



Fortinet Security Architecture and Fabric

Firewall Definitions

Next-generation firewall (NGFW)

Advanced network security device with features like application awareness, integrated intrusion prevention, identity awareness, and threat intelligence.

Data center firewall (DCFW)

Provides robust threat protection for data center traffic with high throughput, low latency, scalability, and virtual domain segmentation.

Internal segmentation firewall (ISFW)

Firewall deployed internally to shield and segment networks, offering protection against internal and bypassed threats which can minimize impact.

Security Fabric

Unites different security tools to share threat information, enhancing visibility and control over the network.

Key features:

Enhanced Visibility:

Provides comprehensive network visibility, including detailed topology and analytics.

Automated Protection:

Automates threat protection and response across the entire network.

Unified Management:

Centralized control and management across all devices and solutions within the fabric.

Fortinet Security Fabric

Scalable

Aware

Secure

Actionable

Open

Advanced Threat
Intelligence

NOC/SOC



Endpoint



Access



Network



Application



Cloud



Scalable Detail

Networks come in all shapes and sizes and are never static during their lifetime.

The network's security infrastructure must be able to keep up with these changes, "blanketing" the entire network.

As well as external environments such as the cloud and do so without compromising the security of the network.



Aware Detail

Without even taking IoT into account, there are more users and devices on the network today than ever before.

More users and devices means more possible ways for the hacker or cybercriminal to infiltrate and implant malware in the network.

The network, and its security infrastructure, can no longer afford to be just a transport system.

Knowledge of the users and their devices is necessary in order to assign security policies to them, granting or limiting access to network resources and reducing the risk of unknown threats.



Secure Detail

The implementation of any security in a network can only be successful if it doesn't slow down the network.

The security infrastructure must have the underlying architecture to support the different security services that will run on it

Regardless of where in the network those services are being deployed.

Cloud adoption is one of the major drivers on today's networks.

Not all organizations adopt cloud technologies in the same way or at the same rate.

Providing a range of security technologies in virtual form is a mandatory requirement in all enterprise and as they grow.



Actionable Detail

End to end.

Access to data center.

IoT to cloud.

These are the challenges that our customers are facing daily.

To successfully respond to these challenges, the customer must have the necessary, appropriate and actionable resources.

Scalable



Aware



Secure



Actionable



Open



Open Detail

No one company can do everything themselves.

It takes an extensive eco-system of products and technologies to meet all the challenges.

As the challenges grow and change so will the eco-system.

This eco-system is enabled through the Fabric and its series of APIs.

Open Detail

Intelligent security is also open.

The Security Fabric is designed around a series of open Application Programming Interfaces (APIs).

Allows organizations to integrate existing security investments from Fabric-Ready partners into the Fortinet Security Fabric.

These solutions can actively collect and share threat information and distribute mitigation instructions to improve visibility and intelligence.

Security Fabric Communication

FortiTelemetry protocol

Used for direct, secure communication between FortiGate devices and other Security Fabric components.

Bidirectional FortiTelemetry connectivity for successful communication is required

FortiTelemetry use TCP/8013

Fabric-object-unification

Controls the sharing of global Central Management Database (CMDB) objects within a Security Fabric which includes

- Firewall address objects

- Address groups

- Service objects

- And others

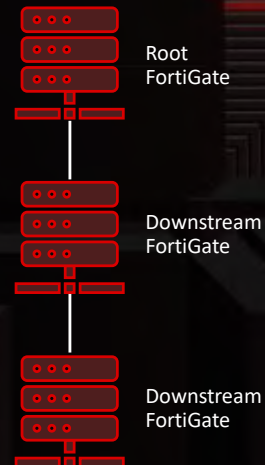
Local mode

- Does not apply synced object

- Sends synchronized object downstream

- Accepts and forwards synced objects

```
config system csf
  set fabric-object-unification local
end
```



Security Fabric Devices

FortiGate

Combines firewall, intrusion prevention (IPS), antivirus, and more in one appliance.

FortiAP

Provides secure and controlled access to wireless networks.

FortiSwitch

Designed to integrate with Fortinet security products and provide secure and scalable Ethernet solutions.

Security Fabric Devices

FortiClient

Protects individual devices from malware, phishing, and other threats.

Offers integrated VPN options for secure remote access.

FortiSandbox

Utilizes sandboxing techniques to detect unknown and zero-day threats.

Includes both static and dynamic analysis for thorough threat evaluation.

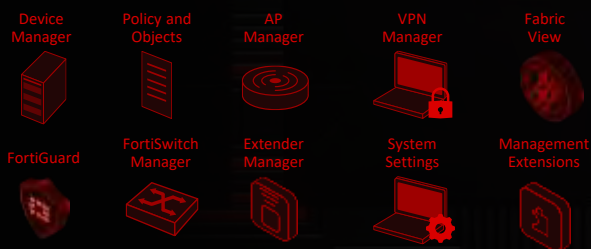
FortiMail

Provides robust protection against spam, phishing, and malware in email.

Helps in safeguarding sensitive information through content inspection.

FortiManager

FortiAnalyzer



Centralizes management and orchestration of the Security Fabric.
Allows bulk configuration changes across different devices.



Provides logging, analytics, and reporting across the Security Fabric.

Conclusions

Terms

NGFW

DCFw

ISFW

FortiGate Security Architecture

Security Fabric

Communication requirements

Fabric-object-unification



FortiGate Resource Management

FortiGate Memory Utilization

FortiGate units use memory for many of its operations:

- logging
- storing configuration
- temporary session data

Memory utilization refers to the percentage of memory being used by the FortiGate unit at a given time.

High memory utilization may not indicate a problem, unless it remains consistently high or reaches a point where it impacts system performance.



Diagnose Hardware sysinfo Memory

Identify high memory usage and understand where the memory is being consumed.

FortiFirewall-VM64-KVM # diagnose hardware sysinfo memory

MemTotal: 1007596 kB
MemFree: 374436 kB
MemAvailable: 346592 kB
Buffers: 116 kB
Cached: 260772 kB
SwapCached: 0 kB
Active: 217984 kB
Inactive: 51828 kB
Active(anon): 217124 kB
Inactive(anon): 47248 kB
Active(file): 860 kB
Inactive(file): 4580 kB
Unevictable: 185428 kB
Mlocked: 0 kB
SwapTotal: 0 kB
SwapFree: 0 kB
Dirty: 0 kB
Writeback: 0 kB
AnonPages: 194368 kB
Mapped: 102104 kB
Shmem: 74372 kB
Slab: 84740 kB
SReclaimable: 6436 kB
SUnreclaim: 78304 kB

KernelStack: 2688 kB
PageTables: 17756 kB
NFS_Unstable: 0 kB
Bounce: 0 kB
WritebackTmp: 0 kB
CommitLimit: 503796 kB
Committed_AS: 13013312 kB
VmallocTotal: 34359738367 kB
VmallocUsed: 0 kB
VmallocChunk: 0 kB
Percpu: 312 kB
AnonHugePages: 0 kB
ShmemHugePages: 0 kB
ShmemPmdMapped: 0 kB
CmaTotal: 0 kB
CmaFree: 0 kB
HugePages_Total: 0
HugePages_Free: 0
HugePages_Rsvd: 0
HugePages_Surp: 0
Hugepagesize: 2048 kB
HugeTlb: 0 kB
DirectMap4k: 28520 kB
DirectMap2M: 1019904 kB

Memory Conserve Mode:

When the FortiGate's memory utilization reaches or exceeds 88% it enters conserve mode to prevent out-of-memory conditions.

Some processes might be limited or temporarily stopped to conserve memory.

```
FortiFirewall-VM64-KVM # diagnose hardware sysinfo conserve
memory conserve mode:      off
total RAM:                 983 MB
memory used:               469 MB  47% of total RAM
memory freeable:           145 MB  14% of total RAM
memory used + freeable threshold extreme: 934 MB  95% of total RAM
memory used threshold red: 865 MB  88% of total RAM
memory used threshold green: 806 MB  82% of total RAM
```

Memory Conserve Mode:

Three memory thresholds exist

Green (normal operation) = Memory utilization is 82% or lower.

Red = Memory utilization is 88% or higher and it triggers conserve mode.

Extreme = Memory utilization is 95% or higher, at this stage new sessions are dropped.

While in conserve mode the antivirus inspection is bypassed.

```
config system global
    set av-failopen { *pass* | off | one-shot }
end
```

While in conserve mode the IPS engine drops all new sessions that require flow-based inspection.

```
config ips global
    set fail-open { enable | *disable* }
end
```

Memory Conserve Mode:

```
# execute log display
1: date=2022-11-02 time=16:58:37 eventtime=1667433517502192693
tz="-0700" logid="0100022011" type="event" subtype="system"
level="critical" vd="root" logdesc="Memory conserve mode
entered" service="kernel" conserve="on" total=997 MB used=707
MB red="877 MB" green="698 MB" msg="Kernel enters memory
conserve mode"
```

```
diagnose debug crashlog read
1: 2022-10-27 14:22:36 service=kernel conserve=on total="997
MB" used="720 MB" red="877 MB"
2: 2022-10-27 14:22:36 green="817 MB" msg="Kernel enters
memory conserve mode"
```

<https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/194558/conserve-mode>

Conserve Modes

System

Action:
Depends on fail-open setting

Kernel

Proxies are bypassed
Configuration cannot be changed

Less Aggressive

More Strict

*The threshold that each is
activated depends on device.

Shared Memory (shm)

It allows multiple processes running on a FortiGate unit to share some amount of memory.

