

Subject.....

Date.....

TMG 2010

Course : 50 - 357

Exam : 70 - 157

Subject.....

Date. 28-9-2014

"1" Introduction to TMG

ForeFront : threat management gateway

utm : threat management
unified threat management technology

utm unified threat management

ISa (Internet Security and acceleration) جيل اختراع دلائل Product clients tmg

① Router ② Firewall

كان لها وظيفة

webfilter & antispm & antivirus بـ ISA

intro provisions system - Ips

وضع كل طماية من نوع واحد

utm

Router

Firewall

Antivirus

Antispam

Ips

webfiltering

① Routing

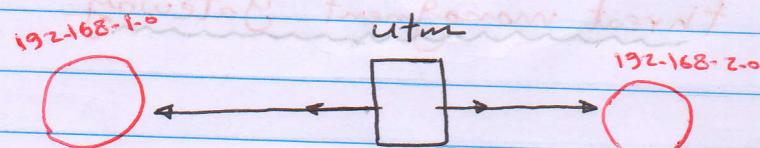
Class A 0 → 126 10.0.0.0 → 10.255.255.255

Class B 128 → 191 172.16.0.0 → 172.31.255.255

Class C 192 → 223 192.168.0.0 → 192.168.255.255

Private Ip

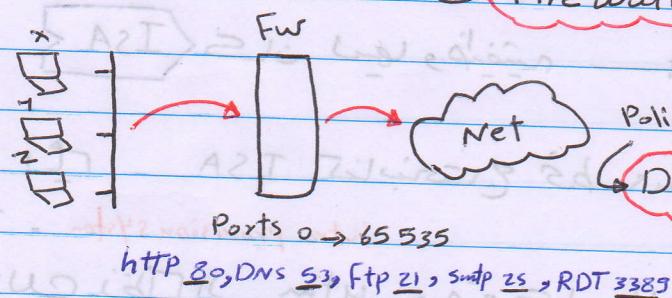
- NAT من أنواع الـ **PAT** بستقام نوع الـ TMG



جاء utm مكان ينتقل antivirus و firewall و Router و utm وجاء antivirus على تخطي utm و Router لاتعرف تحطيم بينهم وبين الـ utm

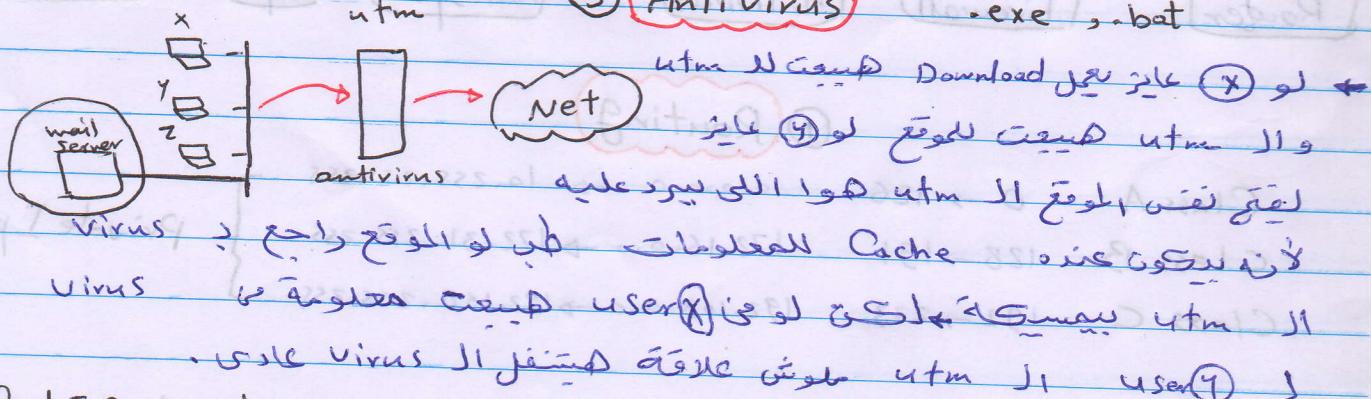
لا يعني عن الـ anti virus الذي ينقط على الـ utm + MG لا يعني من سيس اجهزة الـ utm لاتعرف anti virus بينهم

② Firewall

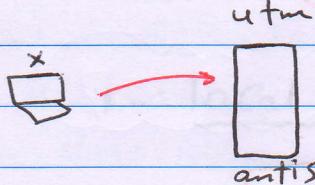


الـ Defant ييقظ كل الـ Ports في أي وقت سواء دخل أو خارج أذاته يفتح الـ Ports الملي ذاتها ولاحظ أن الـ Policy الذي يعدل Deny مبنية على ترتيل.

③ Anti Virus

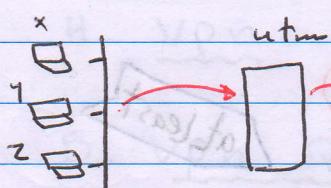


④ Anti Spam



كل أهميته لمنع الاعلانات إنها تجلد من برا
ويمكن بقى ، ظهاره ينبع منه virus يجلد بيعت
رسائل ببراءة لذلك utm يمنع برصده إنك تجتهد المحتوى
بمقابل ذلك Smtp

⑤ web Filtering



لو نحن في موقع مستان نستان لازم أحبله Real IP
وآخر الـ Service Provider اسم الموقع الذي انتقام منه
يحيطه على أي DNS على مستان يرس الاسم داخل على الـ Real IP

ما هو مستان يحط اسم الموقع على DNS على لازم يحيط الموقع حتى تذهب
محبي حب الموقع.

