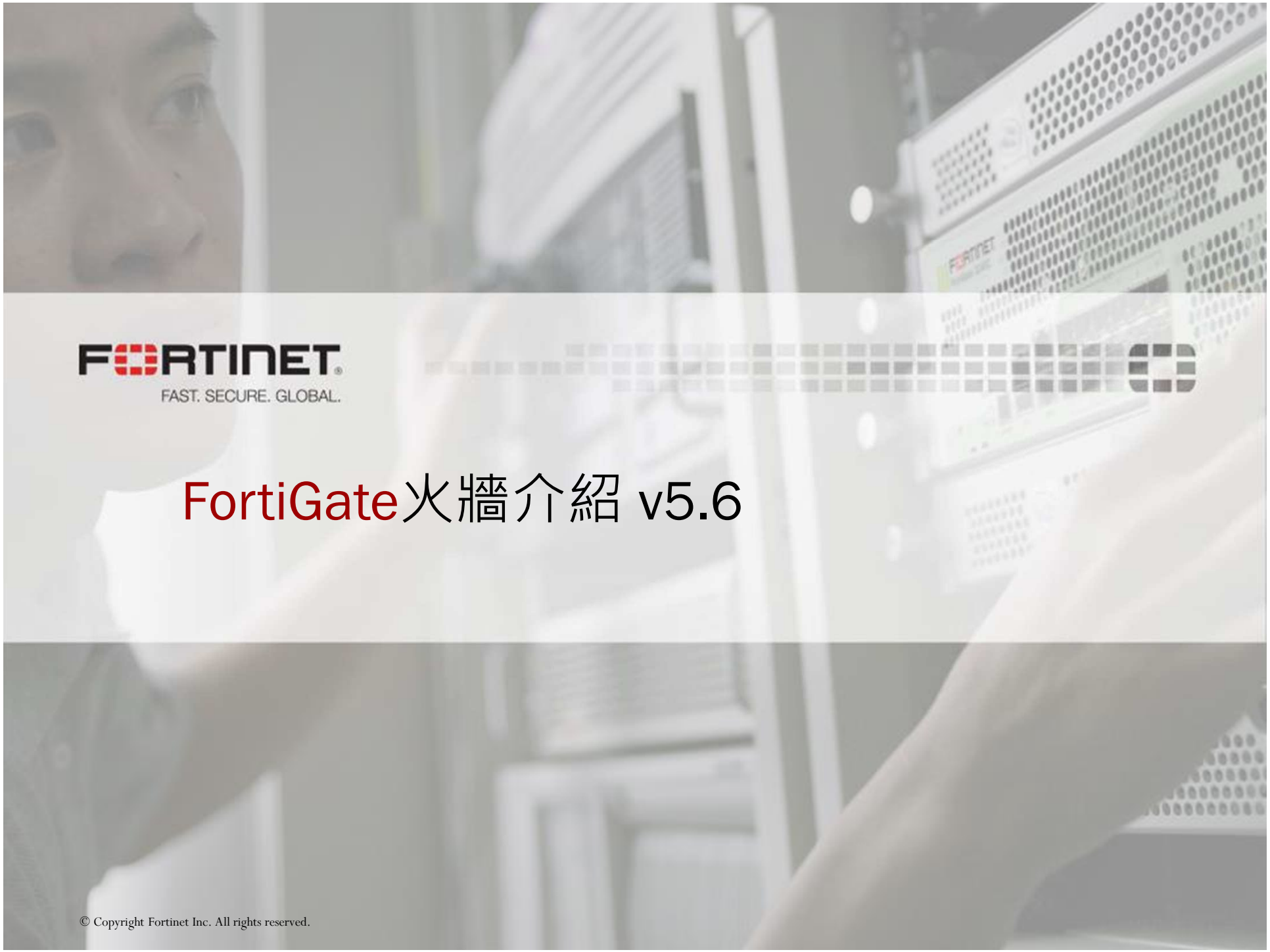


FAST. SECURE. GLOBAL.

FortiGate火牆介紹 v5.6

資深工程師：詹東隆

alva@sintel.com.tw

博聯資訊有限公司 Sintel Information Inc.

www.sintel.com.tw

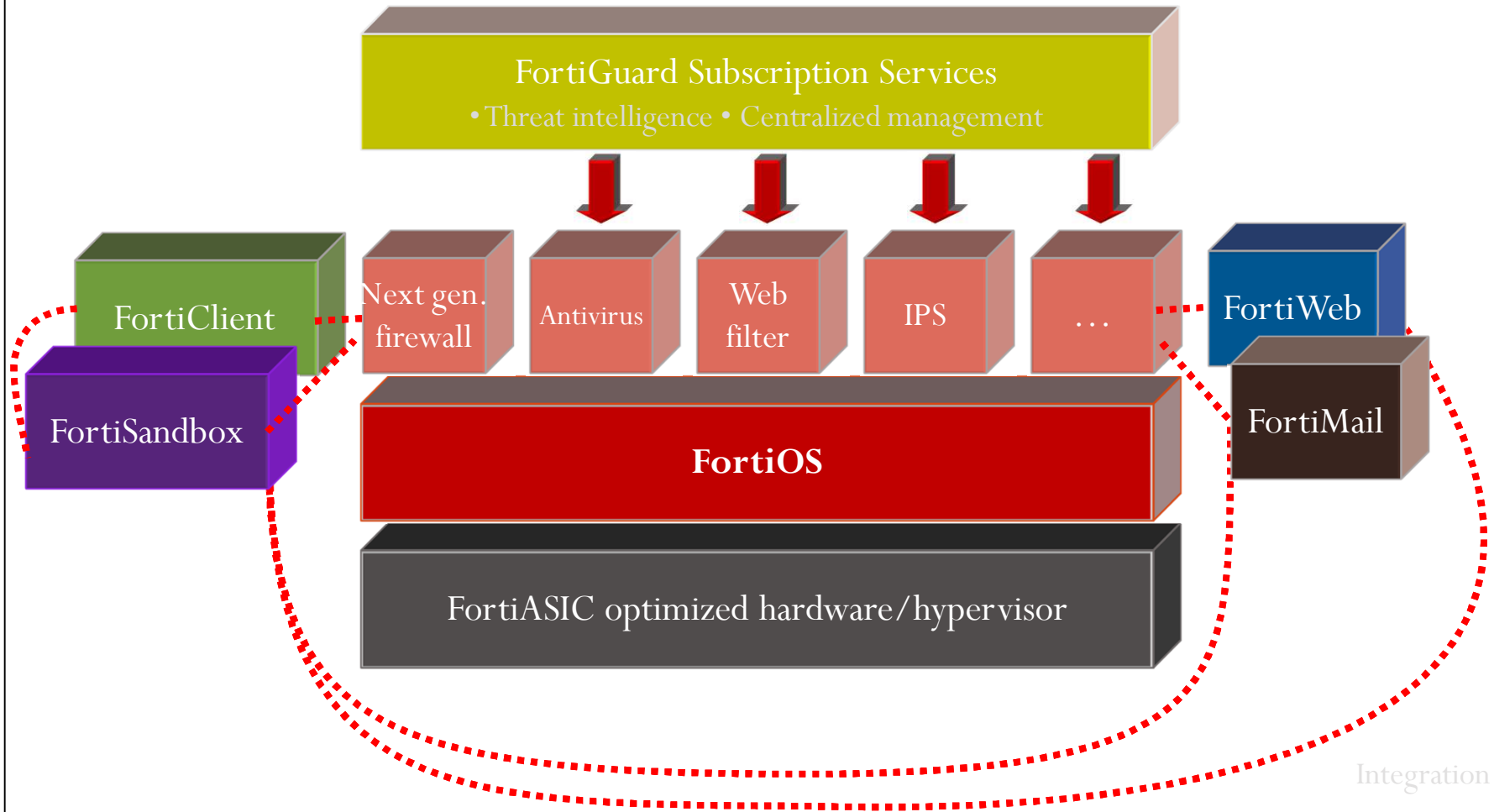
宜蘭縣羅東鎮中華路57-2號四樓之二 T 03-9568441 F 03-9548424

內容

- 前置基礎作業設定
- 設備管理權限
- 防火牆規則政策定義
- 防火牆規則政策 - 設定 & 管理
- NAT & 記錄
- 策略路由

Platform Design

FortiGate 次世代防火牆、UTM平台



處理器提供極高的性能、超低延遲和 (**Content processors & Network processors**)

前置基礎作業設定

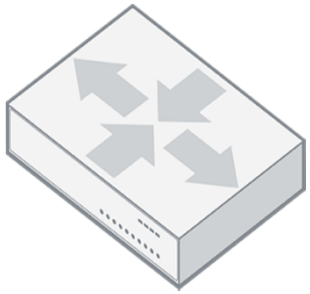
Objectives

- Identify the factory defaults
- Select an operation mode
- Understand FortiGate's relationship with FortiGuard and distinguish between live queries and package updates

Modes of Operation

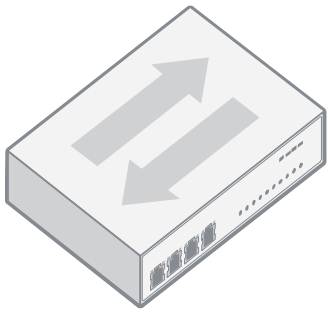
NAT (routing)

- FortiGate is an OSI Layer 3 **router**
- Interfaces have IP addresses
- Packets are routed by IP



Transparent(switching)

- FortiGate is an OSI Layer 2 **switch** or **bridge**
- Interfaces do *not* have IPs
- Cannot route packets, only forward or block

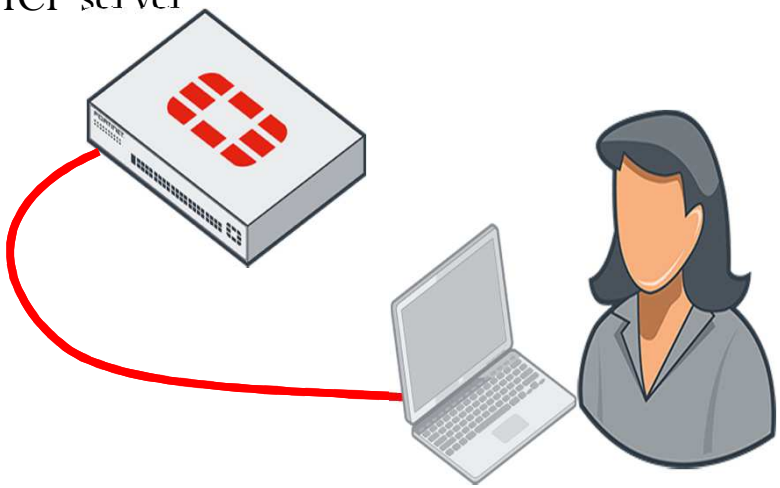


Factory Default Settings

- Port1 or internal interface IP: **192.168.1.99/24**
- PING, HTTP, HTTPS, and SSH protocol management enabled
- Built-in DHCP server is enabled on port1 or internal interface
  - Only on entry-level models that support DHCP server
- Default login:

  User: admin

  Password: (blank)
  - *Both* are case sensitive
  - Modify the default (blank) root password
- Can access FortiGate on the CLI
  - Console: without network
  - CLI Console widget and terminal emulator, such as PuTTY or Tera Term
  - # cli : show system interface



FortiGuard Subscription Services

- Internet connection and contract required
- Provided by FortiGuard Distribution Network (FDN)
  - Major data centers in North America, Asia, and Europe
    - Or, from FDN through your FortiManager
  - FortiGate prefers data center in nearest time zone, but will adjust by server load
- Package updates: FortiGuard Antivirus and IPS
  - update.fortiguard.net
  - TCP port 443 (SSL)
- Live queries: FortiGuard Web Filtering, DNS Filtering, and Antispam
  - service.fortiguard.net
  - Proprietary protocol on UDP port 53 or 8888

設備管理權限

Objectives

- Manage administrator profiles
- Manage administrative users
- Define the configuration method for administrative users
- Control administrative access to the FortiGate GUI and CLI
- Manage specific aspects of the network interfaces

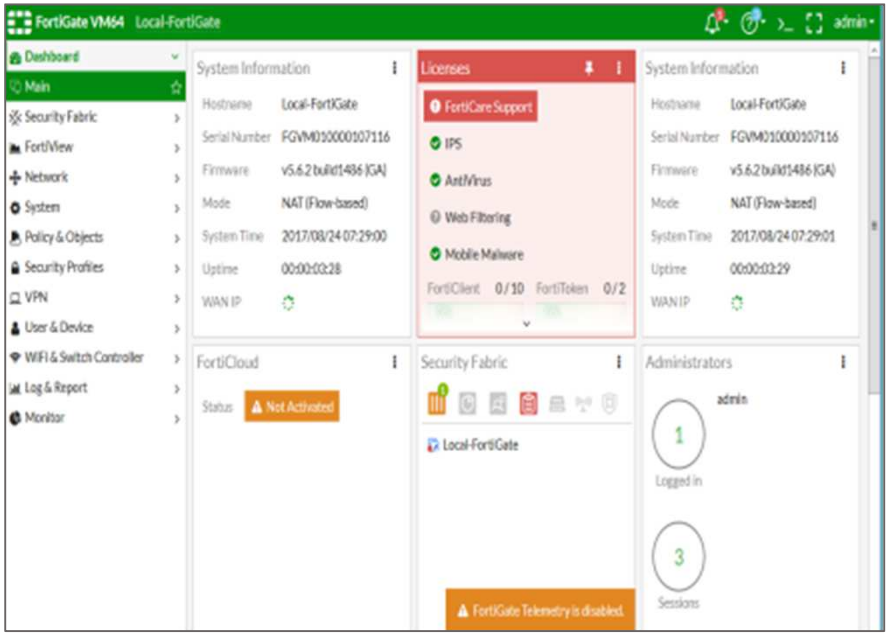
管理方式

CLI

Console, SSH, Telnet, GUI Widget

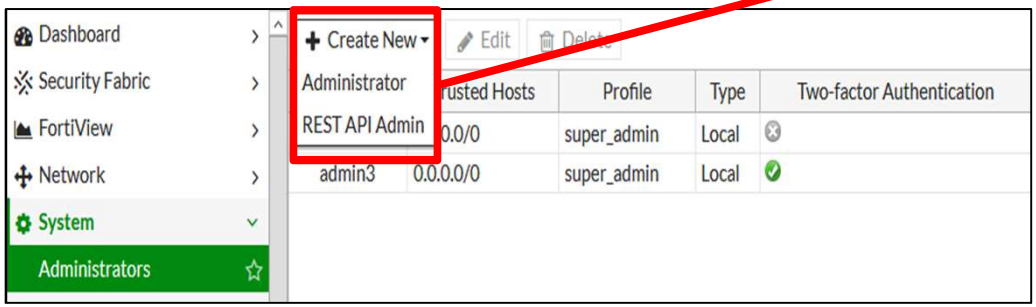
GUI

FortiExplorer, Web Browser (HTTP, HTTPS)