If in conserve mode there will be additional output stating it is on.

```
FortiFirewall-VM64-KVM # diagnose hardware sysinfo shm
```

SHM FS total:	481988608	459 MB
SHM FS free:	478343168	456 MB
SHM FS avail:	478343168	456 MB
SHM FS alloc:	3645440	3 MB

Reducing Memory Utilization

Shorten Session Timers

Tcp-halfclose-time

Default is 120 sec

Wait after one peer has sent a FIN packet but the other has not responded

Tcp-halfopen-timer

Default is 10 sec

Wait after one peer has sent an open session packet but the other has not responded

Tcp-timewait-timer

Default is 1 sec

Udp-idle-timer

Default is 180 sec

```
FortiFirewall-VM64-KVM # config system global
FortiFirewall-VM64-KVM (global) # set tcp-halfclose-timer 30
FortiFirewall-VM64-KVM (global) # set tcp-halfopen-timer 5
FortiFirewall-VM64-KVM (global) # set tcp-timewait-timer 0
FortiFirewall-VM64-KVM (global) # set udp-idle-timer 60
```

Reducing Memory Utilization

Reduce Session active time

Default is 3600

Reduce maximum file size for inspection

Reduce service caches

```
FortiFirewall-VM64-KVM # config system session-ttl  
FortiFirewall-VM64-KVM (session-ttl) # set default 300
```

CPU Utilization

get system performance top

See entries using most cpu resources

```
Run Time: 0 days, 1 hours and 19 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 983T, 362F
  cmdbsvr    1816    S    0.0    5.2    0
    node     1852    S    0.0    5.2    0
    cw_acd    1894    S    0.0    4.0    0
  ipshelper   1859    S <    0.0    4.0    0
  miglogd     1874    S    0.0    3.8    0
  forticron   1863    S    0.0    3.8    0
  miglogd     1907    S    0.0    3.7    0
    csfd      1897    S    0.0    3.5    0
    autod     1905    S    0.0    3.4    0
    httpsd    1851    S    0.0    3.3    0
    newcli    2036    S <    0.0    3.3    0
initXXXXXXXXX 1      S    0.0    3.3    0
  fgfmd      1892    S    0.0    3.3    0
    wad       1899    S    0.0    3.1    0
    wad       1900    S    0.0    2.9    0
  fnbamd     1861    S    0.0    2.8    0
  fcnacd     1871    S    0.0    2.7    0
  authd      1865    S    0.0    2.7    0
    wad       1908    S    0.0    2.6    0
    wad       1875    S    0.0    2.6    0
```


CPU Utilization

Code	Description
U	Percentage of user space applications that are currently using the CPU
N	Percentage of time that the CPU spent on low priority processes since the last shutdown
S	Percentage of system processes (or kernel processes) that are using the CPU
I	Percentage of idle CPU resources
WA	Percentage of time that the CPU spent waiting on IO peripherals since the last shutdown
HI	Percentage of time that the CPU spent handling hardware interrupt routines since the last shutdown
SI	Percentage of time that the CPU spent handling software interrupt routines since the last shutdown
ST	steal time Percentage of time a virtual CPU waits for the physical CPU when the hypervisor is servicing another virtual processor
T	Total FortiOS system memory in MB
F	Free memory in MB

<https://docs.fortinet.com/document/fortigate/6.2.15/coolbook/232929/troubleshooting-high-cpu-usage>

```
Run Time: 0 days, 1 hours and 19 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 983T, 362F
cmdbsvr 1816 S 0.0 5.2 0
node 1852 S 0.0 5.2 0
cw_acd 1894 S 0.0 4.0 0
ipshep 1859 S < 0.0 4.0 0
miglogd 1874 S 0.0 3.8 0
forticron 1863 S 0.0 3.8 0
miglogd 1907 S 0.0 3.7 0
csfd 1897 S 0.0 3.5 0
autod 1905 S 0.0 3.4 0
httpsd 1851 S 0.0 3.3 0
newcli 2036 S < 0.0 3.3 0
initXXXXXXXXX 1 S 0.0 3.3 0
fgfmd 1892 S 0.0 3.3 0
wad 1899 S 0.0 3.1 0
wad 1900 S 0.0 2.9 0
fnbamd 1861 S 0.0 2.8 0
fcncad 1871 S 0.0 2.7 0
authd 1865 S 0.0 2.7 0
wad 1908 S 0.0 2.6 0
wad 1875 S 0.0 2.6 0
```

Crashlogs

Generated when a critical error causes a system failure.

Process/Daemon

Errors

Conserve Modes

```
FortiFirewall-VM64-KVM # diag debug crashlog read
1: 2023-07-20 12:24:06 from=license
sn=FFVMEVFCA5AT3F9 msg=Server replied error code:0
2: 2023-07-20 12:24:07 the killed daemon is
/bin/sflowd: status=0x0
3: 2023-07-20 12:40:23 the killed daemon is
/bin/getty: status=0x0
4: 2023-07-20 14:12:27 the killed daemon is
/bin/getty: status=0x0
5: 2023-07-28 14:16:47 the killed daemon is
/bin/getty: status=0x0
6: 2023-07-28 14:16:49 the killed daemon is
/bin/getty: status=0x2
7: 2023-07-28 14:45:49 the killed daemon is
/bin/getty: status=0x0
Crash log interval is 3600 seconds
Max crash log line number: 16384
```

Conclusions

Memory Utilization

Conserve Mode

Shared Memory

Reducing Memory Utilization

CPU Utilization

Crashlogs

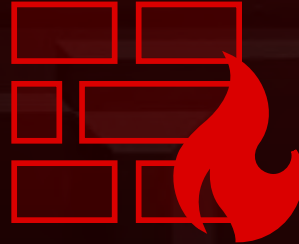


FortiGate Firewall Policies and Applications

Firewall Policy

The firewall policy is the axis around which most of the other features of the FortiGate firewall revolve.

Any traffic going through a FortiGate unit must be associated with a policy.



Firewall Policy

Name and UUID:

Identifies the policy as "Allow-Ping-All" with a unique identifier

Source Interface (srcintf):

"any" allows traffic from any interface

Destination Interface (dstintf):

"any" allows traffic to any interface

Action:

"accept" permits the traffic

Source Address (srcaddr):

"all" includes all source addresses

Destination Address (dstaddr):

"all" includes all destination addresses

Schedule:

"always" ensures the rule is active at all times

Service:

"ALL" includes all available services

```
config firewall policy
edit 1
    set name "Allow-Ping-All"
    set uuid e8cfa100-36c5-51ee-4758-
301486898730
    set srcintf "any"
    set dstintf "any"
    set action accept
    set srcaddr "all"
    set dstaddr "all"
    set schedule "always"
    set service "ALL"
next
```

Fortigate Accept or Deny

When the Fortigate firewall receives a connection packet;

- it analyzes the packet's source address,

- destination address

- service (by port number).

It also registers the incoming interface

The outgoing interface it will need to use

Time of day.

If it finds a policy that matches the parameters it then looks at the action for that policy.

- If it is ACCEPT the traffic is allowed to proceed to the next step.

- If the Action is DENY or a match cannot be found the traffic is not allowed to proceed



Fortigate Accept or Deny (Actions)

ACCEPT or DENY, the two basic actions;

If the Action is ACCEPT, the policy action permits communication sessions.

There may be other packet processing instructions.

If the Action is DENY, the policy action blocks communication sessions.

You can optionally log the denied traffic.

If no security policy matches the traffic, the packets are dropped.

A DENY security policy is needed when it is required to log the denied traffic, also called "violation traffic".



FortiGate Firewall Policy Parameters

Incoming/Outgoing Interface

Source/Destination Address

Schedule

Service

FortiGate Firewall Policy Parameters

Incoming



The interface or interfaces that the traffic is first connection to the FortiGate unit by.

Except for traffic that the FortiGate generates itself.

Not limited to the physical Ethernet ports found on the device.

Incoming interface can also be a logical or virtual interface such as a VPN tunnel, a Virtual WAN link or a wireless interface.

Outgoing



After the firewall has processed the traffic it needs to leave a port to get to its destination and this will be the interface or interfaces that the traffic leaves by.

Like the Incoming Interface, is not limited to only physical interfaces.

The Outgoing interface can also be a logical or virtual interface such as a VPN tunnel, a Virtual WAN link or a wireless interface.

Source Address



Addresses that a policy sets that can receive traffic from can be wide open or tightly controlled.



Public webserver that the world at large should be able to access

Best choice will be “all”.



If the destination is a private webserver that only the branch offices of a company should be able to access

A group of preconfigured addresses is the better strategy.

Source Address Parameters

Source Users;

Based on a user identity that can be from several authentication authorities.

It will be an account or group that has been set up in advance that can be selected from the dropdown menu.

The exception to this is the feature that allows the importing of LDAP Users.

When the feature is used, a small wizard window will appear to guide the user through the setup.

The caveat is that the LDAP server object must be already configured to allow the use of this import feature.

Destination Address



In the same way that the source address may need to be limited, the destination address can be used as a traffic filter.

When the traffic is destined for internal resources the specific address of the resource can be defined to better protect the other resources on the network.



One of the specialized destination address options is to use a Virtual IP address.

The destination address doesn't need to be internal.

You can define policies that are only for connecting to specific addresses on the Internet.

Schedule



This can be something as simple;

A time range that the sessions can start such as between 8:00 am and 5:00 pm.



Something more complex;

Business hours that include a break for lunch and time of the session's initiation may need a schedule group because it will require multiple time ranges to make up the schedule.

Service



The service or service chosen here represents the TCP/IP suite port numbers that will most commonly be used.

This will be a little different than Application Control which looks more closely at the packets to determine the actual protocol used to create them.

Explicit Deny by Default



Out of the box, once you have your FortiGate device connected into your network and hooked up with your ISP your network is protected.

Nothing is getting out or in so it is not very convenient

You don't have to worry during setup and policies configuration that someone could have gotten in and done something to your resources.



You cannot assume that any traffic will be allowed just because it makes sense to do so.

If you want any kind of traffic to make it past the FortiGate firewall you need to create a policy.



To maintain the protection of the network, you should also make sure that the any policy you create allows only the traffic you intend.

Policy Order

Another important factor in how firewall policies work is the concept of precedence of order

“First come, first serve.”

It’s highly likely that after only a relatively small number of created policies that there will be some that overlap.

When this happens there must be a method to determine which policy should be applied to the packet.

The method which is used by most firewalls is based on the order of the sequence of the policies.

Policy Application

If all the policies were placed in a sequential list the process to match up the packet would start at the top of the list and work its way down;

- 1 The interface the packet connected to the FortiGate firewall
- 2 The source address of the packet, and possibly the sending user and device.
- 3 The destination address of the packet
- 4 The interface the packet would need to use to get to the destination address based on the routing table
- 5 The port the packet is destined for
- 6 The time that the packet connected to the FortiGate

As soon as a policy is reached that matches all the applicable parameters, the instructions of that policy are applied the search stops.