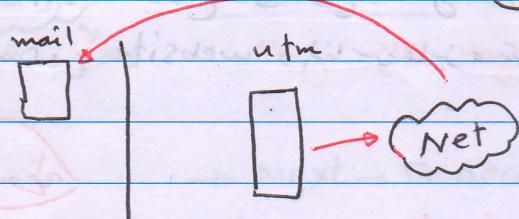
* لذلك web filtering يحدد من يدخل على Port 80 عبر

الـ Category التي أنتا هم فيه .

* أقسام الـ ISA تمت بحسب الموقع بأيدي فكان يفتح user يدخل عن طريق الـ name,ip (Category) لذلك utm يطبق على طرق الـ IP

⑥ IPS

intrusion Prevention System



لو user من خارج ، لست فضل ينزل Ping
حالاً إلـ mail server ينبع ذلك مكان يوضع
إلـ Server بتاسي.

Ips يحدد لا traffic الذي هيجللي
يمكن اعداد الذي يعدل Ping ينزل لمده دقائق بين او اسفل من 200
انما بس وبعد ما هيصل تات.

utm يعتبر

tmg فقط بين

firewall

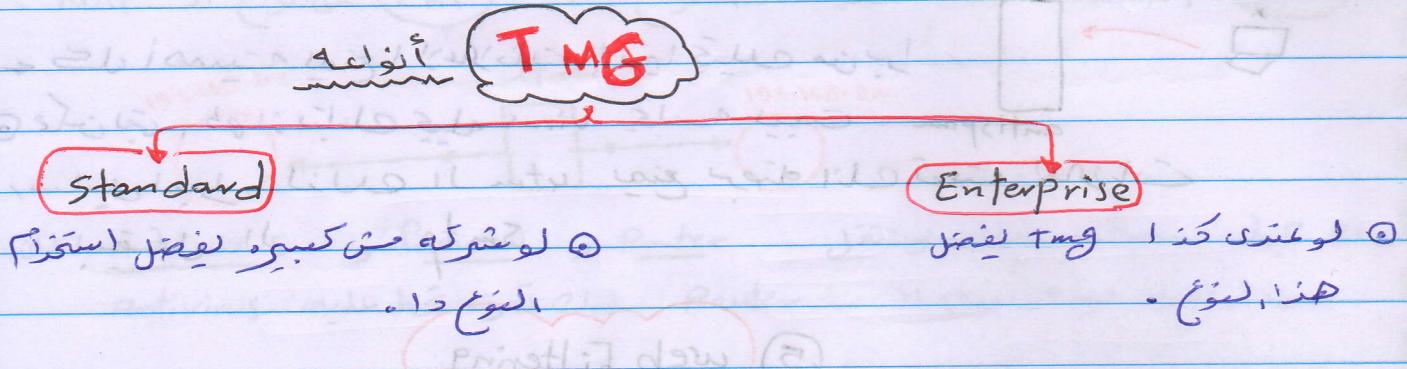
يعتبر

ما هو الـ ISA

Subject.....

Date.....

"2" Installing TMG



TMG Requirements

at least

1- win Server 2008 R2 64 bit.

Standard Enterprise

2- RAM 1 GB → Rec 2 GB

3- Cpu Dual Core at least

4- Hard Free space 2-5 GB

Cache

① Forward: يفتح user لو Cache على موقع و يطبع على user +

② Reverse: Cache يفتح على موقع user الـ website site +

internal network كيسياتي tmg ن install
address Range → LAT

الاهم امثل *

مانع يفتح الـ IP بتاع الـ Range على المفتوح

لامانع بتاع الـ network ١) power tmg ن install اول مانع

tmG 5 Network

1- Local Host.

2- Internal.

3- External.

4- Vpn

5- Vpn Quarantine (NAP) network access protection *

من Rule tmg لفتح اتصال admin لوحة *

• Local Host internal

من Rule يفتح Net من خارج Internal *

• External internal

- Rules ② policy من لوائح *

Install tmg "Standard"

Join domain jai server 2008R2 -1

Run preparation tool نعمل tmg على Soft * -2

Real IP Router ونعمل tmg على Hardware * -3

Net Framework check Required

→ Next → accept → Next → Forefront tmg Service and management

→ Next → Service Run وهمي ويفعل → Finish

- Install تمكين خدمات *

• tmg] ISA

upgrade لفتح امثل *

ما هو فيه

ISA 2004 → SP3

ISA 2006 → SP1

sp2 → sp1 في وقت tmg

لتحديث *

Subject.....

Date.....

