بتابعه 172.16.1.0

Internet ||| VPN

Internal Network ||| Clients

الافتراضي يأخذوا IP من المجموعة

بيانات المراقبة فيهم

Range & Object

Policy & objects → Objects → Address → + Create New →

Name **VPN**

Type **IP Range**

Ip **10.10.10.1 - 10.10.10.10**

Interface **Ports**

المتصفح

Show address list **OK**

OR

4- ندخل بـ Policy

Policy & objects → Policy → IPv4 → Incoming interface **Ports**

Source address **VPN**

Outgoing interface **Port**

Destination address **All**

Schedule **always**

Service **All**

Action **accept**

OK



198

(PPTP) (PPTP) Configure VPN . فتحVPN

Cmd طرق اول من ينفع

FG ١١ de Jan - 5

System → Dashboard → status → Cli →

```
# Config vpn as PPTP
(ppp0) # Set status enable
( ) # Set sip 10.10.10.1
# Set eip 10.10.10.10
# set usrgrp HRI → Domain مجموعه الموارد
# end
```

6- فتح VPN على باد باد Client

open Network and Sharing Centers + Setup New Connection →

→ Setup New Network → Next →

Connect new work places

I'll Setup internet Connection later →

Internet address 41.1.1.1

Destination Name FG

Next → Create

Setup adapter setting ١١ فتح ترتيب اداة

Network Adapter

Username mali

Password 123456

Connect

Verify verify



لوحة زر لتوسيع IP Range ملحوظة ٤

# Show VPN PPTP

ملحوظة ٤، لفتح VPN لـ user اللي هعمل فيه ركيون واحد

mali → properties → Dialin → Allow access

OK

ملحوظة ٥، Connect to the server

لفتح IP user لـ دلوقت يعرف بـ ping على الموسين وليهو

ويعمل اي حاجة Sharefolder

Normal

ملحوظة ٦

افضل حالات VPN Connect بـ Client

VPN Concept

داخل

نظام Net من خلال الشركة

Policy & Objects → Policy → IPv4 → Incoming interface Port3VPN

Source address VPN

Outgoing interface Port2

Destination address all

Schedule always

Service all

Action accept

OK

بس عرض اهم متصفح

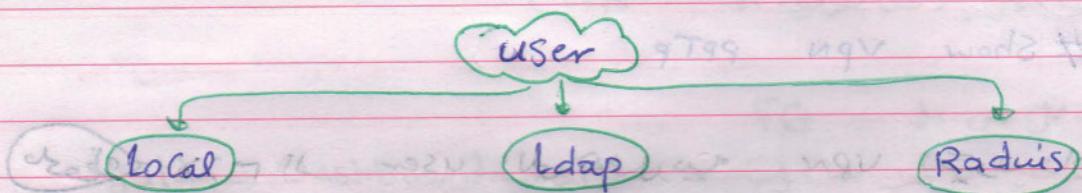
Default gateway

VPN 0.0.0.0

Manual



وـ ٤، ٣، ٢، ١

"33" Single Sign On poll Active directory


لما كنا يستخدم LDAP و Radius  
 ما يجي دخول على موقع دخل user اهنا السهاره  
 automatic authenticate قبل SSD  
 user

Network Type
Domain

Centralized administration

TGT → "single signon"

work Group

Per-to-Per

Single Sign on FG
Poll AD
Forti Net Agent

من صنوع (Agent)

LDAP لـ

DC لـFortinet no Agent n6  
 user فنيسترو قـFortiGateـ مع authentication

Poll AD
التحقق العملي

FG مع LDAP لـ SSD

user Device → Authentication → LDAP Servers → Create New Domain

2- User & Device → Authentication → Single sign on → Create New

Type  Poll AD

IP

User  → Domain admin

Pass

LDAP  Domain

Enable polling

OK

LDAP tree Groups

Group المجموعات  
Group ترتيبها على

اصير دعوة لـ 6000 Status

SSO Group فعل - 3

User & Device → User → User Groups → Create New →

Name

Type  FSSO

Members

الملحقات المجموعات جعل

OK

Policy Rule - 4

Policy & Objects → Policy → IPv4 →

Incoming  Port (Int)

Source Address

Source users  Active directory

outgoing  Port (Ext)

Destination Address

Schedule

Service

Action  Accept

OK

فتح Internet Client بـ شرط الـ Client تكون

SSO Group تكون الـ Group ينضم إلى جماعة

Pass & user

هذا يتحقق إنترنت هو غير ماركeting



AD (This Group), Computer user لـ 102 في المخطىء

Domain على 101

Group أسمى 102 Source users شـ 102 Policy لـ 102

SSO LDAP

Any user will auto login

Any user will auto login

auto login

auto login

auto login

auto login

P-AD will sign on

Any user will auto login

Any user will auto login



103

Sub:

Date:

### "34" Single Sign on FortiAgent

DC على نفس IP ونسبة على DC موقع على Forti Agent نزل - 1  
 سطيف administrator على نفس IP Pass > User كليب  
 كل مستخدم على DC كمس كمس users على Domain على المتصفح  
 لـ monitor

#### WorkMode

① DC Agent Mode → Next → Yes

Domain & Restart

FG درج زراعة على FG - 2

User & Devices → Authentication → Single Signon →

② Fortinet Single Sign on Agent →

Name [AD agent]

DC Agent على المتصفح

Primary [172.16.1.200]

password [\*\*\*\*\*]

LDAP [ ]

User/Group [SCTE/IT]

Group [IT]

Configure

FortiAgent على المتصفح Domain بعد حفظ - 3

Password [\*\*\*\*\*]

الى دكتها

[APPLY]

FG على المتصفح

Group [IT] Policy [IT] - 4

User & Device → User → UserGroups → Name [IT]

Type [Firewall or FSSO]

Members [ ]

Remote groups

+ Create new

كتابات امداد

[OK]



5 - مرجع على DC من ندخل DC من اد user IT Group

6 - لم يتم إضافة IT -> Group to user → جهيز

نوع سارطب و user و password

7 - حذف جميع الأدوار التي تم إنشاؤها

removal /

show group

group show traps 300

group -> traps of group

8 - configuration 27

-> named signs and shared variables 27

traps or signs traps 27

find sign trap all 30

traps QA function

traps grouping

named signs grouping

group grouping

group grouping

9 - last name of group is last trap 27 → changed

traps 27

27 27

YMA

10 - last name of group

group grouping grouping grouping grouping grouping

group grouping 27

group grouping

group grouping

group grouping

group grouping

group



105

Sub:

Date:

### "35" FortiGate Devices Detection

نفهم الـ Devices || FG التي ظهرت وبناء عليه اذتم منهم

وامسحونهم في هتلاتي كـ Groups هنا

User & Device → Device → Device Groups → Groups اذتم كـ

OS عن طريق Device هذا انه يعرف الـ

Interface الـ هذا اذتم معرف ما

System → Network → Interfaces → Device management

Detect and identify device

التطبيق العملي

1- User & Device → Device → Device Definition →

Alias Sales

Mac 00:0C:29:8C:10:1D Client IP Domain من Mac الـ 172.16.1.200 getmac /s

DeviceType Windows PC

Custom Group

OK

Policy Rule - 2

Policy & Objects → policy → IPv4 → Incoming

SourceAddress Port1

Source Device Sales

Outgoing Port2

Destination all

Schedule always

Service all

Action Deny

OK

106

3- لورسيت من الـ Device Definition

User & Device → Device → Device Definitions →

Assignments →

Device → Device Definition →

Redefinition ID: Direct ID: 20

Device → X → Redefinition ID: Direct

From configuration device → configuration → interface → interface

Redefinition

→ configuration → Device → Device Definition /

20102 / 2011A

20102 → 20102 configuration → 20102

20102 [configuration]

20102 [quarantine]

[OK]

S-146 [OK]

config → config → 20102 → 20102 & 20102

20102 [configuration]

20102 [OK]

20102 [quarantine]

20102 [OK]

20102 [OK]

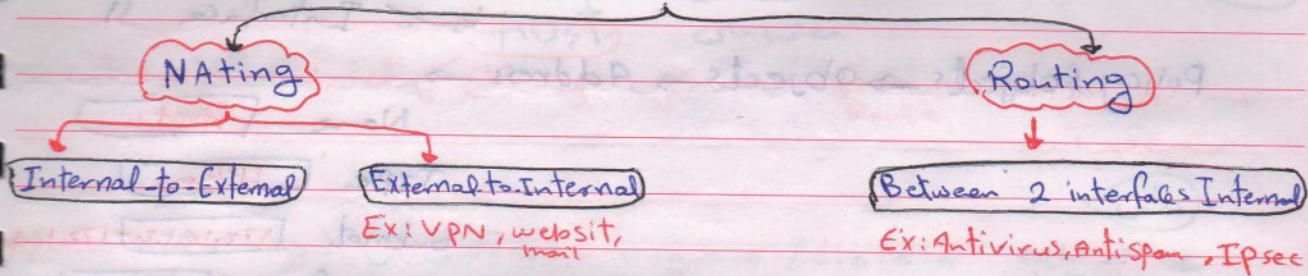
20102 [OK]

20102 [OK]

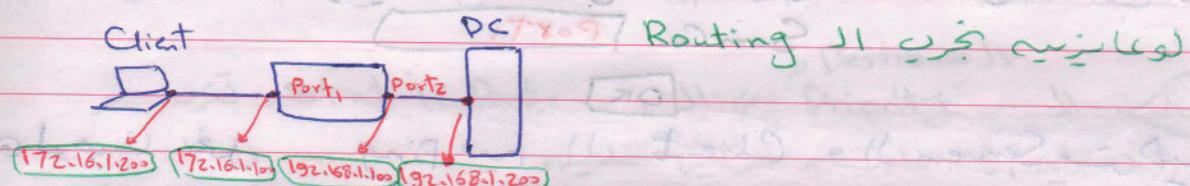
[OK]