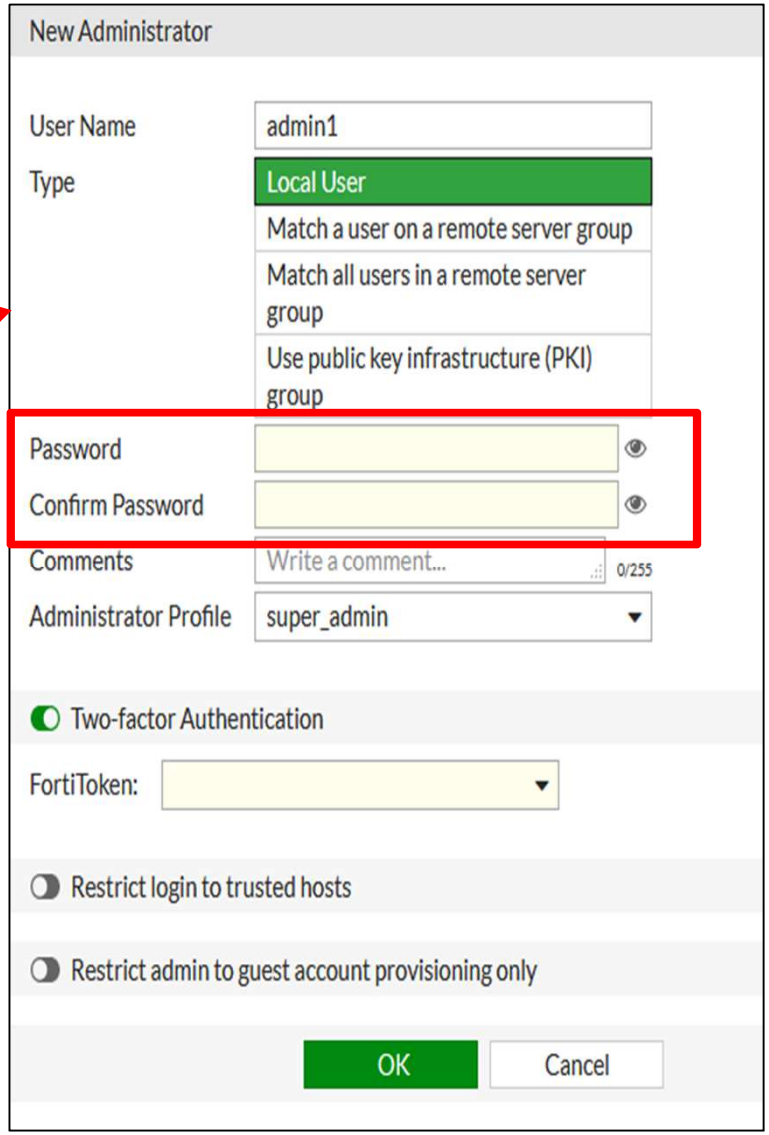


Create an Administrative User

System > Administrators

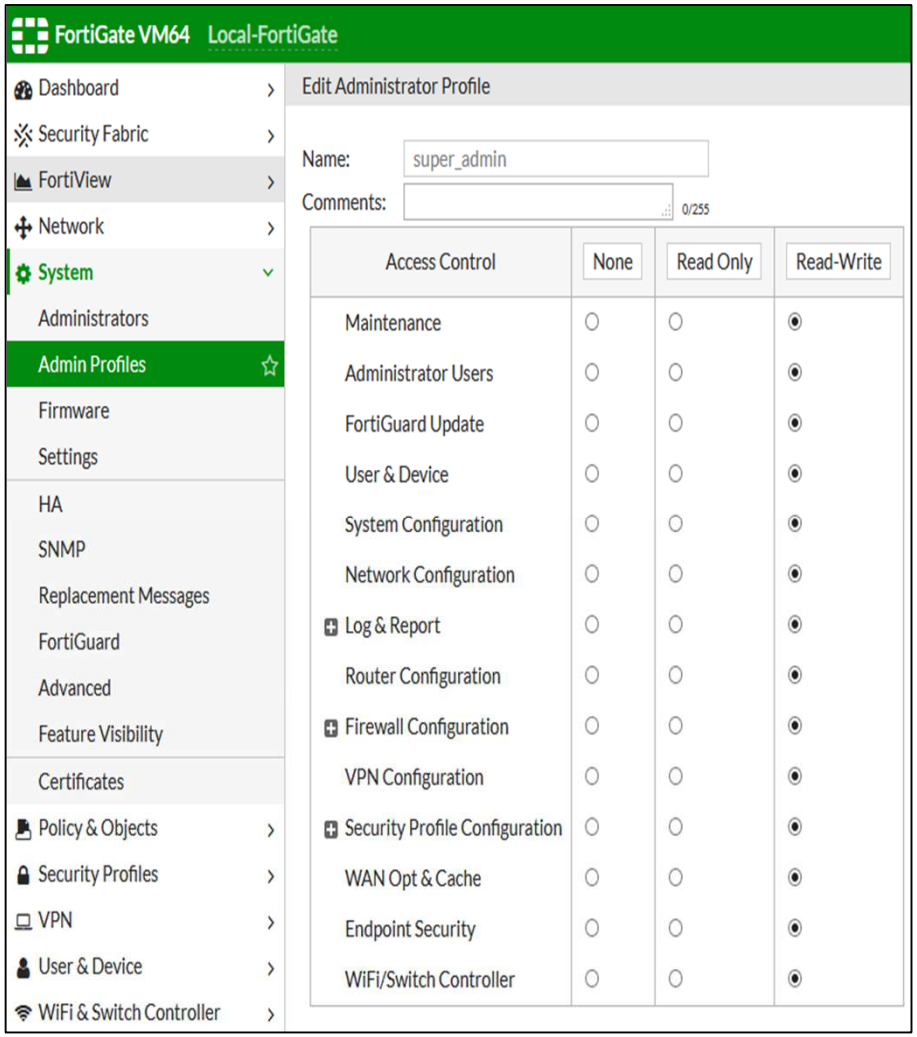


REST API

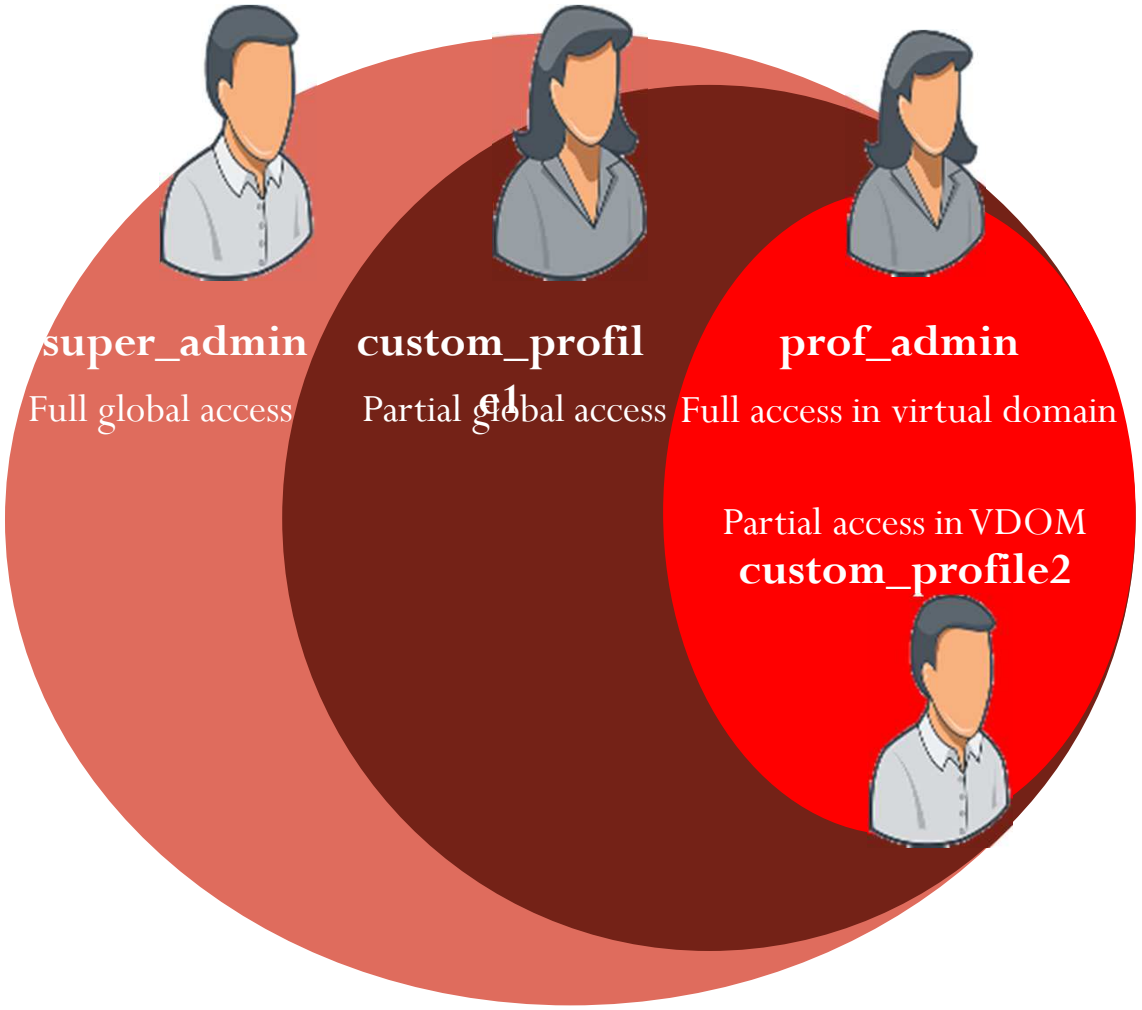


Administrator Profiles: Permissions

System > Admin Profiles

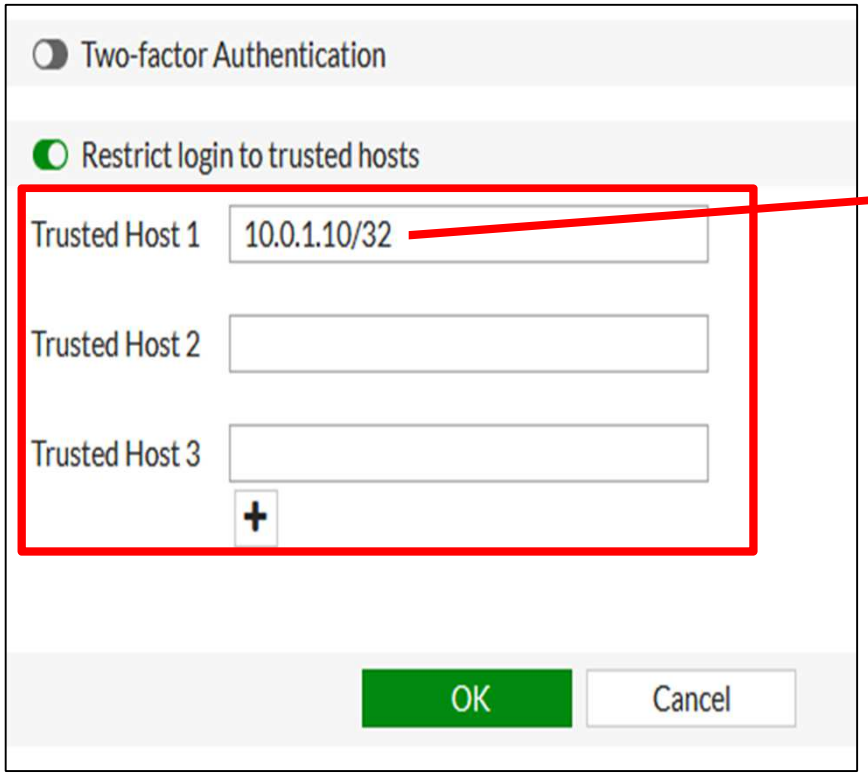


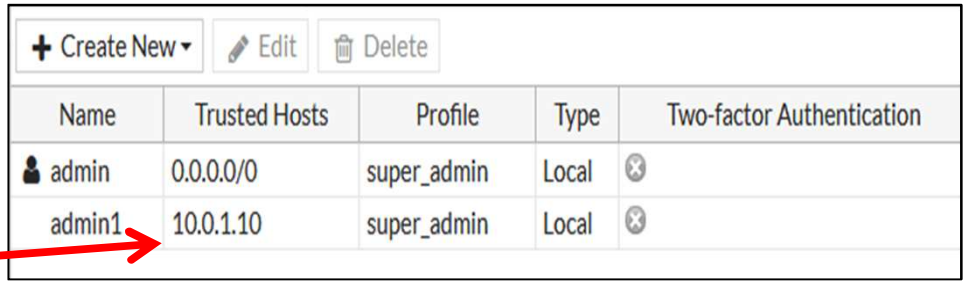
Administrator Profiles: Hierarchy

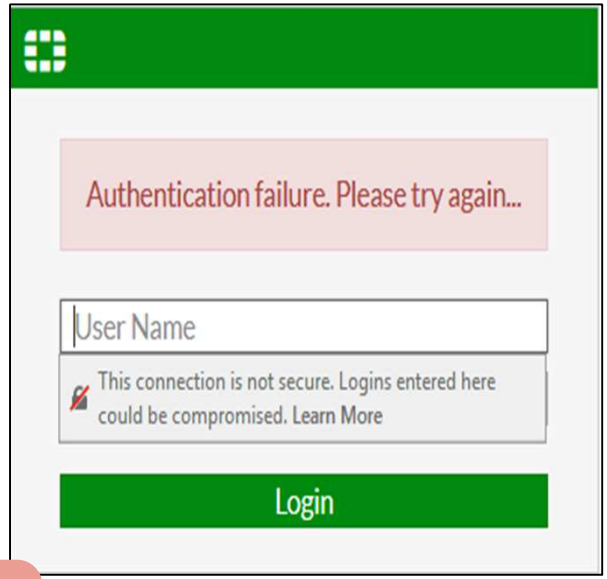


Administrative Access: Trusted Sources

System > Administrators





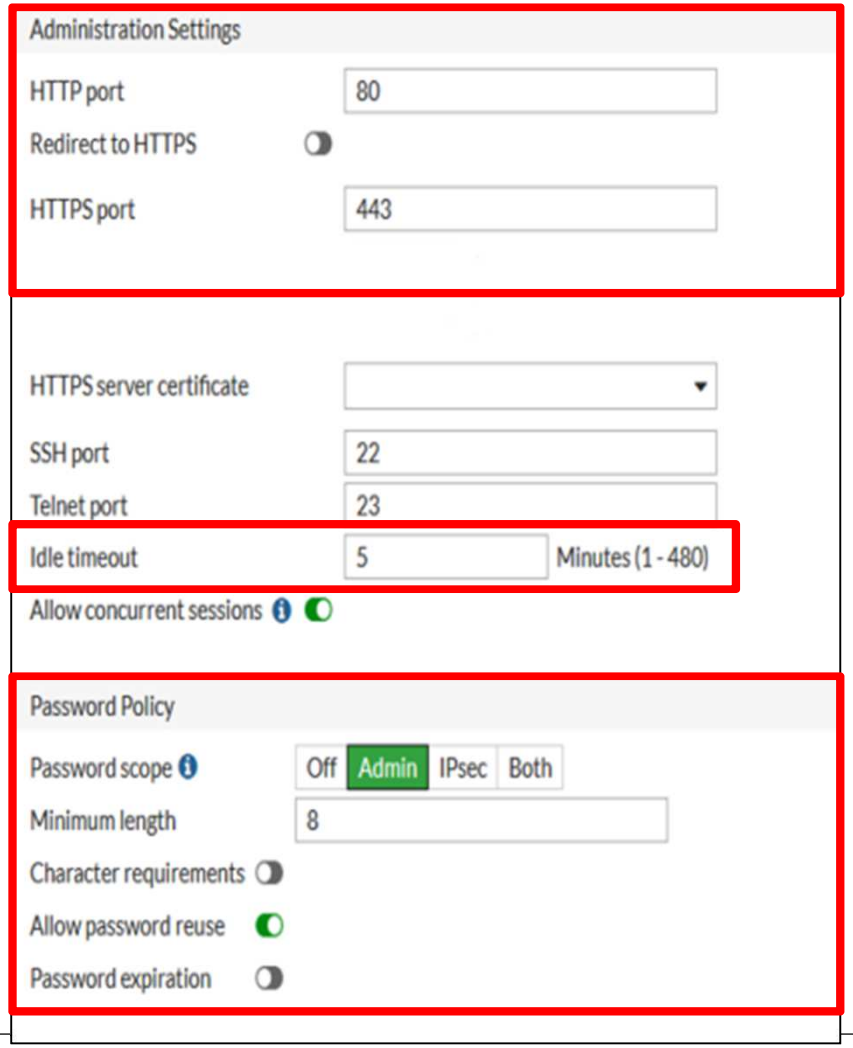


If **admin1** attempts to log in to the FortiGate GUI from any IP other than `10.0.1.10`, they receive this message.

Administrative Access: Ports and Password

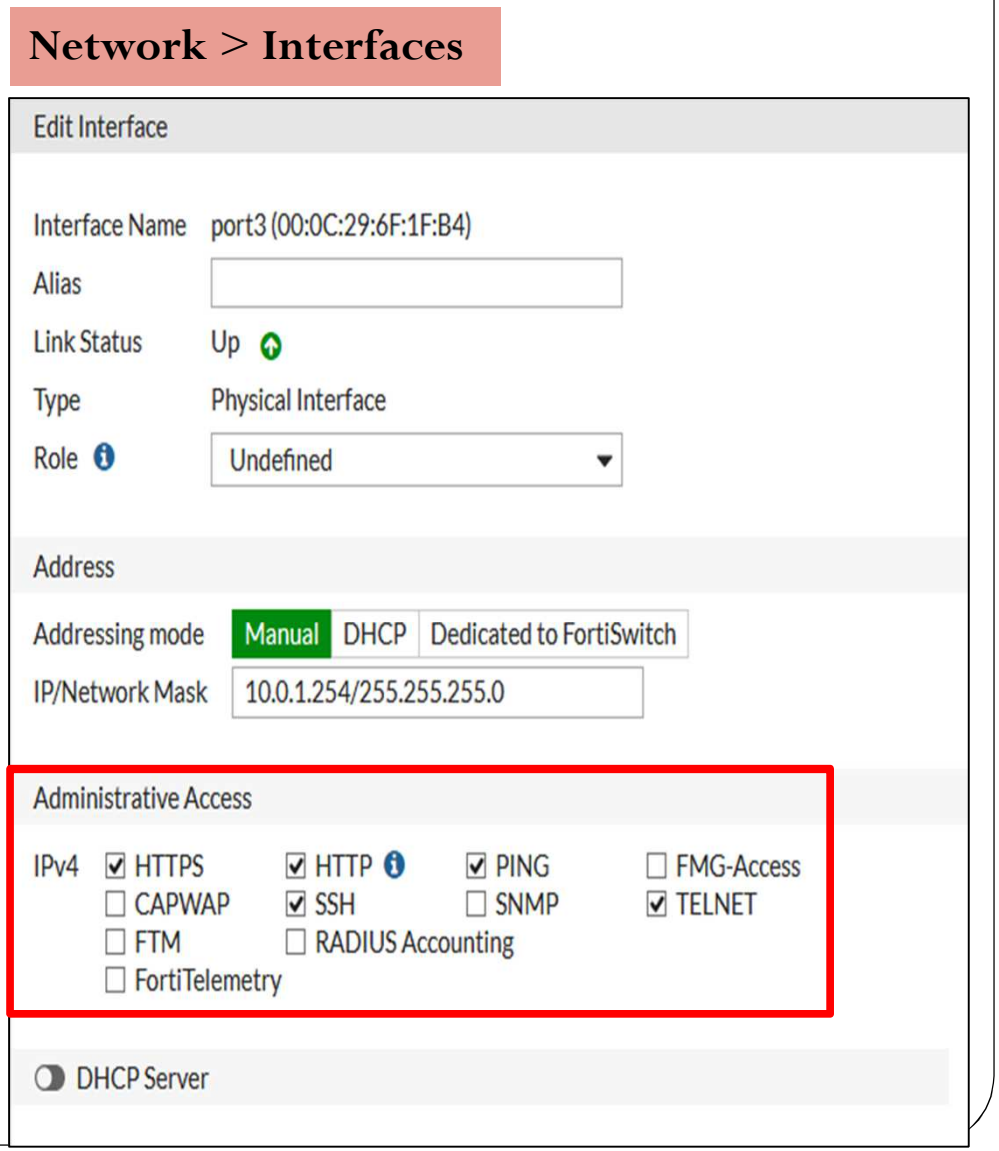
- Port numbers are customizable.
- Using only secure access (SSH, HTTPS) is recommended.
- Default **Idle timeout** is 5 minutes.
- 變更管理埠

System > Settings



Administrative Access: Protocols

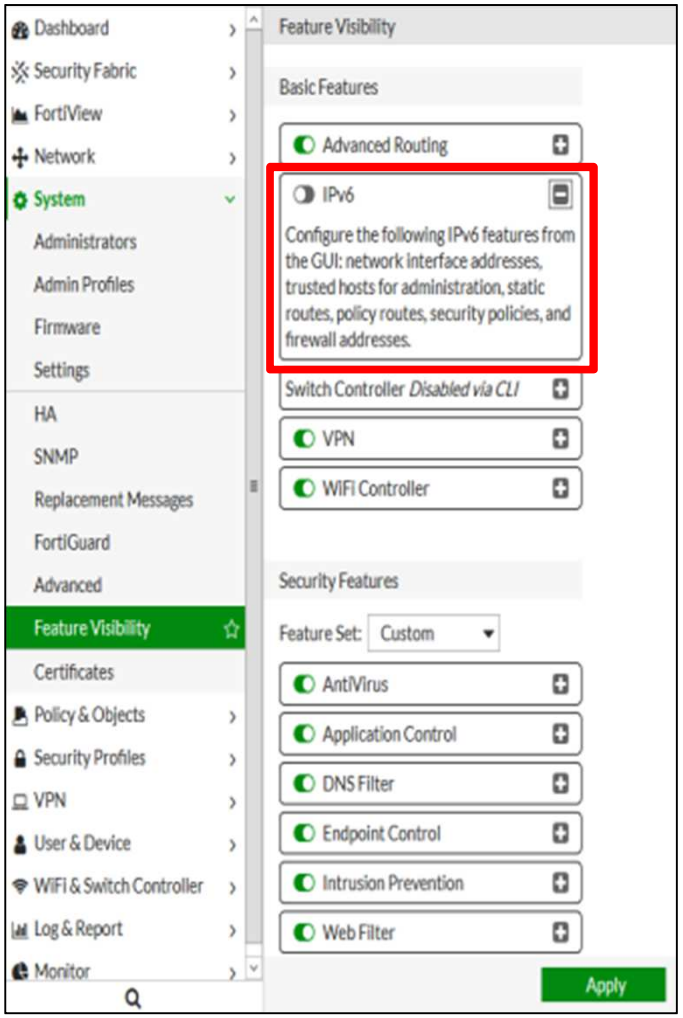
- Enable acceptable management protocols on each interface independently:
  - Separate IPv4 and IPv6
  - IPv6 options hidden by default
- Also protocols where FortiGate is the destination IP:
  - FortiTelemetry
  - CAPWAP
  - FMG-Access
  - FTM(Fortinet Security Fabric)
  - RADIUS Accounting



Features Hidden by Default

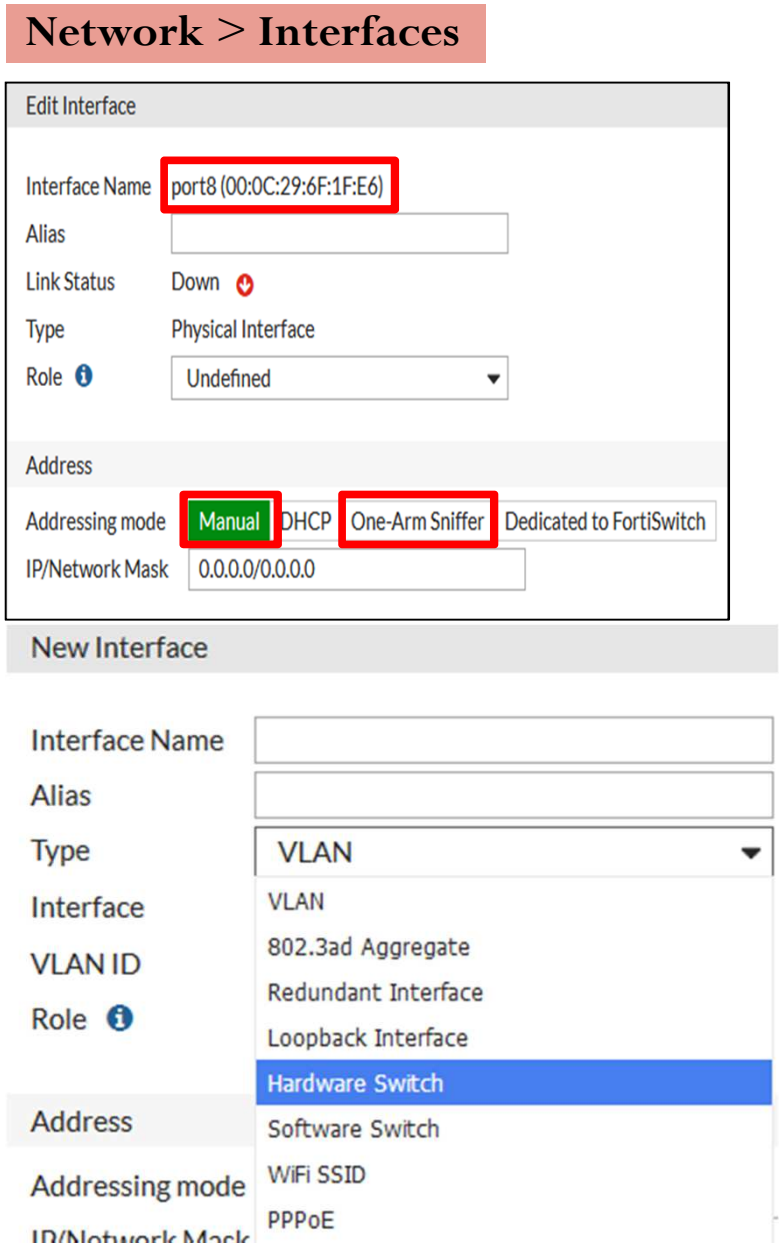
- By default, some features like IPv6 are hidden on the GUI.
  - Hidden features are not disabled.
- In **Feature Visibility**, select to hide/show groups of features commonly used together.

System > Feature Visibility



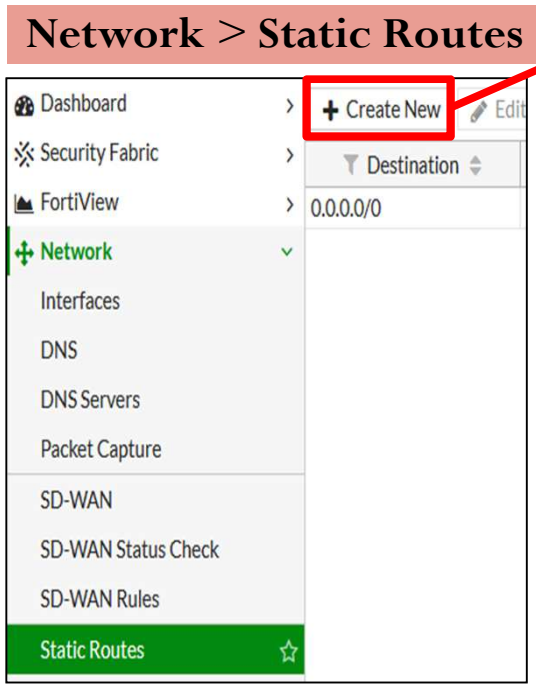
Interface IPs

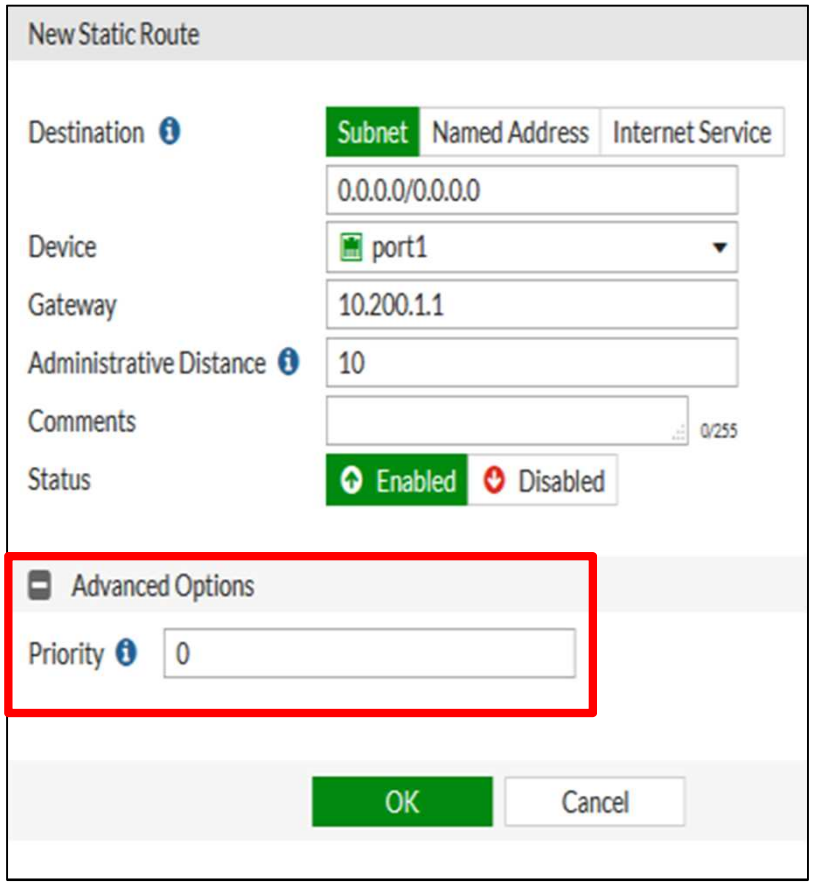
- In NAT mode, interfaces cannot be used until they have an IP address:
  - Manually assigned
  - Automatic
    - DHCP
    - PPPoE
- Exceptions: **Dedicate to FortiSwitch** and the **One-Arm Sniffer**
- Interface , ZONE, vwpair
- **Type …..**



Static Gateway

- Must be at least one default gateway
- If the interface is DHCP or PPPoE, the gateway can be added dynamically.

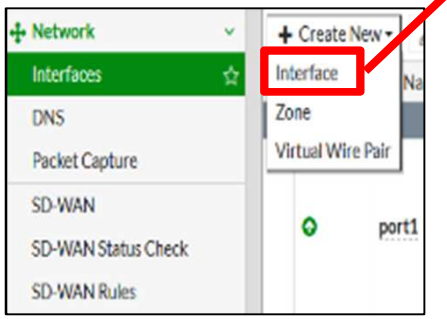


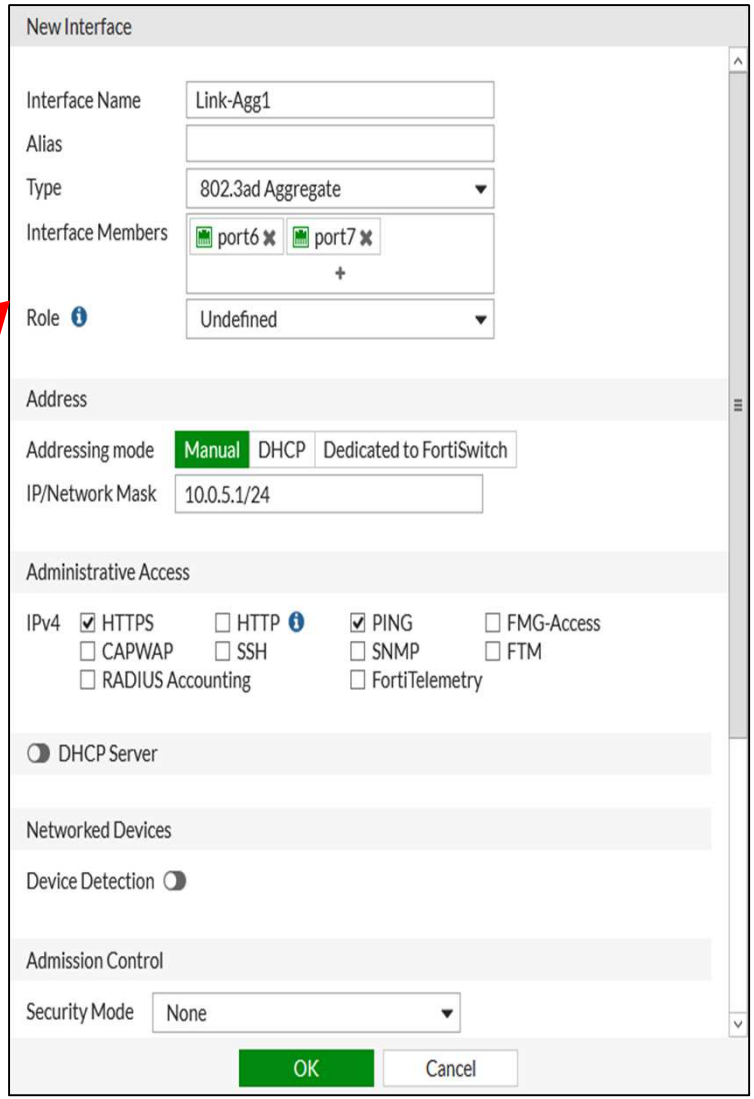


Link Aggregation

- Bundles several physical ports to form a single point-to-point logical channel with greater bandwidth.
  - Increases redundancy for higher availability

Network > Interfaces





防火牆規則政策定義

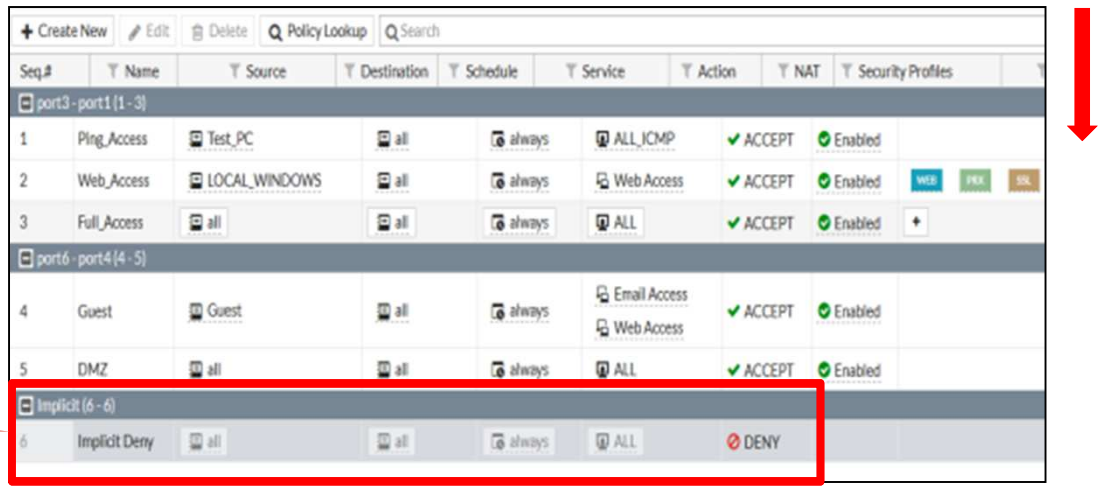
Objectives

- Identify components of firewall policies
- Identify how FortiGate matches traffic to firewall policies

What Are Firewall Policies?