All subsequent policies are disregarded. Only 1 policy is applied to the packet.

Implicit Policy

If no matching configured policy is found, it will drop to the last implicit policy.

One of a few that are referred to by the term “policy0”.

This policy denies everything.

The implicit policy is made up of the following settings:

Incoming Interface: any

Source Address: any

Outgoing Interface: any

Destination Address: any

Action: DENY

Logical Best Practice

Make sure that the more specific or specialized a policy is, the closer to the beginning of the sequence it should be.

The more general a policy is the higher the likelihood that it could include in its range of parameters a more specifically targeted policy.

The more specific a policy is, the higher the probability that there is a requirement for treating that traffic in a specific way.

UUID Support

Universally Unique Identifier (UUID) attributes have been added to policies to improve functionality when working with FortiManager or FortiAnalyzer units.

If required, the UUID can be set manually through the CLI

```
config firewall
{policy/policy6/policy46/policy64}
edit 1
set uuid <example uuid:
8289ef80-f879-51e2-20dd-
fa62c5c51f44>
next
end
```

Firewall Policy - Lab



Create multiple Firewall Policies

VLAN

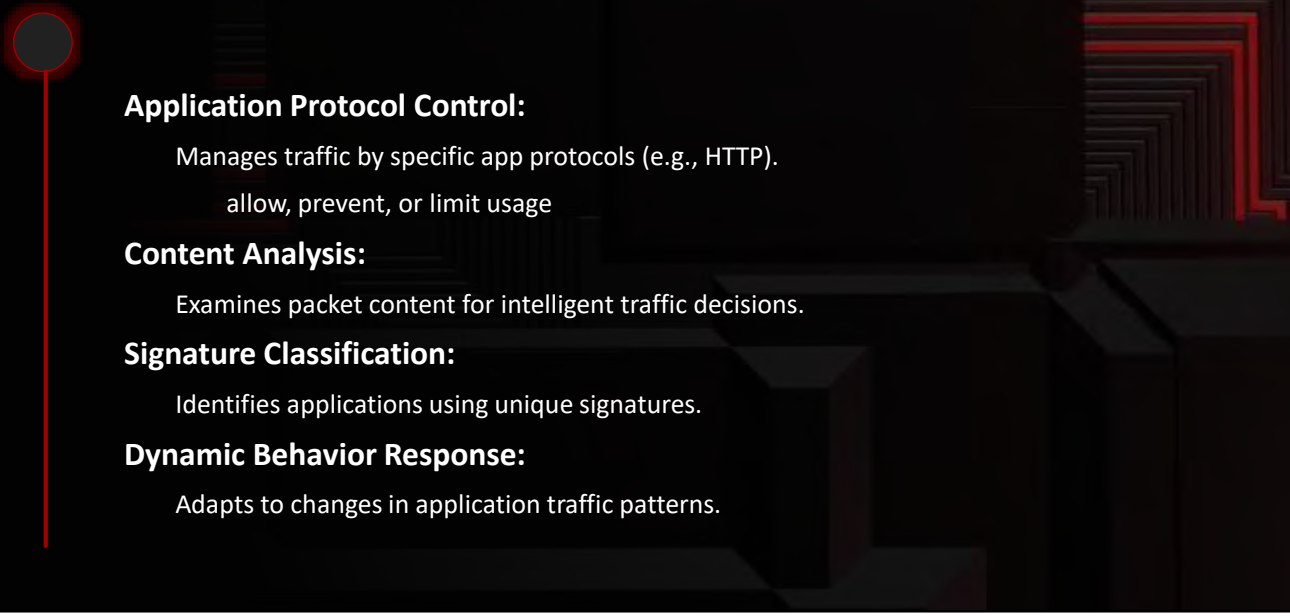
Specific applications

Open



Application Controls and Signatures

Application-based Policy



Application Protocol Control:

Manages traffic by specific app protocols (e.g., HTTP).
allow, prevent, or limit usage

Content Analysis:

Examines packet content for intelligent traffic decisions.

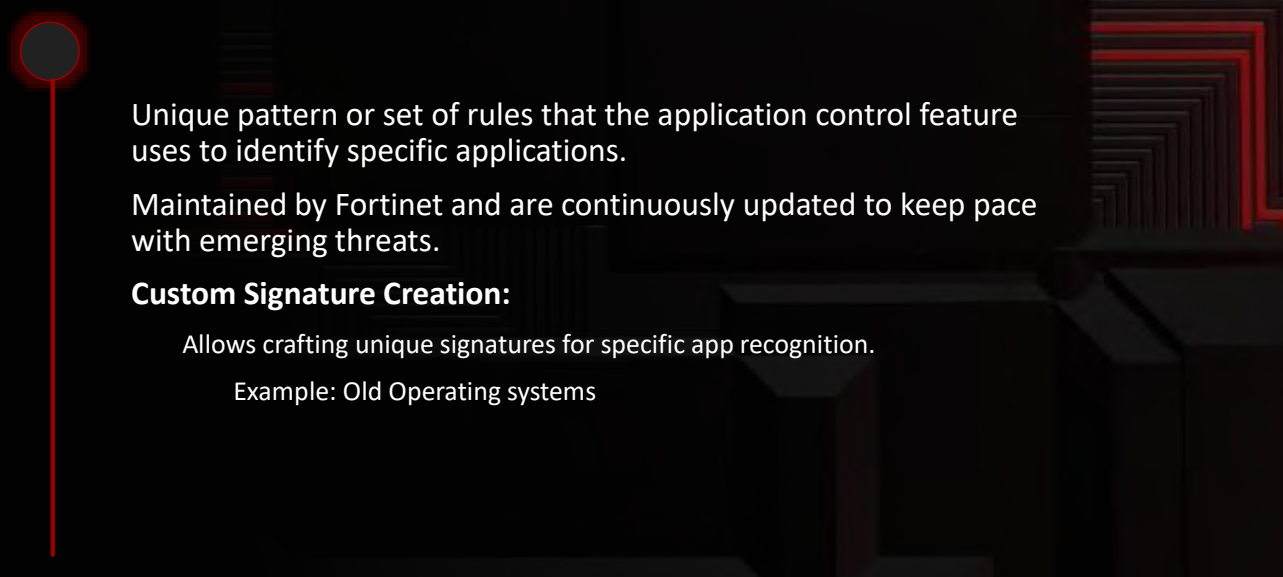
Signature Classification:

Identifies applications using unique signatures.

Dynamic Behavior Response:

Adapts to changes in application traffic patterns.

Application Signatures



Unique pattern or set of rules that the application control feature uses to identify specific applications.

Maintained by Fortinet and are continuously updated to keep pace with emerging threats.

Custom Signature Creation:

Allows crafting unique signatures for specific app recognition.

Example: Old Operating systems

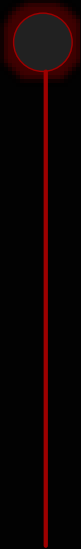
Configuring Application-based policy - LAB

Security Profiles -> Application Signatures

Show creation of custom signature and blocking of application



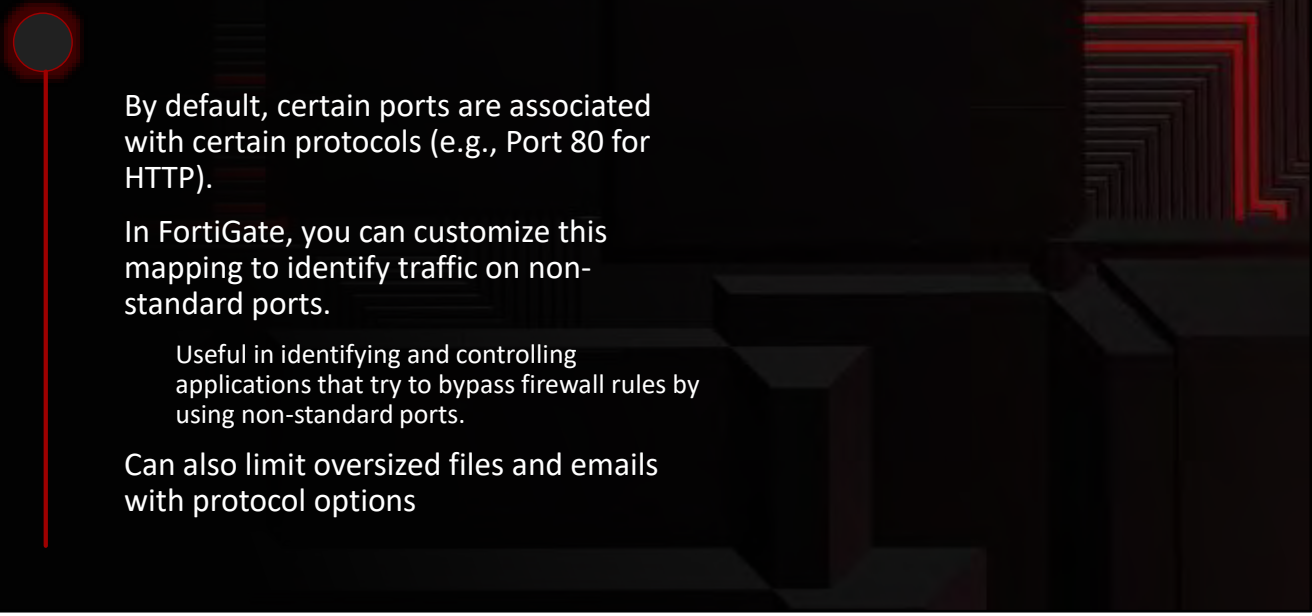
Protocol Options



Protocol options are advanced settings in FortiGate that allow administrators to modify the default behaviors of certain protocols.

Offer granular control over various protocols like HTTP, DNS, FTP, and many more.

Port Mapping



By default, certain ports are associated with certain protocols (e.g., Port 80 for HTTP).

In FortiGate, you can customize this mapping to identify traffic on non-standard ports.

Useful in identifying and controlling applications that try to bypass firewall rules by using non-standard ports.

Can also limit oversized files and emails with protocol options

Configure Protocol Options -Lab

Policy & Objects -> Protocol Options

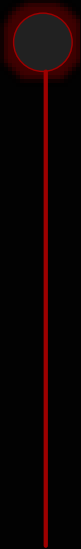
Tour protocol options

Port mapping

Others



Protocol Enforcement



Configure networking services on known ports.