107  
"36" Intro FortiGate Policy



نفسي العناصر ④ يستخدمها من كل طبقة سواء NAT او Routing أو Route Objects



لو عارضه بخوبه

Client → Domain (or Routing) → Policy → Action

Policy objects → policy → IPv4 → Incoming → Port1, Port2  
Source all

Outgoing → Port2, Port1  
Destin all

Action Accept

(off) NAT

OK

Policy من اخراج

Reply والعكس DC → Client من Ping

Interface ② InLine Policy → Routing او اتصالات او سيرفرات

StaticRoute من Device ③ من Device

site-to-site VPN و هي هستوريا للبدل

FG مع FG او Router مع FortiGate صغاراً لو



لادخن ممكن نحدد الا Routing من على Range IP من Routing كـ Interface

Policy objects → Objects → Address →

Name Port1

Type IPRang

Subnet 172.16.1.20 - 172.16.1.3

Interface any

② لاتقدر المهمة التي تحدى المنهجية او على طلب

غير معرفة موافق المنهجية وتحدد المنهجية

Source PORT1

OK

لوجهت بعمل Client 11 one Ping من Server 172.16.1.100 Client 11 IP يفتح معه خارج

Policy to Range المنهجية

20 - 30 Range من IP ادخلReply لمواصلة العمل

Natting المنهجية

NAT

لابد من داخل Net لازم تكون طالع NAT

Internal | External ادخل من External | Internal يدخل من

Natting مع دفعه Static Route ولازم ادخل

Router → static → static Route → Destination IP

Device Port 4

الموجه

Gateway 41.1.1.1

Router

Distance 10

IP Router

Priority 10

OK

log

Sub:

Date:

٨٥

### Static Route

ADSI

عندما

أجد كل IP بناءً على Subnet

Static

Route

تحت

تحت

Networks ٠.٠.٠.٠ / ٠.٠.٠.٠

Networks

تحت

NAT rule Policy

عمل staticRoute

عمل

لفرقة لو Static Route

و Destination

Priority

تحت

الاتصال خارج من Internet

link → Port ٤٤٣

te-data → Ports ٦٢.١.١.٢/٢٩

Ports N StaticRoute

Router → static → Static Route → Destination IP ٠.٠.٠.٠ / ٠.٠.٠.٠

Device Ports (te-data)

Gateway ٦٢.١.١.١

Distance ١٠

Priority ٠

OK

active-passive أو active-active

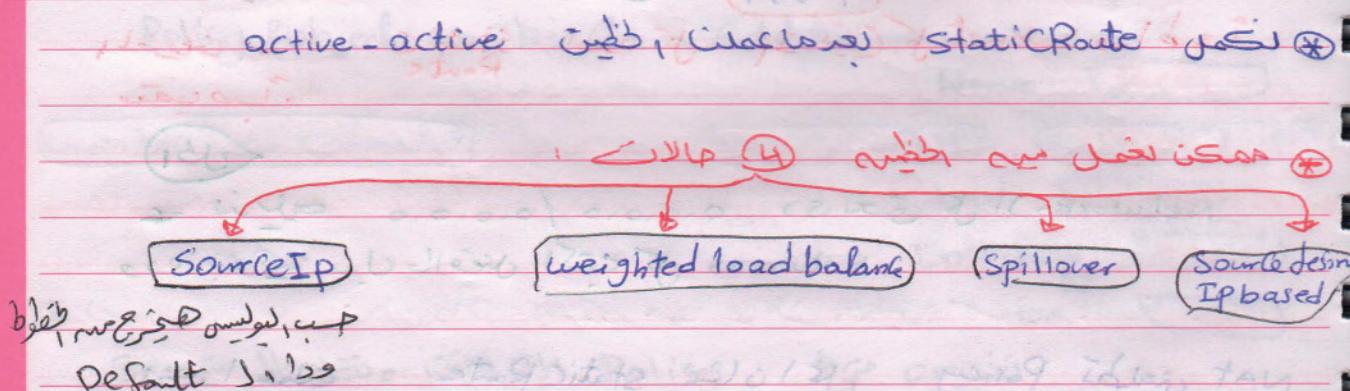
active-active من هيسنفون Priority و Distance

FortiGate

Link = Active - Active  
Distance Priority = Active - passive



.. 37. Static Route Setting



Router → Static → Setting → Source IP based →

Policy

Policy objects → Policy → IPv4 → Incoming Ports

Source Port IP

172.16.1.20-30 Range

Outgoing port link

Destination all

Schedule always

Service All

Action Accept

on NAT

OK

port 172.16.1.20-30 Range misal دكترا

link

172.16.1.1-10

the HR NGL Range

To data

To ports or خلاص policy





دبياستي (ا) It هبط مع HR (ا) وData (ا) هبط مع IT (ا)

لوعان (ا) يطلع من مروه (ا) بطبع (ا) It (ا) (خط)

inCom Port (a)

Source Address (a)

Outgoing Port (link) (a)

Ports (tedata)

Destinat (a)

Action Accept (a)

ON NAT (a)

the nat will be nato (OK) (a)

Sourcebased IP setting (a)

لوكات (ا) هم يطلعون (ا) وData (ا) هم يطلعون (ا) وData (a) وlinks (a) مروه (a) (خط)  
لوكات (ا) هم يطلعون (a) وlinks (a) مروه (a) وData (a) (خط)  
ونفع الـ FG (a) (خط)

Router → Static → Setting → link health

+ Create New →

Name Google

Interface Port 1 (a)

Gateway (a)

Health check

Name (a)

Interface (a)

Gateway 192.168.1.1 (a)

Probotype Ping (a)

Server 8.8.8.8 (a)

Recovery threshold 5 (a)

Ping (a)  
طريق (a)  
تحتاج (a)

ادخل اس انه رفع اجل update Routing table (a)  
واسلك (a)

Bring Down (a)  
الاسن وفوا (a)



تعريفه الموصول Ports

Setting → link health

⊕ Create New

② weighted

setting →

⊕ weighted load balance

Priority Static Route مع العلم انه لـ static route

Port ① weight 1000

Port 4 weight

Port 5 0

نسبة 10% هي weight للخط الرابع و 90% للخط الخامس

الى هنا link 4 و 5

الفرصية weight وال Source

ال weight صرف على داومره على 100% source

يعرف على واحد من الـ 5 lines

③ Spillover

KB traffic و يتبع بال bandwidth على الـ 5 lines

Port 4	Spillover	أول 3 lines بـ 1Gb
Ports	(1024 * 1024 * 1024) + 2	كذلك على خط السادس

لود balancing على الـ 5 lines

④ Source-Destination IP based

هنا تعيينه الدوالي مثل بديهي صرف هنا وهو خطأ

كل مجموعة سينجزها على طريق مقطوع واحد

modem



# "38" STATIC ROUTING SETTING



"38" Static Routing Setting  
التطبيق العملي

Network Connections & Configure (خط 1)

System → Network → Interface → Alias [Vodafone]

IP [10.10.10.1 / 24]

HTTPS  ping  HTTP

Register automatic  نتيل دى تي - تاس سعى Fct-Access

[OK]

[Portz] ونفرى

Alias [Tedata]

IP [192.168.1.254]

[OK]

172.16.1.100 IP (internal) Ports  خط 2

Routing (خط 2)

Router → Static → Static Route → Destination [10.0.0.0 / 0.0.0.0]

Device [Portz (tedata)]

Gateway [192.168.1.1] Router

Distance

Priority

[OK]

دستور نفس خطوة وتعل StaticRoute بين تغير مينا vodafone

[10.10.10.100]

Gateway

[OK]

adapters  VMnet8 VMnet1 VMnet5 VMnet10 VMnet12 VMnet13

VMware workstation → Edit → Virtual Network Editor → [Change setting]

VMnet0 Bridged → Bridge to [broadcomEthernet]  Intel PRO/1000 MT Desktop   
[apply]

VMnet8  Intel PRO/1000 MT Desktop

VMnet8 Bridged → Bridge to [intelultimate]  Intel PRO/1000 MT Desktop   
[apply]



٤١ / ١١٤

نقطة كروت ال FG بناءً على te data و VM8 بناءً على wireless اصلية على

لازم نتأكد منه طابع من الايتن لفضل كل واحد منه وتجرب بخل Ping

لاحظ في ال Priority وال Distance الاولي تكون الاقل

من ال الاول بحسب ابتعاد Priority و Distance اول الاول الاول والا الاول من واحد بسي

Link Health FG رخص لاملاط يقع بخل

Setting → Create New → Name Google → Vodafone  
 Interface Port 3 → Up date  
 Gateway 192.168.1.1 → Bring

رخص وهمه تابعه لـ IP و IP

Gateway 192.168.1.1

Interface Port 2

لاحظ ال FG من سيسونز انه يتعرض من اي كابل فنيهم غيرها تخلع  
 الكابل لذلك احتاج اطرافه وهي مسنان لا دلت ليفصل

ينفذون Policy بناءً على خطة

Policy → address → Range

Policy & Objects → Objects → Address

Name IT

Type IPRange

Subnet 172.16.1.1 - 172.16.1.10

Interface Port 1

Visibility

OK



Policy نحن - 5

IPv4 → + Create New → Incoming

Source

Port 1

IT

Outgoing

Port 2

Tedafon

Port 3

Vodafone

Destin

All

Action

Accept

ON Nat

OK

172.16.1.1

IP ونعمل FG Client

Reply من IP 8.8.8.8 من client Ping

internal

DNS لكي لا يخطىء انه من هيفيف يفتح موقع himanjoindomain.com ونادى ما من هيفيف

من هيفيف غير المألوف

Incoming Port 1

Source Address Domain

172.16.1.200/132

Outgoing Port 2

Port 3

Service DNS

عن طريق فتحها

Action Accept

OK

7- نطبق حملة DC

IP 172.16.1.200

Gateway 172.16.1.100

OK

\* لكي الواحات افتح موقع himanjoindomain.com Client يطبع عادي

\* weight لونيرنا من static route setting

\* ونستخراج موقع Client no ShowIP ونكتبه كذا فيه فتح من ورها

\* IP يفتح منه tedata وسروره tedata معن كذا انه يطبع عنده

\* من هنها ومره من هنها ولكن لونيرنا weight يفتح وعده فترهم

يطبع منها الوهي على

ما يعنى

لو كان هناك بروتوكول HR و IT وكل واحد لديه Policy يطبع من خط معين like tedata , vodafone كل قسم يطبع من خط ولكن لو عنبرت في المكان الذي لا يطبع منه Client مثله مثل Client من هم يطبعون فيه اصل الفوري هي من هم يطبعون فيه .