- Policies define:
  - Which traffic matches them
  - How to process traffic that matches
- When a new IP session packet arrives, FortiGate:
  - Starts at the top of the list to look for a policy match
  - Applies the first matching policy
- **Implicit Deny**
  - No matching policy?
    FortiGate drops packet

Policy & Objects > IPv4 Policy



Implicit Deny

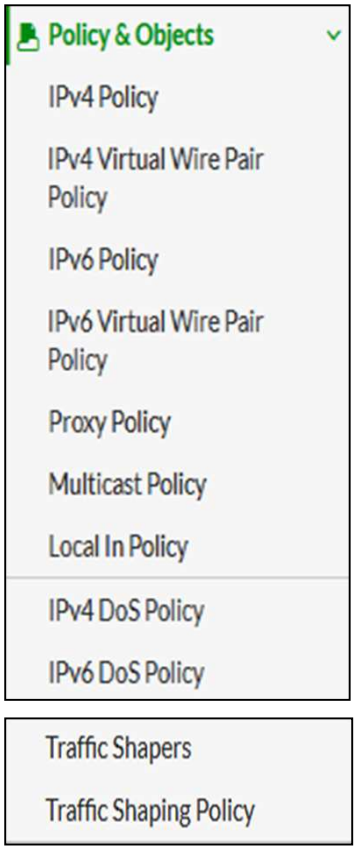
Components and Policy Types

Objects used by policies

- Interface and interface groups
- Address, user, device, and Internet service objects
- Service definitions
- Schedules
- NAT rules
- **Security profiles**

Policy types

- IPv4, IPv6
- Virtual wire pair (IPv4, IPv6)
- Proxy
- Multicast
- Local In Policy (Origin and destination is FortiGate itself)
- DoS (IPv4, IPv6)
- Traffic shaping

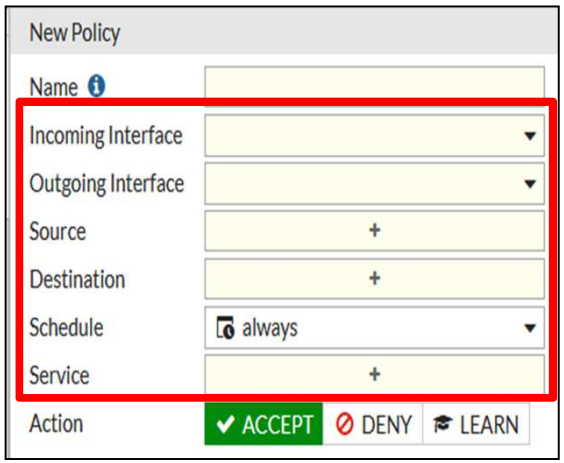


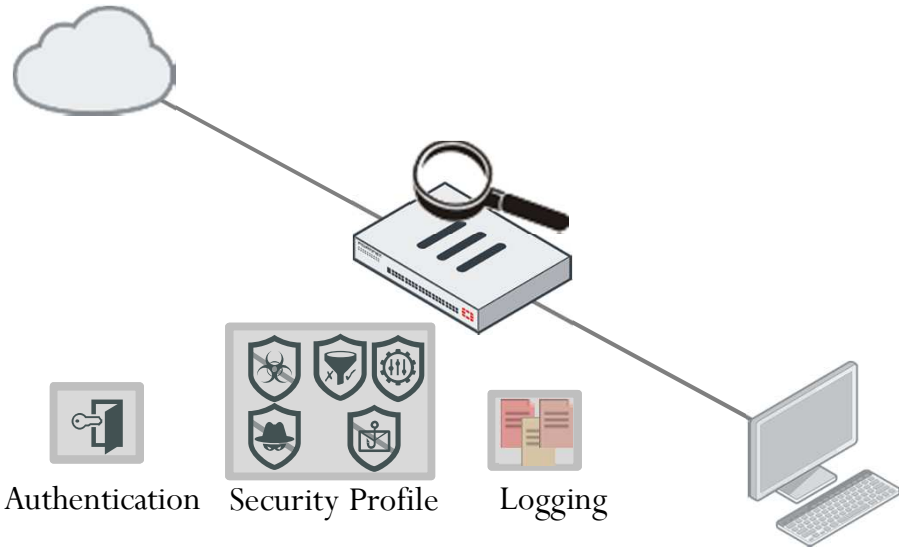
How Are Policy Matches Determined?

- Incoming and outgoing interfaces ✓
- Source: IP address, user, device ✓
- Destination: IP address or Internet Services ✓
- Services ✓
- Schedules ✓

Action = ACCEPT or DENY

Policy & Objects > IPv4 Policy

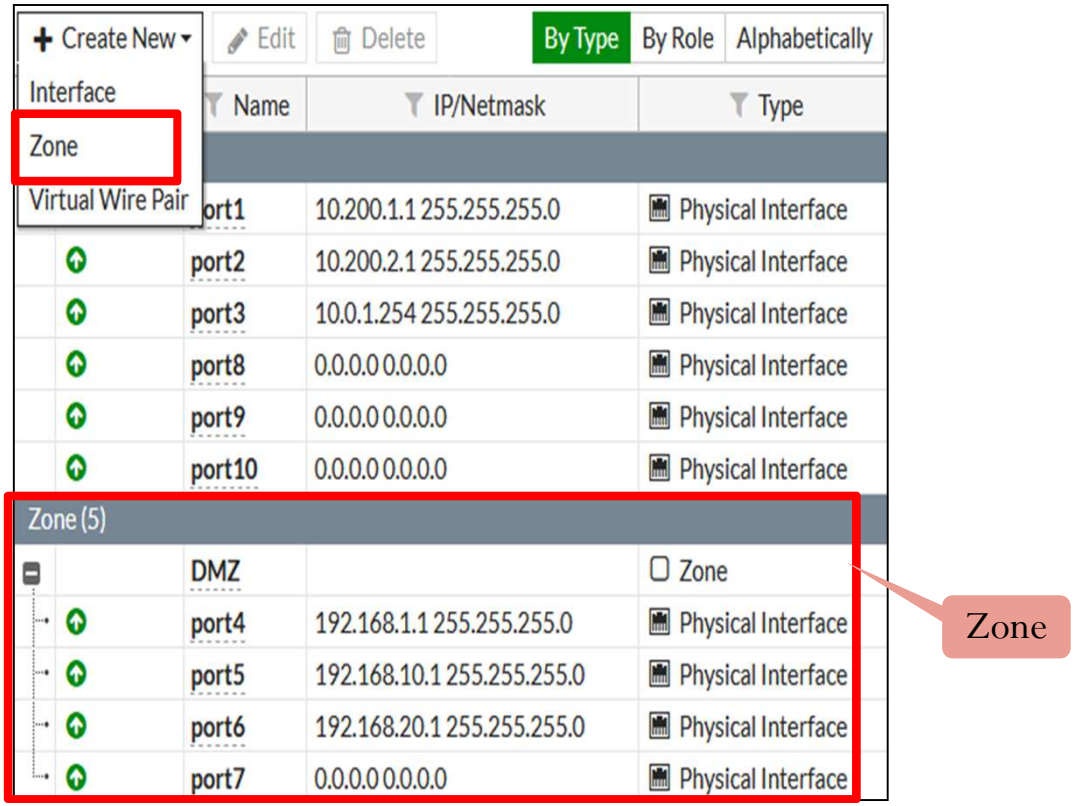


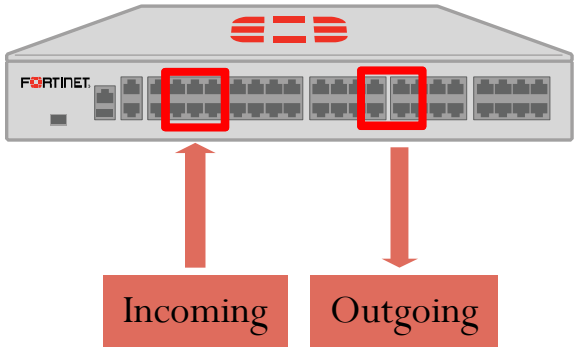


Simplify–Interfaces and Zones

- **Incoming Interface** and **Outgoing Interface** can be interface(s) or a zone
  - Zone: Logical group of interfaces
- To match policies with traffic, select one (or more) interfaces or **any** interface

Network > Interfaces

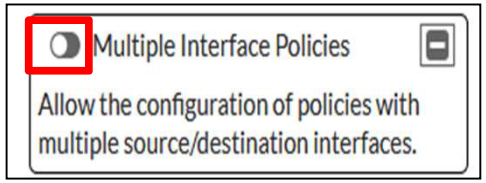




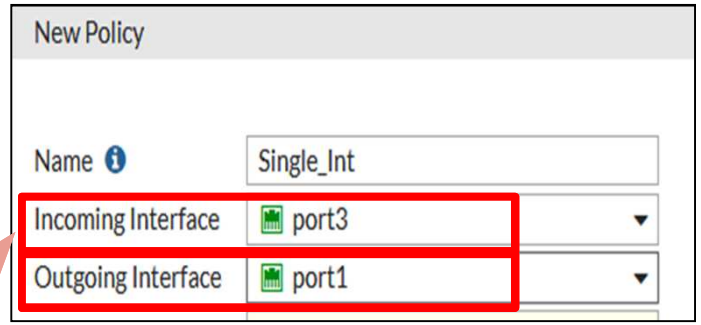
Selecting Multiple Interfaces or Any Interface

- Disabled by default
  - Cannot select multiple interfaces or any interface in firewall policy from the GUI
- Can be made visible in the GUI

System > Feature Visibility

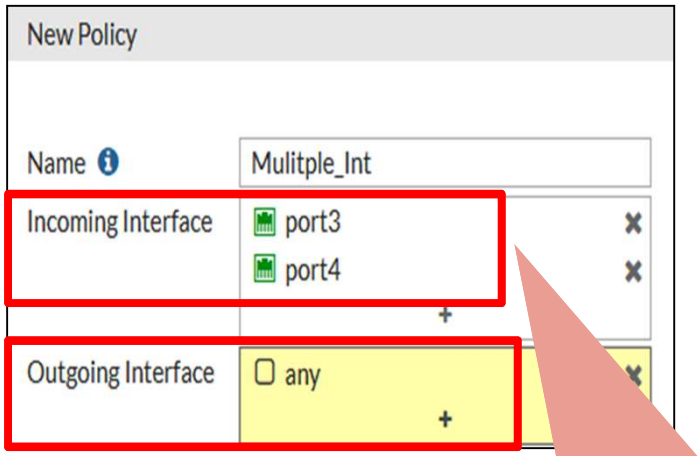


Policy & Objects > IPv4 Policy



Multiple interface policies disabled

Policy & Objects > IPv4 Policy



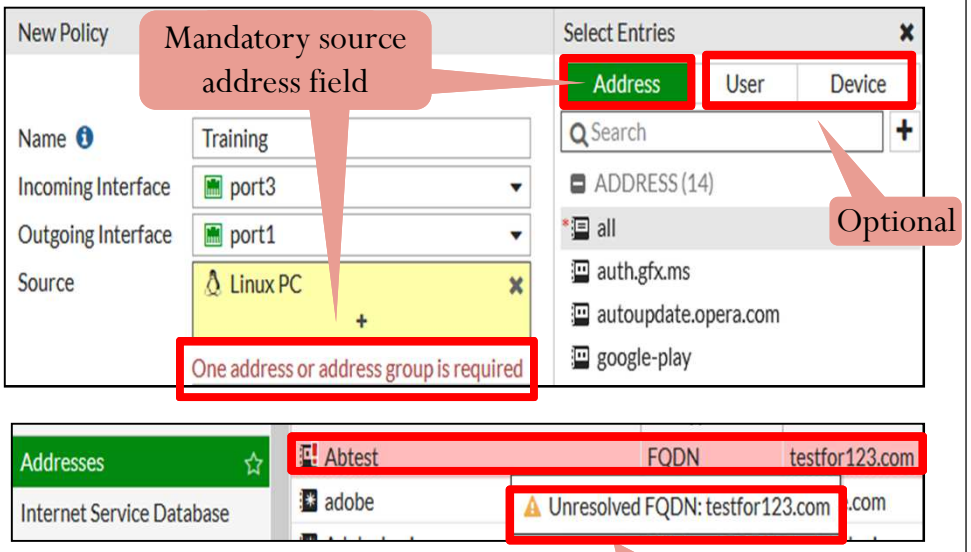
Multiple interface policies enabled

Matching by Source

- *Must* specify at least one source (address)
- *May* specify either, neither, or both:
  - Source User
  - Source Device

- Source Address
  - IP address or range
  - Subnet (IP/Netmask)
  - FQDN
  - Geography

Policy & Objects > IPv4 Policy

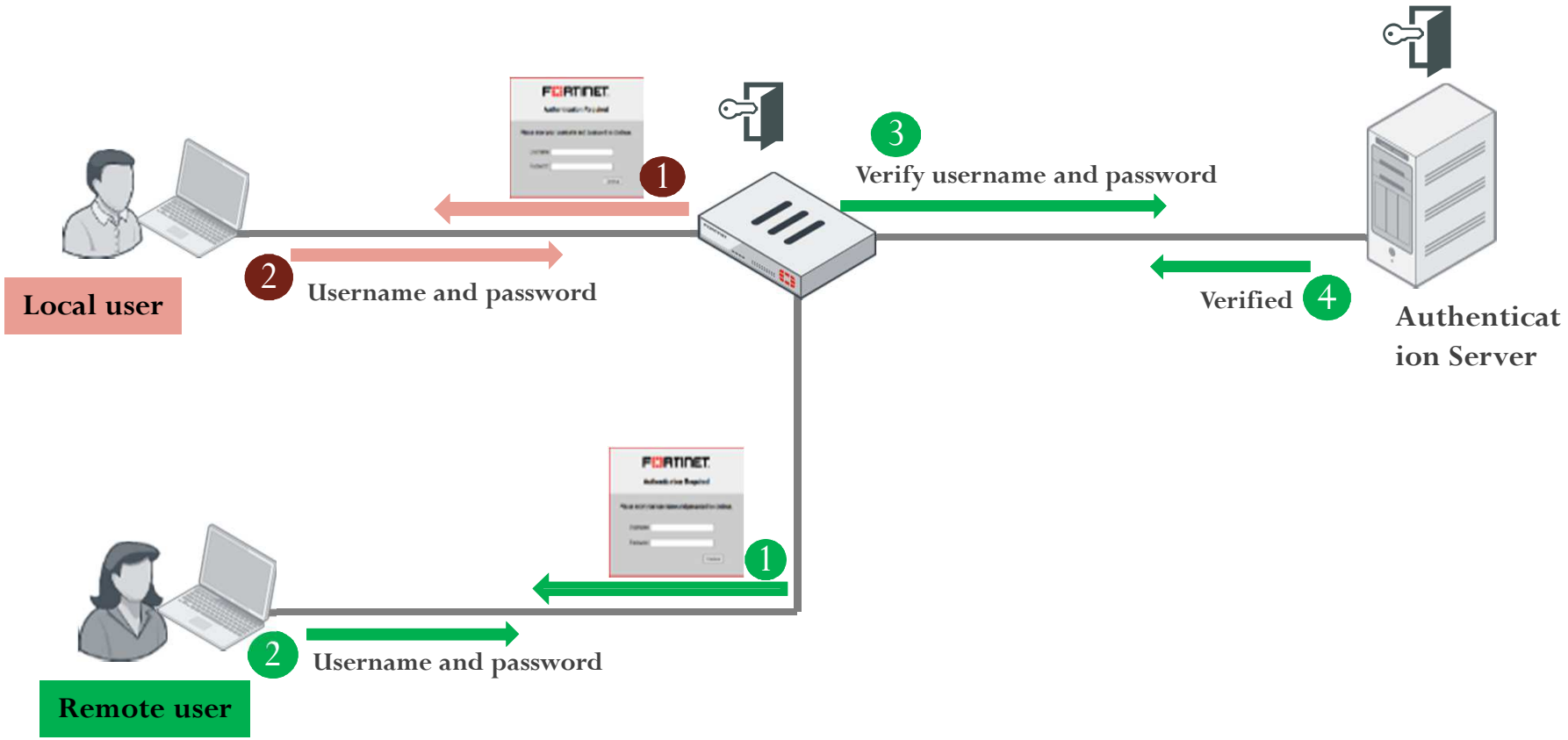


- Source User–Individual user or user group. This may refer to:
  - Local firewall accounts
  - Accounts on a remote server (for example, Active Directory, LDAP, RADIUS)
  - FSSO
  - Personal certificate (PKI-authenticated) users

- Source Device–Identified or manually defined client device
  - Enables device identification on the source interface

Source-User Identification

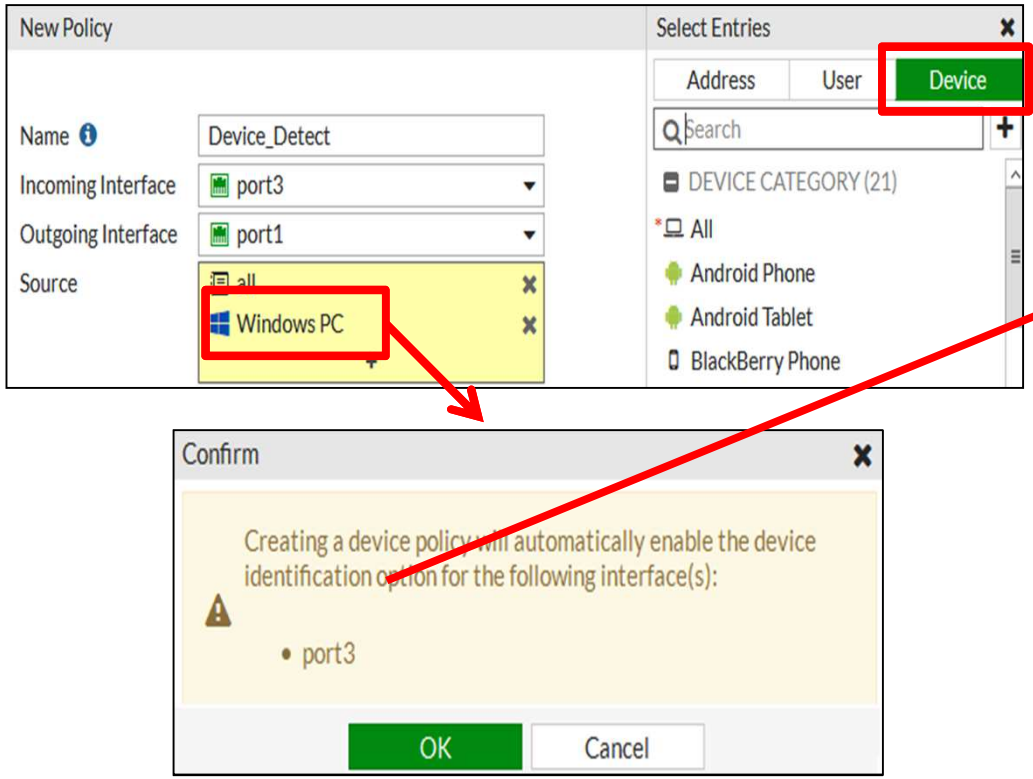
- Confirms identity of user
- Access to network is provided after confirming user credentials



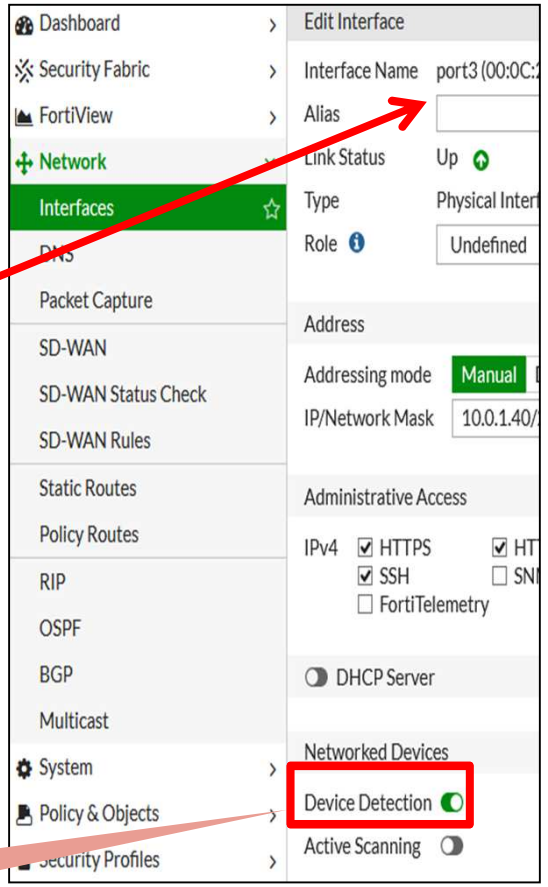
Device Identification

- **Source Device** type enables **Device Detection** on the source interface(s) of that policy

Policy & Objects > IPv4 Policy



Network > Interfaces



Can enable **Active Scanning**

Device Identification: Device List (GUI and CLI)

- Detected devices are saved in the FortiGate flash drive for 28 days
  - A device expires and is removed from the **Device Inventory** list if no traffic is seen for that device
  - Can change the duration on the CLI

```
config system settings
set discovered-device-timeout <days>
end
```

User & Device > Device Inventory


```
Local-FortiGate # diagnose user device list
Hosts
vd root/0   00:0c:29:e0:c1:87   ...
created 575s   gen 82   seen 1s   port3   gen 68
ip 10.0.1.10   src http
type 17 'Windows PC'   src http   ...

vd root/0   00:0c:29:64:ca:2c   ...
created 311s   gen 91   seen 52s   port3   gen 70
ip 10.0.1.39   src arp
type 17 'Windows PC'   src forticlient   ...
os 'Windows'version 'Server' src forticlient
endpoint 2 'EBE211861C2E4628946B2BDD1DEAED32'
```

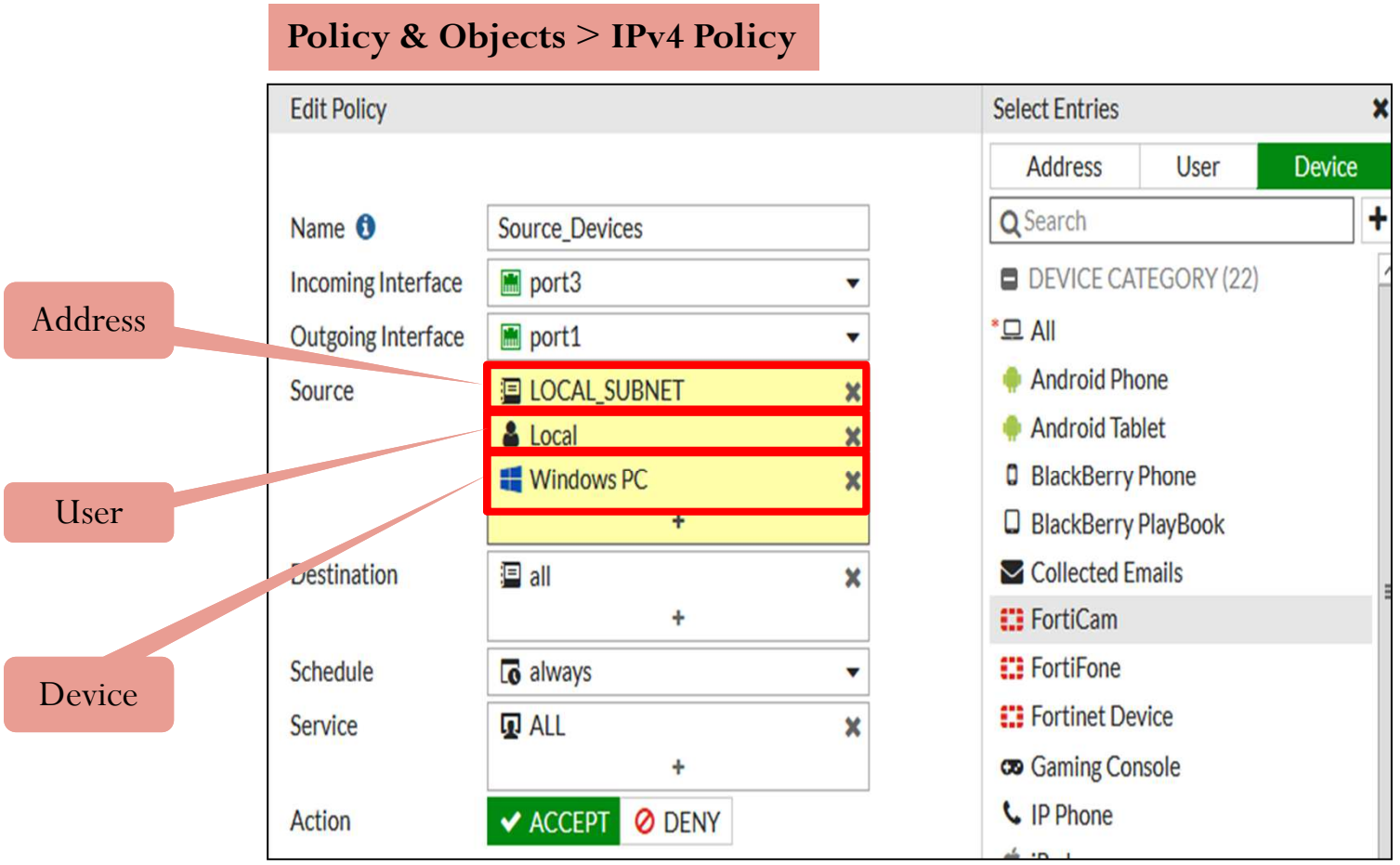
Detected devices

Detection method

Detection method

Example–Matching Policy by Source

- Matches by source address, user, and device type



Matching by Destination

Like source, destination criteria can use:

- Address objects:
  - Subnet (IP or netmask)
  - IP address or address range
  - FQDN
    - DNS query used to resolve FQDN
  - Geography
    - Country defines addresses by ISP's geographical location
    - Database updated periodically through FortiGuard
- Internet service database (ISDB) objects

Internet Services

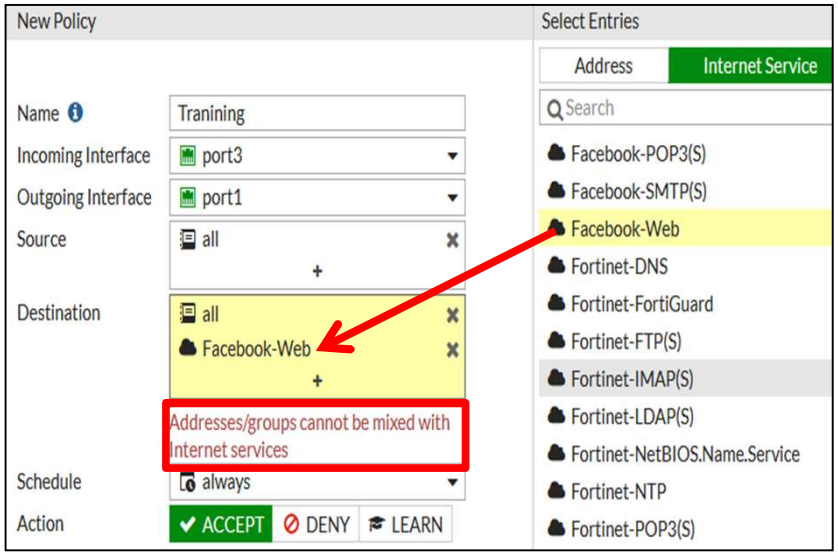
- Database that contains IP addresses, IP protocols, and port numbers used by the most common Internet services
  - Regularly updated through FortiGuard

Policy & Objects > Internet Service Database

Name	Protocol Number	Port	# of Entries
LinkedIn-Web	TCP	80,443	2496
LogMeIn-DNS	UDP	53	3
LogMeIn-NetBIOS.Name.Service	UDP	137	6
LogMeIn-SMTP(S)	TCP	25,465,587,2525	3
LogMeIn-Web	TCP	80,443	1095

- Can be used as **Destination** in the firewall policy
- If **Internet Service** is selected as **Destination**:
  - You cannot use **Address** in the **Destination**
  - You cannot select **Service** in the firewall policy