FTP, HTTP, HTTPS

21, 80, 443

Protocols which are not whitelisted under select ports, the IPS engine performs the violation action to block, allow, or monitor that traffic.

Set Up Protocol Enforcement in CLI

```
config application list
  edit "protocol-GUI"
    set other-application-log enable
    set control-default-network-services {enable I
disable}
  config default-network-services
    edit 1
      set port 80
      set services http
    next
    edit 2
      set port 53
      set services dns
      set violation-action {pass I monitor I block}
    next
  end
next
end
```

Set Up Protocol Enforcement in CLI

1

Go to Security Profiles > Application Control.

2

Create a new application sensor or edit an existing one.

3

Enable Network Protocol Enforcement.

4

Enforcement entries can be created, edited, or deleted.



Set Up Protocol Enforcement in GUI

- 1 Click Create New in the Network Protocol Enforcement table.
- 2 In the New Default Network Service pane:
- 3 Enter a Port number.
- 4 Select Enforced protocols.
- 5 Choose the Violation action.
- 6 Click OK.



Troubleshooting applications

Diagnose test application

Run various test on different applications and daemons.

```
FortiFirewall-VM64-KVM # diagnose test application dns
worker idx: 0
1. Clear DNS cache
2. Show stats
3. Dump DNS setting
4. Reload FQDN
5. Requery FQDN
6. Dump FQDN
7. Dump DNS cache
8. Dump DNS DB
9. Reload DNS DB
10. Show SDNS rating cache
11. Clear SDNS rating cache
12. DNS debug bit mask
13. DNS debug obj mem
99. Restart dnsproxy worker
```

Conclusions

Firewall Policies

Application Signatures

Protocol Options



Central Management

FortiManager

Centrally manage and control multiple FortiGate devices and their features.

Monitor network security, manage device configurations, perform updates, and more across multiple FortiGate devices.

Can provide local FortiGuard services

Device
Manager



Policy and
Objects



AP
Manager



VPN
Manager



Fabric
View



FortiGuard



FortiSwitch
Manager



Extender
Manager



System
Settings



Management
Extensions



FortiGate to FortiManager Connection

Set type fortimanager

Determines device is managed by Fortimanager

set fmg "X.X.X.X"

Sets IP for the FortiManager

```
config system central-management
set type fortimanager
set fmg "172.18.37.148"
config server-list
edit 1
set server-type update
set server-address 172.18.37.150
next
edit 2
set server-type rating
set server-address 172.18.37.149
next
end
set fmg-update-port 443
set include-default-servers enable
```

FortiGate to FortiManager Connection

set server-type

Update

Antivirus and IPS updates

Rating

Web filtering services

URL ratings

Categories

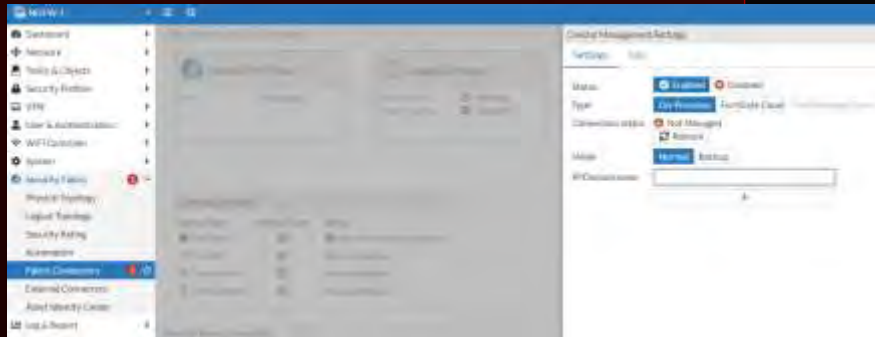
set include-default-servers enable

Uses Fortinet's default update and rating servers

If ones configured is unreachable

```
config system central-management
set type fortimanager
set fmg "172.18.37.148"
config server-list
edit 1
set server-type update
set server-address 172.18.37.150
next
edit 2
set server-type rating
set server-address 172.18.37.149
next
end
set fmg-update-port 443
set include-default-servers enable
```

Fabric Connectors



Wizards within FortiManager

Add Device

Add devices to FortiManager

Import Configuration



Add Device



ADOMS and VDOMS

ADOMS and VDOMS

VDOMs (Virtual Domains)

VDOMs are a method of dividing a FortiGate into two or more virtual units that function as multiple independent units.

Allows separate firewalls within a single device.

Each VDOM can have different policies and settings.

Useful for large organizations and managed service providers.

ADOMs (Administrative Domains)

ADOMs are used in FortiManager to logically group devices for easier management.

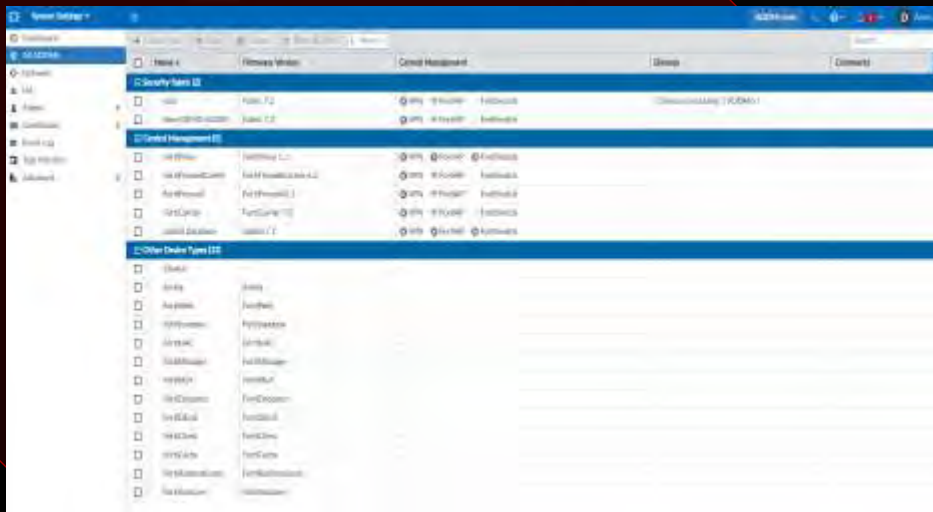
Allows separate management spaces within FortiManager.

Each ADOM can manage different devices and configurations.

Useful for managed service providers and multi-department organizations.

VDOMs divide a single FortiGate into multiple firewalls, while ADOMs group different devices under a single FortiManager.

Creating ADOMs



Creating ADOMs

Firmware
Type
Mode
Management
Device Selection
Policy Check
AutoPush
Status



Diagnose dvm device list

Provide information on all devices managed by FortiManager

Important information:

Dev-db

device database status

Conf

configuration status

Dm

device manager status

Conn

connection status

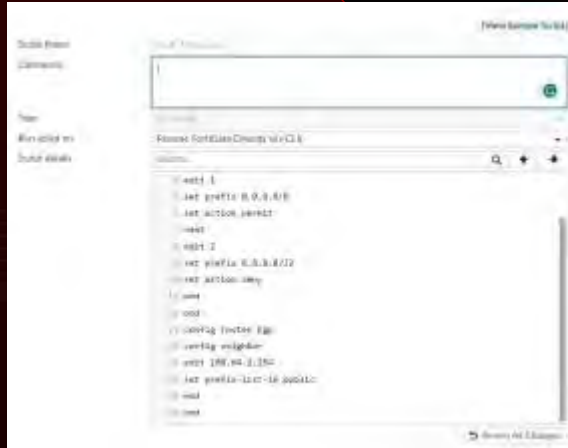
```
FortiManager # diagnose dvm device list
--- There are currently 6 devices/vdoms managed ---
--- There are currently 6 devices/vdoms count for license ---
TYPE      OID  SN      HA  IP      NAME      ADOM  IPS      FIRMWARE
fmgfz-managed 273  FGVM910000075546  10.1.0.1  FGVM010000077646  DC  6.00741 (regular)  7.0 MR2 (1396)
[- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
[- vdom: [3]root flags: 0 adom:DC pkg:[never-installed]
fmgfz-managed 309  FGVM010000077648  10.1.0.100  FGVM010000077648  DC  6.00741 (regular)  7.0 MR2 (1396)
[- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
[- vdom: [3]root flags: 0 adom:DC pkg:[never-installed]
fmgfz-managed 297  FGVM010000077649  a-p 10.1.0.254  FGVM010000077649  Core 6.00741 (regular)  7.0 MR2 (1396)
[- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: retrieved; conn: up
HA cluster member: FVM010000077649 (primary); conn: up; conf: in sync
[- vdom: [3]root flags: 0 adom:Core pkg:[imported]FGVM010000077649
unregistered 285  FGVM010000077650  10.1.0.253-9443  FGVM010000077650  root N/A 7.0 MR2 (1396)
[- STATUS: dev-db: unknown; conf: unknown; cond: unregistered; dm: none; conn: unknown
[- vdom: [3]root flags: 0 adom:root pkg:[never-installed]
fmgfz-managed 321  FGVM010000077651  100.64.3.1  Spoke-1  Core 6.00741 (regular)  7.0 MR2 (1396)
[- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
[- vdom: [3]root flags: 0 adom:Core pkg:[installed]Spokes
fmgfz-managed 333  FGVM010000077652  100.64.5.1  Spoke-2  Core 6.00741 (regular)  7.0 MR2 (1396)
[- STATUS: dev-db: not modified; conf: in sync; cond: OK; dm: installed; conn: up
[- vdom: [3]root flags: 0 adom:Core pkg:[installed]Spokes
--- There are currently 0 FortiAP managed ---
--- There are currently 0 FortiSwitch managed ---
--- There are currently 0 FortiExtender managed ---
--- End device list ---
```

CLI Scripts

These are scripts written in FortiGate's command-line interface (CLI) language.

They allow you to automate virtually any task that can be performed through the CLI.

*more complex scripts are less likely to work across different FortiGate versions.