لوعاينيه نجرب النوع الثالث الـ Spillover

نغير Port 5000 لخليها 5001 ولنجرب نطبع الى Client

اول ما يحصل هو هنلاقيه طبع من الثاني .

لادى لوعايل Policy إنما It يخرج من طبقته من حالة الاسئله لهم لقتى او Priority وال Distance او user هنخرج منه هنا ومرة من هنا لكن لو عنبرت في المكان و اهم منه هنخرج من المكان او من المكان او من المكان الاول الاولاني فعل .

العنبرات تجيء من المكان الاول

(X) (X) (X) (X) (X) (X) (X)

(X) (X) (X) (X) (X) (X) (X)

and so on

117

Sub:

Date:

### Nov "39" HA For Internet Connection

Link Health Routing (الناتج) Setting (الإعدادات) ديناميكية من حيث الاتصال (Dynamic)

system → Config → HA → Mode (active-active) HA (تعتمد على طرق)

Priority

Ports 0

Ports 0

Priority لوحظت active-passive لازم اغير من ال Passive (المنفذ) يعود تحدده من FG وActive (المنفذ) تمايمهم عسان ال

Active-Active لو دخلنا من هنا Client (الموقع) show my IP (لديه خاصية Client) بحسب خاصية من ال Active Policy (الناتج) تكون مخرجية او الاتصال

هتلاماً مره يخرج من Vodafone و مره من tedata

nat source nat 27

on NAT

nat source → routing → wan1 → wan1 → wan1 → wan1

→ wan1 → wan1 → wan1 → wan1

→ wan1 → wan1 → wan1 → wan1

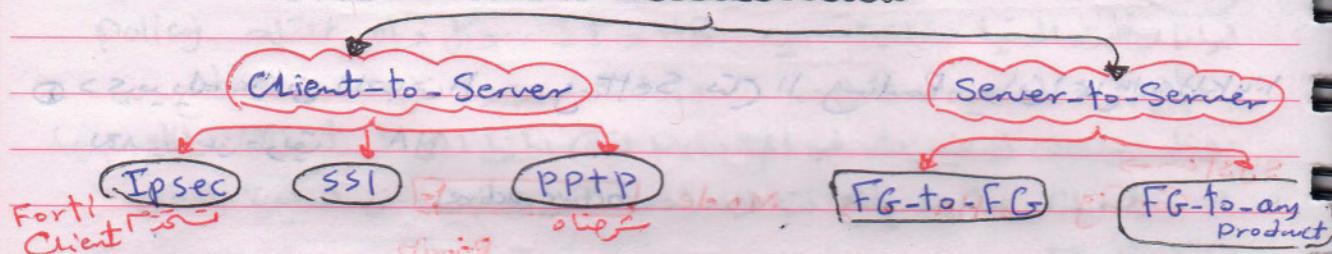
Pass related-out

nat source wan1 → wan1



118

رايتري فورتيجي على FortiGate VPN



VPN IPsec

التطبيق العملي

من تطبيقه متى ومتى (اعتنها)

System → Features → Policy based IPsec VPN

الإعدادات المطلوبة لفتح الباب

VPN → IPsec → tunnels →

IP Address

PPTP

التطبيق العملي

لبنحدر

Group and users  
active directory or sam

FG de local user

user & Devices → user → user Definition → + create New

+ Local → Next → user Name [Ahmed] CAS Sensitive → Next →

Pass [.....]

Email [ ] → Next →  Enable → Create  
 two-factor

المجموعة Group

user & Devices → User Groups → Create New →

Name [VPN-PPTP]

Firewall

Members [Ahmed]

OK

119

Sub:

Date:

VPN N Interface Alias -3

System → Network → Interface → Alias **VPN**

IP **41.1.1.1/29**

**OK**

Route Access (n9v) VPN N Range IP -4

Policy & Objects → Objects → Address → Name **PPTP ADDN**

IP Range **20.20.20.1 - 20.20.20.15**

Type **subnet**

Interface **Port4**

Visibility **ON**

**OK**

Policy N -5

Policy & Objects → Policy → IPv4 → Incoming **Port4**

SourceAddress **PPTP ADDN**

Outgoing **Port1**

Destination **all**

Action **Accept**

**ON NAT**

**OK**

PPTP N Configure dedic Cmed N -6

— login: Admin

— Pass: ...

# Config vpn pptp

# Set status enable

# Set Sip 20.20.20.1

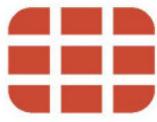
# Set eip 20.20.20.10

# Set usgrp VPN-PPTP

# Show alias

# End





120

Range IP of FG u to switch to connect to client -7

mgv 2019

192.168.1.100 597

Connection in Client List no -8

Setup anew Connection → Connect to workplace → Next

→ use my Internet Connection (vpn) →

→ I'll Setup later → Internet Address 41.1.1.1-3.109

wireless connection 597 Name **VPN to FG** Next →

trunk 297 Create

192.168.1.100 597

Change adapter setting → C:\Windows

VPN to FG

user ahmed → FG الاتصال

Pass ...

Connect

Connection جاري -8

IPSec

Setup Client with FortiClient -1

**Complete** or **VPN** → **Complete** → Next → Install

2. install the certificate to the client -999

FG real device -2

VPN → IPSec → tunnels → Create New → Custom VPN

Name **Forticlient**

Next →

41.1.1.1-3.109

IP Address 41.1.1.1-3.109 → FG جيت

Interface Port 4

Pre-Shared Key 11111111



Local Address

172.16.1.0/24

Range |||  
الى 192.168.1.100  
الى 192.168.1.254

Remote Address

20.20.20.0/24

الى 20.20.20.254

OK

VPN

ازدياد اسماط لفتح Client ||| فتح Client + Lic - 3

Remote Access → Configure VPN →

IPsec VPN

Connection Name FG

Remote Category 41.1.1.1

Preshared Key -----

APPM

-----

Pass 112 user 112 - 4

Ahmed

-----

Connect

Open New Rule FG Use Policy 112 - 5

Inbound FortiClient

Source all

Source users

VPN-PPTP

Outbound Port (internal)

Destination all

on NAT

OK

-----

-----

V (MP)S

+ لفتح بروتوكول 98 على 192.168.1.100

-----



12A  
"41" Format FG OS and upload Firmware + "42"

From TFTP Server & USB

لدي بتحصل على اكود عايز اعمل اعاده صيغة المصينع ولو عملته من خارج امثل

لابطبيه غير من طبيعه الـ Putty او الـ Console او Hyperterminal  
صيغه على XP

Hyperterminal FG وفتح الـ FG بـ XP لوصن حمل

Hyperterminal → OK → [Restore Defaults] → Bit per second 9600

Data bit 8

Parity None

Stop bits 1

Flow Control None

[OK]

لدي قلت على صفحة يistica كـ ادفوا دخل على اطمها:

Status → Restart ← نعمل بقى FG وبنهم على طبع اول ما تورك رايتفون دخلي على اطمها

Login: admin

Pass:

#

دخل على الـ terminal

دخل على اطمها:

Command ادفوا ديكى الـ Reset  
system → Dashboard → Status →

لو عايز اعمل محوفره هاده

# exe Factoryreset

?(y/n) Y

لورسيت من الـ terminal خلاصه يطلع \*

رسنه خطا الـ تبنت ويعين نهل على

لوقتنا طها: حمل كل حاجه، جب للاعدادات. (طبع)

لاظن<sup>ك</sup> الى يعلم Device هي الـ Configuration او Reset وليس OS  
او OS من بيعليه Reset ولكن يعمليه Format او من يفتح اجل Reconfigure ولا يفتح لوقت لاعطوه:

ReConfigured Fortigate

TFTP Server

or

USB

ومن كلامي او دليل

Reset<sup>ف</sup> سهل على ال Hyper terminal فتح اجهزة وتنقله تان بعد ما عدت و هو اجهزة يفتح على ال terminal نضغط على اي حرف هنلاق اختيارات

[G]: get Firmware From TFTP Server

[F]: Format boot device

[B]: Boot with backup Firmware

[I]: Configuration and information

[Q]: Quit menu and Continue to boot

[H]: Display this List options

Y نعم، F لذا OS او Format

OS يجي او اجهزة ديجي دا من صيغة Formating

لوقتنا طها دخليه هيحمل موي مع ال terminal

Open Boot device failed

عندما تنزل Firmware يجب به Tftp Server او USB

Xcd

TFTP Server

التطبيق العملي

1- على نسخة XP تطلب البرنامج TFTP Server ونفتح لادخال البرنامج من حيث لازم يكون داخل دفنه IP اجهزة -

2- ننزل ال Firmware وطبعاً لازم fortinet تكون الى Firmware من على .out

3- من البرنامج Configure ← File ← TFTP نقوم بوضع Path على حمله ، ياضي البرنامج من Firmware الذي نزله في المولدر

4- نعمل start ل البرنامج الـ TftpsServer

5- نرفع البرنامج FG لنقل الـ FG ونسفله وهو

Hyperterminal [G] يفتح لمنفذ [G] على IP 192.168.1.100

Enter tftp Server address: 192.168.1.100

Enter local address: ستاع الـ FG ودليها قافية

Enter Firmware image file name [.out]: FG.out image

Device to connect على Ftp

MAC: 00090FD3C44

Same as Default Firmware/Backup Firmware/Ram Image without same?