Policy & Objects > IPv4 Policy

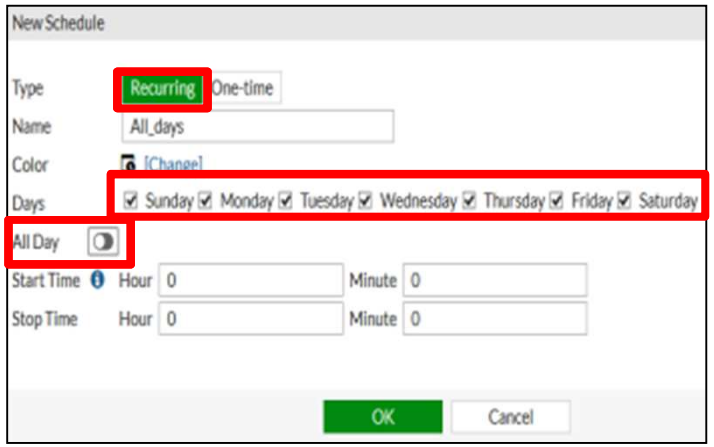


Scheduling

- Policies apply only during specific times and days
  - Example: A less restrictive *lunch time* policy
  - Default schedule applies all the time

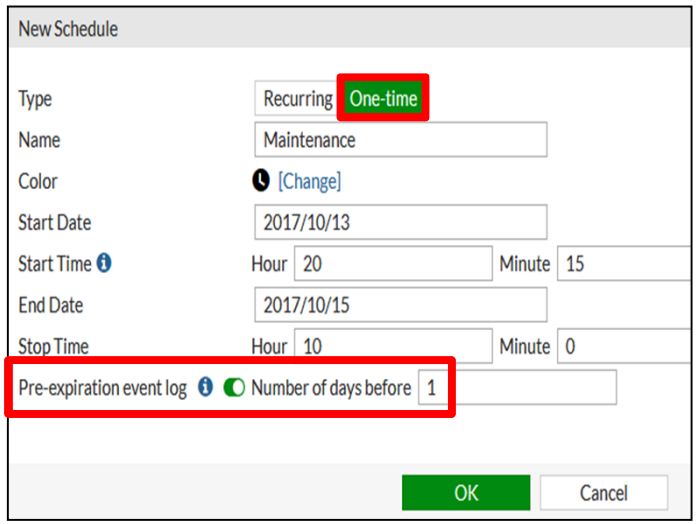
- Recurring
  - Happens every time during specified day(s) of the week

Policy & Objects > Schedules



- One-time
  - Happens only once

Policy & Objects > Schedules



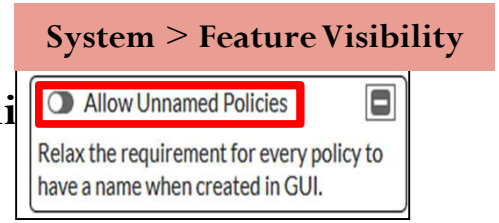
設定 - 防火牆規則政策

Objectives

- Restrict access and make your network more secure using security profiles
- Configure logging
- Configure learning mode to evaluate and analyze traffic

Configuring Firewall Policies

- Mandatory policy name when creating on GUI
  - Can relax the requirement by enabling **Allow Unnamed Poli**



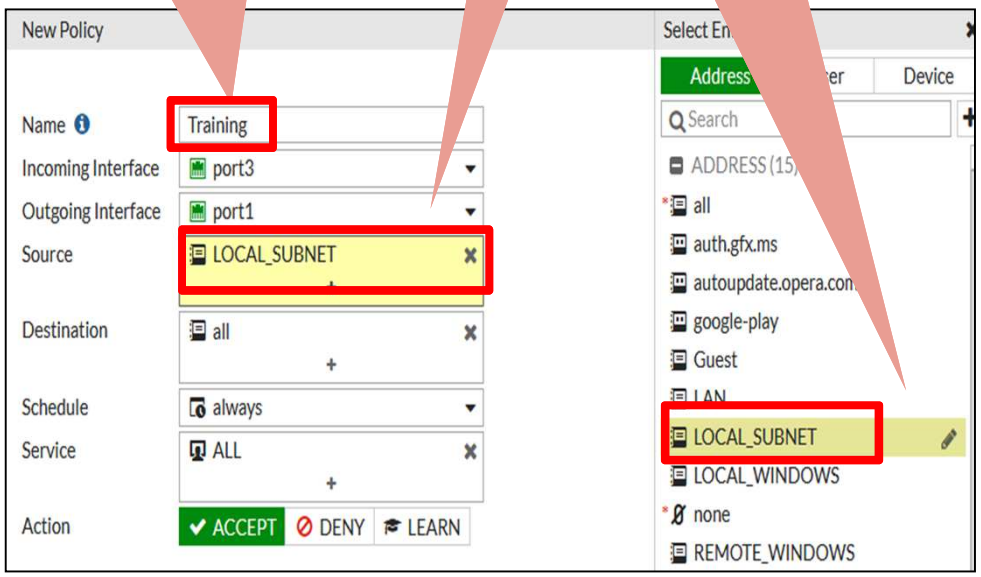
- Flat GUI view allows:
  - Select by clicking
  - Drag-and-drop

```
config firewall policy
 edit 1
  set name "Training"
  set uuid 2204966e-47f7-51..
```

Universally Unique Identified (UUID)

Enabled by default
MUST specify unique name

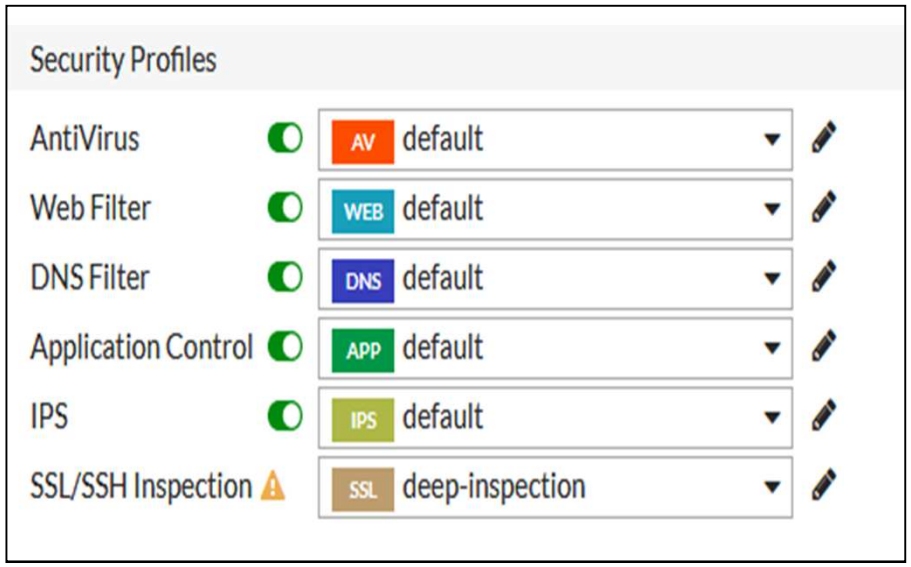
Highlights selected entry



Security Profiles

- Firewall policies limit access to configured networks
- Security profiles configured in firewall policies protect your network by:
  - Blocking threats
  - Controlling access to certain applications and URLs
  - Preventing specific data from leaving your network

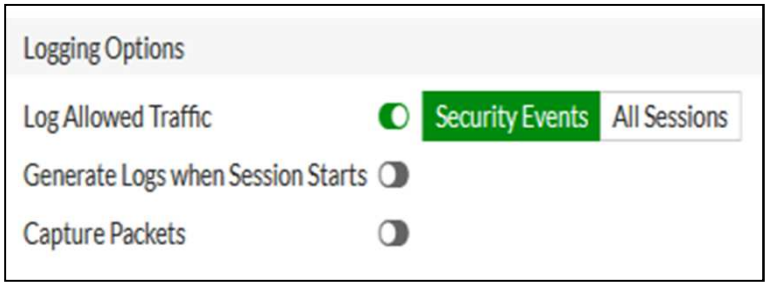
Policy & Objects > IPv4 Policy



Logging

- By default, set to **Security Events**
  - Generates logs based on applied security profile only
- Can change to **All Sessions**

Accept

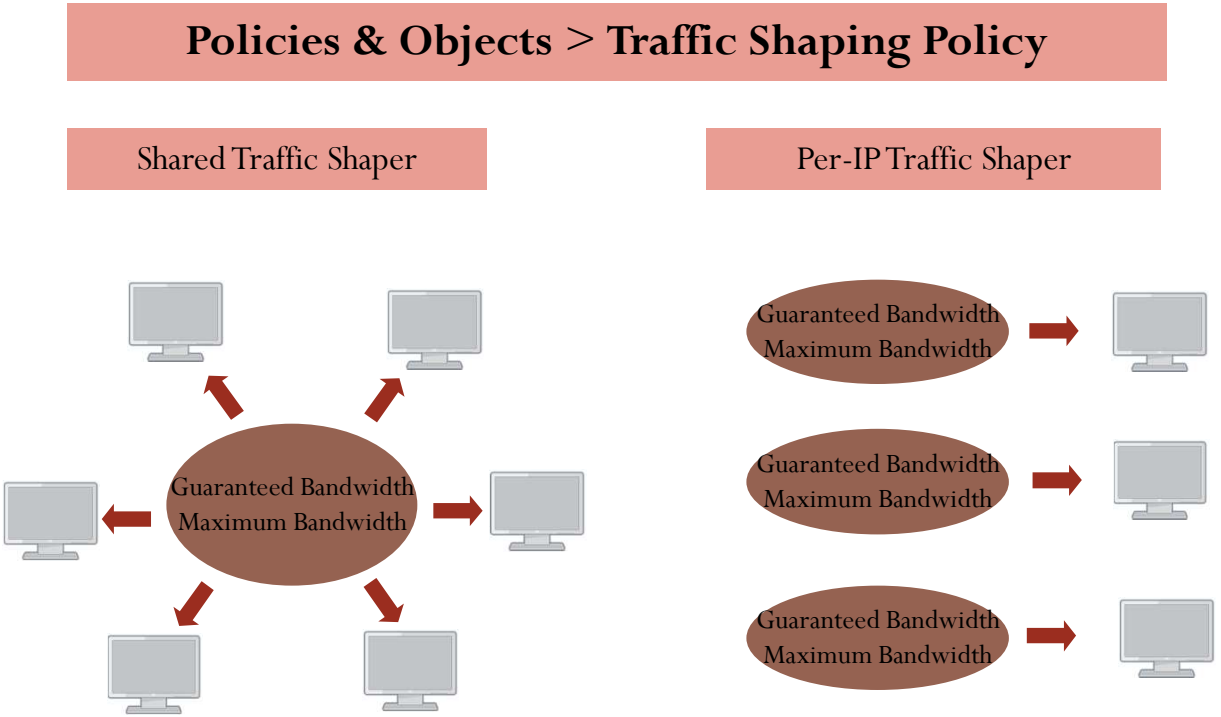


Deny


```
config system setting
set ses-denied-traffic <disable | enable>
end
config system global
set block-session-timer <1-300>
end
```

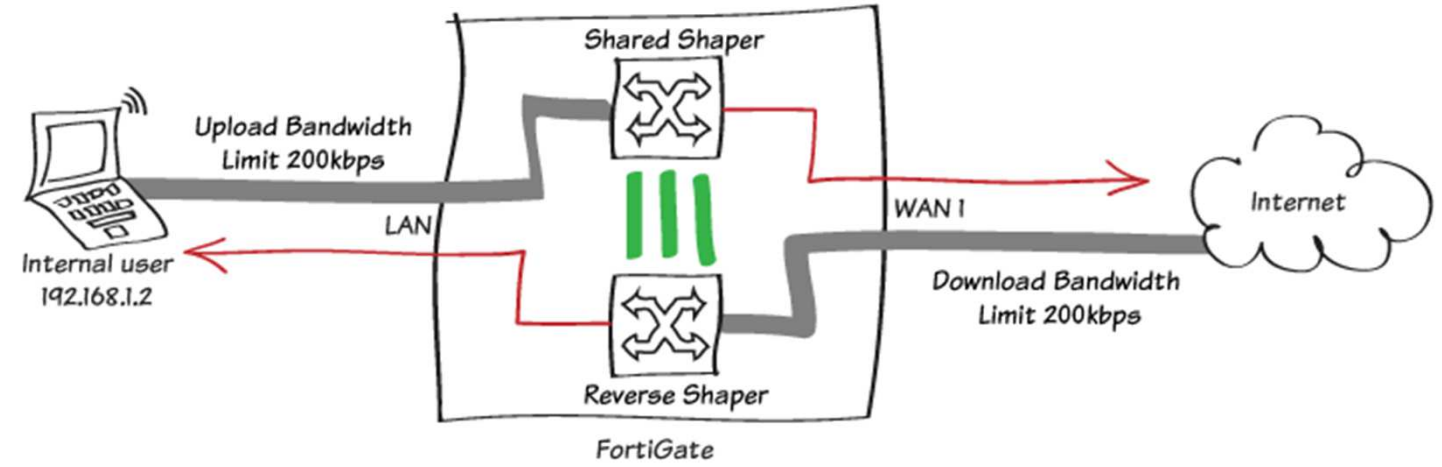
Traffic Shapers

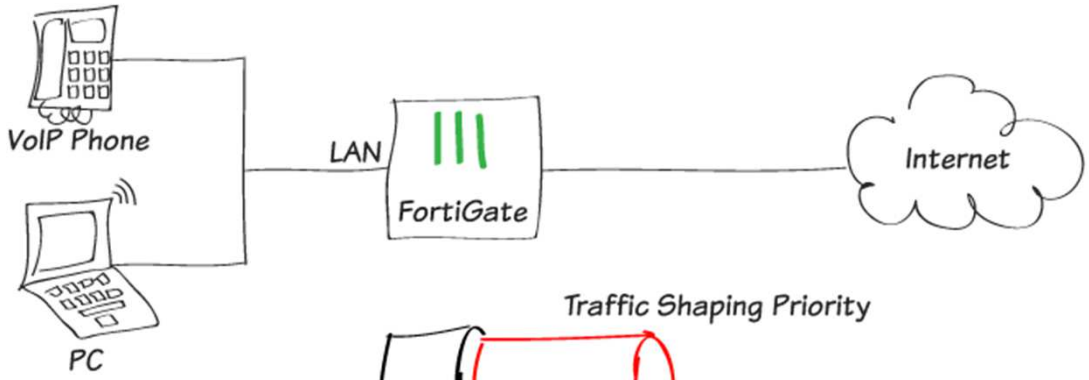
- Rate limiting is configurable
  - In bandwidth and out bandwidth
  - Defines maximum and guaranteed bandwidth

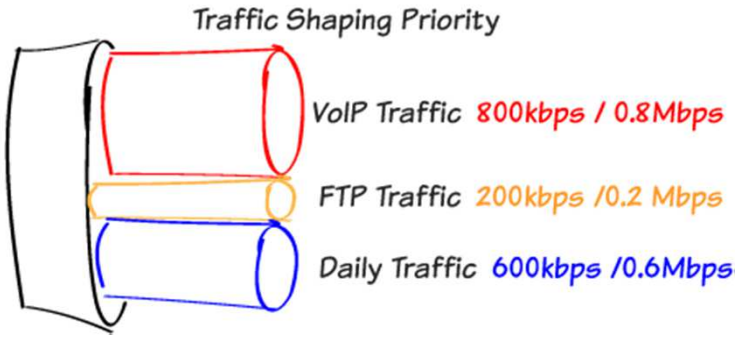


Traffic Shapers

- 限制上下頻寬







管理 - 防火牆規則政策

Objectives

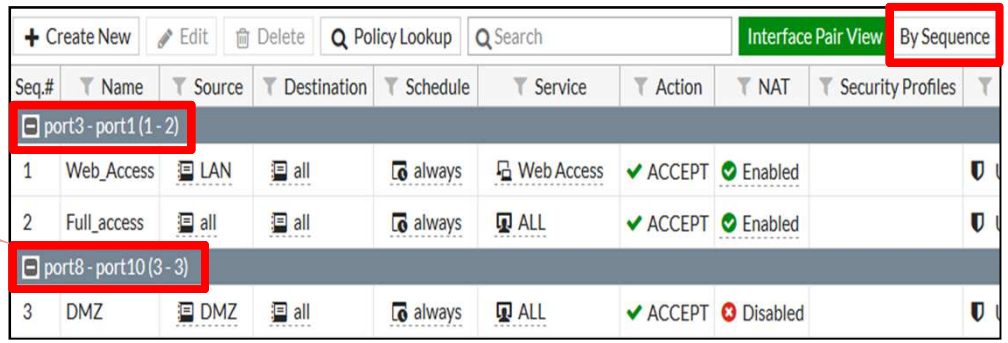
- Identify policy list views
- Understand the use of policy IDs and sequence numbers
- Identify where an object is referenced

Policy List–Interface Pair View and By Sequence

- **Interface Pair View**
  - Lists policies by ingress and egress interfaces

Can view **By Sequence** also

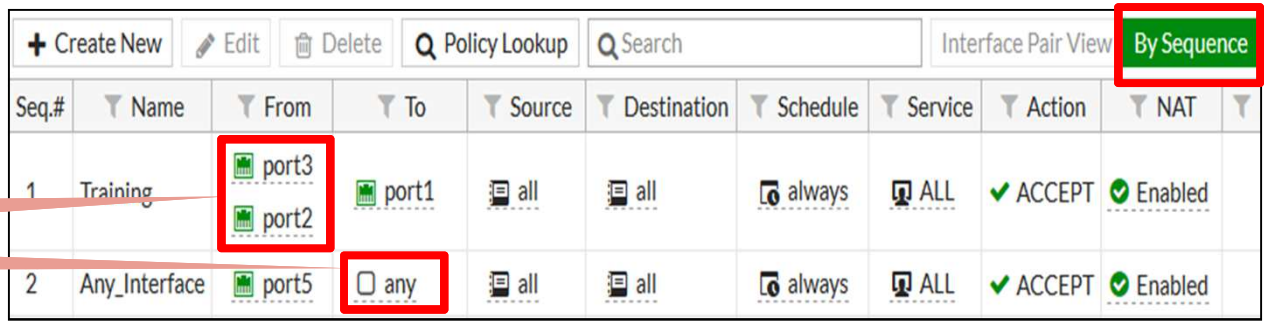
Policy & Objects > IPv4 Policy



Interface policy pairs

- **By Sequence** *(only)*
  - If policies are created using multiple source and destination interfaces or **any** interface

Policy & Objects > IPv4 Policy



Multiple interface

any interface

Policy ID

- On the GUI, firewall policies are primarily ordered by **Seq. #**
- Policy IDs are identifiers
  - CLI commands use policy ID instead of sequence number
  - Policy ID is assigned by the system when the rule is created
  - The ID number never changes as rules move higher or lower in the sequence

Policy & Objects > IPv4 Policy

Seq.#	ID	Name	Source	Destination	Schedule	Service	Action
port1 - port10 (1 - 1)							
1	3	DMZ	DMZ	all	always	ALL	✔ ACCEPT
port3 - port1 (2 - 3)							
2	4	Unrestricted	all	all	always	ALL	✔ ACCEPT
3	5	Block_FTP	all	all	always	FTP	⊘ DENY

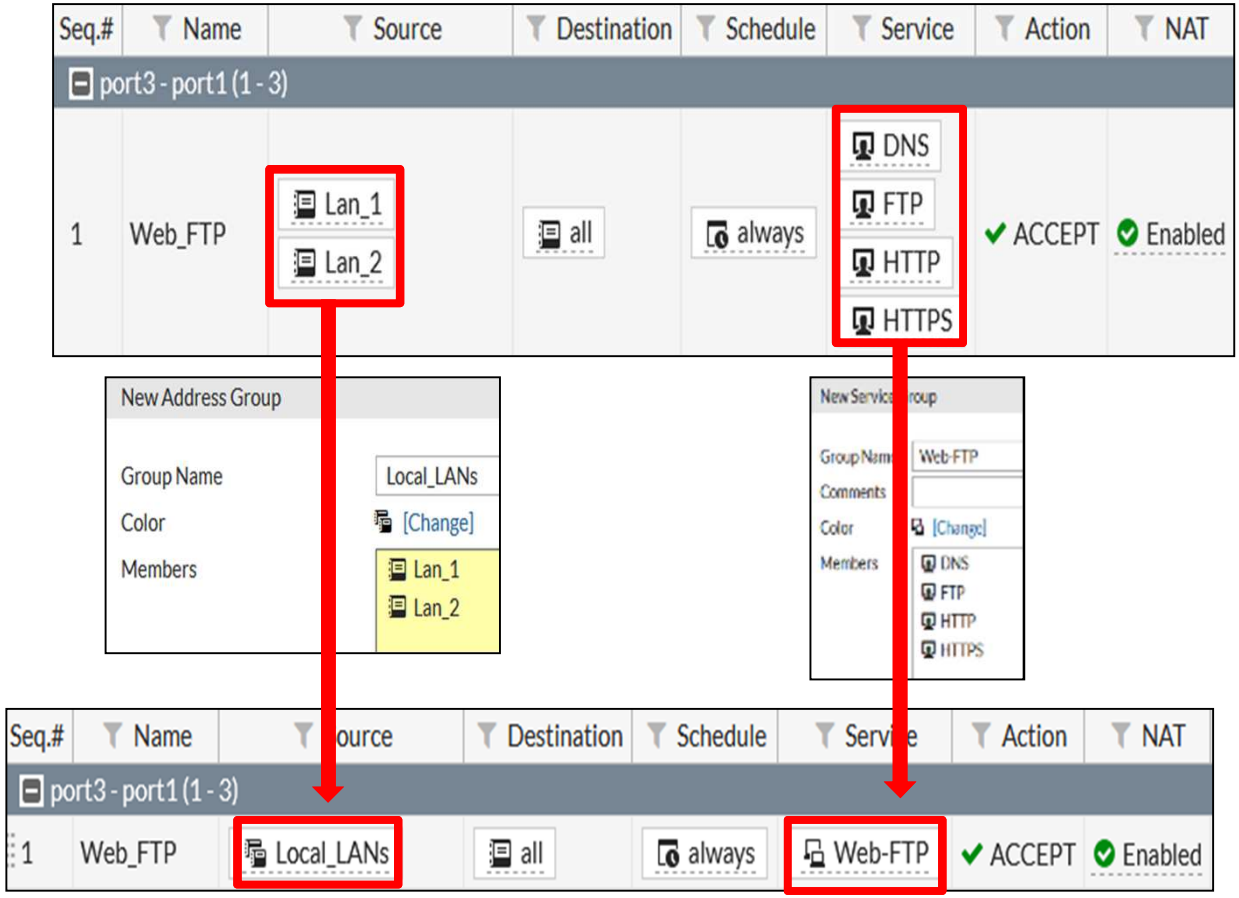
```
config firewall policy
edit <policy_id>
end
```

Policy ID

```
config firewall policy
  edit 4
    set name "Unrestricted"
...
next
  edit 5
     set name "Block_FTP"
```

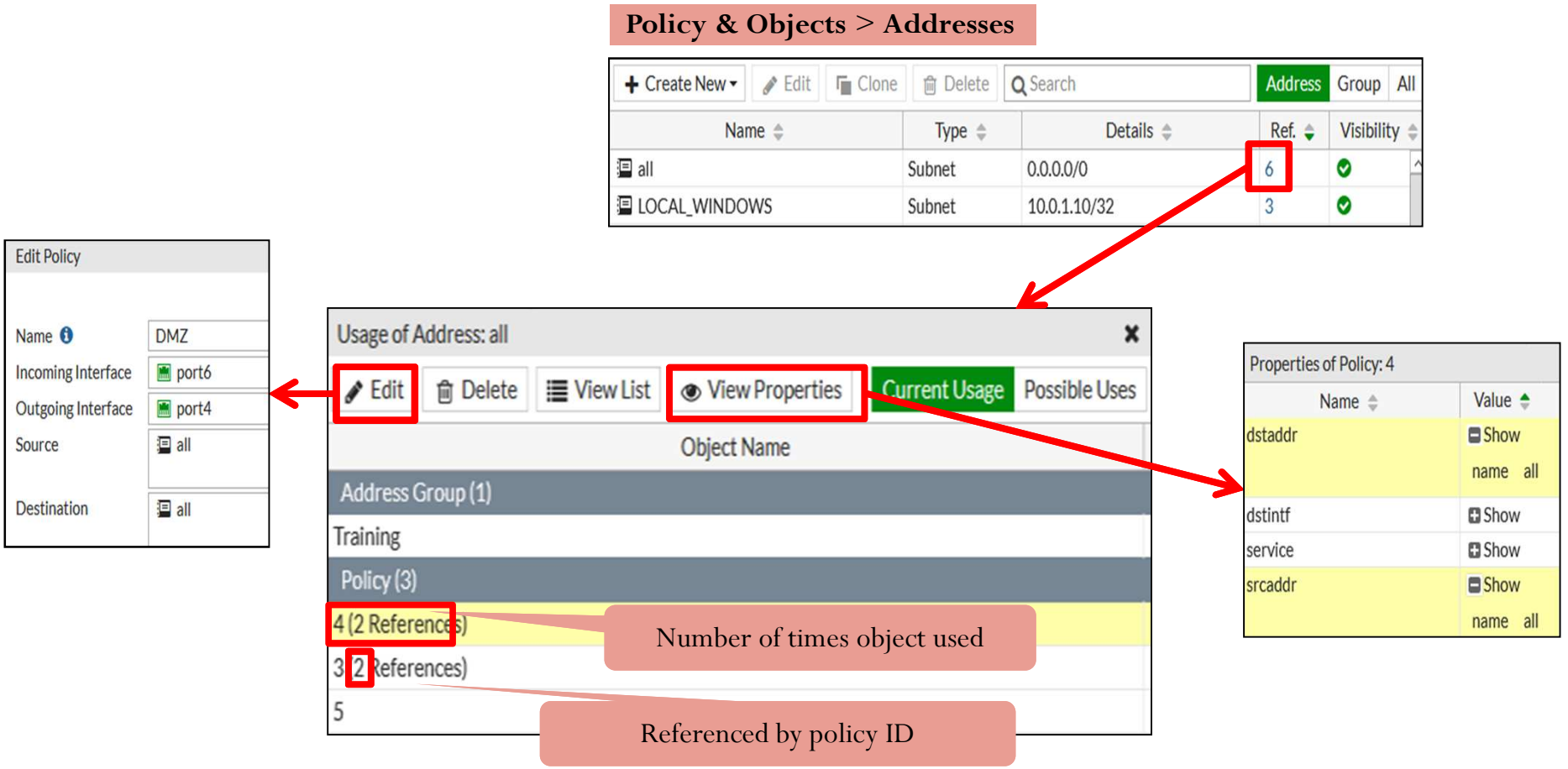
Simplify–Groups of Sources or Services

- You can reference address and service objects individually, or use groups to simplify policy configuration