CLI Scripts

Requirements

Full CLI commands

No short form

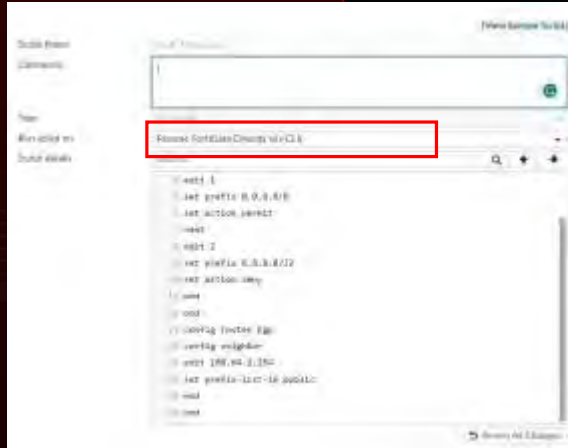
```
# mark comments
```

Can be run in three different ways:

Device database

Policy package, ADOM database

Remote FortiGate directly



TCL Scripts

More advanced and allow for greater control and flexibility

Conditional statements

Loops

Variables

TCL scripts do not run through the FGFM tunnel like CLI scripts

```
#!/
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# " 15]
}
set num_users 10
do_cmd "config vdom"
do_cmd "edit root"
do_cmd "config user local"
for {set i 1} {$i <= $num_users} {incr i} {
  set name [format "usr%04d" $i]
  puts "Adding user: $name"
  do_cmd "edit $name"
  do_cmd "set status enable"
  do_cmd "set type password"
  do_cmd "next"
}
do_cmd "end"
do_cmd "end"

do_cmd "config vdom"
do_cmd "edit root"
do_cmd "show user local"
do_cmd "end"
```

<https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/914165/tcl-scripts>

TCL Scripts

Requirements

SSH authentication required

Can only be run on the remote FortiGate directly

No exit commands

Starts with #!

```
#!/
proc do_cmd {cmd} {
  puts [exec "$cmd\n" "# " 15]
}
set num_users 10
do_cmd "config vdom"
do_cmd "edit root"
do_cmd "config user local"
for {set i 1} {$i <= $num_users} {incr i} {
  set name [format "usr%04d" $i]
  puts "Adding user: $name"
  do_cmd "edit $name"
  do_cmd "set status enable"
  do_cmd "set type password"
  do_cmd "next"
}
do_cmd "end"
do_cmd "end"

do_cmd "config vdom"
do_cmd "edit root"
do_cmd "show user local"
do_cmd "end"
```

<https://docs.fortinet.com/document/fortimanager/7.4.0/administration-guide/914165/tcl-scripts>

Wizards within FortiManager

Add device

Discover and add supported devices to FortiManager

Install

Install configuration changes from Device Manager or Policies & Objects to one or more devices

Import configuration

Import policies, objects, AP profiles, and FortiSwitch templates from managed devices to FortiManager.

Lab- CLI and TCL Scripts

Setup and apply a CLI and TCL script



FortiManager as a Local FortiGuard Distribution Server (FDS)

Used for networks without internet access

Distribute updates for services such as antivirus, intrusion prevention system (IPS), and web filtering

Updates and licenses downloaded and uploaded to FortiManager



FortiGuard -> Settings

FortiManager as a Local FortiGuard Distribution Server (FDS)

UPDATE URLs and Ports:

URL: Generally connects to FortiGuard servers (e.g., `update.fortiguard.net`).

Port: Typically TCP 443 for secure HTTPS connections or TCP 80 for HTTP.

Purpose: These are used to download antivirus definitions, IPS updates, and other security-related updates.

LICENSE URLs and Ports:

URL: Licensing may involve connection to Fortinet's licensing servers (e.g., `support.fortinet.com`).

Port: Usually TCP 443 for secure HTTPS connections.

Purpose: This connection is utilized to validate, renew, and manage licenses for Fortinet products, including FortiManager itself.

FortiManager as a Local FortiGuard Distribution Server (FDS)

Network should be closed to use
FortiGuard as local FDS

```
config fmupdate publicnetwork
set status disable
end
```

Conclusions

FortiManager

Adding Devices

ADOMs and VDOMs

CLI and TCL Scripts

FDS



Access Management

Configuring Users

Local users

Stored on the FortiGate unit

Remote users

Stored on an external server

RADIUS

LDAP

User groups

Simplify the task of applying security policies and authentication rules to multiple users at once

Setting Up Administration Access

Public-facing ports could potentially be accessed by individuals who should not be accessing to the FortiGate unit.

During the FortiGate unit setup, you can set the protocol type an administrator must utilize in order to access the FortiGate unit.

The options include:

- HTTPS
- SSH
- SNMP
- PING
- CAPWAP
- RADIUS Accounting
- FortiManager Access (FMG-Access)
- FortiTelemetry

Setting Up Administration Access (Example)

This example will add an IPv4 address (172.20.120.100) to the WAN1 interface. It also sets the administrative access to HTTPS and SSH.

GUI:

- 1 Go to Network > Interface.
- 2 Select the WAN1 interface row and select Edit.
- 3 Select the Addressing Mode of Manual.
- 4 Enter the IP address for the port of 172.20.120.100/24.
- 5 For Administrative Access, select HTTPS and SSH.
- 6 Select OK.

CLI:

```
config system interface
    edit wan1
    set ip 172.20.120.100/24
    set allowaccess https ssh
end
```

Secure Administration Access (Best Practices)

For greater security **NEVER** allow **HTTP** or **Telnet** administrative access to a FortiGate interface.

Only allow **HTTPS** and **SSH** access.

GUI:

- 1 Network > Interfaces (GUI)
- 2 Adjusting the administrative access to each interface.

CLI:

```
config system interface
    edit <interface-
name>
        set allowaccess https ssh
    end
```

Restrict Access from Trusted Hosts (Best Practices)

Setting up trusted hosts for an administrator limits the addresses from where they can log into FortiOS.

- HTTPS
- SSH
- SNMP
- Etc

When you identify a trusted host for an administrator account, FortiOS accepts that administrator's login only from one of the trusted hosts.

A login, even with proper credentials, from a non-trusted host is dropped.

Two-Factor Authentication for Administrators

FortiToken and FortiToken Mobile 2-factor authentication are both supported by FortiGate

FortiToken Mobile is available on Android and iOS devices.

FortiGate units that are registered receive two trial tokens for free.

You can purchase additional tokens from your reseller or from Fortinet.

GUI:

- 1 System > Administrators
- 2 'Enable Two-factor Authentication'

FortiGate Registration



To receive full access to Fortinet Support as well as FortiGuard Services, register your FortiGate unit.

Register this FortiGate with FortiCare by logging in or creating a new account

in or

There are no limitations on the number or type of customers, users, devices, IP addresses, or number of VPN clients being served by the platform.

These factors are limited solely by the hardware capacity of each given model.

FortiGate Setup

There are several system settings that should be configured once your FortiGate is installed:

- Default administrator password
- Settings
- Changing the host name
- System Time
 - Ensure that accuracy for effective scheduling and logging
- Administration Settings
- Password Policy
- View Settings
- Administrator password retries and lockout time
- CPU and memory thresholds

Administrator Password Retries and Lockout Time



By default, the FortiGate will set the number of password retries to three

Allows the administrator a maximum of three attempts to log in before locking the account



Both the number of attempts (admin-lockout-threshold) and the wait time before the administrator can try to enter a password again (admin-lockout-duration) can be configured

Resetting a Lost FortiGate Admin Password

You'll need to directly log on to the unit and reset the password using the "maintainer" account.

The password will have its own format and it will be `bcpb<serial-number>`.

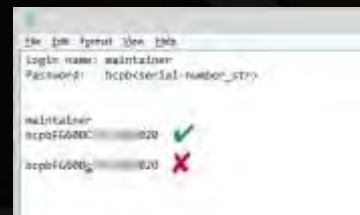
You will have only 14 seconds to type in the username and password.

Having the Username and Password on hand or copied is good practice.

There is no indicator when your time runs out, so it might take a few tries to login and reset.

Resetting a Lost FortiGate Admin Password

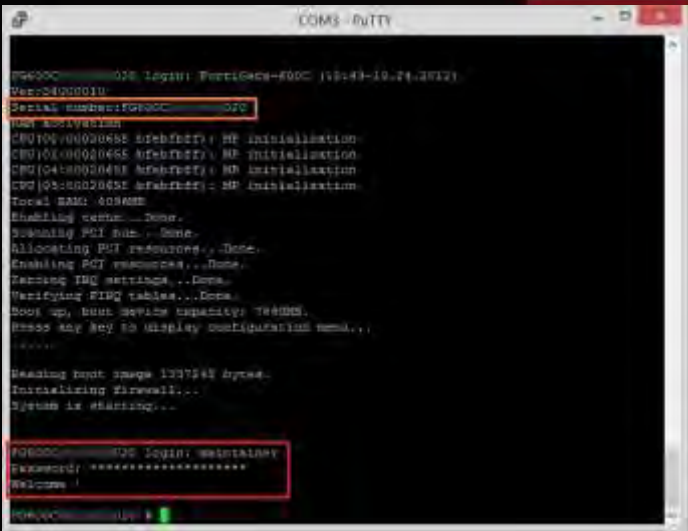
- 1 Connect to the Firewall through console port using terminal emulator such as Putty.
- 2 Power off the Fortigate Firewall/Analyzer.
- 3 Power on the Firewall.
- 4 Wait for the Firewall name and login prompt to appear.
- 5 Copy and paste the username and the password.
- 6 Username: maintainer
- 7 Password: bcpbFG600CXXXXXXXXXX



Resetting a Lost FortiGate Admin Password

Execute following commands to reset the password:

```
config system admin
edit admin
set password XxXXxXxx
end
```



```
COMS - PuTTY

FG600C-----QDE login: FortiGate-F600C (v3:43-10-24-2012)
Ver:34000010
Serial number:FG600C-----QDE

ROM Activation
CPU100(00020082 0Feb18C7): MP Initialization
CPU101(00020082 0Feb18C7): MP Initialization
CPU104(00020082 0Feb18C7): MP Initialization
CPU105(00020082 0Feb18C7): MP Initialization
Total RAM: 4096MB
Loading cache...Done.
Loading PCP bin...Done.
Allocating PCP resources...Done.
Loading PCP resources...Done.
Loading BIOS settings...Done.
Verifying BIOS tables...Done.
Boot up, boot device capacity: 768MB.
Press any key to display configuration menu...
[Enter]

Loading boot image 1277568 bytes.
Installing Firewall...
System is starting...

FG600C-----QDE login: admin
Password: *****
Welcome !

FG600C-----QDE login: k
```

Administrator Profiles

Administrator profiles allow you to define what the administrator can and can't do when logged into the FortiGate.