0/ default

Firmware will reboot after download

او ماكان له المهم رفع الـ Status لبيان اذا تم تثبيت Firmware

الـ IP 192.168.1.99 browser على default

وبيان خلاصه - user 1، pass 1،

Configuration Restore

6- اول ما افتح الجهاز ، اختر هنا دخل اجل Backup بسقا

• System → Dashboard → Status → System Configuration [Restore]

USB

ينداني الطريقة الثانية باختصار

Hyperterminal FG من USB N Format زر 1

# exe usb-disk Format (Y)  
رجاءً Format

out Firmware 11cabis - 2

ونادر كمان Configuration backup وخطه برمجه FG ساقع اذ ونادر كمان Configuration backup ونادر كمان Configuration backup ونادر كمان Configuration backup على لعنود قاع امتداده Conf

3- تركب FG في usb ونافر Restart

4- ندخل على FG Hyper-terminal

```
# Config system auto-install
# Set autoinstall default-Config-File Site.conf
# Set auto-install-Config enable
# Set default-image-file FG.out
# Set auto-install-image enable
#end
# exe reboot
```

• ايجي المهم ; هفتح FG قبل ما خل Configuration Format OS

Forti Explorer او TFTP Server من المهم خل FG Formate OS (ادى)

لكن عذر اسطو معندي تفاصيل تكون اهم فـ "firmware"

"43" Reset FortiGate password

أهنا هنكلم في حاله إنك نسيت Password ودي ملهاش حل غير  
FortiGate Reset لـ 14 ثانية فقط منع تفعيل لـ 14 ثانية

التطبيق العملي

1- نوصل الـ FG بجهاز الكمبيوتر عن طريق الـ RJ45

2- ندخل على الـ login في Hyperterminal والـ Pass

3- نكتب من الـ login

Login : maintainer

Password: bcpbFGT80C3909644140

لأنّي نسيت الكلمة السرّ

SN 11  
FG 11  
بتاح 11

Login : maintainer

Password: \*\*\*\*\*

COPY  
تمّ 14 ثانية

Welcome! pass !!Reset

# Config system admin

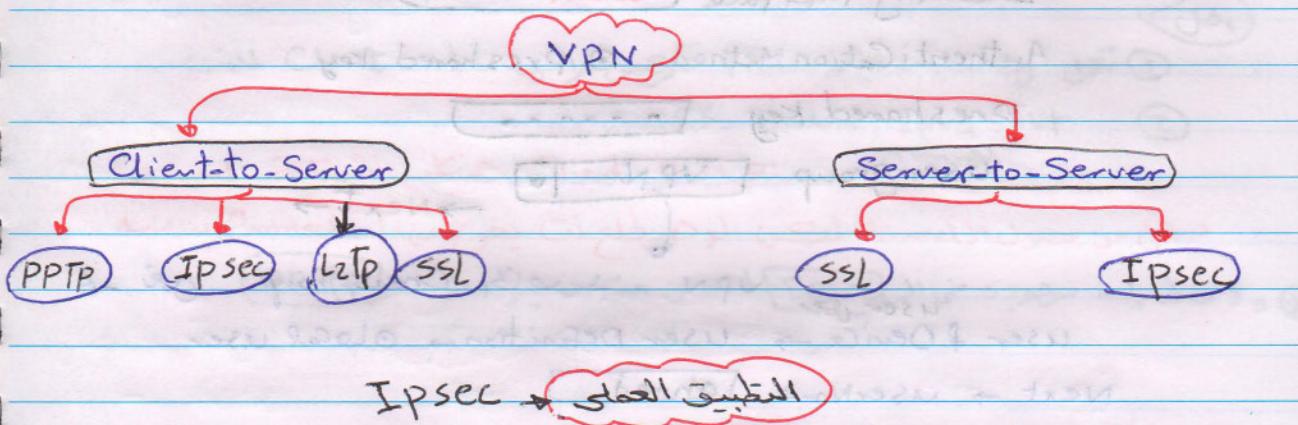
(admin) # edit admin

(admin) # set Password 456

اطير

# end

دبرنا Password أتغيرت نوع فعل Login فيها بحرب

"44" VPN Client-to-Server IPsec FortiClient

وأن يصل معاشر الـ Range ونطليه منه FG في Client له Configuration IPsec 1  
 FG على IP 192.168.1.99 ونطليه منه FG على IP 192.168.1.1 ونطليه منه FG على IP 192.168.1.99

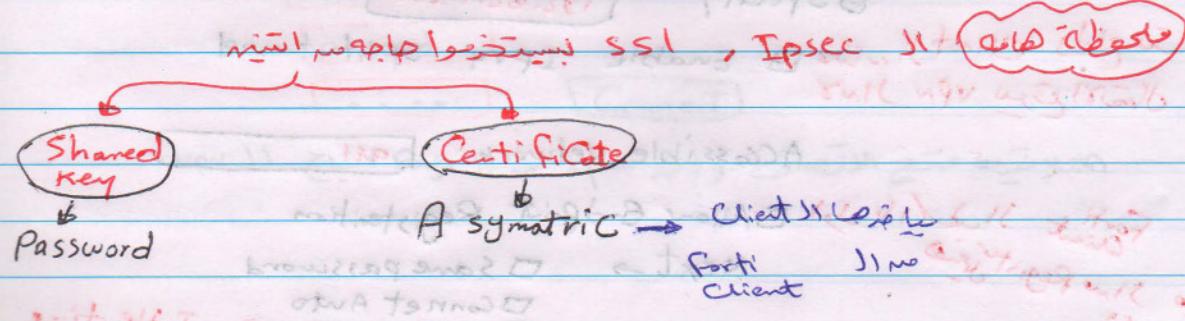
- FG على interfaces في Configuration IPsec 2  
 Network → interfaces → + internal 192.168.1.99  
 wan → 192.168.1.1 255.255.255.248

- نعمل على إعدادات bridget الشبكة internal 3  
 192.168.1.50 ← IP من FG يفتح على IP

- FG على IPVPN 4  
 VPN → IPsec → Tunnels → + CreateNew → Name site-VPN

⇒ Dialup-FortiClient

⇒ Next



128

- 5

Incoming interface  ١٥

Authentication Method  preshared key

preshared key

User group

VPN

→ Next →

user user  ٢٠٢٩١  
user & Device → User Definition →  Local user

Next → UserName

Pass

Next →  Enable →

Group

User Groups → Name

Type  Firewall

members

OK

VPN ١١٦٦ - ٧

Local interface

Local address

Client address Range

Subnet

DNS Server

Specify

عنوان المعنون

عنوان Client IP  Enable IPv4 split tunnel  
عنوان VPN  عنوان الاتصال

Accessible Network

Forti Client  اورڈر / ١٦٠  
License  No Register until

Allow Endpoint Registration

Next →

Save password

Connect Auto

Always up → Idle time

Create



لخط ١- اول ما احصل على Client بتهم التي يحصل على IP من

Client على FG يخرج من خارج FG على Policy ①

Enable Ipv4 split tunnel ②

دي معنده لواز Client يخرج internal

دخل من خارج او tunnel لكن لو هيطلع منه يخرج من Connection

PPTP لكن هي موجودة في IPsec ولا خط ٢ موجود في IPsec \*

لخط ٣- اول ما افتح VPN Range وال Create object FG

Configure VPN يفتح اول VPN الذي عدته ونambahle

Wan وخط ٤- هنا انتي بعد Configuration افتحه وتحدد him internal

8- دخلت تطبيق استغل ال FortiClient

Remote Access → Configure VPN →

[IPsec VPN]

Connection Name [site]

Remote Gateway [41.1.1.1]

Authentication mode

[Pre-shared key] ...

[Apply]

9- فتح صورة ال Client

[Site]

[ahmed]

[...]

[Connect]

هذا ماتفتحه فتح الاتصال وامان IP من IP Range

130

internal IP من الجهاز او على الماء او Ping

Reply

حول

لواجهة شفافة لـ VPN Connection

VPN → Monitor → IPsec monitor → Client

لواجهة شفافة لـ Client

لواجهة شفافة لـ L2TP

VPN Client

لواجهة شفافة

android L2TP

وتحقيقه خطوات البقاء

Client لـ VPN Connection setup

Security → Properties وتحقيقه

type of VPN L2TP

[OK]

[Advanced]

Shared Key

[OK]

Connect

userName ahmed

Pass \*\*\*\*

Connect

e-mail

atia

bentot

(final)

---

OK



131

Sub:

Date:

### "45" FortiClient Profile

FC  Register

التطبيق العملي

الاول ازاي تحد على FC  Interface ونخلي على IP

Network → Interface → IP 41.1.1.1/255.255.255.248

FCT-Access

Device Management

Broadcast Discovery Messages

OK

Cancel

- ندخل الاتصال VPN طريقه المراجعتات لكن على FC

Allow Endpoint Registration

FG  Registration ونفسه في FG  FortiClient

Accept

باتجاه

4- نرجع على FG ولفتح FG

user & Device → Monitor → FortiClient → Client  هيكل IP داد بقاعة IP

FC

Profiles

User & Device → FortiClient Profiles →

Profile name VPN

Device Group Windows

User Group VPN

Users ahmed

قبل حائل

الطلوبات دى المفروض

عن دى Group

antivirus

web Category

client web Filter

OK



- Device → Device Group → Name **FortiClient**  
 Member **win PC** [OK]

- FC Client Register يدخل Client كالتالي - 7  
 → Device Definition → Create New Edit - 8  
 Alias **Client**  
 Mac **00:0C:02:91-**  
 additional **Sales-mon**  
 Device type **win PC**  
 Group **FortiClient** [OK]