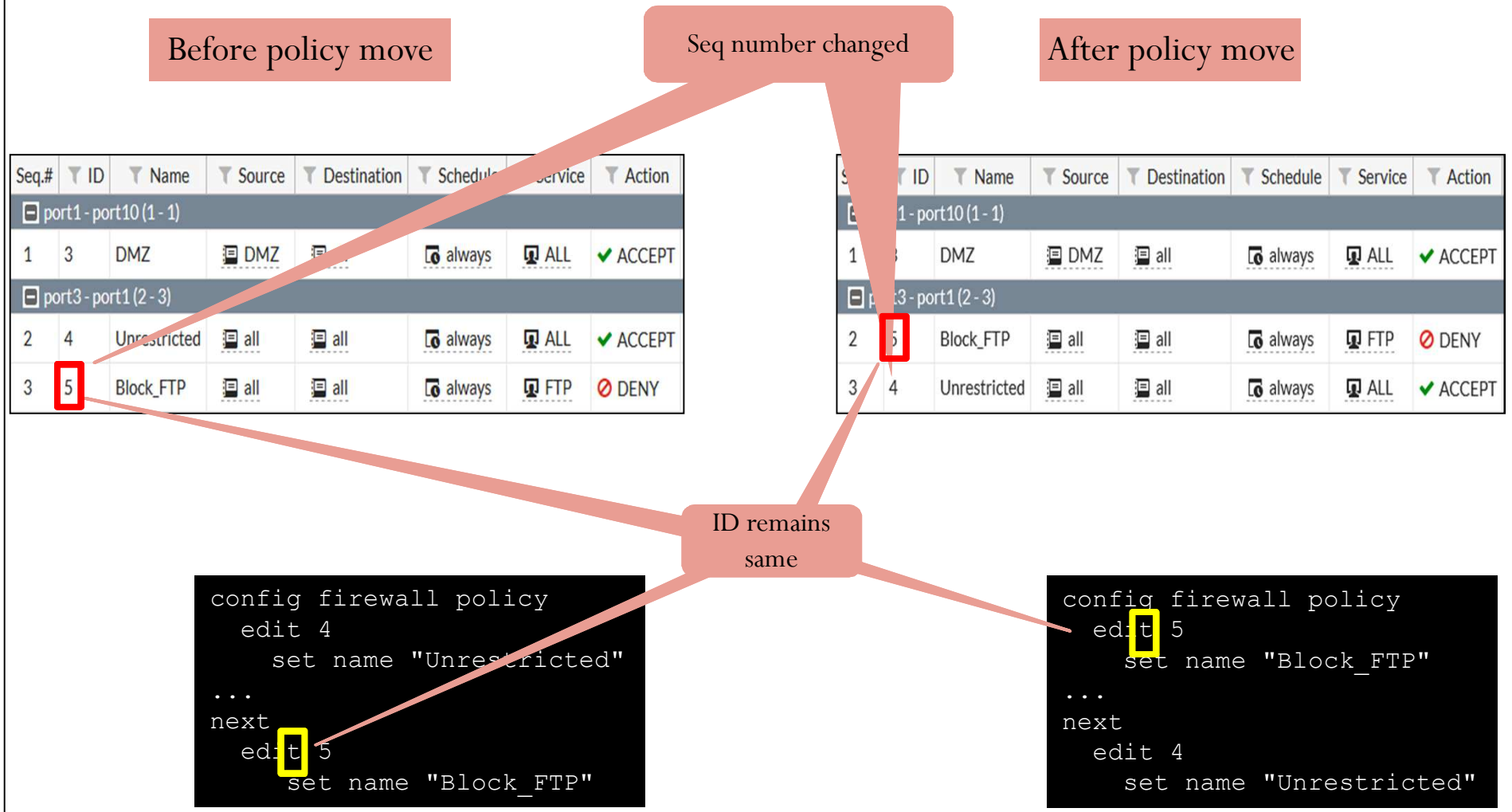
Object Usage

- Allows for faster changes to settings
- Reference column shows *if the object is being used*
  - Links directly to the referencing object



Adjusting Policy Order

- On the GUI, drag-and-drop **Seq. #**



Introduction to NAT

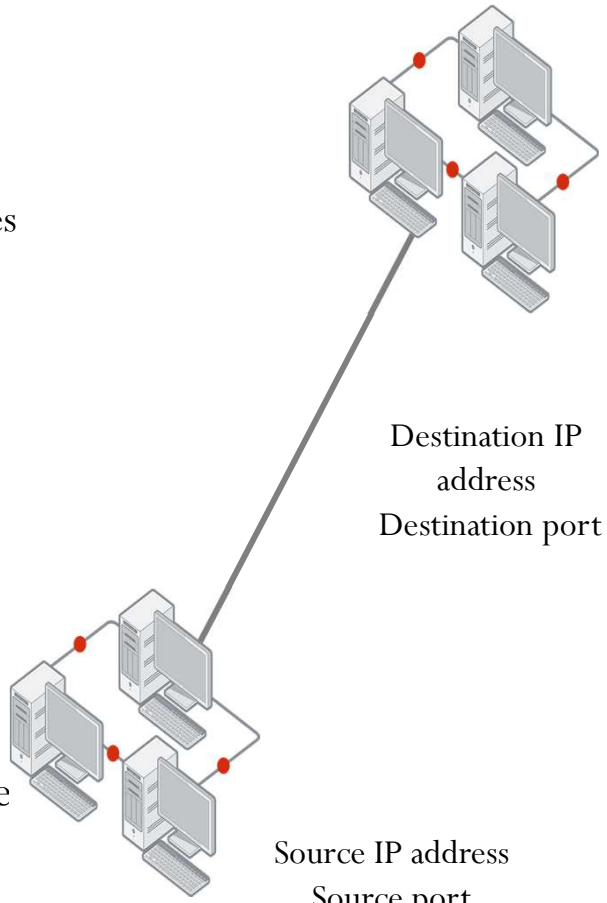
Objectives

- Understand NAT and port address translation (PAT)
- Understand the different configuration modes available for NAT

NAT and PAT

- NAT
  - Changes the IP layer address of a packet
    - Some protocols, like SIP, have addresses at the application layer, requiring session helpers or proxies
  - Source NAT (SNAT)
  - Destination NAT (DNAT)
- PAT
  - Changes the IP layer port number of a packet
- NAT64 and NAT46
  - A mechanism that allows IPv6 addressed hosts to communicate with IPv4 addressed hosts and the reverse
- NAT66
  - NAT between two IPv6 networks

.



Configuration Modes for NAT

- There are two ways to configure SNAT and DNAT:
- Firewall policy NAT
  - SNAT and DNAT must be configured for each firewall policy.
    - SNAT uses the outgoing interface address or configured IP pool.
    - DNAT uses the configured VIP as the destination address.
- Central NAT
  - SNAT and DNAT configurations are done per virtual domain.
  - It applies to multiple firewall policies, based on SNAT and DNAT rules.
    - SNAT rule is configured from central SNAT policy.
    - DNAT is configured from DNAT and VIPs.

Firewall Policy NAT

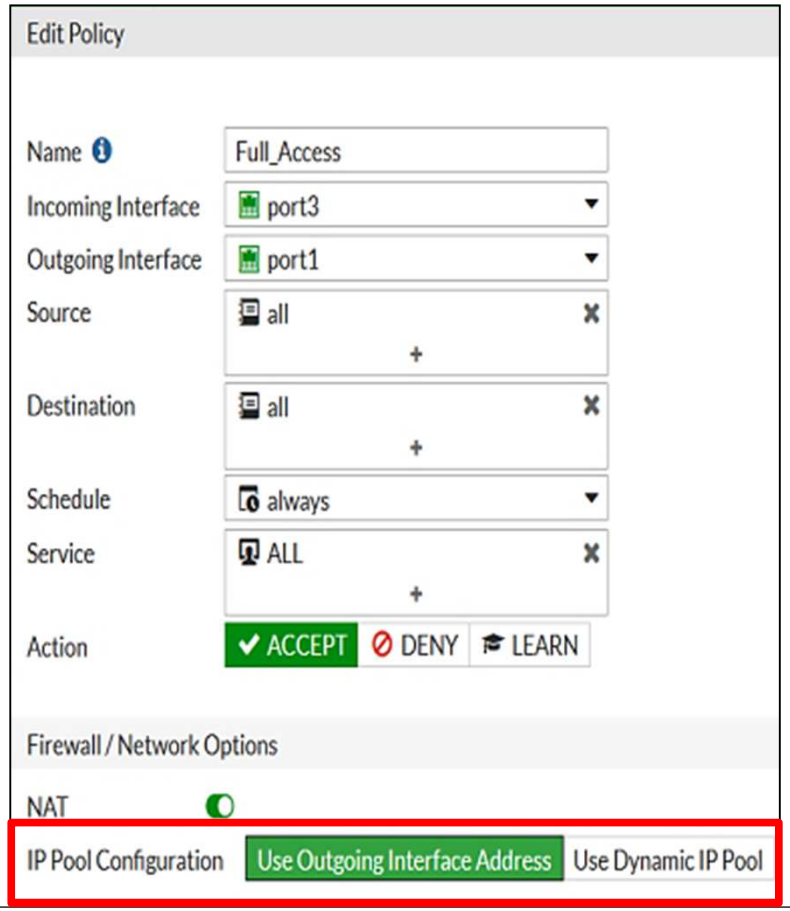
Objectives

- Configure a firewall policy to perform SNAT and DNAT (VIP)
- Apply SNAT with IP pools
- Configure DNAT with VIPs or a virtual server

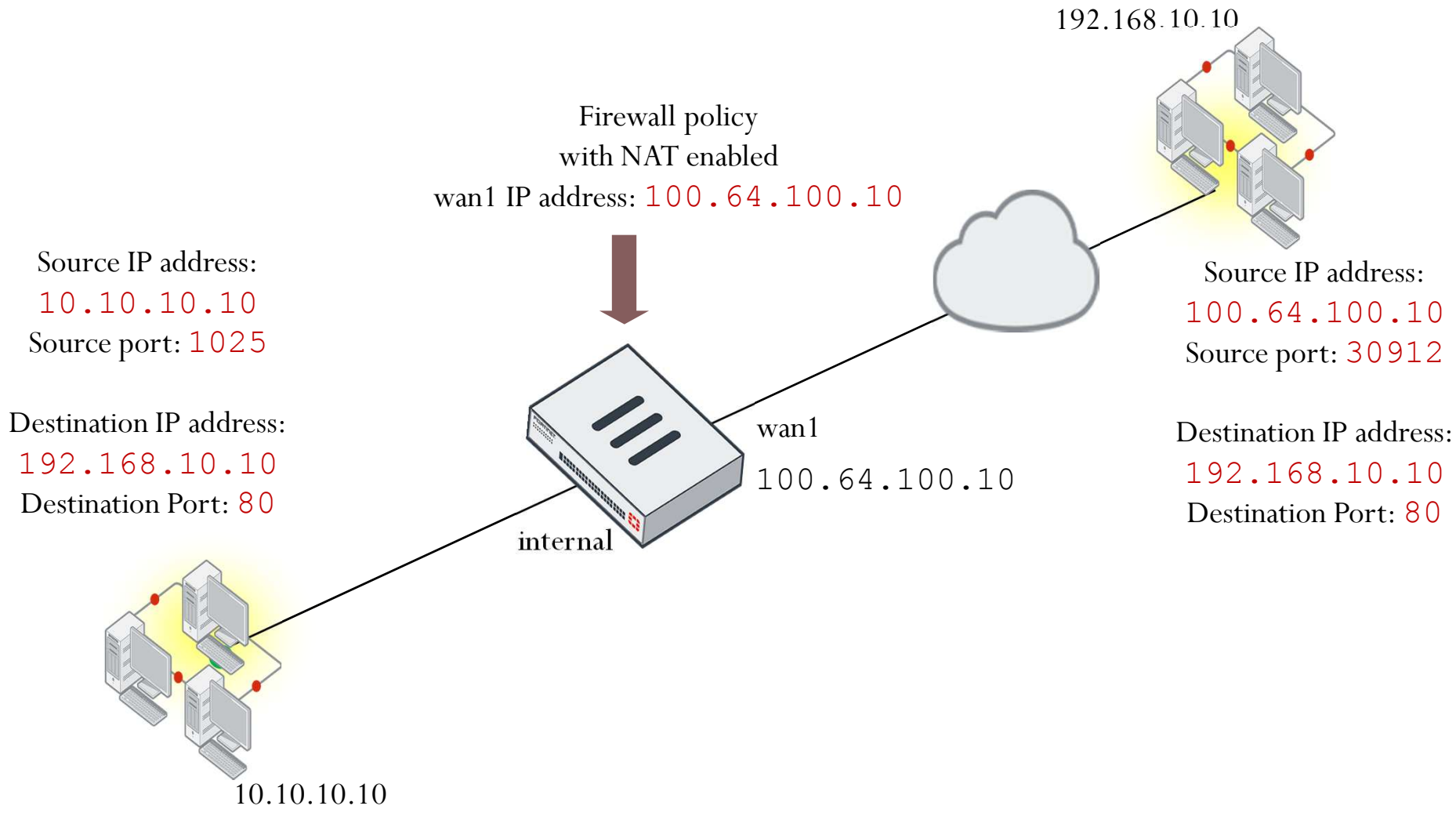
Firewall Policy SNAT

- There two ways to configure firewall policy SNAT:
  - Using the outgoing interface address
  - Using the dynamic IP pool

Policy & Objects > IPv4 Policy



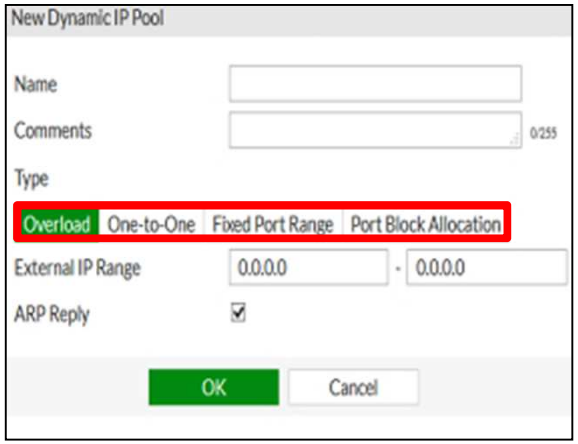
Firewall Policy SNAT Using the Outgoing Interface



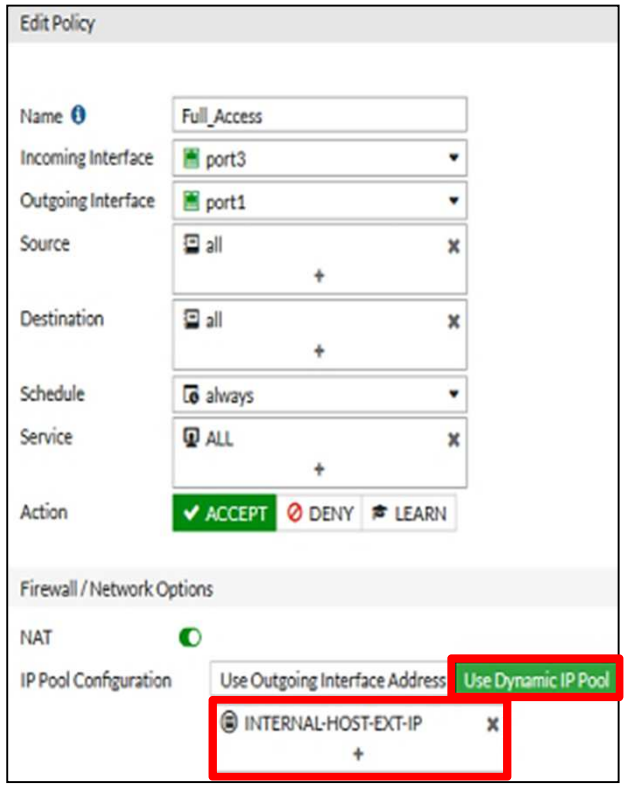
IP Pools

- IP pools defines a single IP address or a range of IP addresses to be used as the source address for the duration of the session.
- IP pools are usually configured in the same range as the interface IP address.
- There are four types of IP pools:
  - Overload
  - One-to-one
  - Fixed port range
  - Port block allocation

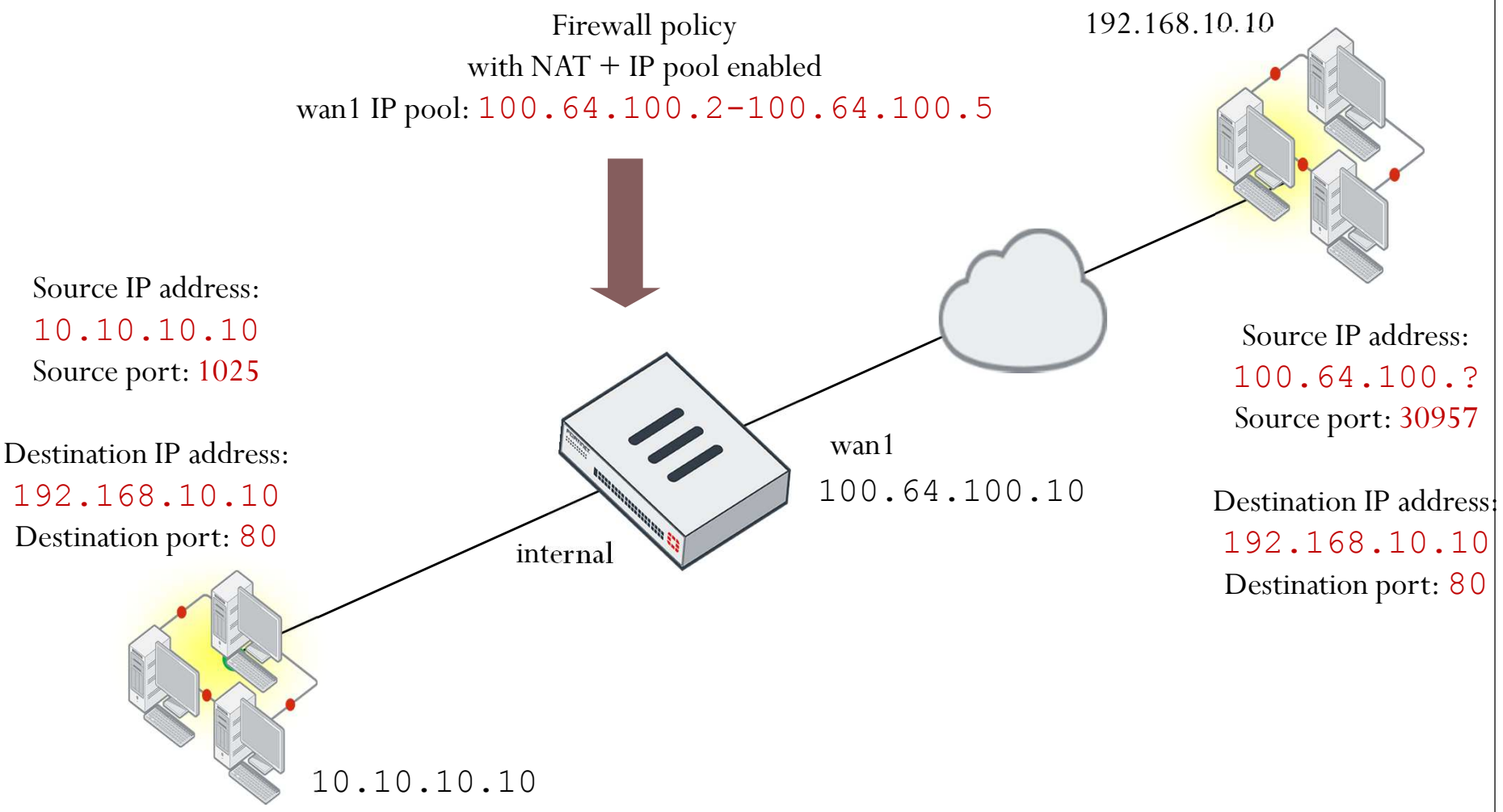
Policy & Objects > IP Pools



Policy & Objects > IPv4 Policy



IP Pool Type: Overload



IP Pool Type: One-to-One

- The default IP pool type is overload.
- The IP pool type one-to-one associates an internal IP with a pool IP on a first-come, first-served basis.
  - PAT is disabled.
  - Refuses the connection if there is no unallocated address

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE          SOURCE-NAT       DESTINATION
DESTINATION-NAT
tcp     3598   10.0.1.10:2706  10.200.1.6:2706  10.200.1.254:80  -
tcp     3598   10.0.1.10:2704  10.200.1.6:2704  10.200.1.254:80  -
tcp     3596   10.0.1.10:2702  10.200.1.6:2702  10.200.1.254:80  -
tcp     3599   10.0.1.10:2700  10.200.1.6:2700  10.200.1.254:443 -
tcp     3599   10.0.1.10:2698  10.200.1.6:2698  10.200.1.254:80  -
tcp     3598   10.0.1.10:2696  10.200.1.6:2696  10.200.1.254:443 -
udp     174    10.0.1.10:2694  -                  10.0.1.254:53  -
udp     173    10.0.1.10:2690  -                  10.0.1.254:53  -
```

IP Pool Type: Fixed Port Range

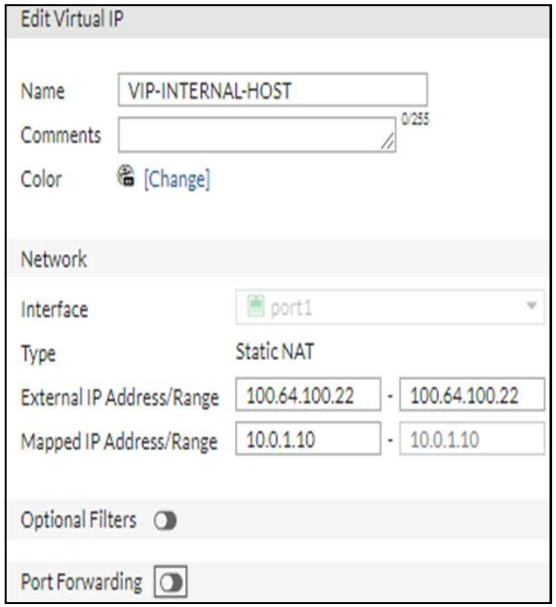
- The fixed port range IP pool type associates an internal IP range with an external IP range.
  - Port address translation is disabled.