You can adjust permissions

Administrator's work

Access level

Seniority

Etc

Administrator profile configuration objects specify the account rights.

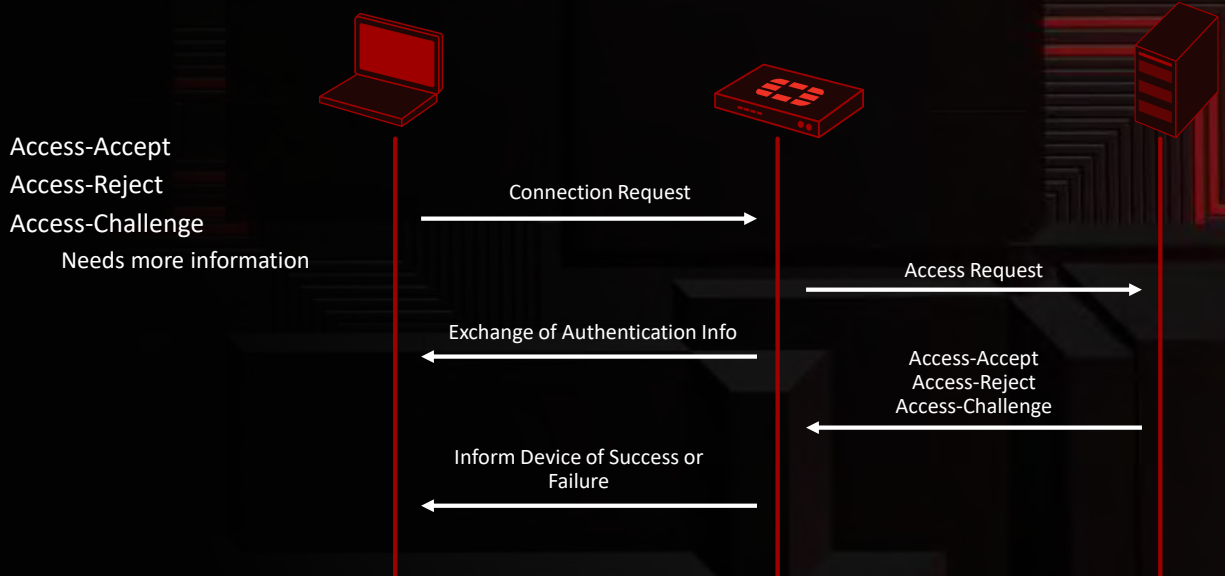
Super_admin Profile

By default, the FortiGate has an admin administrator account that uses the super_admin profile. This profile has access to all components of FortiOS.

For certain administrative functions, such as backing up and restoring the configuration, super_admin access is required.

The super_admin profile can't be deleted or modified.

RADIUS Authentication Process



Configuring RADIUS Server

```
config user radius
edit "<NAME>"
    set auth-type {auto | ms_chap_v2 | ms_chap | chap | pap}
    set nas-ip <IPv4_address>
    set all-usergroup {enable | disable}
    set server <ip address or FQDN>
    set secret <password>
next
end
```

Troubleshooting RADIUS

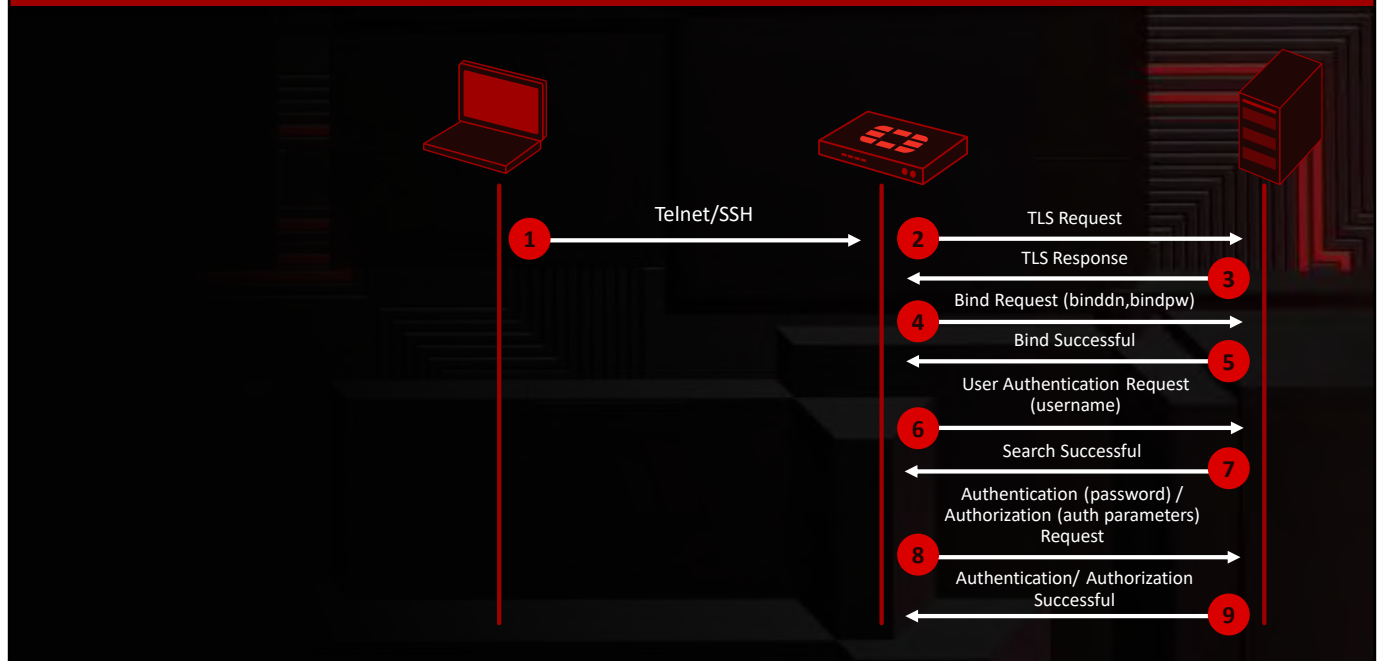
Test Radius

```
diagnose test authserver radius <radius  
server_name> <authentication  
scheme><username> <password>
```

Troubleshoot Failure

```
diagnose debug application fnbamd
```

LDAP Authentication Process



Configuring LDAP Server

```
config user ldap
edit "<NAME>"
  set server "<IP>"
  set cnid "<commonnameidentifier>"
  set dn "dc=fortiad,dc=info"
  set type regular
  set username "cn=admin,dc=domain"
  set password <password>
  set secure ldaps
  set ca-cert "CA_Cert_1"
  set port 636
next
end
```

Troubleshooting LDAP

Test Radius

```
diagnose test authserver ldap <LDAP  
server_name> <username> <password>
```

Troubleshoot Failure

```
diagnose debug application fnbamd
```

Fortinet Single Sign-on (FSSO)

Provides access to multiple resources using single set of credentials

Done by the FSSO Collector Agent (CA)

The Agent monitors user logon activity from domain controllers.

It informs the FortiGate unit about user logon events (who logged in and from which IP address).

It also notifies the FortiGate unit when a user logs out or a session times out.

*Formally called FortiGate Server Authentication Extension (FSAE)

FSSO Collector Agent

The CA is installed on a Windows server and configured to connect to one or more domain controllers.

The agent configuration involves setting the IP address, login credentials, and other details of each domain controller.

The agent also needs to be configured to communicate with the FortiGate unit (IP address, password, etc.).

Diagnosing Issues with FSSO logons

FSSO logons map IP addresses to usernames and groups for policy enforcement.

Correct association of IP address with the user workstation is essential for effective policy execution.

DNS name resolution ensures correct translation between hostnames and IP addresses.

Verification of the source IP of traffic can help pinpoint network misconfigurations.

Reverse DNS lookups help verify the authenticity of hosts in the network.

Internet Issues with FSSO Logons

FSSO users' network access depends on their configuration.

Ignore lists in the CA can limit user access.

Group membership defines user access to resources.

Ensure Group access is allowed in firewall

Troubleshooting FSSO

diagnose debug authd fsso

list

List current logons

refresh-logons

Resync logon database

Installing the FSSO Agent Step 1

1

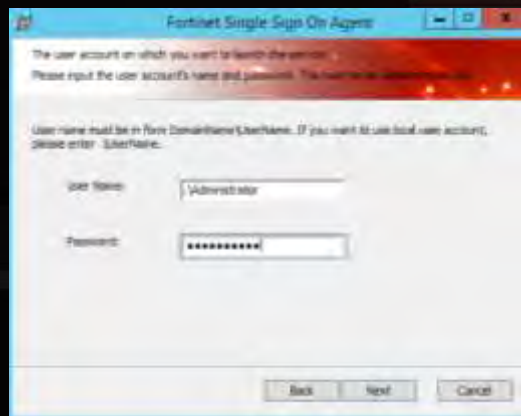
Connect to the Windows AD server and download the FSSO agent from Fortinet Support.

2

To install the agent, open the installer file and use the installation wizard.

3

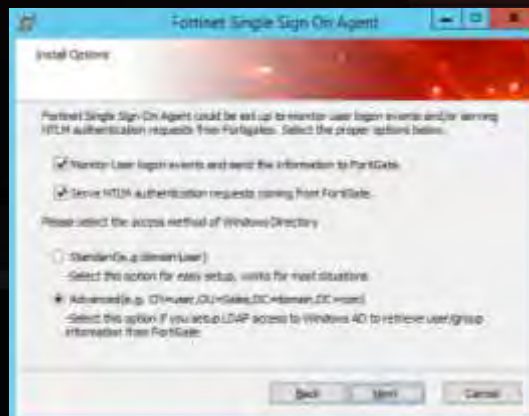
Set a User Name and Password for the FSSO domain administrator.



Installing the FSSO Agent Step 2

1

For the Install Options, select Advanced to use advanced mode instead of standard.