نحوه من مواقع عنان ثجبي Security profile - 9

Security Profiles → Web Filter → + → Name **IT**  
 FortiGuard Categories  
 Block وتحل لسوبيات اسعار

نحوه من المواقع FortiClient Profile - 10

تحل لظواه رقم ⑤ ولكن بعد

الى عدتها الى web Category Filter **IT** →

نحوه من المواقع

نحوه من المواقع FG وتحل register وتحل User Monitor من المواقع  
 user & Device → Monitor → FortiClient → FC Profile المعرفة في المربع الملايو  
 IT

نحوه من المواقع وتحل web filter

١٥ دلو Shutdown user معرفتني بـ userFc أو limiteduser

unregister

نحوه ها

user register userFc user limiteduser

Liberal

Setting Rule

user register userFc user limiteduser

Liberal

user register userFc user limiteduser



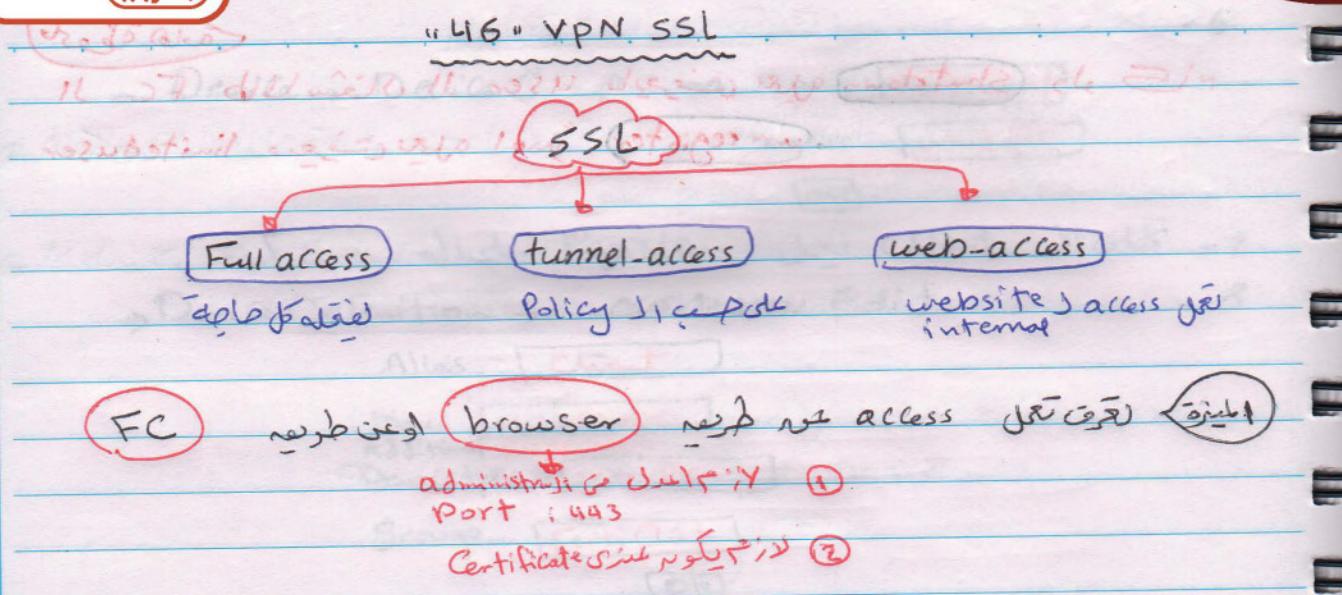
"46" VPN SSL

11-57 دليل المبتدئين في التعلم والتكنولوجيا

عنوان المنهج: 11-57 دليل المبتدئين في التعلم والتكنولوجيا

عنوان المنهج: 11-57 دليل المبتدئين في التعلم والتكنولوجيا

عنوان المنهج: 11-57 دليل المبتدئين في التعلم والتكنولوجيا



FC

ابعد طريقة browser

ادخل طريقة  
Port : 443

Certificate will be issued

طريق

غير معرف

access

التطبيق العملي

1- تفعيل خاصية SSL

System → Config → Features → [Show more]

(ON) Certificates

(ON) SSL-VPN Personal Bookmarks

(ON) SSL- Realm

[Appm]

mahmoud نسمة user > Create نعم -2  
Mahmoud دخل في VPN-SSL المجموعة Group >

ssl نعم Configuration نعم -3

VPN → SSL → Portals → Full access → Edit →

Enable tunnel Mode

Enable split tunnel

Source IP Pool  Default Range

Enable web mode

Portal message

welcome

الرسالة  
تعود

theme

Blue



Date:

Page layout

Include login History Monitor logs

Predefined Bookmarks

⊕ Create New **RDP**

Category **Remote**

Name **RDP**

Type **192.168.1.200**

Host **192.168.1.200**

UserName **mathimond**

Pass **.....**

Limit user  
used  
ببساطة لوضع حد على المستخدم

**OK**

Setting ٤ - ترتيب التطبيق

Vpn → SSL → Setting →

listen interface **wan1**

listen on port **443**

Port ٤٤٣

Administrative Conflict

Address Range ⊕ Specify Custom IP

IP Range **SSLVPN**

DNS Server ⊕ Specify

DNS **192.168.1.200** → Domain ١٩٢.١٦٨.١.٢٠٠

Allow end point Register

Authentication ⊕ Create New

User/group **VPN-SSL**

**Apply**

Policy ٤ SSL ١٧٣ Error

Policy ٥ - 5

Policy objects → policy → IPv4 → Create New → InComin **ssl.root**

SourceAddress **SSLVPN**

SourceUser **VPN**

Outgoing **internal**

Destination **all**

Action **accept**

**OK**



136

FG

IP

لوكيت

من المتصفح او

فتح الصفحة حق IP

add new Connection

ويمكن نفتح جميع صفات

Name Site-ssl

Remote Gateway 192.168.1.1

apply

User Name mahmoud

Pass \*\*\*\*

Connect

هذا الاتصال

Ports

0 → 65535

0 → 1023

نحوه 1023 → 65535

ويمكن نفتح Real IP داخل المتصفح لاكتساب سيرفر بين بنيه

Port الى جي

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

192.168.1.100

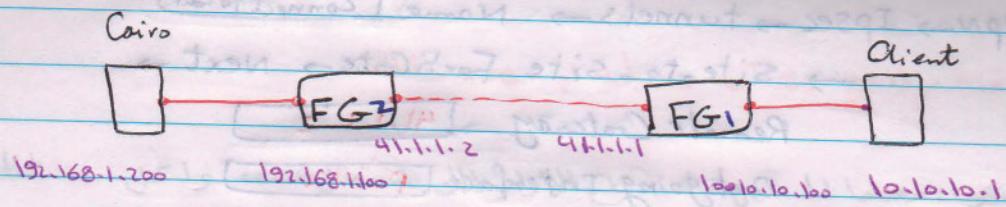
192.168.1.100

192.168.1.100

192.168.1.100



### “4.7” VPN Site-to-Site (Fortigate-to-Fortigate)



#### التطبيق العملي

1- بعد حفظ تطبيق الـ IPs على FG1 كما في الصورة تخلص الـ Ping من FG2  
 والعكس صحيح لأنهم سايتيني بعضهم البعض

2- نفتح على FG1 المتصفح ونفع الـ Features من VPN

System → Config → Features → Presets **FULL UTM**

Policy-based IPsec VPN

**ON**

SSL-VPN Personal

**ON**

**Apply**

3- ندخل نفس خطوة على FG2

4- نفتح على FG2 ونسارع لإعدادات الـ VPN  
 VPN → IPsec → tunnels → **Create New** → Site-to-Site fortiGate → Next

Remote Gateway **41.1.1.1**

Outgoing Interface **Port2**

Authentication  Preshared key

Preshared key **.....**

Next → Local Interface **Port1**

Local Subnet **192.168.1.0/24**

Remote Subnet **10.10.10.0/24**

**Create**

automatic or Policy **Policy** mode come up **ما يطلب**  
 Address **Objects** **عنوان** **عنوان**

برفع ٥ - خل نظر FG1 . FG1 .

VPN → IPsec → tunnels → Name [Connect to Gair]

→ Site-to-Site Fortigate → Next →

Remote Gateway [41.1.1.2]

Outgoing Interface [Port]

Authentication ○ preshared key

Preshared Key [\*\*\*\*]

Next →

Local Interface [Port]

Local Subnet [10.0.0.0/24]

Remote Subnet [192.168.1.0/24]

[Create]

staticRoute ومل<sup>ف</sup> Policy It's address N Range [192.168.1.0/24] automatic

Monitor حمل برفع -

N - VPN → Monitor → IPsec monitor → State

↑ UP

1.1.1.1 used interface idle ping

FG (2) حمل برفع من الـ up تك<sup>ف</sup> State حمل برفع

[\*\*\*\*] good bonding

[17.0.9] interface local active

[17.1.1.10.1] tunnel local

[10.0.0.1] tunnel status

[down]

مل<sup>ف</sup> 192.168.1.10.1 192.168.1.10.1 192.168.1.10.1 192.168.1.10.1

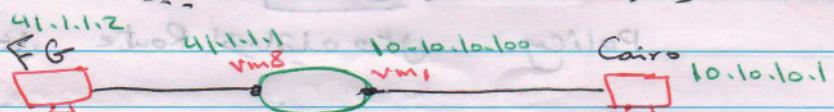
### "48+ VPN Site-to-Site (FortiGate to Cisco)"

\* نسخة برنامج GNS3 وارتبطة بـ VMware

لأنه يكون معايا image دى الماوتر اللي هستعمل عليه وامثل واربعتها ستر امرأة استعمل عليه.

