

Policy FortiGate



Osama Raad

www.linkedin.com/in/osama-raad-9608081ba

Policy

Policy : هي القواعد التي تتحكم بالترافيك الي داخل وخارج من الفورتي جيت وتعتبر من اهم المواضيع في الفايروول

ملاحظة : جميع الفايروول في العالم تكون by default policy

Deny any any

بمعنى منع جميع الترافيك من الداخل الى الخارج والعكس

ملاحظة : الفايروول يقرأ البوليسي من الاعلى الى الاسفل

تعتمد البوليسي على Accept and deny

تعمل accept or deny بالاعتماد على :

- Source
- Destination
- Service
- Protocol
- Users
- Schedule

Object Addresses

هي طريقة يتم استخدامها لتسهيل تحديد source and destination عند عمل بوليسي مما يجعلها اكثر مرونة وسهولة في هذه الصورة في الاسفل هو لانواع Object Addresses

Interfaces	> Incoming interface > Outgoing interface > Any > Type > Physical Interface > Sub interface (VLAN) > Zone
Address	> Type > Subnet > Range > FQDN > MAC > Geography
Service	> Type > Protocol > Port
Schedule	> Type > Recurring > One Time
Action	> Type > Allow > Deny

Interface -1

موجود في Network > Interfaces

الذي يقصد به هو واجهه الشبكة LAN , Wan , DMZ

ونحدد من اين تأتي الترافيك والى اين تذهب

فائدته : التحكم في الترافيك عن طريق الانترنت

أنواع الـ Interface في FortiGate

- **WAN** : تمثل الواجهة التي تكون متصلة بالإنترنت أو الشبكة العامة.
- **LAN** : تمثل الواجهة التي تتصل بشبكتك الداخلية.
- **DMZ** : تمثل الواجهة التي تتصل بالشبكة المحيطة (الشبكة المتوسطة بين الإنترنت والشبكة الداخلية).

FortiGate VM64-KVM									
<div> <div>1 3 5 7 9 11 13 15 17 19 21 23</div> <div>2 4 6 8 10 12 14 16 18 20 22 24</div> </div>									
<div> <div>Create New</div> <div>Edit</div> <div>Delete</div> <div>Integrate Interface</div> <div>Search</div> <div>Group By Type</div> </div>									
Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref	Security Mode	
802.3ad Aggregate									
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2		
Physical Interface									
LAN (port2)	Physical Interface		10.0.0.1/255.255.255.0	PING HTTPS SSH SNMP QoS			2		
port3	Physical Interface		0.0.0.0/0.0.0.0				0		
port4	Physical Interface		0.0.0.0/0.0.0.0				0		
WAN (port1)	Physical Interface		192.168.100.15/255.255.255.0	PING HTTPS SSH HTTP TELNET			2		
Tunnel Interface									

في هذه الصورة في الاعلى Interface من واجهه fortigate

Address -2

Policy & Objects > addresses > create new موجودة في

مثال على استخدام Object Address في policy:

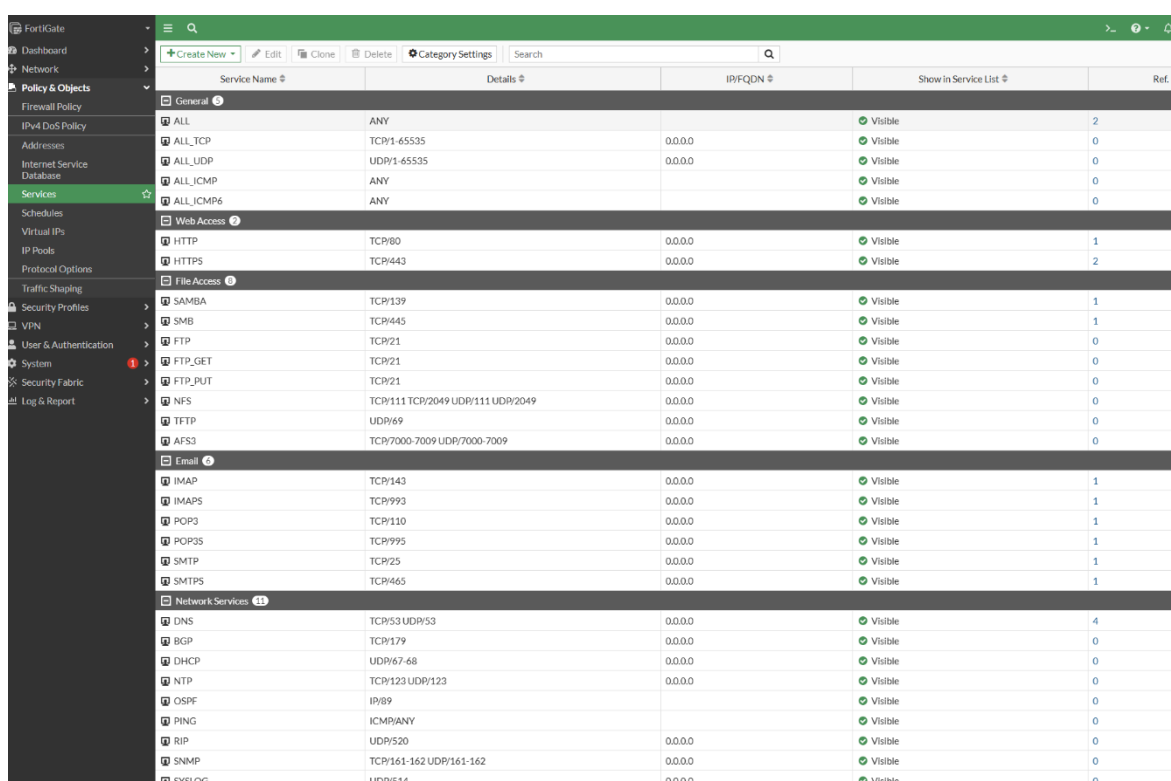
1. إنشاء Object Address :
 - في واجهة الإدارة، انتقل إلى Policy & Objects ثم اختر Addresses.
 - اضغط على Create New لإنشاء كائن جديد.
 2. تحديد نوع object :
 - حدد نوع الكائن IP Address ، FQDN ، Subnet
 - أدخل قيمة العنوان ك IP أو Domain
 3. استخدام object في policy :
 - عند إنشاء Firewall Policy جديدة، يمكنك اختيار object التي أنشأتها ك Source Address أو Destination Address
- على سبيل المثال، إذا كنت تريد السماح بحركة المرور من شبكة داخلية محددة إلى الإنترنت، يمكنك تحديد Source Address كـ 192.168.1.0/24 و Destination Address كـ all أو أي عنوان آخر

Service -3

Policy & Objects > service موجودة في

تعتمد على protocol مثل http,https,ftp,dns والكثير

وتعتمد ايضا على port مثل بورت 80 او 443 او 21 او 22 وغيرها من البورتات



Service Name	Details	IP/FQDN	Show in Service List	Ref
General				
ALL	ANY		Visible	2
ALL_TCP	TCP/1-65535	0.0.0.0	Visible	0
ALL_UDP	UDP/1-65535	0.0.0.0	Visible	0
ALL_ICMP	ANY		Visible	0
ALL_ICMP6	ANY		Visible	0
Web Access				
HTTP	TCP/80	0.0.0.0	Visible	1
HTTPS	TCP/443	0.0.0.0	Visible	2
File Access				
SAMBA	TCP/139	0.0.0.0	Visible	1
SMB	TCP/445	0.0.0.0	Visible	1
FTP	TCP/21	0.0.0.0	Visible	0
FTP_GET	TCP/21	0.0.0.0	Visible	0
FTP_PUT	TCP/21	0.0.0.0	Visible	0
NFS	TCP/111 TCP/2049 UDP/111 UDP/2049	0.0.0.0	Visible	0
TFTP	UDP/69	0.0.0.0	Visible	0
AFS3	TCP/7000-7009 UDP/7000-7009	0.0.0.0	Visible	0
Email				
IMAP	TCP/143	0.0.0.0	Visible	1
IMAPS	TCP/993	0.0.0.0	Visible	1
POP3	TCP/110	0.0.0.0	Visible	1
POP3S	TCP/995	0.0.0.0	Visible	1
SMTP	TCP/25	0.0.0.0	Visible	1
SMTPS	TCP/465	0.0.0.0	Visible	1
Network Services				
DNS	TCP/53 UDP/53	0.0.0.0	Visible	4
BGP	TCP/179	0.0.0.0	Visible	0
DHCP	UDP/67-68	0.0.0.0	Visible	0
NTP	TCP/123 UDP/123	0.0.0.0	Visible	0
OSPF	IP/89		Visible	0
PING	ICMP/ANY		Visible	0
RIP	UDP/520	0.0.0.0	Visible	0
SNMP	TCP/161-162 UDP/161-162	0.0.0.0	Visible	0
SSH	TCP/22	0.0.0.0	Visible	0

في هذه الصورة في الاعلى service من واجهه fortigate

Schedule -4

موجودة في Policy & Objects > schedules

تستخدم لتحديد الاوقات التي تطبق بها بوليسي معينة

في هذه الصورة يوجد طريقتين لل schedules هي :

-1 One-Time Schedule جدول زمني مرة واحدة :

- يتم تفعيل السياسة خلال فترة زمنية واحدة فقط (تاريخ ووقت محدد).
- مفيد للحالات الخاصة مثل السماح بالوصول أثناء الصيانة.