Run Installation Wizard, تفتح (3)

Installation Tools Preparation بفتح جميع أدوات التثبيت (Prepare tools available) (1)

Next → I accept → Next → Next →

Ntfs و NTFS المكان الذي يتم فيه نصب البرامج (Install location) (2)

→ Next → Define internal network NAT (تحدد عناوين) (3)

Start 192.168.1.1

End 192.168.1.254

[add]

[add Range]

Range add (تحدد نطاق) (4)

[add private]

Internal Network على الـ (192.168.1.100) (5)

[add adapter]

[OK]

→ Next → Next → Install → Finish

Service pack 1 Install (تحديثات الخدمة) (6)

all programs → Start (فتح جميع برامج الكمبيوتر) (7) (جاء من هنا)

→ Microsoft Forefront TMG → ForeFront TMG management (فتح إدارة فورفرونت تي إم جي) (8)

tmg على Consol (فتح فورفرونت تي إم جي على كونسول) (9)

Getting start (فتح المقدمة) (10)

Interface (فتح واجهة)

Forefront TMG على Consol (فتح فورفرونت تي إم جي على كونسول) (11) (ملحوظة)

Networking → Networks (فتح الشبكة) (12)

Network Rules (فتح قواعد الشبكة) (13)

Internet access (فتح الاتصال بالإنترنت) (14)

Network relationship (فتح العلاقات بين الشبكات) (15)

Firewall Policy (فتح политика الحماية) (16) (ملحوظة)

Rule (فتح القواعد) (17) (ملحوظة)

Schedule (فتح جدول) (18), Protocol (فتح بروتوكول) (19), users (فتح المستخدمين) (20)

to (فتح إلى) (21) و From (فتح من) (22)

Action (فتح العمل) (23) و بعد (After) (24)

"3" TMG after installation

: Networks ⑤ بینرول بینسیم الاینباي Firewall او سالم ظرف

① Internal .

② External .

③ local Host .

④ VPN .

⑤ VPN Quarantine .

طبعاً بعد مانزلت هنلاعفيه فقل كل حاجة

حيث لم تملت عليه Replay Ping فالطيبي لازم بيعتبر انه internal Client واللي يجعل عليه localHost في Network

ماهرين 30 policies اسلات كل ، لكنها هي على microsoft (لادخ) يعملا allow خاصية يستخدمها المولايير لتسويفها بين من مستعملين .

+ Forefront TMG كل او بعض policies في local Host

Firewall policy → Show system policy Rules →

طبعاً لو نفتح هنا Ping (لادخ) (لادخ)
 ① allow ICMP → From → Remote management Computer → Edit
 → Add → Computer → IP 192.168.1.200 → Browse [Advanced] [Find now]

طبعاً دا في حالة انك جاكي في المكان → Apply [عنفون] join domain

لو مس حيبها او IP بس join

طبعاً لو رحست علىك Ping منه اوي جهاز ضبط IP بتاعة

Replay

طبعاً لو عايز افتح او Remote Desktop

+ ForeFront TMG → Firewall policy → Show system policy Rules →

③ Allow remote management → From → Enterprise Remote [Edit]

Add → Computer → Add → start 192.168.1.199 End 192.168.1.202

Subject.....

Date.....

لقطة لـ Policy جديد خاص به بدلًا من قاعده اولى

Hide system policy Rules

وختار

Configure advanced VoIP Setting

وربط بحال من على اليمين

Create access Rule

لقطة

لـ Create Rule هي قاعدة هي اول Rule هي قاعدة اول Rule هي قاعدة من نوع المثلثة .
لـ Create Rule هي قاعدة من نوع المثلثة .
لـ Create Rule هي قاعدة من نوع المثلثة .

Creat Rule

بدأ بعمل بحال

- Create access Rule → access Rule Name [Allow internal] → Next →
- Action to take ① Allow → Next → applied to [Allow external] *
- Next → ② Don't enable malware → Next → [Add] → Network
 + internal
 → add
- Next → [Add] Networks → Next → All users → Finish → [Apply]

كما عملت رابح من user السير تعيين Policy من ذي وقت اعمله allow

ربما لفت الانتباه كل الناس يستطيعون عادي لأنها يطبق بالترتيب .
لنفسها يعني مسافة زنكم شرح .

Categories في Toolbox

لـ Categories لو شفتو حقوق على نفس هتلاري .
Host اهمها عابرين بحال Service provider ببيانات Real IP .
انطباع وحنا يستمر Category على حسب نشاطه .

Subject.....

Date.....

حالياً الـ tag^{mg} يُغلق الـ Category علطول وطبعاً دا أسهل .

3. 12 - 100% with only 100% @ 25%

Page 1 of 1

+ Page 19 - 1

Page 10 of 2023

~~tail? Human?~~

www.3000000000.com

www.dynamilis.com

1-2023-000032 Page 201 of 201 - Hazel Bristol

Digitized by srujanika@gmail.com

• A 3D rendering tool allows you to see how your design will look.

Digitized by srujanika@gmail.com

Page 10 of 10

www.english-test.net

www.EasyEngineering.net

Page 29 of 30 | Last page of the document | Page 29 of 30 | Last page of the document

1988-89 t.96 WAITING FOR 32nd - ENTRANCE HALL

Digitized by srujanika@gmail.com

Address: 1007 25th Street - May 9 close student to 58 cont

water + [metabolism] + transport + excretion + energy

• **W**hy do we have to learn about the environment?

and an in-line ~~too~~ ~~so~~ ~~183~~ tight tight silent

Artemesia salina (trap) ~~2000m~~

Page 10 of 10

• $\text{FeCl}_3 \text{H}_2\text{O}$ •

Second stage: now the system should have 1000 nodes

BROWNSVILLE, TEXAS

Algebra - Chapter 10 - Radical Expressions and Functions

Copyright © The McGraw-Hill Companies, Inc.

19.5.7. *Thlaspi* - *monocarpum* + *sp.* 0.5-1 m.