#### التطبيق العملي

- على Edit نعمل GNS3 ونرفع المايج دى على C7200 وننته ونقدر Host من هنا (المهاجر دى على VMware).
- عن طريق دى نختار نوع الكابل ونوصله من الماوتر لل Host FG ويعبر عن القاهرة (Client) و Host تانى يعيش على FG



\* حظ التوصيل على كروت الشبكة ادخل على خواص الـ Network adapter طبيه هنلازم باتى كل دايرد كروته على ادراجه كارتى .

3 - نفتح Router -> Rightclick -> Start

R2# Conf t

R2(Config)# interface FastEthernet 1/0

R2(Config-if)# ip address 10.10.10.100 255.255.255.0

# no shutdown

R2(Config-if)# Exit

R2(Config)# interface FastEthernet 1/1

# ip address 41.1.1.1 255.255.255.248

# no shutdown

# wr

FG. 10.10.10.1 Client 11.1.1 Ping.

VPN → IPsec → tunnels → Name Connect to Alex

Site-to-site Cisco

→ Next →

Remote Gateway 192.168.1.1

outgoing interface Port 2

pre-Shared key .....

Next →

Local interface Port 1

local Subnet 192.168.1.0/24

Remote Subnet 10.10.10.0/24

Create

Policy اتوماتيکاً Route جعل

5 - نزع لراديو سيموكو ونكتي ال Configuration

R2# Conf +

# Crypto isakmp policy 1

# encryption aes 256

# authentication pre-share

# group 1

# lifetime 28800

# exit

# Crypto isakmp key P@ssword address 192.168.1.2 FGv FGv 256-256-256

# crypto isakmp keepalive 10 5 FGv(FGv)

# Crypto ipsec transform-set des256-sha esp-aes

256 esp-sha-hmac

# exit

# Crypto ipsec profile "Connect Cairo"

# Set transform-set des256-sha on

# Set PFS group1

# exit

```

# interface tunnel 161
# ip unnumbered FastEthernet 1/1
# tunnel source 41.1.1.1
# tunnel destination 41.1.1.2
# tunnel mode Ipsec Ipv4
# tunnel protection ipsec profile "Connect Cairo"
# exit
# ip route 192.168.1.0 255.255.255.0 tunnel161
# run
# show crypto isakmp sa detail

```

ملاحظة، تجربة مفيدة (ipsec tunnel)

# "49"

## NATING (STATIC, DYNAMIC, PAT)



Topic:  
Date:

142

Network Address Translation "49" Nating (Static, Dynamic, PAT)



للحاجة لـ 12 او يطلع عن Device ويعمل NAT على  $\rightarrow$   $\leftarrow$  TCP/IP يستعمل

PAT ن Support يسلوا Devices على 9680  $\rightarrow$  محوظة  
modem Router Jig Dynamic  $\rightarrow$  Static لكن على

① Static one-to-one  
Assign one public IP to one private IP

Policy  $\rightarrow$  serviceprovider 5  $\rightarrow$  8  
② Deny any traffic from any private IP Access internet

Ex: 192.168.1.1  $\rightarrow$  41.1.1.1  
192.168.1.2  $\rightarrow$  41.1.1.2

③ يحيز Real IP لكل جهاز

Mail Server او website يستخدمه فقط في الـ

التطبيق العملي



website او يحيز على FG لـ IP 41.1.1.1 Client



### staticNAT . حل - 1

Policy & address → Objects → virtual IPs → Name **website**

Interface

Source address

External IP **41.1.1.2**

FG NIC

Mappe IP

**192.168.1.200**

**192.168.1.200**

Port Forwarding

TCP

Protocol **External Service port**

**80**

Map to port

**80**

**OK**

**192.168.1.200** **declared** **41.1.1.2**

② ركي ا لمود حابلا على الInterface

- دين على Policy هي تفعيل

### Policy . حل - 2

Policy & objects → Policy → IPv4 → inComin **Portz**

Source Address **all**

Source User **all**

Outgoing **Ports**

Destination **website**

Action **Accept**

Service **HTTP**

**OK**

3- نزع نافذة browser Client **IP** المكتوب على **web site** **41.1.1.2**

RDP

نقطة الاتصال بـ RDP مع الـ Exchange Server من **Port 3389** مدعوم

Policy

RealIP **192.168.1.200** كذا مهازن **Port 3389** لـ RDP

مكتوب على **mapped Port** **3389** المكتوب على **External Port** **3389**. يفتح بـ **Port 3389** على **Port 3389** المكتوب على **External Port** **3389**



## ② Dynamic

Assign **pool** public IPs  to **pool** Private IPs

Ex: Private IP 192.168.1.1 → 150

Public IP 41.1.1.1 → 5

النطاق المعنوي

Objects → IP pools → Name **pool1**

Type  Overload

External Range **41.1.1.10** **41.1.1.15**

**OK**

Dynamic object الى النطاق المعنوي

Policy & Objects → Objects → Address → Name **IT**

Type **IP Range**

**192.168.1.100 - 250**

Interface **Port1**

**OK**

Policy  Create

Policy & objects → policy → IPv4 → In Comin **Port1**

Source **IT**

Outgoing **Port2**

Destination **all**

Action **accept**

Firewall/Networks

Ip  اكتسب مبطئا  use Dynamic IP pool **pool1**

فقط اكتسب  بـ Edge Fixed port





① Fixed port افتتحت IP pools بناءً على options لاحظ

External [41.1.1.10 - 41.1.1.15]

internal [192.168.1.150 - 192.168.1.155]

قطع الـ Public (5) بـ Private (5) بين كبار

### Oport Block Allocation

External [41.1.1.10] [41.1.1.15]

Blocksize [4] → 4GB

Block per user [5] → users عدد كل ما يعطى لهم 5 IPs

OR

② لعدد 11 users (5) هي تقبل عليهم النسبة

### ③ PAT

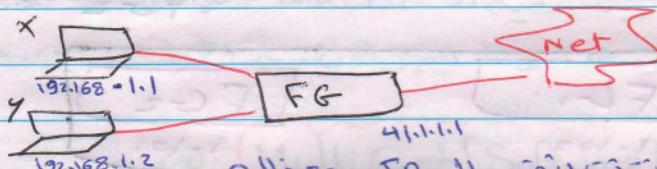
Assign one public IP to all private IP

Port, ConnName, DName, mac, IP لتعنى أن كل Socket يفتح

Port [+] Conflict ولكن يعملوا

(+) IPorName [+] Socket

Conflict يسجلوا لو واحد مختلف من يعطى



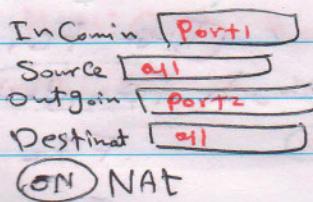
فما الآلة يطلعوا الانترنت بعنوان IP ومع ذلك

من يجعلوا هذه Conflict وهم الآلة Port + IP

وهو ما يعادل Port Scanning كل واحد يأخذ Port مختلف.

النطاق العلوي (Default Port 5100)

1- نعمل Policy



أنا أطبق كل المكونات في application (8 خط)

multiCast او uniCast او Software  
Applicaion  
Classless  
Applicaion  
Loadbalancer  
FG

Application

Classfull

Microsoft

DFs Replication

web1 web2

الخطوة الثانية DFs Replication

Software

التحريك الشفاف

IIS على نفس IP 192.168.1.10 & IP web1 server 1 - نعمل  
Service Add roles → Next → Next → webServer(IIS) →

→ Next → install

IIS على نفس IP 192.168.1.20 & IP web2 server 2 - نعمل

.html files في نفس Folder 3 - نعمل

Policy object → load balance → virtual Servers → Create New  
Name [web] type [Http] Interface [Port]  
virtual Server IP [192.168.1.254] Port [80]

load balance mode [SourceIPHash] من هيكلاع غير المتعارض

RR, WS ← Round Robin

Weighted priority  
First active

least RTT AT Right  
least session Session

HTTP Host Session

Least Connection

OK testing

١٩٦

## 50. FortiGate Load Balance ( HA, Failover )

### Failover (load balance)

MultiCast

one-to-many

Non Failover (Active-Active)

uniCast

one-to-one

(Failover)

(Active-Passive)

محتوى: مراجعة ملخص لـ Failover مع بعض المفاهيم المترتبة عليه

### Loadbalance (FG)

Hardware

استثنى FG يتغدو اجمع بعده

Software

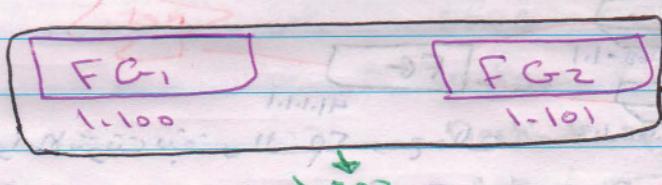
traffic حاصل ونوع FG Servers

Active - Passive

① uniCast [Hardware]

(HA)

FG2 < FG1



نرى هنا المسار من IP وهمي و IP FG1 < FG2

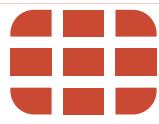
التي يذهب من IP وهمي الى IP FG1 او FG2 Connect

يرجع على حسب الاقل priority

او او FG2 < FG1 او FG1 IP الوهمي

FG1 يرجع الى IP الوهمي على FG2

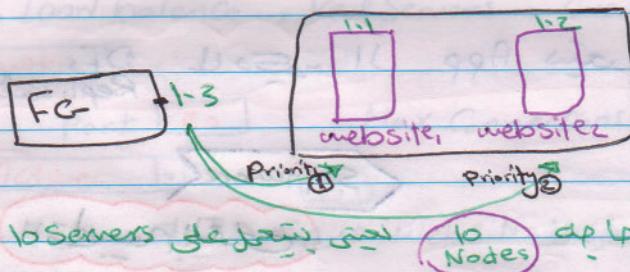




لاظ اى او اي Configuration Policy يتعل على الاقل ليسمح من التأمين  
اى يمس Backup او Copy فيه او