-2 Recurring Schedule جدول زمني متكرر :

- يتم تفعيل السياسة بناءً على تكرار معين (يومي، أسبوعي، شهري).
- يُستخدم عادةً للتحكم بحركة المرور خلال ساعات العمل أو أوقات معينة بشكل منتظم

Action -5

بعد تحديد كل شي من الذي ذكرناه في الاعلى

ماذا نفعل في هذه البوليسي هل نمنع او نسمح Allow or deny

- Allow
- Deny

Interface

- 1- Incoming Interface : هي الواجهة التي تستقبل البايت
- 2- Outgoing Interface : هي الواجهة التي تُرسل البايت إليها

عند إنشاء Firewall Policy على FortiGate :

تقوم بتحديد Incoming Interface لتحديد الجهة التي ستدخل منها الحزم.

تقوم بتحديد Outgoing Interface لتحديد الجهة التي ستخرج إليها الحزم.

مثال:

إذا كانت الشبكة (LAN) متصلة بالواجهة port1 ، وشبكة الإنترنت متصلة بالواجهة port2 الحزم القادمة من الأجهزة في الشبكة المحلية ستدخل عبر (Incoming Interface) port1 إذا كان هدف الحزم هو الإنترنت، فستخرج عبر (Outgoing Interface) port2. تحدد السياسات (مثل السماح/الحظر، الفحص الأمني) على أساس هذه الواجهات.

Zone interface : هي مجموعه من port or interface يتم تجميعها حتى يسهل تطبيق البولييسي

مثال :

لديك ثلاث شبكات محلية متصلة بـ FortiGate:

الشبكة 24/192.168.1.0 على الواجهة port1.

الشبكة 24/192.168.2.0 على الواجهة port2.

الشبكة 24/192.168.3.0 على الواجهة port3.

بدلاً من إنشاء سياسات منفصلة لكل واجهة، يمكنك وضع port1 و port2 و port3 في منطقة واحدة تُسمى "LAN Zone" ثم إنشاء سياسة واحدة للتعامل معها.

Zone and Multiple interface policy

إذا كان لدي port1,2,3 اريد ان يطلعون على النت شنو هي الحلول الممكنة :

1- اول حل هو ال zone اخلي بداخلة البورتات الثلاثة

2- اسوي ثلاثة بولييسي لكل بورت

3- تفعيل multiple interface policy

Address

هي العناوين المستخدمه لتحديد source و Destination في Firewall Policies

أنواع Address في FortiGate:

1. Subnet Address

- يُكتب باستخدام CIDR
- مثال 192.168.1.0/24 :يمثل جميع العناوين من 192.168.1.1 إلى 192.168.1.254.
- ملاحظة : اذا كنت اريد تحديد ip واحد فقط تتم عن طريق subnet حيث اقوم بكتابة ال ip ويكون 192.168.1.10/32 subnet /32
- مثال : بهذه الحالة يتم تعيين ip address واحد فقط وهو 192.168.1.10

2. Range Address

- يُستخدم لتحديد range من العناوين
- مثال 192.168.1.10-192.168.1.20 :

3. FQDN

- يُستخدم لتحديد عنوان استناداً إلى اسم نطاق (Domain Name)
- مثال www.example.com :
- عندما اضع نجمة في بدايه ال domain مثل *.example.com فانه يحدد جميع العناوين الفرعيه لهذا الدومين

4. Geography Address عنوان جغرافي:

- يُستخدم لتحديد منطقة جغرافية بناءً على البلد أو القارة.
- مثال :منع حركة المرور القادمة من "China"
- يتم تحديد دولة التي تأتي منها الترافيك عن طريق address ISP location ال ip الخاص ب isp
- ويتم تحديث قاعدة البيانات عن طريق fortiguard

5. MAC Address عنوان:MAC

- يُستخدم لتحديد أجهزة معينة بناءً على عنوان MAC.
- مثال 00:1A:2B:3C:4D:5E :

6. Wildcard Address

- يُستخدم لتحديد عناوين تتطابق مع نمط معين.
- مثال 192.168.1.* :يمثل جميع العناوين التي تبدأ ب 192.168.1.