"4" TMG Client"Web proxy , Secure NAT"

Firewall Client مفهوم مفهوم Client
 لاتخاذ إن مفهوم Client Client لاتخاذ
 طرق ③ Net يطلع Client si لـ si لـ

1- web proxy →2- Secure Nat →3- Firewall Client →① web proxy

1- يكون هناك proxy Server internet explorer application على Proxy Server Net

يسمى على Client منفذ ذلك أن عملية NAT عن طريق Server

عن طريق internet explorer

دورة برمجية ② Client عن طريق proxy Server عن طريق proxy Server

Internet Explorer → tools → internet Options → Connections →

[LAN Setting] → use proxy server for LAN Port 8080 tmg IP Port 8080 Default port

* بن لاحظ إن المتصفح يكون عامل اصحاب *

Forefront → Networking → Internal → web proxy →

Enable web proxy Client Connections For this network

Enable http http port 8080 Port Client

وتحت فيه عدد ②

"Outlook"

إن الـ mail Server هو يشغل في web proxy

browsing فقط. لذلك يستخدم أحد الطرق المعاين

لـ ② Client مش هيكون واحد ولكن Clients web proxy

admin tools → gp management → Domains → abc.com → Default Domain policy

→ user Config → Policies → win setting internet explorer

Subject.....

Date.....

② Secure Nat

internal "outlook" External mails مكتبي اعنى الخامن مع webProxy سستكة او
Switch . tmG . عن طريق Switch عنى بىنهم .
كذا كذا هينفع لانى واصل بىنهم

Default gateway دى تعنى إيه على بارك المتر بتاع الـ user بىنهم

الميزة دى هطلع بت و هستقبل وهو رسائل من Outlook عارى

③ بناءً على Domain DHCP مش هدى على كل جهاز لكن تطبخ IP gateway

ومنه هو ياخو IP gateway

Domain → Server manager → Roles → add Roles → + DHCP Servers
→ Next → Next → Next → Wins not Required → Next → DisableDHCPv6
→ Next → install.

هاد ظاهر حاجة tools في الاشتراك tools و بتايميلات proxy

+ Bypass proxy Server for local address

تعنى لو انا عايز افتح website بتاعي من المتر لكن بعزمهم local

④ بناءً على DHCP

admintools → DHCP → IPv4 → New Scope → Next → Name [main]
→ Next → start ip [192.168.1.1] End ip [192.168.1.254] → Next →
Exclusion → Start [192.168.1.200] add → Next →
+ msg [192.168.1.100] add → Next →
 Yes, Configure options now → Next → gateway, IP [192.168.1.100] add → Next →
Next

⑤ نزع التحول Client

Cmd → C:\> ipConfig /release

C:\> ipConfig /renew

متلاشى خد او IP

DHCP من

Subject.....

Date.....

"5" TMG Client

يمكن اخذ من خلال DHCP امر من يعرف باى Classes و ميعرف عن طريق انى اقسمهم

① DHCP → IPv4 → Right click → Define user class → [add]

Default option اذن افع ال

name [TMG] ID [asci tmg]

② IPv4 → Scope option → Router → Delete

→ Right Click → Configure Options → [Advanced] →

User Class [+MG]

Router

ip [192.168.1.100] add → ok

بما الا Class ي الأخذه من gateway

وطبعاً الا Default Class الى عنده في Clients الى عايزه

Cmd client his

اسم الفئة

اسم او Class

③ C:\ ipconfig /setclassid "Local Area Connection" TMG

Gateway هنا يعنى في زرته +MG

Class

موجودة

لو عايز العنيها هكتب نفس الامر بـ **None**

طبعاً لو عايز اعادها على كذا جهاز هره واحد هعجاها

TMG.bat → واعط الاصغرها

On ← gp ← ندخل على ←

tmg → Edit → Computer Config → wind setting → Scripts → logon

Show Files → Script او خط او Paste & Copy → [add] → ونعمل [Browse] → خطاقة

[App1]

→ [OK]

Run الدل Script

③ Firewall Client

* اهم طريقة وافق مع tmg او ISA او Forti Client Net بحكم من مدخلها Client اسمها batch دفعاً

خاصية webproxy لوالتي تسمى (Proxy) تسمى تابعه policy

- userConfig → admin templates → wind Components → Internet explorer
→ Disable Changing Proxy Setting → Enable → **Apply**

Firewall Client نكمل *

Client ينجز على كل أجهزة tmg مع tmg Client نجدها عن طريق الـ Computer ، و user سواء gp

* نجدها الاول على الـ user

User Configuration → Software setting → Software installation → New → package

و يكون الملف msi
* Shared folder لازم تكون موجود على Domain
New folder → tmg → client 1, 2, 3 → Properties → Sharing → Advanced
 Share this folder → **permission** Read من Client او المهام او apply → ok

New → package → msi → نجده في local network
لاختلاف لازم يكون في local network
هذا هو الملف الذي سنكتبه في allprograms → Start → اول ما يدوس عليه ابدأ تشغيل

gp install Program From network
published → cp لـ published user
assigned → assigned user

بعد ما يفتح الملف update او modification او assigned publish

* طبعاً يجري العمل على مستوى Computer وذا اللي المعروض نعمل

Computer Config → Policies → Software setting → Software installation → New package
Network → Assigned → دعوه للانشاء → وما يضر على الـ comp الجهة التي نرسل