### (Load balance) ③ (uniCast [Software])

FG ① website وندى FG ② sites FG ③ اجهزة خارجية  
virtual IP Connect Client ④ Virtual IP  
Priority ⑤ website ⑥ ليرمى على ⑦ Virtual IP  
و ⑧ website ⑨ ليرمى على ⑩ Virtual IP



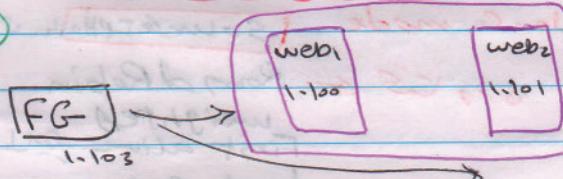
### [Active-Active] ① Multi Cast [Hardware]

استئن FG1 و FG2 و الستينه لنقوم بـ virtualIP وندى كل واحد  
virtual IP بين لاظ الفرق بينها وبينها Active-Active uniCast او Active-Active

Round Robin هنا دعوه هنا وهذا يعني توزيع الحال ويسعى

### ② Multi Cast [Software]

لاظ استئن  
website  
Active Active



لاظ احتمالية استئن او MultiCast او unicast

على مدار راه دوسر لواستئن لفترة الدهور يترخيص

لو ماحتلة دهار دوسر ينبع



6/149

Sub:

Date:

5- خلق الموقع على website

tools → IIS → Default site → Stop

Sites → Add → name web1 Application pool Path1 Select

OK

Default Document → Add → Name web1.htm OK

Default

Document

Add

Name

web1.htm

OK

Default

Document

Add

Name

web1.htm

OK

6- إنشاء الموقع

Policy &amp; Objects → Load Balance → Real Servers → Create New →

Virtual Server web1IP 192.168.1.10Port 80Max Connections 0Mode Active

OK

7- نحن نريد أن نقوم بـ Round Robin لـ Active Server 2 website

Round Robin

virtual IP 192.168.2.254Client 192.168.1.1

الاتصال

web1

web2

موقع

web1

web2

موقع





150

## "52" Network Load balance 2

### NIB with DFS Replication

لابد من Statefull

← application de Loadbalance || اتحاد ||

DFS  
Replication

Load balance في نفس المكان من غير تغيير DFS Replication ||

DFS Replication

multi purpose

Folder

Folder

Data Collection

Folder

Subfolder

الخطوة الأولى

web1, web2 على DFS

web1 دنسن بـ ②

join Domain

Server manager → add roles → Next → Next → Next →

File and storage → File and iSCSI → DFS Replication

Next → install

web2 خل نفسم الخطوه من

Configuration وينتقل الـ DFS web1 و web2

tools → DFS → Replication → New Replication group →

① Multipurpose → Next → Name Data

Domain Site.com Browse

→ Next → Server web1 web2 Add

Next → ② Full mesh → ③ Replicate during specific day

Replicate الوقت الذي يحدده Edit Schedule



Next → Primary [Web1] → Next →  
 Add → [Data] → **Replicate** (الغولدر المقدم)  
 Next → Member details  
 Server (جهاز) [web2] → Edit →  Enable  
 local path Folder [Data] [browse]  
 OK → Create

4 - نعمل الأخطوات على شفوف الـ Web2  
 tools → DFs → Replication → **Data** ← (الغولدر المقدم) لوحدة

لورقة على **Data** (ملحوظة) قوائم **options** (متقدمة) **Advanced** (متقدمة) **Replication** (متقدمة)  
 Conflict and Delete path → Conflict time (المدة التي تختلف فيها الملفات)  
 C:\Data\DFs\Private\ConflictandDelete\Replication

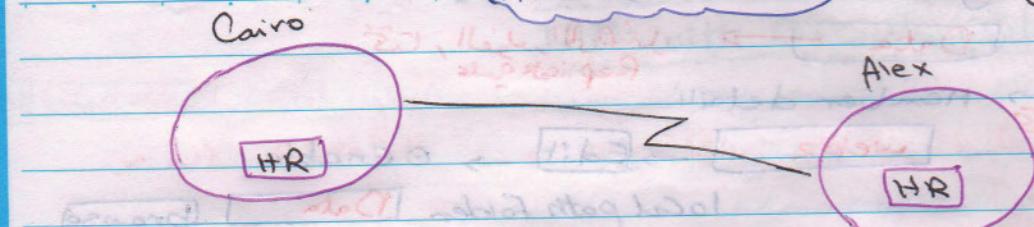
Replicate (عمل نسخة) Replicated folder → **OK**  
 Data → properties →

عمل نسخة على **web1** (عمل نسخة) **Connection** → Data (لورقة على) **Replicate Now**

6 - ندخل على الغولدر **web1** ونختار فيه أي ملفات  
 ونخوب بعد Replicate ونرجع **web2** نلاحظ تسوية ملفات ولنعمل  
 Replicate المرة من أي ملف يختلف في واحد (هستوفه من الثاني).

عمل نسخة للConflict (الغولدر يستلم) (الغولدر يستلم) للConflict (الغولدر يستلم)

### Data Collection



عزا خلي الـ SubFolder مـ Alex بـ HR  
 Cairo SubFolder وـ HR بـ Cairo بـ Alex  
 مستخـ الفـ SubFolder متـ Alex

### التطبيق العملي

HR-Alex web و HR Cairo اـ web G Foder

DFS نـ على -2

DFS → Replication → New Replication → Replication data collection

Next → Name [HR] → Next → Name [HR-Alex]  
 Browse

Next → Name [HR-Cairo] → Destination  
 الى HR-Alex  
 Next → Create

Cairo متـ HR-Alex متـ HR Cairo متـ HR

Next

2 -

2 -

3 -

4 -

"53" HA Between FortiGate Devicesالتبسيط العملي

1 - جهاز FG1 لعنده IP 192.168.2.100 وينتهيConfigure لعنده FG1 على Port 1 على IP 192.168.1.1 وينتهي على Port 1 على bridge VM كانت المترتبة مع الجهاز يتاتي من خط الـ IP وينتهي على Port 1 مع انتهاء بـ IP 192.168.2.100.

2 - نعمل نفس المخطوات على FG2 على IP 192.168.2.200 وينتهي على Port 1 على FG2 و FG1 وينتهي على IP 192.168.1.1 وينتهي على Port 1 على FG2 و FG1.

3 - نطبق على FG1 عسان يطلع نت Router → Static → Static Route → Destination [0.0.0.0/0.0.0.0] Device [Port10] Gateway [192.168.1.1] → المفترض بتاتي

4 - نبدأ بـ HA Configuration

System → Dashboard → Status → HA Status → Configure → Mode [Active-Passive]

Group Name [Site-FG]  
 Password [.....]  
 Port 5 [Enable Session] [Heartbeat 10] [Apply]

Priority [200] [Enable Session] [Group Name Site-FG]  
 Port 5 [Enable Session] [Heartbeat 10] [Apply]

5 - نرجع إلى FG2

System → Config → HA → Mode [Active-Passive]

Priority [200] [Enable Session]  
 Group Name [Site-FG]  
 Password [.....]  
 Port 5 [Enable Session] [Heartbeat 10] [Apply]

System information ← Clustermember 8 (GEN3)  
 System ← Status State master (جهاز master)

0.000 كرونة السويدية Cluster 11 نم FG أو مطاعم **مكتبة هان**

HA → 

Disconnect From Cluster

ولكن لا **لاتغير Policy**

1. ~~نحو 157 120~~ ~~mp7~~ ~~نحو 157 120~~ ~~97~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~97~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~

2. ~~نحو 157 120~~ ~~نحو 157 120~~ ~~97~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~ ~~157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~

~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~ ~~نحو 157 120~~





155

Sub:

Date:

"54" Configured FortiGate proxy.

هي طريقة للخروج لا Net ولكنها لا تتعارض مع إرسال البريد الإلكتروني

نماذجها الأولى من Features

System → Config → Features → Explicit proxy  [APPLY]

التخصيص العالمي

FG على Router Routing - 1

Router → Static Route → Static 0.0.0.0 192.168.1.1

Port، ولدي Net ويعمل Client من على Interface الى التخطي - 2

IP [192.168.1.100/24]

DNS على Client من علىGateway IP

FG على Proxy التخطي اعدادات - 4

System → Network → Explicit proxy → Enable  HTTPS  FTP

HTTP Port [8080] Default policy  Allow

Enable Explicit Ftp Proxy  Pray for Ftp لوكاين افتخار

Ftp Port [21] Default Firewall Policy  Allow

internal client

[APPLY]

Part,

لنفس Interface على Proxy - 5

Enable Explicit proxy

Enable Explicit Ftp proxy

[APPLY]

Proxy : dual Policy - 6

Policy & Objects → Policy → Explicit proxy → Create New →

Source [all]

out going [Portia]

Destination [all]

Schedule [always]

Action [Accept]

[OK]



7- يُوجِّه Client إلى سلسلة من الـ Gateway وـ Proxy وـ مُنْتَهِيَّاتِ لـ Internal Network (192.168.2.200) وـ Internet.