```
STUDENT # get system session list
PROTO   EXPIRE SOURCE           SOURCE-NAT         DESTINATION
DESTINATION-NAT
tcp     3574   10.0.1.11:60843  10.200.1.8:60843   216.23.154.83:80
tcp     3570   10.0.1.11:60809  10.200.1.8:60809   216.23.154.81:80
tcp     3590   10.0.1.11:60819  10.200.1.8:60819   216.23.154.74:80
tcp     3599   10.0.1.11:60817  10.200.1.8:60817   216.23.154.74:80
tcp     3586   10.0.1.11:60815  10.200.1.8:60815   216.23.154.81:80
tcp     3564   10.0.1.11:60807  10.200.1.8:60807   216.23.154.74:80
tcp     9      10.0.1.10:7112   10.200.1.7:7112    10.200.1.254:80
tcp     7      10.0.1.10:7110   10.200.1.7:7110    10.200.1.254:80
tcp     5      10.0.1.10:7108   10.200.1.7:7108    10.200.1.254:80
tcp     3      10.0.1.10:7106   10.200.1.7:7106    10.200.1.254:80
tcp     1      10.0.1.10:7104   10.200.1.7:7104    10.200.1.254:80
```

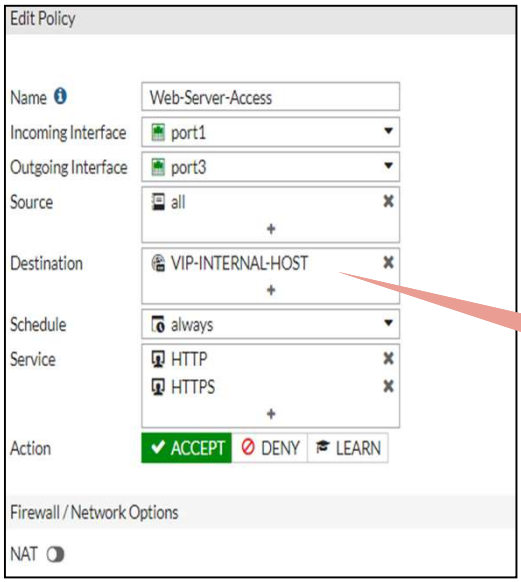
Virtual IPs (VIPs)

- DNAT objects
- Default type is static NAT
  - Can be restricted to forward only certain ports
- From the CLI, you can select `load-balance` or `server-load-balance`.
- VIPs should be routable to the external facing (ingress) interface for return traffic.

Policy & Objects > Virtual IPs



Policy & Objects > IPv4 Policy



VIP used as destination in firewall policy

Matching Policies – VIP

- Default behaviour: firewall address objects do not match VIPs.
  - Doesn't block an egress-to-ingress connection, even when the deny policy is at the top of the list.
- VIP policy (WAN to LAN)

Seq.#	Name	Source	Destination	Schedule	Service	Action
WAN (port1) - Internal_network (port3) (2 - 4)						
2	Deny	Deny_IP	all	always	ALL	DENY
3	Allow_access	all	Web_server	always	ALL	ACCEPT

Action = Deny

Can still access the VIP from the policy below, even though the deny policy is at the top of the list.

- Two ways to resolve it by modifying the deny policy:
  - Enable match-vip in deny policy

```
config firewall policy
edit <policy ID for deny>
set match-vip enable
end
```

  - Set the destination address as VIP object

```
config firewall policy
edit <policy ID for deny>
set dstaddr "VIP object"
end
```

Sessions

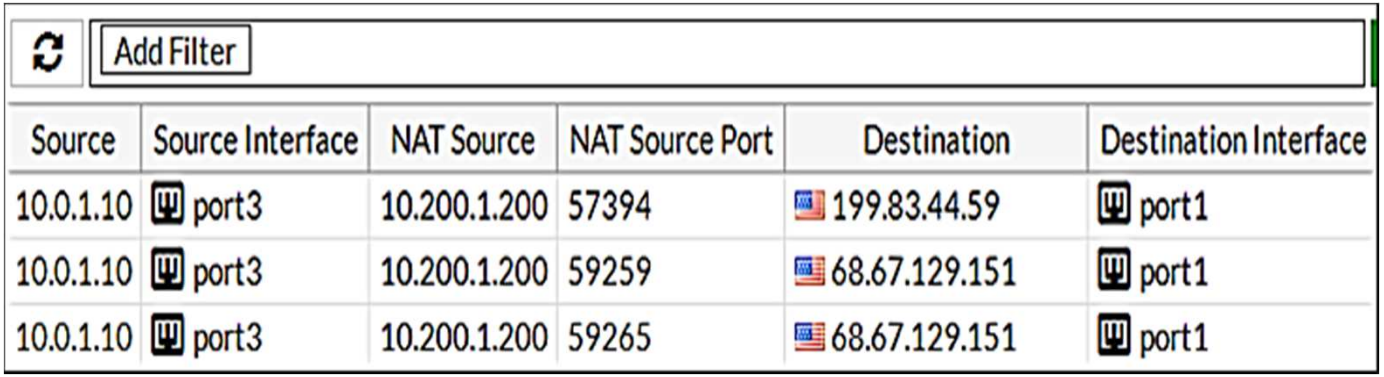
Objectives

- Understand the session table on FortiGate
- Understand the session time to live (TTL)
- Analyze `session diagnose` command output
- Understand the TCP, UDP, and ICMP states on FortiGate

Session Table

- Accepted IP sessions are tracked in the kernel's session table, but this can be affected by hardware acceleration.
- The session table stores the following information about the session:
  - The source and destination addresses, port number pairs, state, and timeout
  - The source and destination interfaces
  - The source and destination NAT actions
- The session table stores the following performance metrics:
  - Maximum concurrent sessions
  - New sessions per second

FortiView > All Sessions



Session Time To Live (TTL)

- When the session table is full, reducing timers may improve performance by closing sessions earlier. However, be careful not to close sessions *too* soon, because this can cause connection errors.

TCP default TTL

```
config system
session-ttl
set default 3600
end
```

Specific state timers

```
config system global
set tcp-halfclose-timer 120
set tcp-halfopen-timer 10
set tcp-timewait-timer 1
set udp-idle-timer 60
end
```

- Timers can be applied in policies and objects, and have precedence:
  - **Firewall Services** > **Firewall Policies** > **Global Sessions**

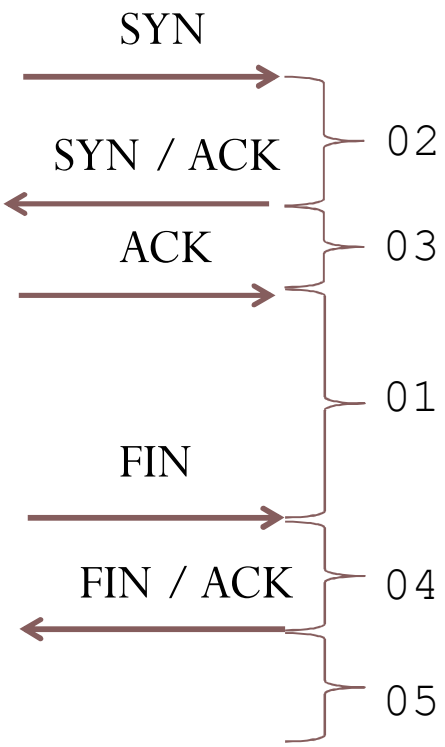
Firewall Session Diagnostics

- diagnose sys session
  - The session table also indicates policy actions.
  - Clear any previous filter:
    - diagnose sys session filter clear
  - Set the filter:
    - diagnose sys session filter ?
    - dport destination port
    - dst destination IP address
    - policy policy id
    - sport source port
    - src source ip address
  - List all entries matching the configured filter:
    - diagnose sys session list
  - Purge all entries matching the configured filter:
    - diagnose sys session clear

TCP States

- proto_state=05
  - First digit: client-side state
    - 0 if not proxy-based inspection
  - Second digit: server-side state

TCP State	Value	Expire Timer in sec (default)
NONE	0	10
ESTABLISHED	1	3600
SYN_SENT	2	120
SYN & SYN/ACK	3	60
FIN_WAIT	4	120
TIME_WAIT	5	120
CLOSE	6	10
CLOSE_WAIT	7	120
LAST_ACK	8	30
LISTEN	9	120

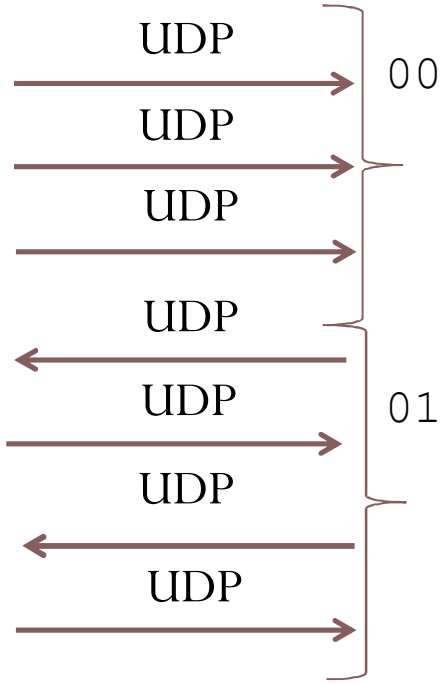


ICMP and UDP Protocol States

- Even though UDP is stateless, FortiGate still uses two session state values:

UDP State	Value
UDP traffic one way only	0
UDP traffic both ways	1

- ICMP has no state
  - `proto_state` is always 00



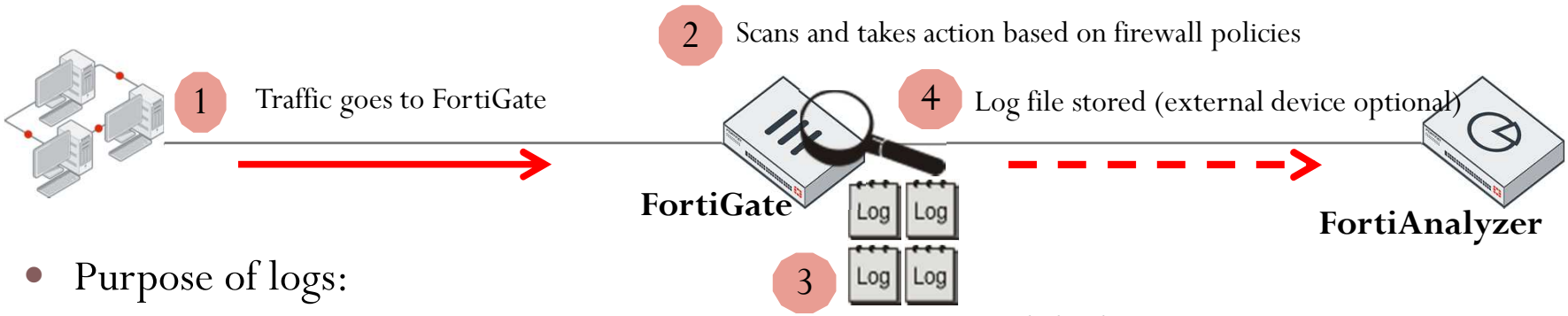
記錄

Objectives

- Describe the log workflow
- Identify log types and subtypes
- Describe log severity levels
- Describe the layout of a log message
- Describe the effect of logging on performance

Logging Workflow

1. Traffic passes through FortiGate to your network.
2. FortiGate scans the traffic and takes action based on configured firewall policies.
3. Activity is recorded and the information is contained in a log message.
4. Log message is stored in a log file and on a device capable of storing logs (local FortiGate device or an external device, such as FortiAnalyzer).



- Purpose of logs:
  - Monitor network and Internet traffic volumes
  - Diagnose problems
  - Establish normal baselines to recognize anomalies and trends

NTP server recommended

Log Types and Subtypes

- *Traffic* logs record traffic flow information, such as an HTTP/HTTPS request and its response (if any).
- *Event* logs record system and administrative events, such as adding or modifying a setting, or daemon activities.
- *Security* logs record security events, such as virus attacks and intrusion attempts, based on the security profile type (log type = utm).
  - If no security logs exist, the menu item does not appear in the GUI.

Traffic	Event	Security
Forward	Endpoint Control	Application Control
Local	High Availability	Antivirus
Sniffer	System	Data Leak Prevention (DLP)
	User	Anti-Spam
	Router	Web Filter
	VPN	Intrusion Prevention System (IPS)
	WAD	Anomaly (DoS-policy)
	Wireless	Web Application Firewall (WAF)

WAN optimization logs are found within traffic logs

GPRS Tunneling Protocol (GTP) logs are handled separately from default event logs

Log Severity Levels

- Each log entry includes a log level (also known as priority level) that ranges in order of importance
  - 0 = high importance / 6 = low importance

Levels	Description
0 – Emergency	System unstable
1 – Alert	Immediate action required
2 – Critical	Functionality effected
3 – Error	Error exists that can affect functionality
4 – Warning	Functionality could be affected
5 – Notification	Information about normal events
6 – Information	General system information
7 – Debug	Diagnostic information for investigating issues

Rarely used, unless actively investigating an issue with Fortinet Support

Log Message Layout

- Log header (similar in all logs)
  - `Type` and `subtype` = Name of log file
  - `Level` = Severity level

```
date=2016-06-14 time=12:05:28 logid=0316013056 type=utm
subtype=webfilter eventtype=ftgd_blk level=warning vd=root
```

- Log body (varies by log type)
  - `policyid` = Firewall policy applied to session
  - `hostname` = URL or IP of host
  - `srcip` and `dstip` = Source and destination IP
  - `action` = Action taken by FortiGate
  - `msg` = Reason for the action

```
policyid=1 sessionid=10879 user="" srcip=10.0.1.10 srcport=60952
srcintf="port3" dstip=52.84.14.233 dstport=80 dstintf="port1"
proto=6 service="HTTP" hostname="miniclip.com" profile="default"
action=blocked reqtype=direct url="/favicon.ico" sentbyte=297
rcvdbyte=0 direction=outgoing
msg="URL belongs to a denied category in policy" method=domain
cat=20 catdesc="Games" crscore=30 crlevel=high
```

Effect of Logging on Performance

- More logs = more CPU, memory, and disk space
- Depending on the amount of traffic you have, and the logging settings that are enabled, your traffic logs can swell and impact the performance of your firewall
- Traffic logs record every session
  - Extra information for troubleshooting
  - Some UTM events
  - More system intensive

Enable performance statistic logging for remote logging devices on FortiGate

```
#config system global
    set sys-perf-log-interval <number from 0-15>
  end
```

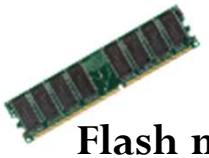
Local Logging

Objectives

- Identify local log storage options
- Enable local logging
- Understand disk allocation and reserved space
- Monitor disk usage
- Configure behavior when disk is full

Log Storage – Local

- Constant rewrites can reduce the lifetime and efficiency of the memory
- Logging disabled by default
- Not recommended for logging, should use external logging device instead



Flash memory

Hard drive

- FortiGate devices that have a hard drive store logs in an SQL database
- Data is extracted from the SQL database for reports

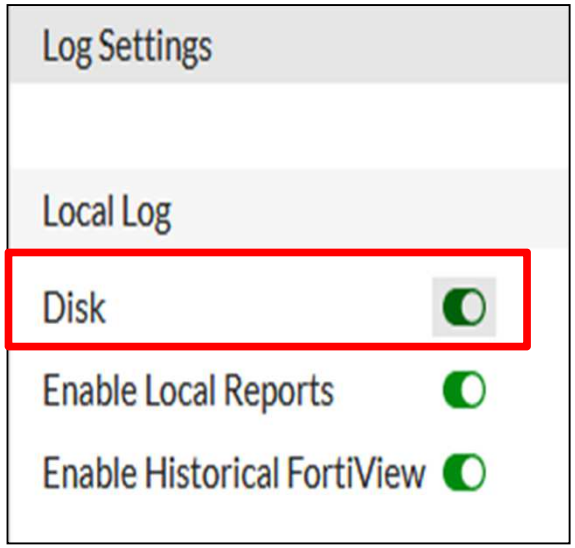
Local logging

Performance may be impacted under heavy strain

Enabling Local Logging

- To store logs locally on FortiGate, you must enable disk logging.
- With disk logging enabled, the report daemon collects statistics used for historical FortiView from disk.
  - If disk logging is disabled, FortiView logs are only available in real-time.
- By default, logs older than seven days are deleted from disk (configurable).

Log & Report > Log Settings




```
# config log disk setting
    set maximum-log-age <integer>
```

```
#config log disk setting
    set status enable
```

FortiGate Disk Allocation – Reserved Space

- The system reserves approximately 25% of its disk space for system usage and unexpected quota overflow.
  - Only ~75% of disk space is available to store logs

```
 FGT_A (global) # diagnose sys logdisk
usage
 Total HD usage: 208MB/118145MB
 Total HD logging space: 88608MB
 HD logging space usage for vdom "root":
0MB/9965MB
 HD logging space usage for vdom "vdom1:"
0MB/104857MB
```

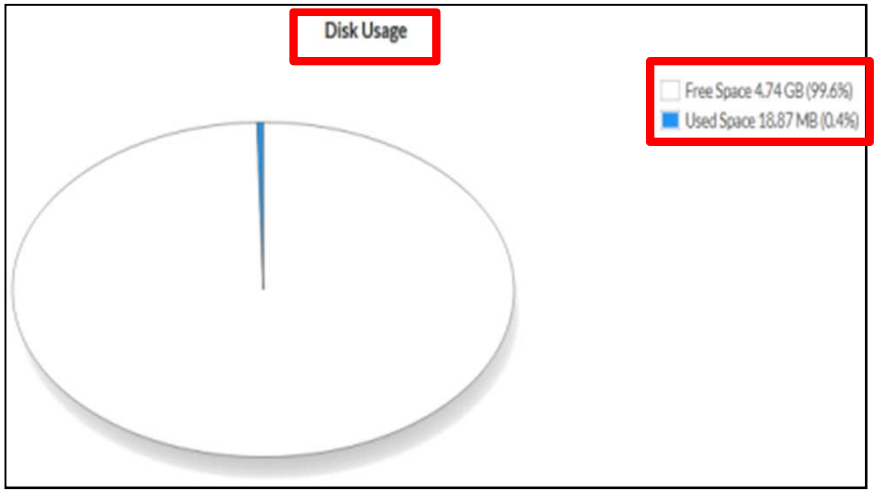
Use this command to obtain the amount of reserved space on your FortiGate

- Formulas:
  - disk - logging = reserved (i.e. 118145MB – 88608MB = 29537MB reserved)
  - reserved/disk*100 = reserved % (i.e. 29537/118145*100 = 25%)

Monitoring Disk Usage

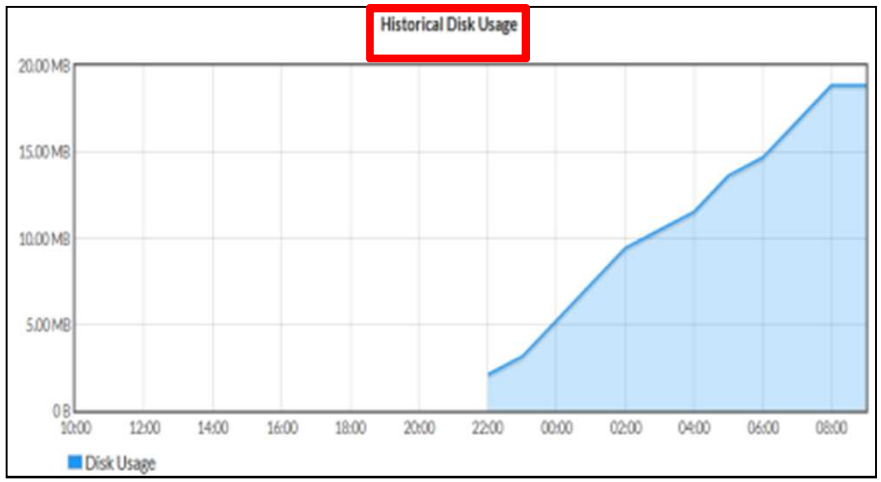
- Local disk usage
  - Free space
  - Used space
- Historical disk usage
  - Volume of disk logging activity over time

Log & Report > Log Settings



Use this command to see how much space is currently being used for logs

```
Local-FortiGate # diagnose sys logdisk usage
Total HD usage: 211MB/31703MB
Total HD logging space: 4755MB
HD logging space usage for vdom "root": 18MB/4755MB
```



Behavior When Disk is Full

- By default, when the disk is full, the oldest logs are overwritten.
  - Configurable—can set to stop logging when disk is full

- FortiGate issues warnings before disk reaches a full state:
  - First warning: 75%
  - Second warning: 90%
  - Final warning: 95%

Default settings (configurable)

```
# configure log disk setting
     set diskfull [overwrite | nolog]
     set full-first-warning-threshold <1-98>
     set full-second-warning-threshold <2-99>
     set full-final-warning-threshold <3-100>
```

Remote Logging

Objectives

- Identify external log storage options
- Configure remote logging
- Understand how remote logging works with VDOMs
- Understand log transmission
- Enable reliable logging

Log Storage - Remote

- Hosted subscription-based service
- Long-term log storage and reporting
- Bound to Fortinet Support account
- FortiGate includes a free tier

(See documentation for quotas)

FortiCloud

FortiSIEM

- Unified event correlation and risk management
- Collect, parse, normalize, index, and store security logs

- Long term, dedicated storage of log data
- Reports
- Log limit dependent on model

FortiAnalyzer

Syslog

- Logging server
- Central repository for networked devices
- Consolidates logs

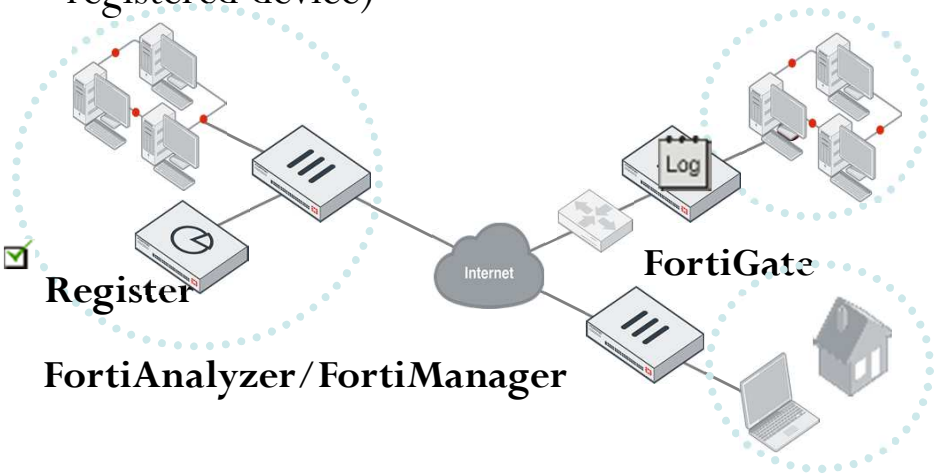
Remote logging

FortiManager

- Like FortiAnalyzer, can also store logs and generate reports, but has fixed amount per day that is less than equivalent size FortiAnalyzer
- Primary purpose: central administrative management of networked devices

FortiAnalyzer and FortiManager Log Storage

- FortiGate can send logs to both FortiAnalyzer and FortiManager (FortiGate must be a registered device)



Log & Report > Log Settings

Remote Logging and Archiving

Send logs to FortiAnalyzer/FortiManager

IP address 10.0.1.210 Test Connectivity

Upload option Real Time Every Minute Every 5 Minutes

Encrypt log transmission

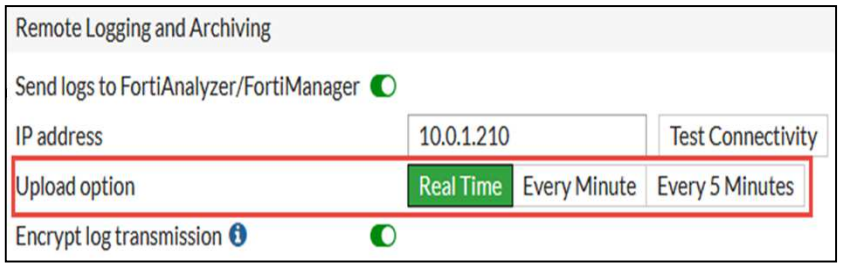
- Can configure up to three separate FortiAnalyzer and FortiManager devices using the CLI
  - Multiple devices may be needed for redundancy
  - Generating and sending logs requires resources—be aware!

```
# config log
[fortianalyzer|fortianalyzer2|fortianalyzer3]
setting
  set status enable
  set server <server_IP>
  end
```

Upload Option

- Near real-time uploading and consistent high-speed compression and analysis
- Configure logging options:
  - `store-and-upload` (CLI configuration
  - **Real Time**
  - **Every Minute**
  - **Every 5 Minutes** (default)

Log & Report > Log Settings




```
# configure log fortianalyzer setting
     set upload-option [store-and-upload
|realtime/1-minute/5-minute]
```

`store-and-upload` only available to FortiGates with an internal hard drive

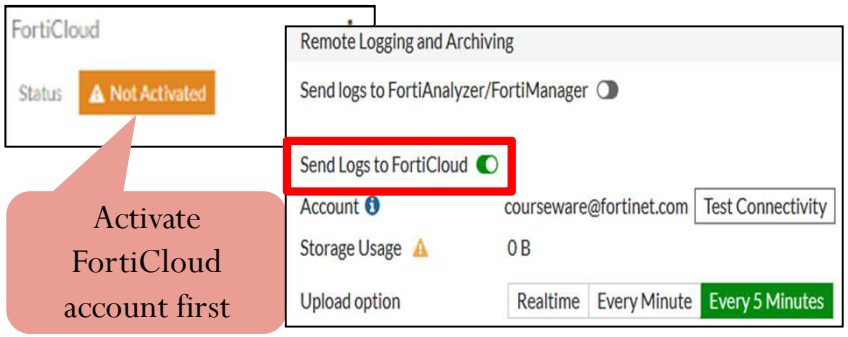
- By default, if the FortiAnalyzer disk is full, the oldest logs are overwritten. However, you can configure FortiAnalyzer to stop logging.

FortiCloud, Syslog, and FortiSIEM Log Storage

FortiCloud

- *Must activate FortiCloud account (dashboard)*

Log & Report > Log Settings



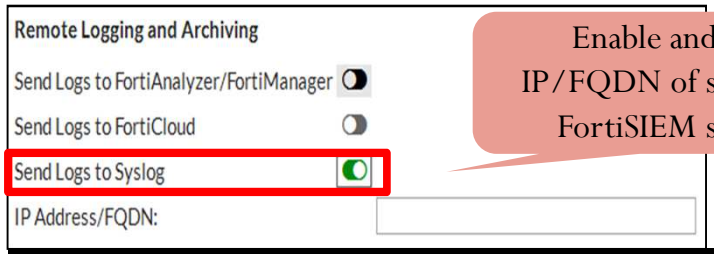
Activate FortiCloud account first

```
# config log fortiguard setting
    set status enable
    set source-ip <src IP used to connect
FortiCloud)
    set upload-option <realtime | 1-minute
| 5-minute>
    set enc-algorithm <high-medium | high |
low |disable>
  end
```

Encryption algorithm setting not available to configure in the GUI

Syslog and FortiSIEM

Log & Report > Log Settings



Enable and add IP/FQDN of syslog or FortiSIEM server

```
# config log [syslogd | syslogd2 | syslogd3 |
syslogd4] setting
    set status enable
    set server <syslog_IP>
  end
```

Can configure up to four remote syslog service or FortiSIEMs using the CLI

- FortiGate logs can be sent to syslog servers in CSV or CEF format

```
# config log syslogd3 setting
    set format [csv | cef]
  end
```

VDOMs and Remote Logging

- If you have a FortiGate with Virtual Domains (VDOMs) configured, you can globally add multiple FortiAnalyzers and syslog servers.
  - On each VDOM, you can override these global settings, which allows you to configure only one FortiAnalyzer and one syslog server for that VDOM.
  - The management VDOM is responsible for sending logs to FortiAnalyzer, if you use the `override-setting` in a VDOM, that VDOM is now responsible for sending its own logs to the new FortiAnalyzer.