ملاحظة : لا يوجد خيار ال user في destination لان خانة Destination مخصصة لتحديد عناوين الوجهة وليس المستخدمين.

الباكيت لا تذهب الى

Internet service database : هي قاعدة بيانات موجود فيها مجموعه من ال service والتطبيقات التي تعتمد على الانترنت

من اين يأتي الفورتي جيت بهذه قاعدة البيانات ؟

يأتي بها من FortiGuard

ISDB: الفائدة من استخدام

1. تبسيط السياسات:
 - بدلاً من إدخال عناوين IP يدوياً، يمكنك تحديد خدمة مثل "YouTube" أو "Microsoft Office 365" مباشرة.
2. إدارة ديناميكية:
 - قاعدة البيانات يتم تحديثها تلقائياً بواسطة Fortinet لضمان توافقها مع التغيرات في عناوين IP أو البنية التحتية للخدمات.
3. تحكم أدق في حركة المرور:
 - يمكنك السماح أو حظر حركة المرور المتعلقة بخدمة معينة دون التأثير على بقية الخدمات.
4. تحسين الأمان:
 - تقليل الأخطاء البشرية عند إعداد السياسات.
 - الحد من الحاجة إلى إدخال عناوين IP يدوياً، مما يقلل من الأخطاء الأمنية.

مثال عملي :

- السماح لموظفي الشركة باستخدام Microsoft Teams فقط.
- حظر الوصول إلى YouTube.

الحل:

1. أنشئ Policy :
 - Source: LAN subnet.
 - Destination: Internet Service > Microsoft Teams.
 - Action: Allow.
2. أنشئ Policy أخرى:
 - Source: LAN subnet.
 - Destination: Internet Service > YouTube.
 - Action: Deny.

عندما احدد ISDB لا استطيع وضع addresses معها لان ال ISDB هي تحتوي على addresses هذه من ناحية source

اما من ناحية ال destination فهي مثل السورس لكن مع عدم امكانية تحديد service لانها تحتوي بداخلها على كل ip and service

الى الان عملنا تقريبا على منع او سماح ل port , IP بمعنى 4 , 3 layer

Service

في أجهزة **FortiGate**، يتم استخدام مجموعة من الخدمات القياسية والمخصصة التي تعتمد على المنافذ (Ports) والبروتوكولات (Protocols). هذه الخدمات تُستخدم في السياسات (Policies) لتحديد حركة البيانات التي يتم السماح بها أو حظرها بناءً على نوع الخدمة.

تتكون من :

1- Protocol : مثل TCP , UDP , ICMP

2- Port : مثل 80 HTTP و 21 FTP

Create service :

service -> create new -> service -> Policy & object

بعدها نحدد البروتوكول والبورت والاسم وهكذا

Schedules

في **FortiGate**، تُستخدم **Schedules** (الجدولة) للتحكم في توقيت تطبيق السياسات (Policies) أو الخدمات المختلفة، مما يسمح بتحديد أوقات معينة لتفعيل أو تعطيل القواعد أو الخدمات بناءً على احتياجات الشبكة.

أنواع Schedules في FortiGate:

1. Recurring Schedules الجدولة المتكررة:

- تُستخدم لتحديد أوقات متكررة خلال أيام الأسبوع.
- مثال: تفعيل سياسة الوصول إلى الإنترنت فقط خلال ساعات العمل (من 8 صباحاً إلى 5 مساءً).

2. One-Time Schedules الجدولة لمرة واحدة:

- تُستخدم لتحديد فترة زمنية محددة يتم تطبيق السياسة خلالها لمرة واحدة.
- مثال: السماح بالوصول إلى خدمة معينة خلال حدث معين مثل يوم تدريبي أو اجتماع.

أمثلة على استخدام: Schedules

- حظر الإنترنت بعد ساعات العمل:
إنشاء سياسة تمنع الوصول إلى الإنترنت خارج أوقات العمل باستخدام **Recurring Schedule**.
- السماح بالوصول أثناء العطلات:
استخدام **One-Time Schedule** للسماح بالوصول إلى خادم معين خلال عطلة نهاية الأسبوع فقط.
- تحديث الأنظمة ليلاً:
تحديد جدول لتفعيل الوصول إلى تحديثات الأنظمة أو التطبيقات خلال ساعات محددة في الليل لتقليل تأثيرها على الأداء اليومي.