### Proxy options

Policy → proxy options → Protocol Port Mapping

Protocol	Enable	Protocol	Inspection port
HTTP	<input checked="" type="checkbox"/>	Any	<input type="checkbox"/> Specify

لما نعمل على دى عستان لوموقع هسيقع على Default Port  
لما نضع اى بروتوكول اى بروتوكول  
واما سار

Protocol port mapping

192.168.2.199 -> 192.168.2.200 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 ->

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 ->

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201

192.168.2.199 -> 192.168.2.201



157

Sub:

Date:

### "55" Configured FortiGate usb modem

جهاز خارجي على الـ 3G للـ FortiGate

نذهب إلى شاشة Device 1، ثم USB و DSL و External modem

System → Network → modem → External modem

Configure Modem

هذا ينطبق على المودems المدعومين من FG

#### التطبيق العملي

1- أدخل كلمة المرور(model) و اسم المودم (password)

لتنشئها درفل الموبايل

2- أدخل USB في FG و افتح

System → Dashboard → Status → +Widget → USB modem info

usb status تظهر هنا عناصر تشغيل USB

3- يمكن تنفيذ الأمر Consol

# Show system modem

# Config system modem

(modem) # Set status enable

# end

ويمكن إدخال الأمر

interface or Consol أو نعمها عن طريق

interface no no Config

System → Modem → PhoneNum

userName internet بعده الطابع

password \*#\*#\*#\*#\*#\*#\*#\*#\*#\*

Mode 0 standalone

دستوى فوريا

Dial mode 0 Dial on Demand 0 Always Connected

الاتصال وفقاً لـ





Status Dial in Connected

modem (هاتلائي و ابرد اسبر) Interfaces (Interfaces)  
و دخول على الـ IP وهما خارج

5- عن توصل على Client FG (Default gateway) FG (Default gateway) FG (Default gateway)

Policy & object → Ipv4 → incoming [internal]

Source [all]

Outgoing [modem]

Destin [all]

Action [Accept]

OK

7- لدخول على اي موقع هاتلائي فتح استونت

Router 5 FG يفتح المتصفح (فتح المتصفح)

ادخل فيه خط التلقيو و اختار او interface

Addressing mode PPPoE

لو حفظت كل ذلك

Rj45 توصل خط التلقيو على و توصل

FG بالـ

side 1 (local) to local 2 (remote)

Ex Rj45 (local) to local 2 (remote)

[External] connection + on meter

[Local] [External] connection

connection to local 2 (remote)

connection to local 2 (remote) 96M

between span 1 to span 2 (remote) about 100m



# "56" LOG AND REPORT



"56" Log and Report

Sub:

Date:

حالات فريدة سهلة الـ **Log** و الـ **Monitor** 85%

فريدة سهلة الـ **Log** موجودة على الـ **Monitor** 11%

FC, Routing, LB, VPN, DHCP ③ ④ ① ② ⑤ ⑥

Policy&object → monitor →  
System → monitor → DHCP  
Router → monitor → Routing  
VPN → monitor → IPsec  
User&Device → monitor → Firewall

من خلالها من يعبر traffic بسرعه بسيه و خل على اي اجهزه IPS من الـ DHCP

Fortiview Logs 11  
نحو ١١ تطلع من خلالها Reports و ممكن تغير مدة now 5minutes 1hour  
System → Fortiview → Sources →  
لوري ١١ traffic او IP او مصدر او مصدر او مصدر  
ولو وقفت على ١١ IP ممكن لم يوصل ، اذ احاجات المتصفح لها دلوقت  
→ Application →

يعرب ١١ Application قرنة  
من هنا صنفته تطلع من Reports قرنة

ما يظهر logs الى ان logs لا بد من تفعيل log Allowed  
نكون على الاختيار ON All Sessions

لعمليات تطلع Reports طمحيات قد يهدى في الـ Logs او Reports  
Log & Reports → traffic Log →

GFI 1 Solarwinds 2 Sysvol Server Fortianalyzer 3  
لو عيني هارد فراصي جلسه 1 اغلب 3 وتحدد المعايير

Log & Reports → Log Config → Log Setting →  Send logs to Fortianalyser  
 Send to FortiCloud  
 Send logs to syslog



للحاجة إلى إنشاء Reports → Email Reports

System → Advanced → SMTP [mail-eg.com]

Authentication  Enable

Default Reply: FG@eg.com

Port 25

Log & Report → Report → Local → Email Generate Report

Run Now

Customize



Report طبع في

Historical Reports

Delete Download View

مكان توجده أو تنزيله Download لتفاصيل

لفتح ملف

للمزيد من المعلومات؟

① Log & Reports → traffic log → Forward traffic → Add filter

وأخيراً، لا يفضل عن طريقه الـ

فوريAnalyzer المترافق به دخلوا عليه

② Log & Reports → Security log → web Filter

فيسبوك، خدمات المتنقلة التي حاولوا الدخول عليها

③ Log & Reports → Security log → web Filter

→ pol report a string & pol

④ Log & Reports → Security log → web Filter

→ pol report a string & pol

Log & Reports → Security log → web Filter

→ pol report a string & pol

→ pol report a string & pol

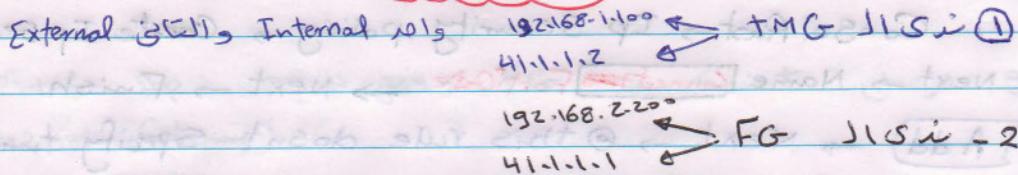
161

Sub:

Date:

### 57. VPN Site-to-Site (FGxTMG)

التطبيق العملي



Ping موقع الاعلی TMG نجاح ١٣

ForeFront TMG → Fire policy → Show system policy → Allow ICMP

Reply رد اي تاك 41.1.1.2 ← TMG نجاح Ping ٤

FG نجاح ٥ Configuration

VPN → IPsec → tunnels → Custom VPN tunnels Next →

Remote Gateway **STATICIP**

IP **41.1.1.2**

Interface **Port2** → FG

Preshared Key **.....**

Local Address **Subnet**

**192.168.2.0/24**

Remote **Subnet**

**192.168.1.0/24**

**OK**

TMG-N object ٦

Policy objects → Objects → Address → Name **TMG**

Type **Subnet**

IP Range **192.168.1.0/24**

Interface **VPN to TMG**

**OK**

policy ٧

Policy → IPv4 → Inbound **VPN to TMG**

Source **TMG**

Outgoing **Port1**

Destin **all**

On NAT **OK**



IPsec جيـ TMG حـ VPN حـ بـ انـ 7

Start → mmc → File → add/remove →  Ip security policy →

② Local Computer → Finish → OK

Console Root → IP Security policy → Create IPsec →

Next → Name  Connect to FortiGate → Next → Finish

[Add] → Next → ② this rule doesn't specify tunnel

Next → ② Remote Access → Next → [Add] →

Next → Source address  My IP address → Next

Destination Address  Any IP

Select Protocol  TCP

Next → Finish → Next →

② New IP Filter → Next → [Add] → Name  New filter

② Negotiate Security

Next → ② Don't Allow unsecure Communication

Next → ② Custom  Setting → Encryption حـ جـ FG حـ CCE

Integrity algorithm  MD5

Encryption algorithm  Des

[OK] → Finish

Next →

② Use String (preshared key)

→ Next →

[OK]

Assign Using

Search?

162.1.1.1 VPN حـ جـ جـ 8

Remote access policy →  Remote sites → Create VPN site-to-site

Name  Connect to FG → Next → ② IP Sec → Next →

② Remote VPN gateway  41.1.1.1 → FG CCE

Local VPN gateway  41.1.1.2

→ Next → ② Use preshared key  162.1.1.1 → Next →

Next → 192.168.2.1, 192.168.2.254  last range

Next → Create network Rule → Next → Apply to protocol [All outgoing traffic]

Next → Finish

APPLY وافق

192.168.2.100 IP address FG → Client - 9 نوصل

192.168.2.200 Gateway

192.168.1.100 start Ping رد

. جزء VPN ردReply رد

5. Test traffic from Client (192.168.1.100) to Internet (192.168.2.100)

(egress) packet capture on interface broadcast envelope

24.12.2019 10:15:15 On Gigabit NIC

\* 0.0.0.0/0 selected -> SELECT Policy: No policy

Source & Destination IP: 192.168.1.100

\* 1.0.0.0/24 selected -> SELECT Policy: No policy

Source & Destination IP: 192.168.2.100

> 1.0.0.1 -> Destination IP: 192.168.2.100

[Internet] match forward interface broadcast - interface

24.12.2019 10:16:07

monitoring traffic - Traffic on interface

Translating Host-to-host port 22 to 22 (192.168.1.100 → 192.168.2.100)

12. 9:40

24.12.2019 10:16:05.1 Nmap version 7.00 (2019-06-20)

Completed 1 scan took 0.000 seconds (0.000 hosts up)



١٦٤

## ٥٨ "FortiGate Configured Policy"

الخطوات على شرائح FG

١- أولاً دخول جهاز واحد طوبوس IP Range

192.168.1.99 FG بـ default

و لكن في الـ browser دخل IP

٢- تغيير الـ HostName (اسم الجهاز)

System → Dashboard → status → HostName Change  
New Name site

٣- تغيير المسار

Status → system time → Change.

٤- تغيير المدير

Current administrator → Change Password

٥- تحويل مدخلات Full UTM

System → Dashboard → status → Security features Full UTM

٦- نظر FG

Status → Widget → Limit operation →

٧- تغيير الـ IP و تعيينها و إيقاف DHCP

And NAT N switch mode

٨- تغيير نوع المكون سقال على الـ Allow Policy

(اصح)



١٠ - **خطاب الانترنت** (IP) **Static Routing** **ج2**  
 Router → Static → Static Route → **+** Create New

١١ - **تحديث FortiGuard** (نقطة)  
 System → Config → FortiGuard → Av & IPS Download  
 Allow push update  
 Every **\_\_\_\_\_**

١٢ - **عنوان IP** (عنوان)  
 Policy & Object → Objects → Address →  
 وايضاً **Local Profile** (لكل إدارة)

١٣ - **نقطة إدارة Policy**  
 Policy & Objects → Policy → Ipv4 → Create new →

١٤ - **لكل إدارة من webfilter profile**  
 Security profiles → web filter → **+** →

١٥ - **لodge VPN** (نقطة مرنة)