لابتكز ميكنش عارق من الـ TMG Client

لذلك نعمل احنا لغرضه من الـ TMG ② طرقاً

Active directory
DC

DNS

DHCP

أى طرق من الالوان

① Active directory

هنا نعملها من درس لوحدتها بالتفصيل المدرس لغافر

② DNS

DNS → IPDC → Forward lookup zone → ABC.Com →
New Host Alias (CName) → Alias WPAD → Capite دارم ساخت کرد او

Browse

تماشا على الـ TMG → OK

ذريعة تروح الـ TMG من webproxy لـ IIS; diping
Forefront → Networking → Internal → Auto Discovery

عليك عزيزي [Publish automatic]

Port
Apply

8980 → OK

③ DHCP

DHCP → IPv4 → Right Click → Set pre defined option

Add Name [TMG] Data type [String] Code [080] → قيمه غير المعرفه
OK

Value

String

IP او name

Join domain

http://TMG

Subject.....

Date.....

Scope options

ونزوح لغرضها

التي تعيده

② Scope options → Configure options → 080 TMG → **apply** → **OK**

③ **ls option** هي امر ال Client يكتبه

لود فلات على **Proxy Setting** وسوفت **interceptor tools** باتجاه tools

Automatically detect setting على **detect**

ملاحظة

لواحدات او **interface** التي هي tmg Client

Setting → **Detect now** → tmg Client

tmg N detect يكتبه

④ **detect** يكتبه **Internet explorer** لود فلات

tools → internet options → Connections → **Ian setting** → address **internet**

"6" TMG Client ③

- هنا نذكر بالطريقه المخزن في TMG Client
- الـ Ldap البروتوكول المسئول عن البحث
- هنا ينتمي طريقه من الـ Active Directory
- هنا يخلي الـ Ldap يعرف الأجهزه فيه هو الـ TMG بتاعهم
- Ad Configpack اسمه Software هو طريقه
- Command Install وبعد زكيت يعرف الامانه من العمله
- tmg ادار

active directory

- 1- معاشر جهاز لينج دينج من الـ Container
- win7 ← join Domain
- بناءً على Computer لونقلات طهنه جوا الـ on المالي عليه الـ Policy
- بناءً على tmg Client فـ tmg Client عليه

active II adConfig عشان يسيب معلومه للـ Domain dc Ad Config نسبيه
directory من الـ tmg

→ Next → I Accept → Next → Path تعيين الـ DC → Next
→ Finish → Copy تعيين الـ DC

بنهاية اسفل على

Copy الى path C:\programfiles(x86)\microsoft\tmg\adconfig
C:\> cd

بنهاية على > tmg adConfig add -default -type winsock
-url http://tmg.abc.Com:80/wspad.dat
tmg هي active directory جوا (الـ IP)

* نوع ايش اشوفه list Mac URIS

> tmg adConfig List

Subject.....

Date.....

عند مشاركة المجلدات join domain ← tmg ← tmg Client

لكن لازم الجهاز اللي هيتكتب عليه الامر يكون join domain

* طبعاً حالياً ذي جهاز join ومستخدم tmg Client
يسوف الا tmg join لوجودها من هيشفته.

لذا طبعاً يفتح اتصال tmgclient نزل وشحال وعامل

11. من بين على الامانة join domain من لازم على Command line

Clients

لا تنسى تذكر في شفاف discovery auto

Forefront

Networking → Internal → Properties → auto discovery → publish automatic

webproxy لفتح المتصفح

web proxy

تحيل العارمه لكن يبيه عادي Enable web proxy

Recommended ← Active directory ← * اقوى نوع صيغة

Setting ← tmg Client ← win7 or windows 10

Advanced → use active directory (recommended)

"7" ISP Redundancy

* كانت بتعمل في الـ tmg ISA برمته بس اتطورت في الـ

Clustering

H/A

Failover

Downtime هيكون فيه

Nonfailover

Downtime معهوس

uniCast "one-to-one"

multiCast "one-to-many"

Cluster web site ② نوعين وعامل يستخدم

Cluster site ② نوعين وعامل يستخدم

Connect Client ينضم لها الـ virtualip

v masch v IP وكمان

Priority يعطيهم يستخدم الـ VIP والـ IP

Connect Client يحصل على IP

موقع اربع اماكن او IP يختار الـ IP

يحدد priority فـ IP هـو بـird وـoject

وقـt التـrnsfer الـ Site يـsقـt وـhـost الـ IP

الـ IP لـ site يـsقـt وـtـrnsfer علىـ priority المـbـe

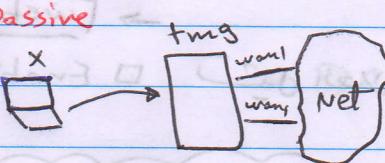
Down time

لـ site بعض من سـمـt

I Sp Redundancy

tmg وـoamr link

Failover mode



active-active

load balancing mode

الـ Client يـsقـt tmg والتـ

الـ load balancer هيـo خـsـtـiـnـg التـ

عن طـرـيق خـطـين لـoamr وـtـmـg وـtـmـg

مجموعـه Clients قـtـlـyـsـtـiـnـg وـtـmـg

الـ t~m~g هـيـo يـsـtـiـnـg بـsـaـkـiـnـg منـ

الـ t~m~g يـsـtـiـnـg دـtـaـlـyـsـtـiـnـg اـnـaـlـyـsـtـiـnـg اـnـaـlـyـsـtـiـnـg