```
# config system global
   config log fortianalyzer setting
       set status enable
       set server 10.0.1.1
   end
   config log fortianalyzer2
setting
       set status enable
       set server 10.0.2.1
   end
```

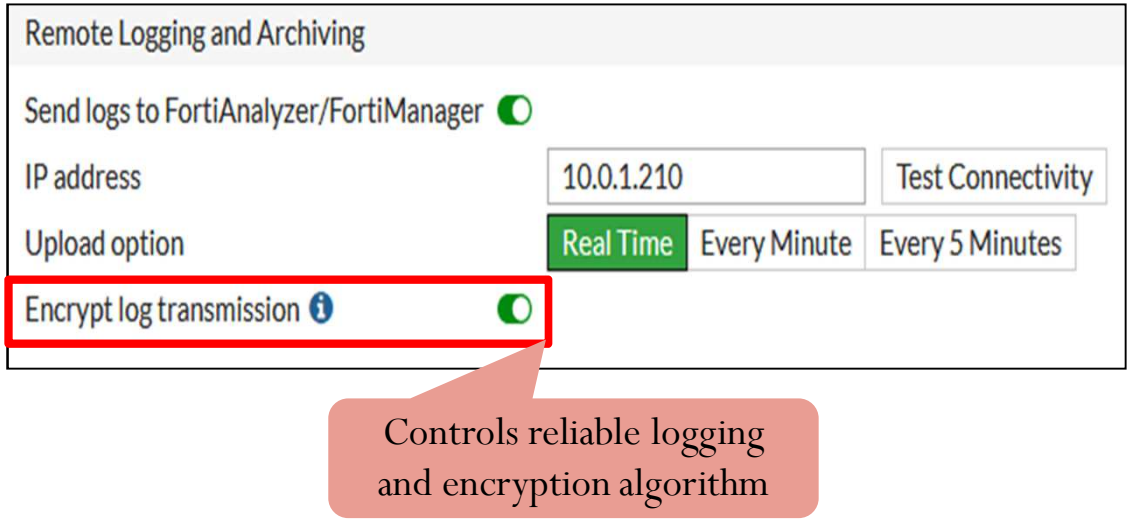
```
# config vdom
    edit Training
    config log fortianalyzer
override-setting
    set override enable
    set status enable
    set server 10.0.1.210
```

FortiGate

```
# config vdom
    edit Training
    config log fortianalyzer
override-setting
    set override enable
    set status enable
    set server 192.168.1.3
   end
```

Log Transmission

- FortiGate uses UDP 514 (or TCP 514 if reliable logging is enabled) for log transmission.



- Log messages are stored on disk and transmitted to FortiAnalyzer as plain text in LZ4 compressed format.
  - Reduces disk log size and reduces log transmission time and bandwidth usage

Reliable Logging

- Changes the log transport delivery method from UDP to TCP
- TCP provides reliable data transfer
  - Guarantees the data transferred remains intact and arrives in the same order in which it was sent
  - Error checking and error recovery
  - Acknowledgement segments to ensure packet is received
  - Connection-oriented protocol (SYN, SYN-ACK, ACK handshake)
- If you enable logging to FortiAnalyzer using the GUI, reliable logging is auto-enabled.
  - If you enable logging to FortiAnalyzer using the CLI, reliable logging is not auto-enabled. You must manually enable using the CLI command:

```
# config log fortianalyzer setting
    set reliable [enable/disable]
```

```
# config log syslogd setting
    set reliable
[enable/disable]
```

When enabled on syslog, the default port becomes port 601

- FortiCloud uses TCP, and you can set the encryption algorithm using the CLI (default setting is high).

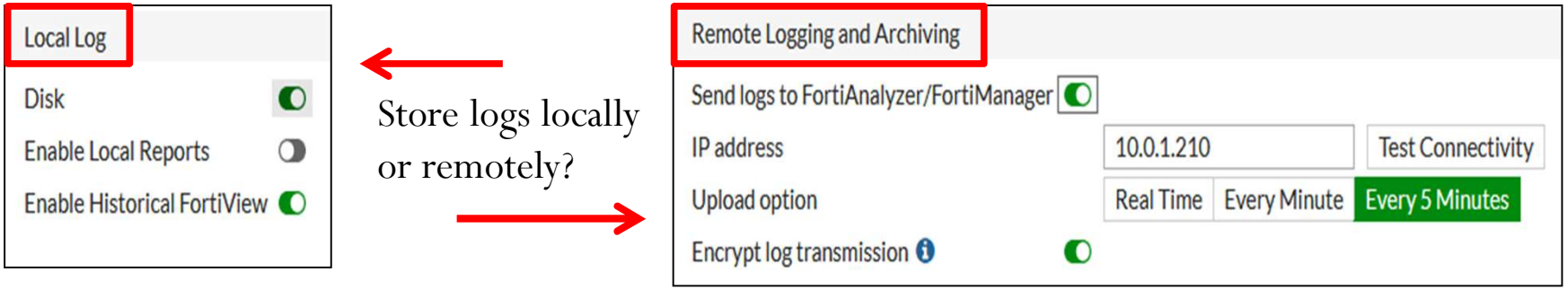
Log Settings

Objectives

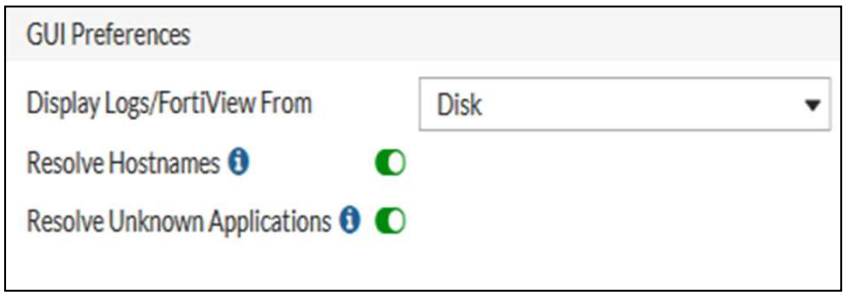
- Configure log settings
- Enable logging on firewall policies
- Hide user names in logs

Logging Settings: If, Where, and How

Log & Report > Log Settings



- Log event logs and traffic logs?
- Local traffic logs = traffic directly to and from FortiGate (disabled by default)
- Event logs = system information generated by the FortiGate device



- Display logs from memory, disk, or FortiAnalyzer?
- Translate IPs to host names for convenience? (Can impact CPU usage and page responsiveness.)

Log Filtering

- Can configure log filter settings to determine which logs are recorded
  - Configure up to four remote syslog or FortiSIEM logging servers:

```
# config log [syslogd | syslogd2 | syslogd3 | syslogd4] filter
```

  - Configure up to three FortiAnalyzer devices:

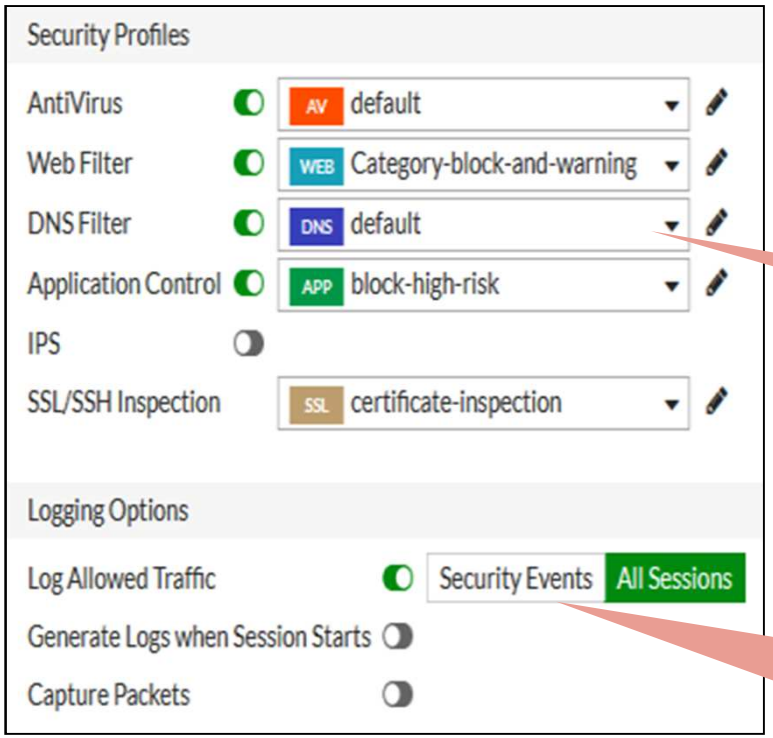
```
# config log [fortianalyzer | fortianalyzer2 | fortianalyzer3] filter
```

- Filters include:
  - Severity <level>
  - Forward traffic [enable/disable]
  - Local traffic [enable/disable]
  - Multicast traffic [enable/disable]
  - Sniffer traffic [enable/disable]
  - Anomaly [enable/disable]
  - VOIP [enable/disable]
  - DLP archive [enable/disable]
  - DNS [enable/disable]
  - Filter [string]
  - Filter type [include | exclude]

Enabling Logging on Firewall Policies

- Firewall policy settings decide if a log message caused by traffic passing through a firewall policy is generated or not

Policy & Objects > IPv4 Policy



- Hardware acceleration affects logging
  - Traffic offloaded to NP processors does not log traffic statistics.
    - Can disable hardware acceleration
    - Can enable NP packet logging (degrades NP performance)

Must enable one or more security profiles on your firewall policy to generate a log message for that profile

Must enable and set which traffic to log. If disabled, *you will not receive logs of any kind*—even if you have enabled a security profile on your firewall policy.

Testing Log Settings

```
Local-FortiGate # diagnose log test
generating a system event message with level - warning
generating an infected virus message with level - warning
generating a blocked virus message with level - warning
generating a URL block message with level - warning
generating a DLP message with level - warning
generating an IPS log message
generating an anomaly log message
generating an application control IM message with level - information
generating an IPv6 application control IM message with level - information
generating deep application control logs with level - information
generating an antispam message with level - notification
generating an allowed traffic message with level - notice
generating a multicast traffic message with level - notice
generating a ipv6 traffic message with level - notice
generating a wanopt traffic log message with level - notification
generating a HA event message with level - warning
generating a VOIP event message with level - information
generating authentication event messages
generating a Forticlient message with level - information
generating a URL block message with level - warning
generating a DNS message with level - warning
```

Test if logs are generating

View, Search, and Monitor Logs

Objectives

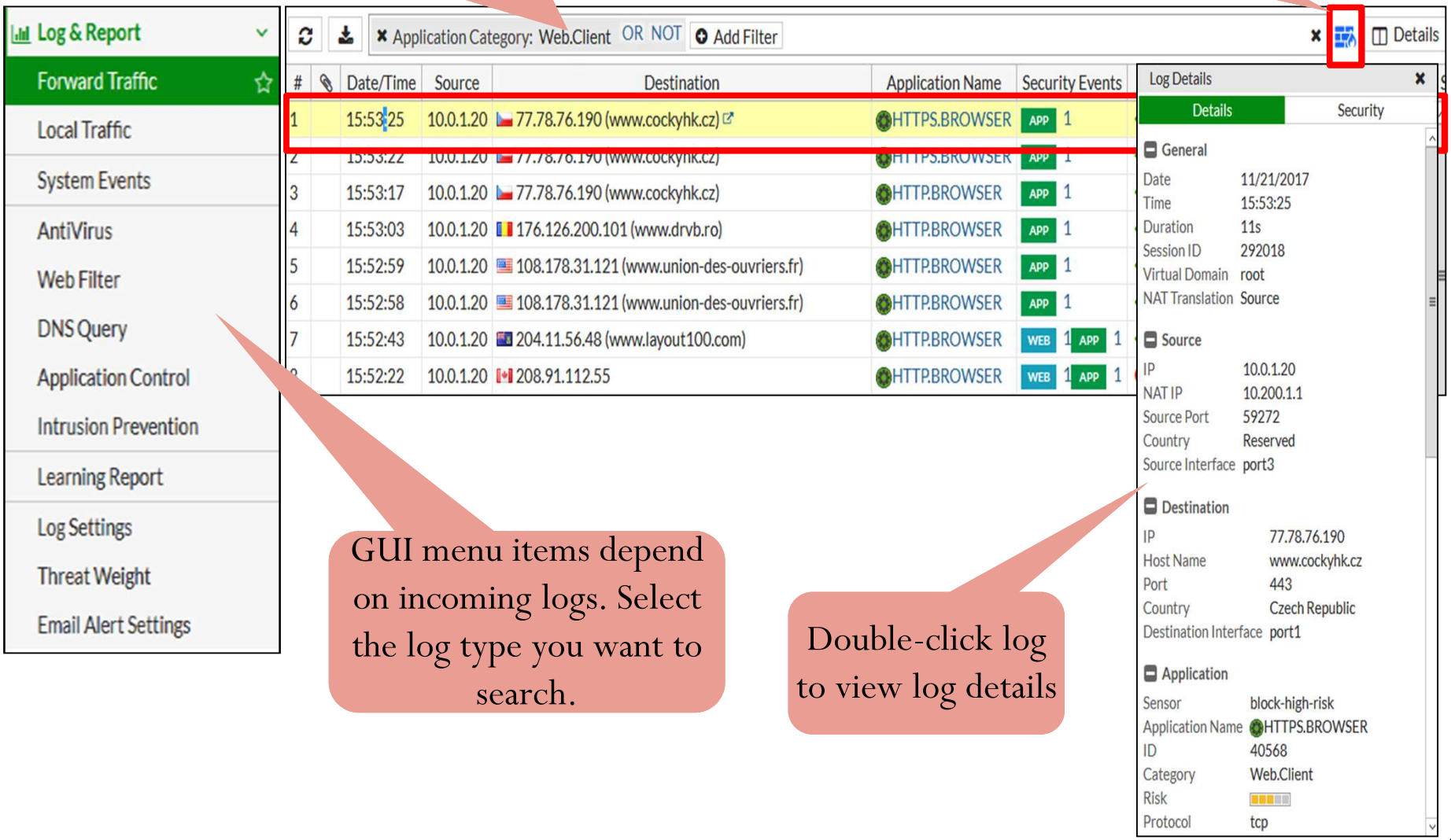
- View and search for log messages on the GUI
- View and search for log messages on the CLI
- View logs through FortiView
- Configure alert email
- Configure threat weight

Viewing Log Messages: GUI

Log & Report

Set log filters to narrow search

Log location = disk



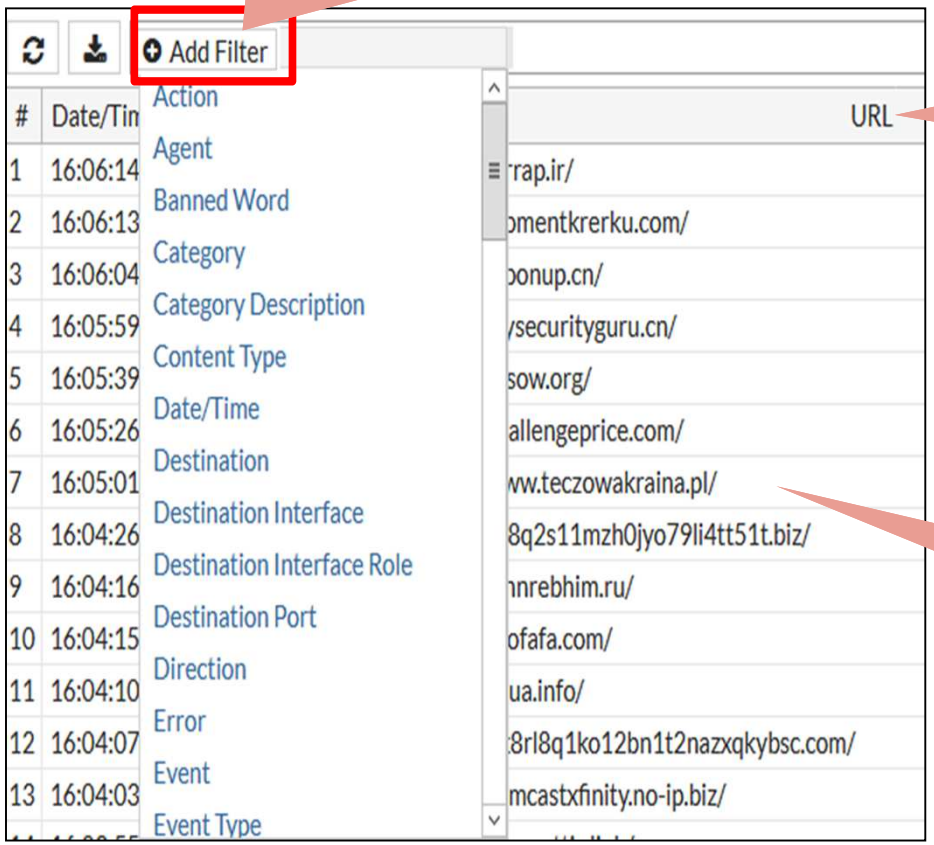
GUI menu items depend on incoming logs. Select the log type you want to search.

Double-click log to view log details

Searching for Logs: Filters

- Add log filters to search for specific

Click **Add Filter** and available filter options appear in the drop-down list



- If the filter you want to add is
showing as a value on the GUI
but does appear in the log itsel
add the table column on the G

Right-click any table column to add a new column to the table

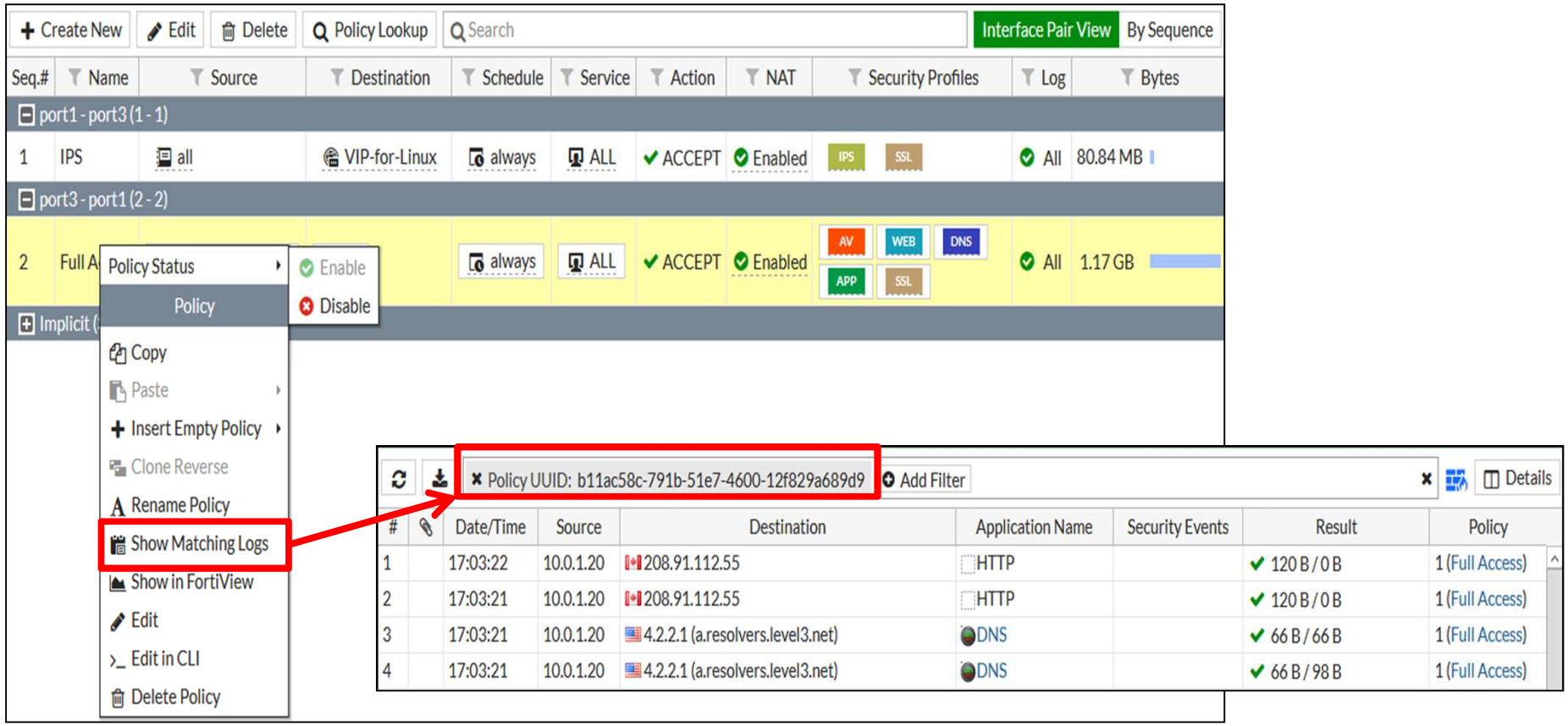
- Use quick filter options to sea
data already in the log table

Right-click the column of a specific log for quick filter options

Viewing Logs Associated with a Firewall Policy

- Access log messages generated by individual policies

Policy & Objects > IPv4 Policy



Viewing Log Message: CLI

```
# execute log filter
```

Configures what log messages you will see, how many log messages you can view at one time (a maximum of 1000 lines of log messages), and the type of log messages you can view.

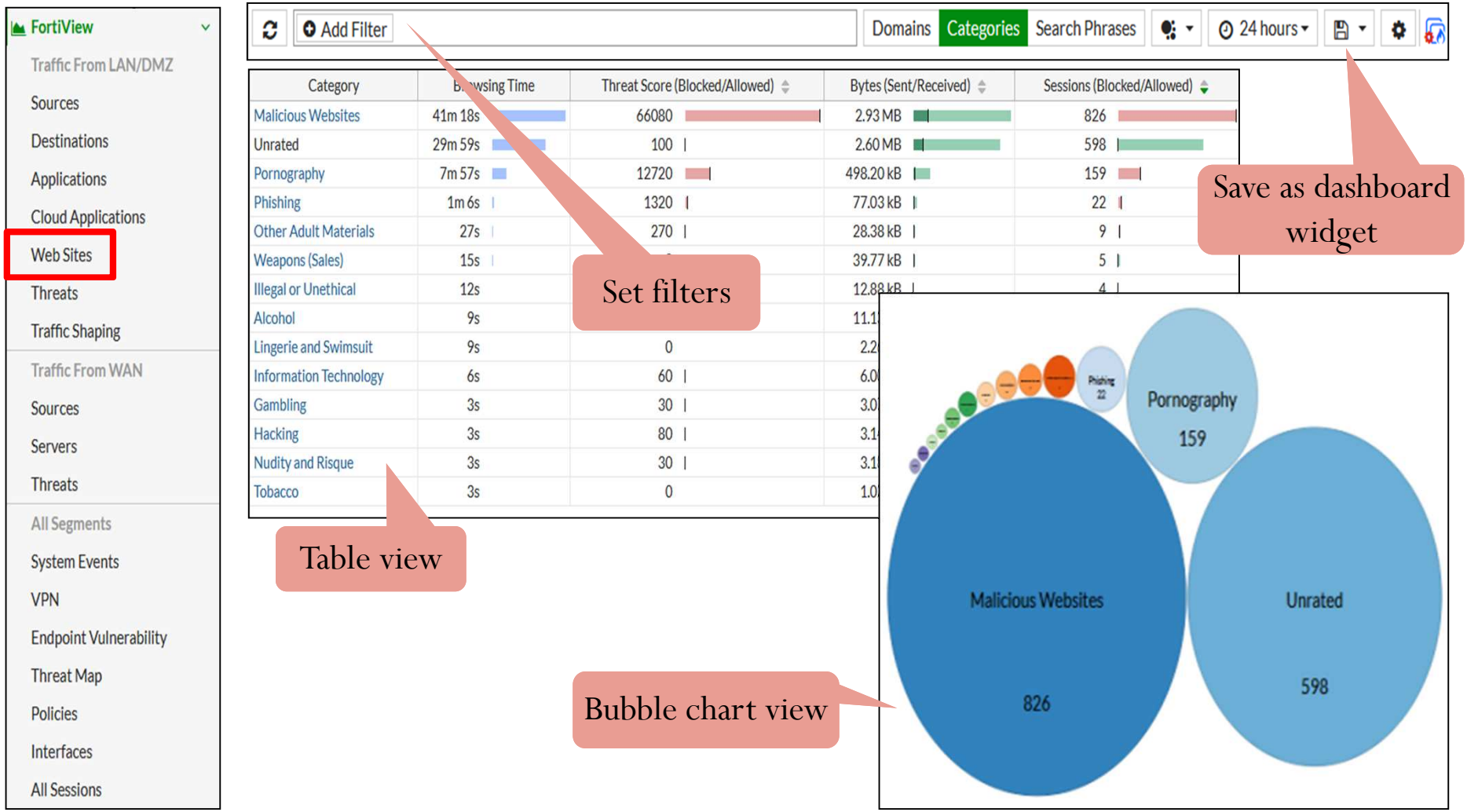
```
# execute log display
```

Allows you to see specific log messages that you already configured within the `execute log filter` command.

```
Local-FortiGate # exe log display
32183 logs found.
10 logs returned.
19.7% of logs has been searched.