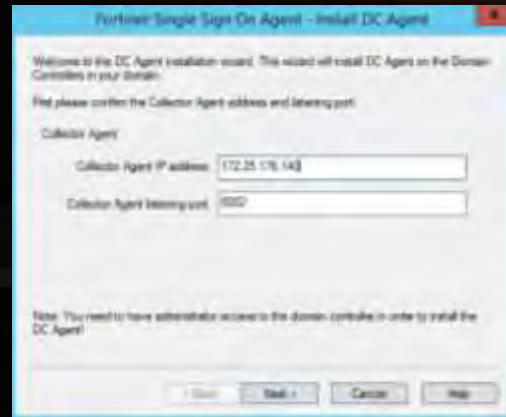
Installing the FSSO Agent Step 3

1

After installing the FSSO agent, run Install DC Agent.

2

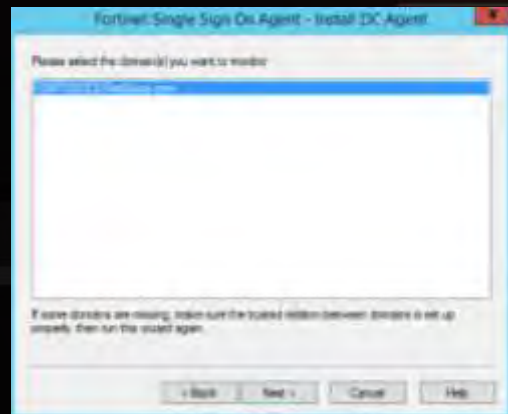
Set the Collector Agent IP address and the Collector Agent listening port.



Installing the FSSO Agent Step 4

1

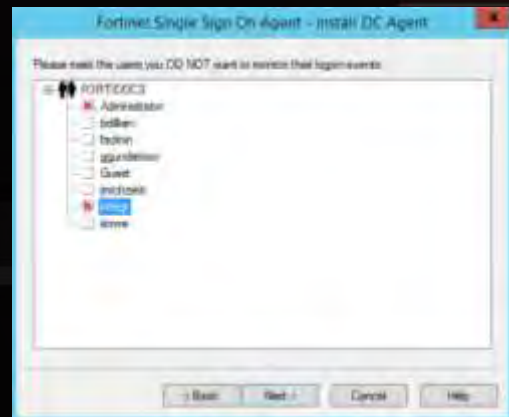
Select the domain you wish to monitor.



Installing the FSSO Agent Step 5

1

Exclude any users that you don't want to monitor, including the administrator.



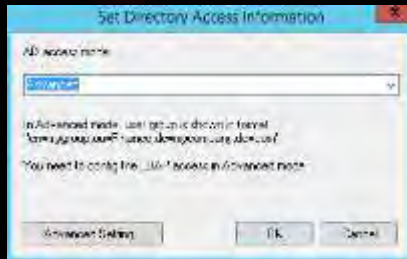
Configuring the FSSO Agent 1



1

To configure the settings for your network, open the FSSO agent. You can use the default for most settings

Configuring the FSSO Agent 2



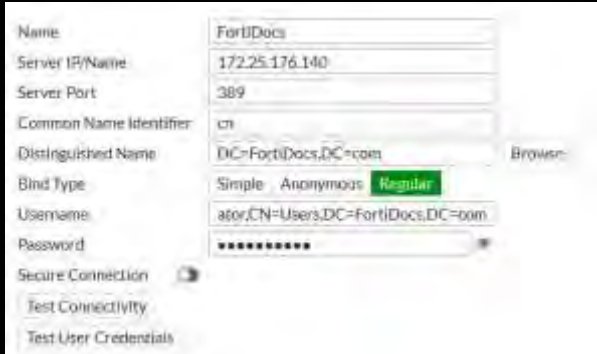
1

Select Set Directory Access Information.

2

Set AD access mode to Advanced.

Setting up FortiGate for FSSO 1



The screenshot shows the 'LDAP Servers' configuration page in FortiGate. The fields are filled with the following information:

Name	FortiDocs
Server IP/Name	172.25.176.140
Server Port	389
Common Name Identifier	cn
Distinguished Name	DC=FortiDocs,DC=com
Bind Type	Simple Anonymous Regular
Username	ator,CN=Users,DC=FortiDocs,DC=com
Password	*****
Secure Connection	☐
Test Connectivity	Test Connectivity
Test User Credentials	Test User Credentials

Because you have installed FSSSO in advanced mode, you need to configure LDAP to use with FSSSO.

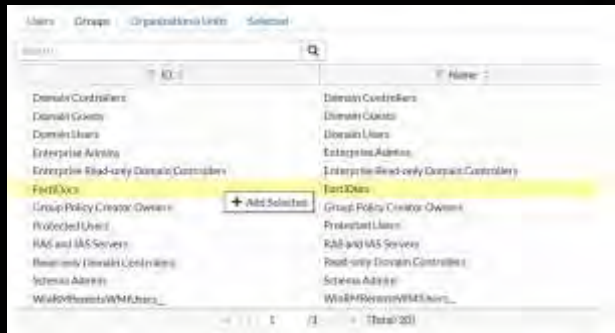
- 1 Go to User & Device > LDAP Servers
- 2 Select Create New.
- 3 Enter all information about your LDAP server.
- 4 Select Test Connectivity.
- 5 If your information is correct, Connection status is Successful.

Setting up FortiGate for FSSO 2



- 1 Security Fabric > Fabric Connectors
- 2 Select + Create New.
- 3 Under SSO/Identity, select Fortinet Single Sign-On Agent.
- 4 Set the Name and enter the IP address and password for the Primary FSSO Agent.
- 5 Set Collector Agent AD access mode to Advanced and set LDAP Server to the new LDAP service.

Setting up FortiGate for FSSO 3



Your FortiGate displays information retrieved from the AD server.

1

Select Groups, then right-click the FSSO group and select + Add Selected.

2

Select Selected.

The FSSO group is shown.

Setting up FortiGate for FSSO 4



To create a user group for FSSO users;

1

Go to User & Device > User Groups

2

Select Create New.

3

Enter a group Name and set Type to Fortinet Single Sign-On (FSSO).

4

Add the FSSO users to Members.

Setting up FortiGate for FSSO 5

The screenshot shows the FortiGate Policy configuration page for a policy named 'Internet-FSSO'. The configuration is as follows:

Field	Value
Name	Internet-FSSO
Incoming Interface	port1
Outgoing Interface	wan1
Source	all FortiDocs FSSO
Destination	all
Schedule	always
Service	All
Action	ACCEPT

Below the main configuration, the 'Firewall / Network Options' section is visible:

- NAT: ☒
- IP Pool Configuration: ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

To create a policy for FSSO users;

1

Go to Policy & Objects > IPv4 Policy

2

Select Create New.

3

For Source, set User to the FSSO user group.

Access Management Lab

Setup a local user



Conclusions

LDAP

Radius

FSSO



Understanding Routing Tables and Static Routes

Static Routes

Manually configured routes

Remain consistent

Used for:

Simple networks

Paths that needs to remain constant

Default Routes

Configuring Static Route via CLI

sequence_number: an arbitrary number to identify the route.

destination_ip: the destination IP address or network.

subnet_mask: the subnet mask of the destination.

gateway_ip: the IP address of the next-hop router or gateway.

```
config router static
  edit <sequence_number>
    set dst <IP & Netmask>
    set distance <integer>
    set gateway <gateway_ip>
    set device <port>
  next
end
```

Understanding and Configuring Priority

Priority determines route order (lower number = higher preference)

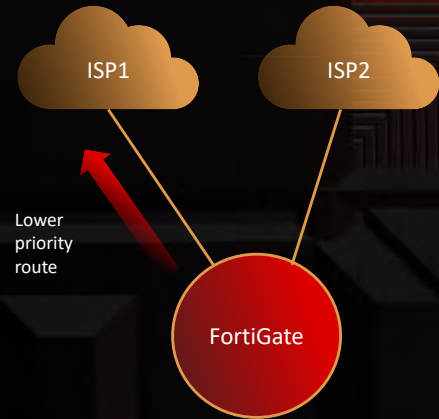
FortiGate uses path with lowest priority when multiple are available

Setting priorities is important for primary and backup routes

```
config router static
  edit <sequence_number>
    set dst <destination_ip>
    <subnet_mask>
    set gateway <gateway_ip>
    set priority
    <priority_number>
    next
  end
```

Understanding Priority

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 78.0.2.1
    set device port1
    set priority 1
  next
  edit 2
    set dst 0.0.0.0 0.0.0.0
    set gateway 203.0.113.1
    set device port2
    set priority 20
  next
end
```



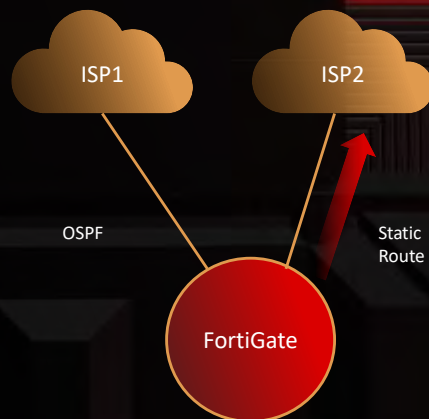
Understanding and Configuring Distance

Serves as a tie-breaker if multiple routes to the same destination exist.

Lower administrative distance will be chosen.

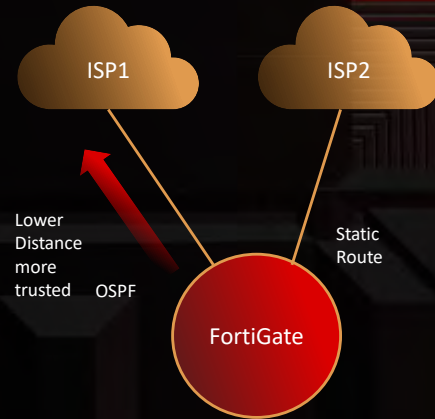
Varies by routing protocol

For instance, OSPF has a different default distance compared to EIGRP.



Understanding and Configuring Distance

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 78.0.2.1
    set device port1
    set distance 175
  next
end
```



Configuring Static Route via FortiManager

Configure Static Route

Device & Groups -> Managed FortiGate ->
Network -> Static Routes



Understanding Routing Tables

Routing tables hold network reachability info.