يـsـtـiـnـg عنـ اـنـاـلـyـsـtـiـnـg وـsـaـkـiـnـg دـtـaـlـyـsـtـiـnـg اـnـaـlـyـsـtـiـnـg

* هل لـاحـظ أـنـه مـعـنـقـش خـطـ عـاـمـل Backup خـطـ ثـانـي طـلـ؟

وـhـost Policy حـمـل اـنـاـلـyـsـtـiـnـg اـnـaـlـyـsـtـiـnـg اـnـaـlـyـsـtـiـnـg

وـhـost 2 تـطـعـم هـنـ وـwan1 وـwan2

ديـكـا كلـ مـجـمـوعـه دـtـaـlـyـsـtـiـnـg منـ دـaـmـe وـmـa~rـe وـm~a~r~e اـhـa~b~i~tـi~n~eـsـ

عاـيـزـين لـغـرـفـه لوـ wan1 وـwan2 هـيـo جـمـوعـه وـhـost

الخطير العملي

١- هنديف لـ IP address ٦٢.١.١.١ Real IP كارت دس تالك وادن tmg ٦٢.١.١.١ ويعمل على Subnet

Subnet mask ٢٥٥.٢٥٥.٢٥٥.٢٤٨

Gateway ٦٢.١.١.٢

DNS ٨.٨.٨.٨

٢- IP address ٤١.١.١.١ كـ IP address ٤١.١.١.١

٣- فتح الـ Consol بـ IP address ٦٢.١.١.١

Networking → [Isp Redundancy] → Configure Isp Redundancy

→ Next → ① Failover → Next →

Isp Connect name External

Network adapter ٦٢.١.١.١ كـ IP address ٦٢.١.١.١

→ Next → Next

Isp Connect name External

Network adapter ٤١.١.١.١

→ Next → Next

Select the primary ISP Connection

External ١

External ٢ → Next → Finish

[Apply]

لوضع كـ IP address ٦٢.١.١.١ External ١ من clients

External ٢

٤- C:\> route print

routing table

External, External, IP address ٦٢.١.١.١

Gateway

٥- ظاهر في cmd

Subject.....

Date.....

Failover 群集
Internet access → ① use Default IP

Network Rules

انلوك لدخلات المتصفح

الخطوة

② use specified IP

جداول IP متعددة لـ Redundancy

C:\> netstat -r

لوكيشناتي الـ cmd

هذا هو الاستئناف الافتراضي

Default gateway

③ خدمة المزدوجة Redundancy *

App1 → Failover Redundancy → N. Disable

Configure Isp Redundancy

① Load balancing → Next

Isp Connect

External

Network Adapter

62.1.1.1

→ Next → Next → External Dns

Isp Connect

External

Network Adapter

62.1.1.1

→ Next → Next → External Dns

→ Next

Link1

Link2

→ Next → Finish → OK

Create Rule

Computers

Internal

→ External Dns

External

* بعد كل نجاح

Subject.....

Date.....

Rule II backup ملحقاته

Isp Redundancy

Export Isp Redundancy → Export → Next → → المزيد
→ Next → Finish

Restore

الآن اجرب ←

Apply

Disable Isp

Rule

اعل II

مندشت يعني دخدار، ← Import Isp Redundancy

→ Next → Name → كتابها → Next → Finish

Apply

هذا يختلف باختلاف ترتيب المدخلات

IP II Interface

[advanced]

لعمليات اغلاقها من غير حفظ على

Automatic metric

نرى لدى رقم

* والكارتر الناتي يتلقى رقم بروتوكول وهو يبحث، الرقم II
العنى لولعاته وقع بيطاع من الناتي

Network Rules

← Rule

فرفع الخطة التي بعدها نظر ال

Internet access

→ Destination Networks

→ NAT Address Selection

use multiple IP

Select IP

load balance

41.1.1.1

Add

62.1.1.1

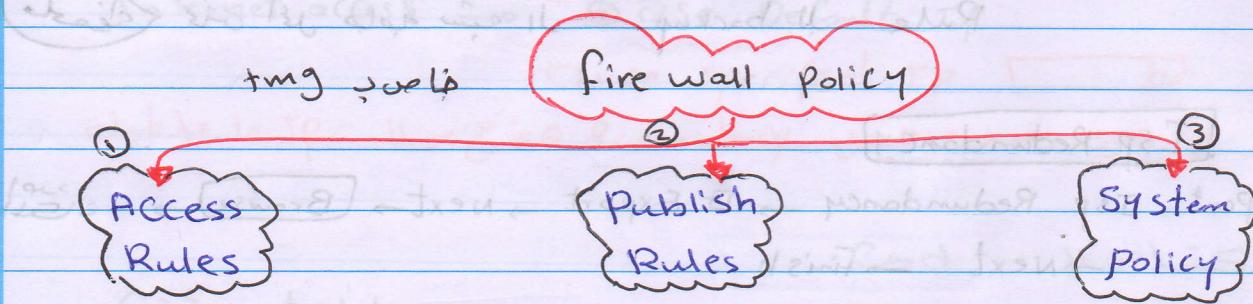
Add

OK

Apply

OK

"8" Intro to Firewall policy



جیلکس ۰۶۵۵۳۵ پورت کے وچھے Firewall سیستم میں Rule کا عالمی نام طریقہ ۱۱ پورٹ کو جو

① Access Rules

* managing any traffic between any network.