1: date=2017-11-21 time=16:04:14 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" logtime=1511309054 srcip=10.0.1.20 srcport=16979 srcintf="p
cintfrole="undefined" dstip=4.2.2.1 dstport=53 dstintf="port1" dstintfrole="undefined" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" sessionid=294174 proto=17 action="a
olicyid=1 policytype="policy" service="DNS" dstcountry="United States" srccountry="Reserved" trandisp="snat" transip=10.200.1.1 transport=16979 appid=16195 app="DNS" app
work.Service" apprisk="elevated" applist="block-high-risk" duration=181 sentbyte=61 rcvdbyte=61 sentpkt=1 rcvdpkt=1

2: date=2017-11-21 time=16:04:13 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" logtime=1511309053 srcip=10.0.1.20 srcport=7172 srcintf="pc
intfrole="undefined" dstip=4.2.2.1 dstport=53 dstintf="port1" dstintfrole="undefined" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" sessionid=294173 proto=17 action="ac
licyid=1 policytype="policy" service="DNS" dstcountry="United States" srccountry="Reserved" trandisp="snat" transip=10.200.1.1 transport=7172 appid=16195 app="DNS" appca
rk.Service" apprisk="elevated" applist="block-high-risk" duration=181 sentbyte=61 rcvdbyte=93 sentpkt=1 rcvdpkt=1

3: date=2017-11-21 time=16:04:13 logid="0000000013" type="traffic" subtype="forward" level="notice" vd="root" logtime=1511309053 srcip=10.0.1.20 srcport=41000 srcintf="p
cintfrole="undefined" dstip=208.91.112.55 dstport=80 dstintf="port1" dstintfrole="undefined" poluuid="b11ac58c-791b-51e7-4600-12f829a689d9" sessionid=294963 proto=6 acti
out" policyid=1 policytype="policy" service="HTTP" dstcountry="Canada" srccountry="Reserved" trandisp="snat" transip=10.200.1.1 transport=41000 appcat="unknown" applist=
igh-risk" duration=12 sentbyte=120 rcvdbyte=0 sentpkt=2 rcvdpkt=0 crscore=5 craction=262144 crlevel="low"
```

Viewing Log Messages: FortiView

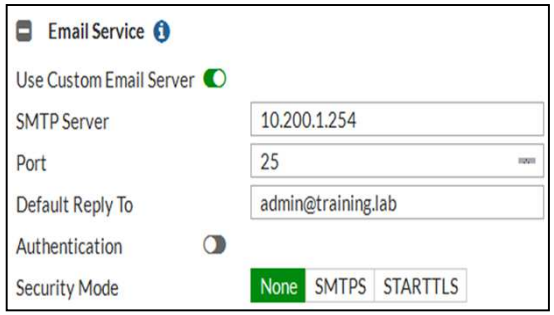
- FortiView integrates real-time and historical data into single, summary



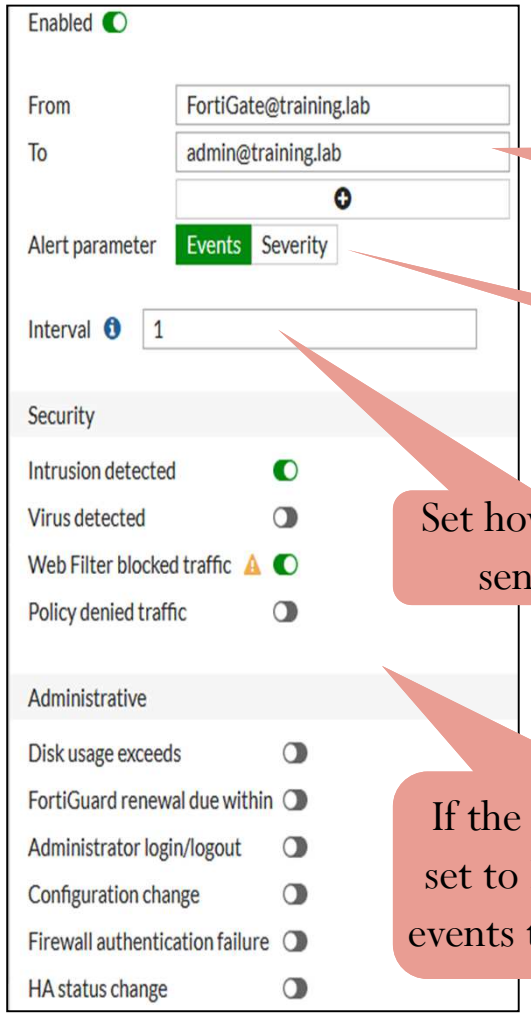
Configuring Alert Email

- Send notification to email upon detection of event
- While there is a default mail server preconfigured, it is recommended to configure your own SMTP server first.

System > Advanced



Log & Report > Email Alert Settings



Configure up to three recipients

Send alert by event or severity

Set how often to send alert

If the alert parameter is set to **Events**, select the events to generate an alert

Local Reports

Top Applications by Bandwidth

Application	Traffic Out	Traffic In	Sessions
YouTube	66.4 GB		56.9 K
HTTPS.BROWSER	36.0 GB		238.0 K
Facebook	28.8 GB		111.9 K
Google.Services	24.5 GB		85.0 K
Naver.Line	19.3 GB		91.7 K
Apple.Store	17.8 GB		10.7 K
MS.Windows.Update	15.1 GB		4.2 K
HTTP.BROWSER	13.7 GB		108.8 K
Google.Cloud.Storage	11.0 GB		342
HTTP.Video	10.9 GB		499

Top Users by Bandwidth

User	Host	Traffic Out	Traffic In	Sessions
10.209.129.23	jmchangde-MBP	14.5 GB		2.4 K
10.209.129.181	DESKTOP-USOR0CQ	8.7 GB		1.7 K
10.209.130.7	a4:e9:75:87:5f:8c	5.8 GB		2.3 K
10.209.17.140	android-d6f2bc26e57b0636	5.1 GB		1.2 K
10.209.17.201	04:d6:aa:97:43:f5	4.4 GB		7.1 K
10.209.18.234	Ł „å gu-PC	4.3 GB		8.1 K
10.209.17.21	d4:0b:1a:3d:e0:e0	3.5 GB		959
10.209.17.86	34:97:f6:b8:28:82	3.5 GB		3.5 K
10.209.17.34	Antonio	3.5 GB		18.7 K
10.209.17.98	android-3b36ff9078484adb	3.1 GB		1.3 K

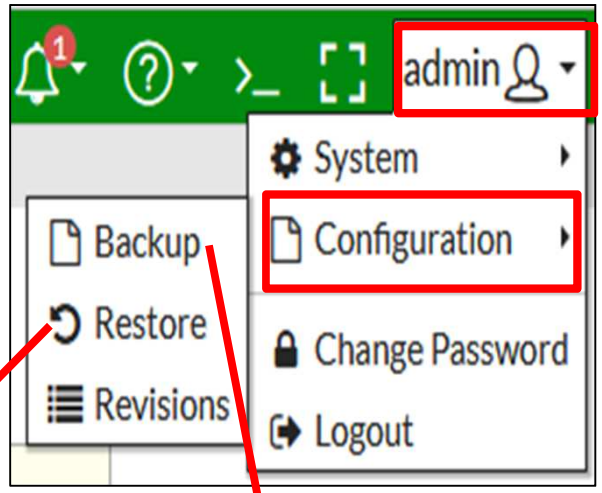
防火牆-備份還原維護

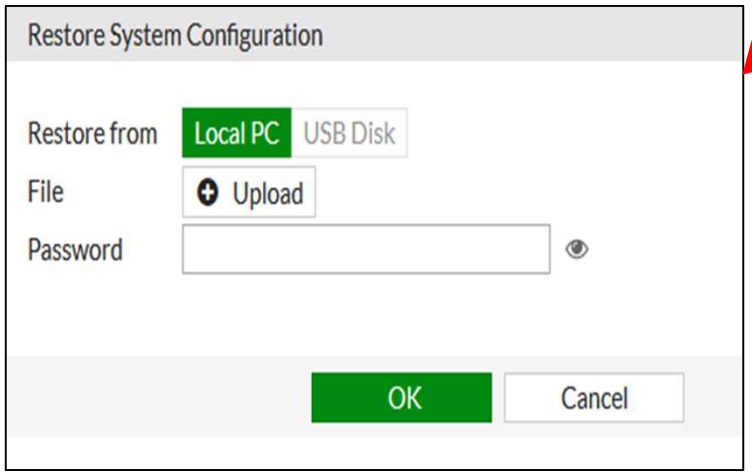
Objectives

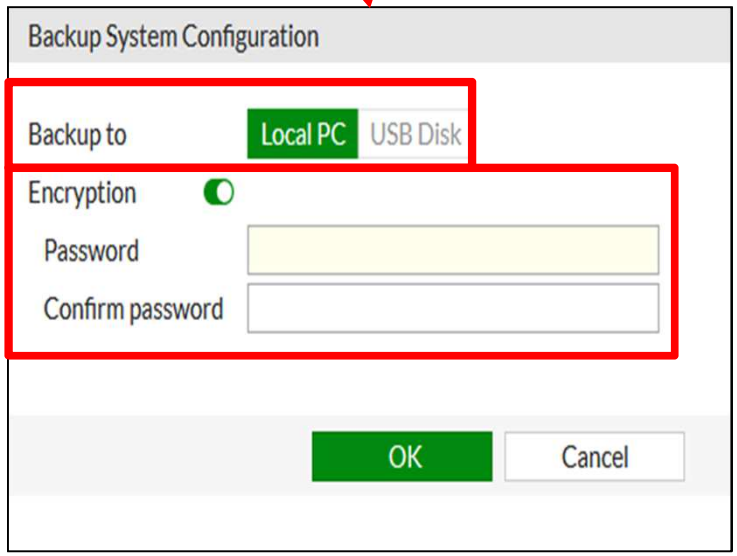
- Back up and restore system configuration files
- Understand the restore requirements for plain text and encrypted configuration files
- Identify the current firmware version
- Upgrade firmware
- Downgrade firmware

Configuration File: Backup and Restore

- Configuration can be saved to an external device
  - Optional encryption
  - Can back up automatically
    - Upon logout
    - Not available on all models
- To restore a previous configuration, upload file.
  - Reboots FortiGate

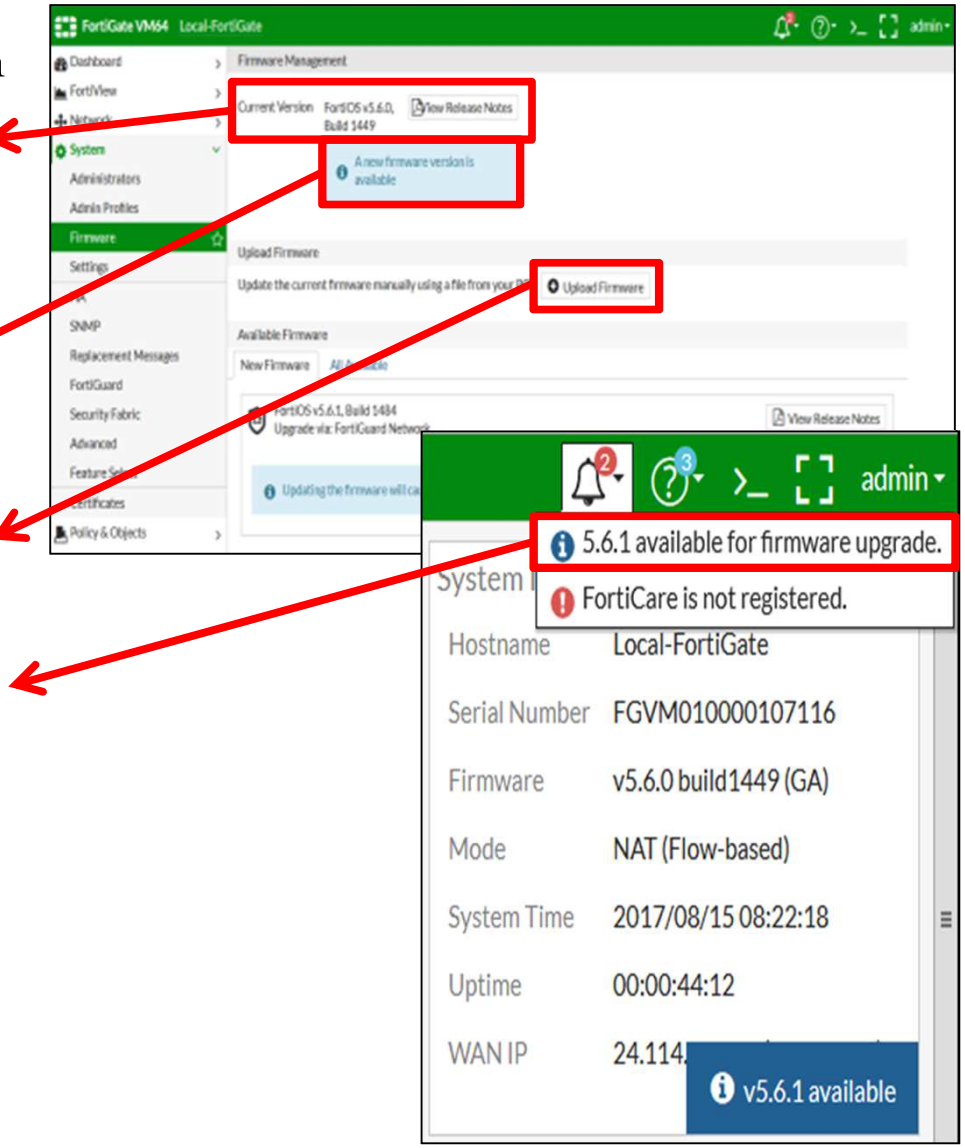






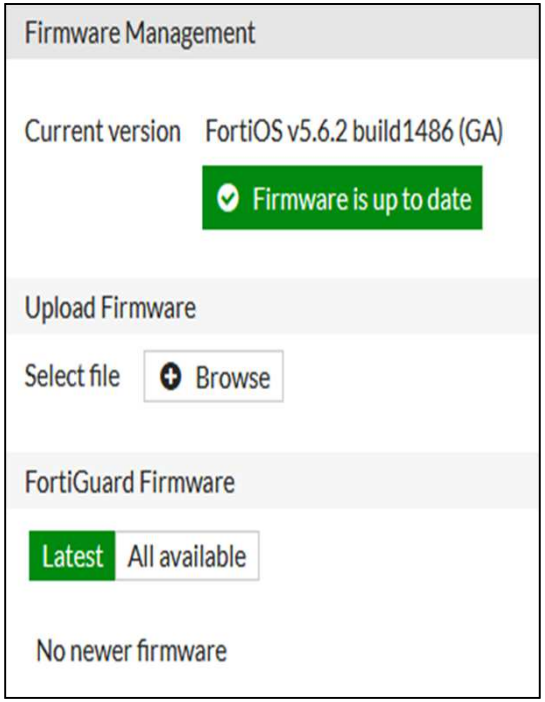
Upgrade Firmware

- The current firmware version can be viewed on the **Dashboard** or in **System** > **Firmware** (or on the CLI: `get system status`).
- If there is an updated firmware version, you will be notified.
- Firmware can be updated by clicking **Upload Firmware** or selecting the upgrade option in the notification icon drop-down list.
- Make sure you read the *Release Notes* to verify the upgrade path and other details.



Upgrade Firmware Process

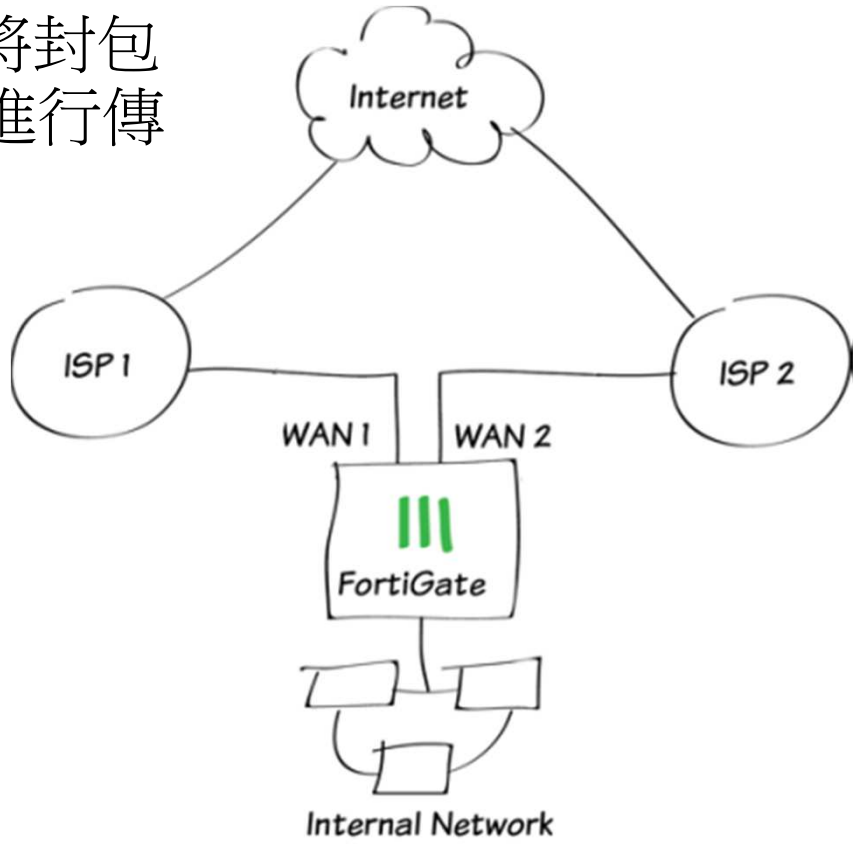
1. Back up the configuration (`full config backup` on GUI or CLI).
2. Download a copy of the current firmware, in case reversion is needed.
3. Have physical access, or a terminal server connected to local console, in case reversion is needed.
4. Read the *Release Notes*; they include the upgrade path and other useful information.
5. Perform the upgrade.



Policy Based Routing (PBR) 基於策略的路由

- 何為 策略路由 Policy Based Routing (PBR) ?
- 在於多WAN的環境之下，而針對進入路由的封包來因應需求而將封包分別丟往不同的WAN端上來進行傳輸。

- **Wan Link Loadbalance**
- **SD-WAN**



Policy Based Routing (PBR) 基於策略路由

- Static Routes 權重

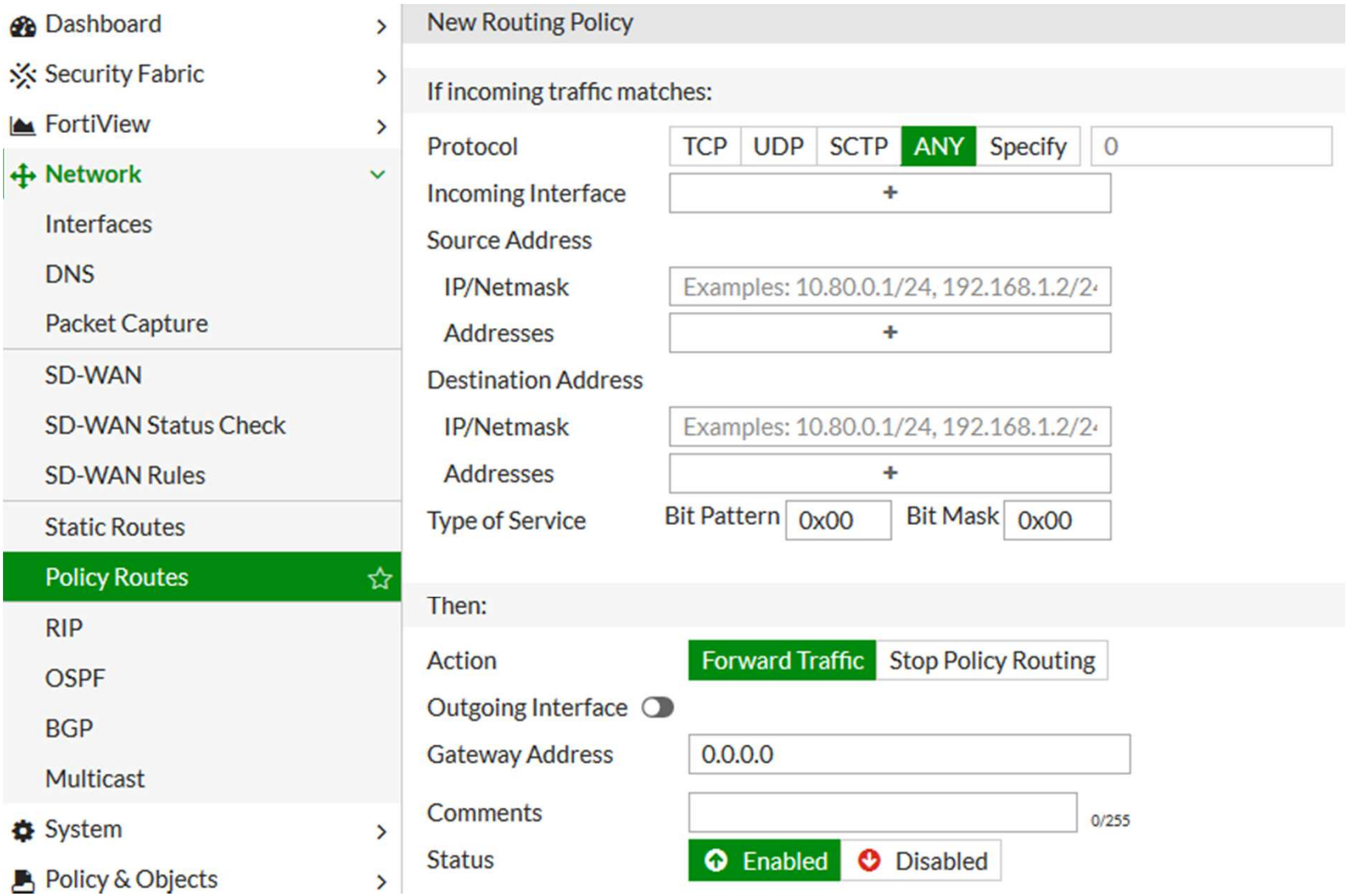
Port1 :管理距離:10, 優先權:0

Port2: 管理距離:10, 優先權:20

- 預設管理距離,優先權不顯示
- (政策路由 > 直接連接或應對 > 靜態路由 >動態路由)

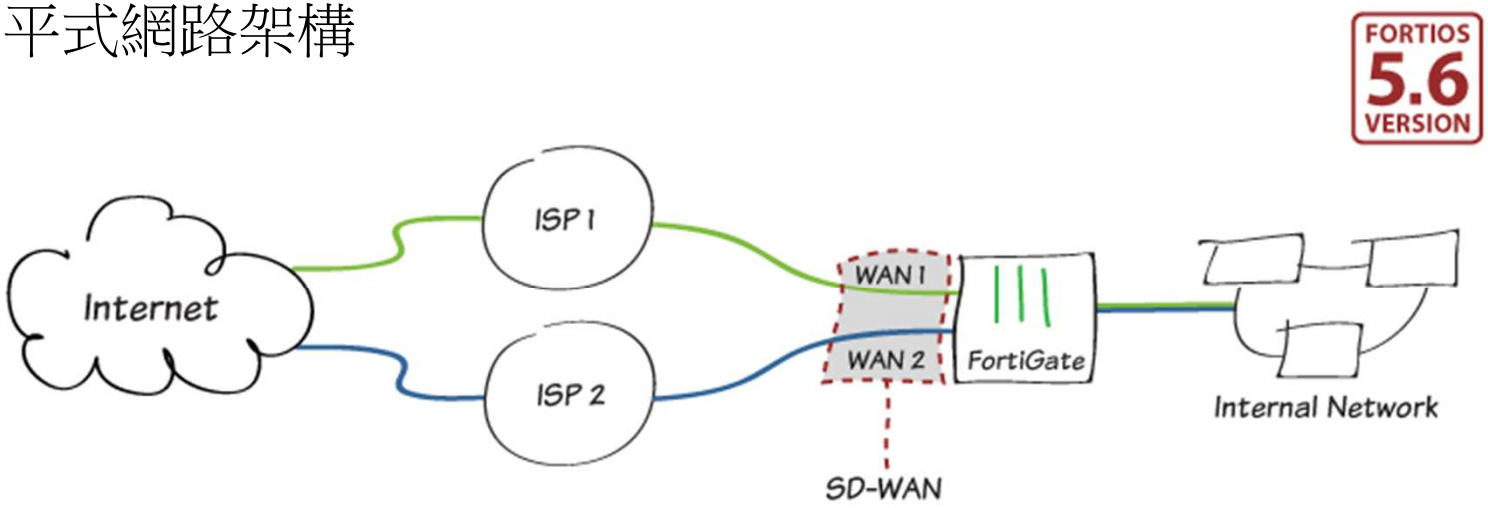
Destination	Gateway	Interface	Comment	Distance	Priority
0.0.0.0/0	[redacted].254	port1		10	0
0.0.0.0/0	[redacted].254	port2		10	20
10.0.0.0/8	10.209.8.254	device (WiFi_219)		10	0
192.168.96.0/24	10.209.8.254	device (WiFi_219)		10	0
192.168.98.0/24	10.209.8.254	device (WiFi_219)		10	0

Policy Based Routing (PBR) 基於策略路由



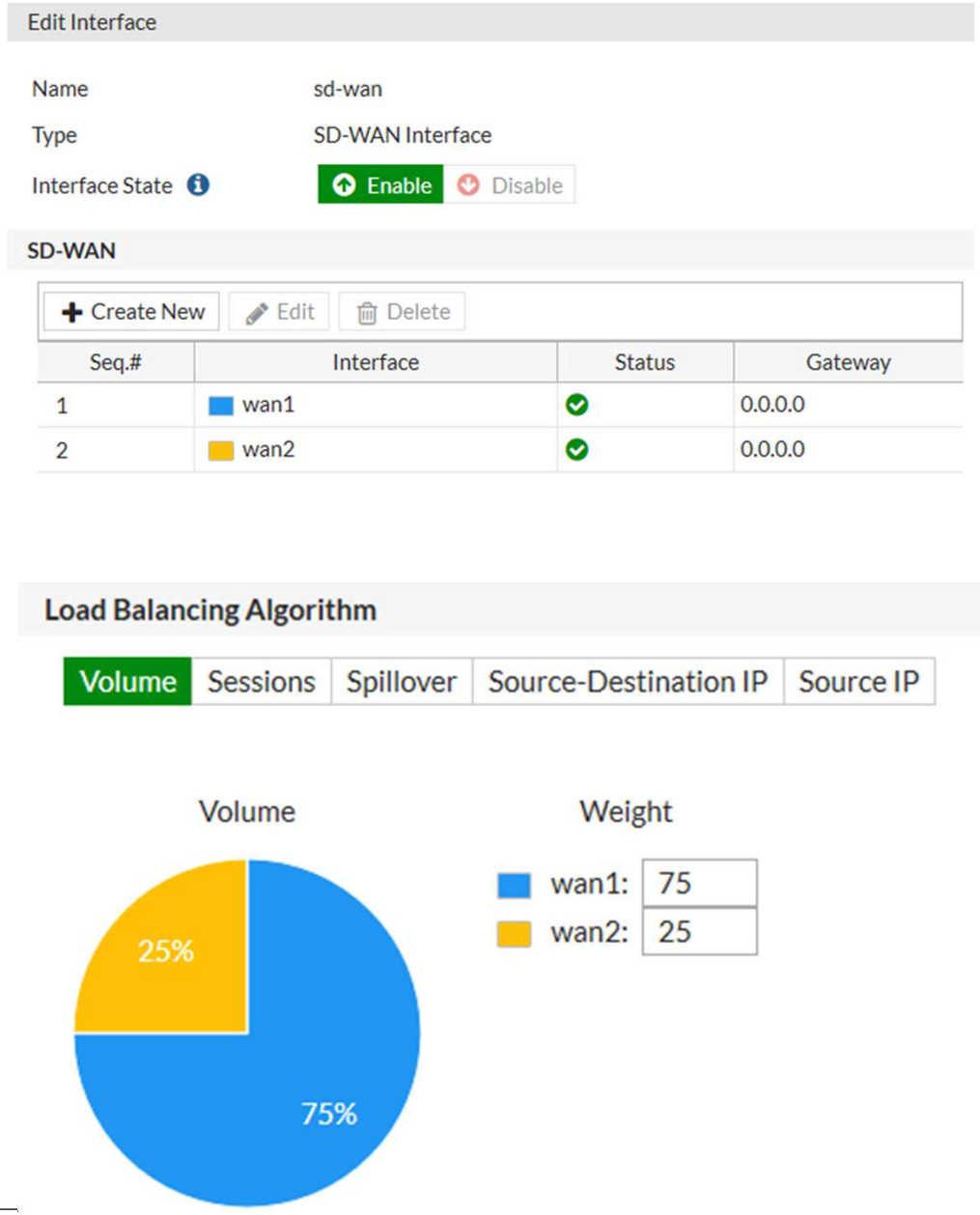
軟體定義廣域網路（SD-WAN）

- 混合廣域網路，提升到軟體定義廣域
  - 早期被動（Active-Passive）的備援線路切換
  - 混合廣域網路支援雙主動（Active-Active）的模式
- 提升線路服務等級協定（SLA）
- 跨線路聰明調度
- 廣域網路最佳化
- 扁平式網路架構



軟體定義廣域網路（SD-WAN）

- **SD-WAN interface**
- **Load Balancing Algorithm**
- **SD-WAN Rule**



線上資源

FortiGate Knowledge Base Libary
http://kb.fortinet.com/

FortiGate Technical Document
http://docs.fortinet.com/

The Fortinet Cookbook
https://cookbook.fortinet.com/

Q&A