1- Internal to Local Host.

2- Internal to External.

3- Internal to VPN.

4- Local Host to Internal.

5- Local Host to External.

6- Local Host to VPN.

7- External to Local Host.

8- External to Internal.

9- VPN to Local Host.

10- VPN to Internal.

11- VPN to External.

② Publish Rules

جیلکس Hacking ۱۱ Private IP اور ۱۱ Real IP کو Remote Machine پر

tmG ۱۱ بیان کرنے والا ۱۱ Remote IP

Ex: web Server, Ftp Server, DVR, mail server, RDP

Subject.

Date.

③ System policy

* Managing traffic between local Host and any network.

• In local Host الى يدخل allow policies لـ Enable او Disable policies دوں بیکوئے

▪ Forefront

Firewall Policy → Show system policy Rules → Rule 50
• تحریم حامیہ تردد کے ساتھ allow

local Host ای جامیہ تردد کے ساتھ

• اپنے Remote Desktop Client کی طرف اسکے اسلوب کا دھن کرو

• دھن کرو اسکے اسلوب کا دھن کرو

• من میں اسکے اسلوب کا دھن کرو

install SQL Server Management Studio

• Run Installation wizard

فقط management Console ای Database tools کا install کرو

Subject.....

Date.....

"9" Access Rules

* managing traffic between any network.

لديك ميزة احجز التي يطبع على الشبكة بحسب اعمدتها **Control** هى خطيتها عن IP username وال طرق

ليس لاحظ ان من من تقع عينه يستخدم **Firewall Client** او **web proxy** من هم ينبعون من **Secure NAT** لكن لو gateway من جهاز واحد من **gateway** - المعرفات

toolbox elements الى يكون في **Access Rules** **Line** ←

Address Ranges → Right Click → New Address Range → Name **[HR]**

Start Ip **192.168.1.10**

End Ip **192.168.1.20**

→ OK

Range واسع **Sales** ← وهذا ينبع من **HR**

Range واسع **IT** ← وهذا ينبع من **HR**

Domain Controller Computers **Domain** ← لاحظ ان لازم من

toolbox Computers → New Computer → Name **[Domain]**

Ip **192.168.1.200** → OK

App1

Domain يكون مدمناً **Clients** ← لاحظ ايقونات DNS

يسطع **Domain** على **Dns** **Forwarders** ← يعرض حقيقة **Dns** على **Domain**

Forwarders من طريق **Real Dns** ← انتبه

DNS → PDC → Forwarders → **Edit** → IP **8.8.8.8** → google

tedata ← **136.128.121.134**

root hints

use root hints if no forwarders are available

* دى تكون جاهزة **Forwarders** لـ **DNS** ← لاحظ

Service DNS **tmG** ← يربط على **Carat** او **External** **Provider** ← لاحظ على **Carat** او **External** ← الميزة او الخدمة

Subject.....

Date.....

Access Rule

نجل اول + MG قياد

ForeFront

Firewall policy → New → Access Rule → Name [Allow DNS server]

→ Next → Allow → applies to [Selected protocol] [Add]

[+] Infrastructure → DNS → Next → [Source] [Add]

[] Computers → [] Domain → Next → [Destination] [Add]

External → Next → All users → Next →

Finish [Apply]

Resolve Clients لغير تجل Rule لا ينبعها

Internal DNS

Categories Net Clients دفعات Rule [Policy]

Firewall policy → New → Access Rule → Name [HR]

→ Next → Allow → Next → applied to [Selected ports]

[Add] → DNS, [Mails] → pop3, smtp [لهم حسب بروتوكوله]

[Web] → ftp, http, https

Download ↙

→ Next → Don't enable mailware

Source → [Add] → Address range → [HR] → add → Next

Destination → [Add] → External → add → Next → All users

[Apply]

لكل اقتضاه على است

لو ناير اعقل حاجة ممكن عن طريقه او

[+] Forefront → webaccess policy → HR Rule → [to] →

Exceptions: [Add] → URL Categories → [Chat] [الى الاقسام التي تتعلقها]

→ OK

* لا تقدر الطريق دى لكن الافق دى

Firewall policy → HR rule → [to] → [Add] → URL Categories

[] Financial, [] News, [] add

بى اجددت الى هيلطعوا عليه والباقي مختلف

[Apply] → OK

Subject.....

Date.....

* طلب لوحة عايزه لستقبال ويعت ايميلات بيب من لشوق الـ
Firewall Rule → New Access Rule → Name Outlook

→ Next → Allow → applied to Selected Protocols

Add → Infrastructure → DNS
 Mail → POP3, SMTP → POP3 S SMTPS → Exchange 2007, 2010
→ Next →

Source → address Ranges → BMRK → [add] → next

Destination → Networks → External → [add] → next

Finish → Apply

رجاءً منكم الـ MRK مس تجعل اي حاجة غير استقبال

وارسال ايميلات -

* طلب لوقي موقع معين للاميلات عايزه افتحه فقط من elements ديعين افتحه

URL Sets → New URL Set → Name Mail →

[add] → HTTP://mail.abc.com → OK

يتابع mail Server

واعل عن new access Rule

New access Rule → Name Mail → Next →

Allow → Selected protocol [add] → Common protocols →

DNS, HTTP, HTTPS → Next → Dont enable mailname

Source → [add] → address Range → BMRK → Next

Destination → [add] → ~~URL Sets~~ → Mail

→ Next → Finish → Apply

* طلب لو عايز مجموعه معين يدخلوا على موقع معين فنـا
accessrule فيها 1 اسم الواقع وعمليه URL sets

allow URL Range Range من 11

URL Categories web E-mail Email

ومنهم Exception مبعـد عـلـى

Subject.....

Date.....

طلب لوحة موقع يفتح موقع تابع منه موجة كل الان

New URL sets → **Add** → http://~~www~~.yahoo.com

http://www.*.yahoo.com

http://www.yahoo.com/*

App14

طلب لوحة مفتوحة *

New access Rule → ① Allow → DNS, Http, Https, Pop3, Smtp, Sftp

Next → Source **anywhere** → Address Range

Destination → External

→ Next → Finish → **App14**

Pornograph, Chat, Games ↗ Exception

P2P, Remote access, Spam URLs, spyware, streaming media, unknown

App14

Subject.....

Date.....

"10" Web ACCESS

[Toolbox]

لوحة ادوات Computers طبعوا وقت معين يمكن من
Schedules → New → وحدة وقت معين Schedule Rule معين نختار من []
والمدخل Rule معين نختار من []

لقطة

يمكن تعيين مجموعة اجمع ال Rules الذي على نفس المدة او
اوقة معاقة و Ctrl دايركت المايز هم وضعه
Right Click → Create group → name [HR] → Apply
ويتم إنشاء group HR ليتم فيه إدخال
Range rules و ذلك لـ

Selected protocol او لـ all traffic لـ المدخلات

لوحة ادوات Protocols مثل موجود ص 1, بحث عن Port 10000 بقاعة Protocol DVR
[Toolbox] → Protocols → New → Protocol → Name [DVR] → Next
[New] → From [10000] to [10000] → ok

ديرا فتحت ال Port 1 وتحده منه *

Finish

بعد ذلك ظهرت All protocols لوانا تم دخولها في
Protocol المدخلات المدخلات

عندما اعدت ال Category الموقع معين عامله موقع
Category عامله دايركت يمكن اسم الموقع فيه يعود عليه ،
Fortinet

لقطة - اتي هناك اربعه ال users عن موافق جميع يمكن بدل قسم :
URI Sets ونذكره اللى يخرج عليه
firewall policy ①
Exception ادخل

tmg من اهمها ← يستخدمها web access policy ②

Subject.....

Date.....

فایروال پولیسی \rightarrow Create Rule ادمین الـ Web access policy \rightarrow Create Rule

Publish

لعله لو صير بيعوس انه من الـ Firewall policy

- ١) web access policy \rightarrow Create Rule
- web access policy \rightarrow Configure \rightarrow URL Filtering \rightarrow Enable URL Filtering
- ٣) نزدک امتحانها Rule \rightarrow Rule \rightarrow Enable \rightarrow نزدک امتحانها
- ٤) \rightarrow Exception \rightarrow احجز ليها تردد \rightarrow web filtering \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow \rightarrow

لهماظن لوماين اعرف بیان موضع بین المتریکو Category \rightarrow Configure \rightarrow URL Filtering \rightarrow **Category Query** \rightarrow URL **www.google.com** **Query**

لهماظن لوماين اعرف بیان موضع بین المتریکو Client

بیانه ولقیة unknown، کل ریکون، \rightarrow **Category Query** \rightarrow **unknown**

طبع من هنقوله لکن \rightarrow **Category Query** \rightarrow **unknown**

URL Category override

Filter by Category **www.yahoo.com**

Add \rightarrow URL **www.yahoo.com** OK Apply

لهماظن لوماين اعرف بیان موضع Rule

Right Click \rightarrow Configure HTTP \rightarrow **Extensions**

Block Specified extension

Add

Extension **.exe** \rightarrow OK

.mp3

لکنها مشوف \rightarrow چیزه الویں کلها ولا الا عندهارے الی اندازه حالیه

Deny ← Action لاحظ المانع والـ

رسالة من tmG يمكن اعدتها Client يظهر هنا

Display serial notification

مفتاح الدخول

او اعمل على موقع تابع ←

Redirect web Client

www.abc.com

App14

+ MC Spec ← لقدركم خط صوره او *

Configure Https من على البيئين خارج webaccess مفهوم ملاحظة

Inspection

دي يختلي الارتباط HTTPS http لالركيت زى اى Secure

Enable Https inspection دايم الواقع دايم

Certificate ستفهم ان الموقع عنده Inspect traffic and validate Certification

Don't inspect traffic, but validate site certificates

اصدار لوعاير ستوريفها Certificate اصدار tmg او ملاحظة

[generate] نعمل

[Import]

وتحتها Certificate وسترى اصدار ستوريفها

لاداري HTTP

لواقع معينة نكتها Destination Exception لاحظ

[Add]

وندخلها

Certification

و دى بجعلها لبيانات البقالة

ممكن اطلب اى Client يكلموا او Site يتابع او طريقة Internal Clients

على Port 80 او على Port 800 يدخلوا عليه من

و يحترم بيعي العمل و Ping