Guide routers on packet forwarding decisions.

Viewing the Routing Table in the CLI

`'get router static'`
command

the configured static routes are displayed.

`'get router info routing-`
`table all'` command

The entire routing table information is displayed, including configured and learned routes of all types.



Routing Database

All routes learned from all routing protocols

Routing Table

Only the best routes learned

Most specific route is given priority

1. In case of a tie (same destination network and subnet mask):
2. lower administrative distance is selected.
3. If equal, all equal routes are included in the routing table.
4. Cost and Priority determine the preferred route.
5. If Cost and Priority are also equal, FortiGate uses Equal-Cost Multi-Path (ECMP) to distribute traffic across these routes.

Get router info routing-table database

Routing table database:

Codes: C - connected, S - static, D - dynamic

```
S 10.10.10.0/24 [20/0] via 192.0.2.2, wan1
C 192.0.2.0/24 is directly connected, wan1
C 203.0.113.0/24 is directly connected, lan
S 10.0.0.0/8 [10/0] via 203.0.113.2, lan
D 10.10.10.0/24 [10/0] via 203.0.113.3, lan
```

Get router info routing-table all

Routing table:

Codes: C - connected, S - static, D - dynamic

```
C 192.0.2.0/24 is directly connected, wan1
C 203.0.113.0/24 is directly connected, lan
S 10.0.0.0/8 [10/0] via 203.0.113.2, lan
D 10.10.10.0/24 [10/0] via 203.0.113.3, lan
```

Example: Viewing Routing Table in CLI

```
# get router info routing-table all
```

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default

```
S* 0.0.0.0/0 [10/0] via 192.168.183.254, port2
```

```
S 1.0.0.0/8 [10/0] via 192.168.183.254, port2
```

```
S 2.0.0.0/8 [10/0] via 192.168.183.254, port2
```

```
C 10.142.0.0/23 is directly connected, port3
```

```
B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m
```

```
C 192.168.182.0/23 is directly connected, port2
```



Example: Examining an Entry

B 10.160.0.0/23 [20/0] via 10.142.0.74, port3, 2d18h02m

B	BGP. The routing protocol used.
10.160.0.0/23	The destination of this route, including netmask.
[20/0]	20 indicates an administrative distance of 20 out of a range of 0 to 255. 0 is an additional metric associated with this route, such as in OSPF.
10.142.0.74	The gateway or next hop.
port3	The interface that the route uses.
2d18h02m	The age of the route (in this example, it's almost three days old).



Virtual Routing and Forwarding (VRFs)

- Allows for creation of multiple virtual routers within one physical router.
- Each VRF has its own independent routing table.
- Enables network segmentation and isolation without additional hardware.
- Useful in multi-tenant environments or for isolating certain types of traffic.

Example: Viewing Routing Table in CLI



```
# get router info routing-table all
```

```
Routing table for VRF=1
```

```
C    192.0.2.0/24 is directly connected, port1
```

```
C    203.0.113.0/24 is directly connected, port2
```

```
Routing table for VRF=2
```

```
C    198.51.100.0/24 is directly connected, port3
```

```
S    192.0.2.0/24 [1/0] via 198.51.100.1
```

```
Routing table for VRF=3
```

```
C    203.0.113.0/24 is directly connected, port4
```

```
S    192.0.2.0/24 [1/0] via 203.0.113.1
```


Always Prefer Healthy Next-hops



Static Routes are only active in the routing table when:

- Active outgoing interface

- Preference

- Static route must be most preferred among any other

- Health monitor (optional) is up

- Next-hop reachability

Snat-route-change



Enable

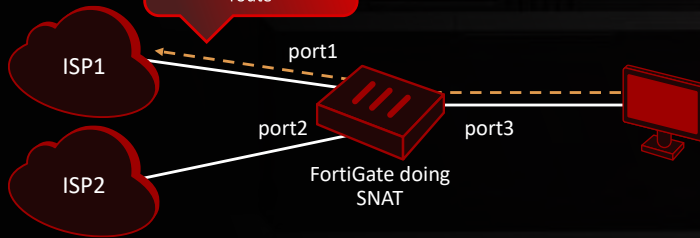
Allows the firewall to change its SNAT decision dynamically if the route used for traffic changes.

Disable (default behavior)

The firewall will not alter the SNAT decision, even if the route used for traffic has changed

FortiGate routing table			
Subnet	Interface	Distance	Priority
0.0.0.0/0	port1	10	0
0.0.0.0/0	Port2	10	10

Traffic for new sessions uses the lowest priority route



```
config system global
  set snat-route-change [ disable | enable ]
end
```

Kernel Routing Table

```
Alza-kvm12 # get router info kernel
```

```
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.47.0.0/32 pref=10.47.1.42 gw=0.0.0.0 dev=3(port1)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.47.1.42/32 pref=10.47.1.42 gw=0.0.0.0 dev=3(port1)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.47.3.255/32 pref=10.47.1.42 gw=0.0.0.0 dev=3(port1)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.115.0.0/32 pref=10.115.1.42 gw=0.0.0.0 dev=4(port2)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.115.1.42/32 pref=10.115.1.42 gw=0.0.0.0 dev=4(port2)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.115.3.255/32 pref=10.115.1.42 gw=0.0.0.0 dev=4(port2)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>127.0.0.0/32 pref=127.0.0.1 gw=0.0.0.0 dev=13(root)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>127.0.0.0/8 pref=127.0.0.1 gw=0.0.0.0 dev=13(root)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>127.0.0.1/32 pref=127.0.0.1 gw=0.0.0.0 dev=13(root)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>127.255.255.255/32 pref=127.0.0.1 gw=0.0.0.0 dev=13(root)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>169.254.1.0/32 pref=169.254.1.1 gw=0.0.0.0 dev=15(fortilink)
tab=255 vf=0 scope=254 type=2 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>169.254.1.1/32 pref=169.254.1.1 gw=0.0.0.0 dev=15(fortilink)
tab=255 vf=0 scope=253 type=3 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>169.254.1.255/32 pref=169.254.1.1 gw=0.0.0.0 dev=15(fortilink)
tab=254 vf=0 scope=0 type=1 proto=11 prio=0 0.0.0.0/0.0.0.0/0-
>0.0.0.0/0 pref=0.0.0.0 gw=10.47.3.254 dev=3(port1)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.47.0.0/22 pref=10.47.1.42 gw=0.0.0.0 dev=3(port1)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>10.115.0.0/22 pref=10.115.1.42 gw=0.0.0.0 dev=4(port2)
tab=254 vf=0 scope=253 type=1 proto=2 prio=0 0.0.0.0/0.0.0.0/0-
>169.254.1.0/24 pref=169.254.1.1 gw=0.0.0.0 dev=15(fortilink)
```

An in-memory table in the operating system's network stack with all currently active routes.

Used in real-time for decision-making on packet forwarding.

Retrieves current information about the kernel routing table.

Helps identify the active routes for packet forwarding on the system.

Useful for debugging and identifying routing issues on the network device.

<https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-display-kernel-route/ta-p/212757>

Labs- Tables and Static Routes



Configure Static Route



VRF/VDOMs



View Routing Table and Kernal Routing Table

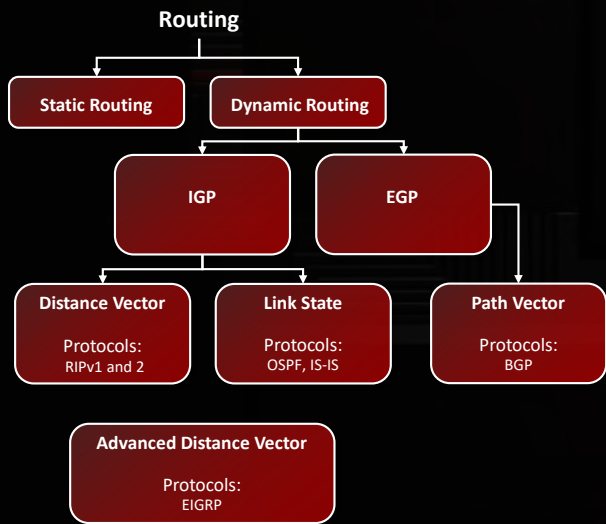
Conclusions

- Static Route
- Routing Table
- Snat-route-change
- Kernel Routing Table



OSPF Review and Basics

Routing Options

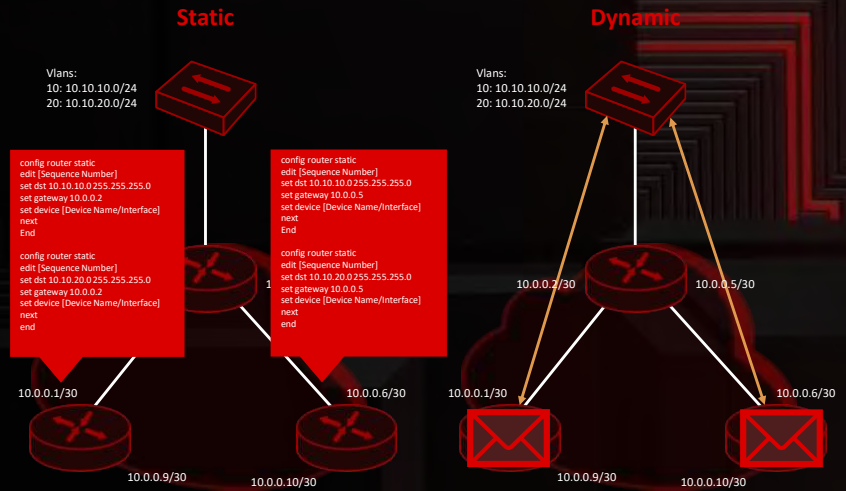


Static vs. Dynamic Routing

Automatically

Adapt to network changes

Provide routes ability to sync routing information



IGP (Interior Gateway Protocol)

Used within an autonomous system (AS).

Examples: OSPF, IS-IS, RIP.

Focus on optimal path and speed.

EGP (Exterior Gateway Protocol)

Used between different AS

Example: BGP.

Focus on policy enforcement and scalability.

AS: Single administrative network domain (think of different companies ISP)

Distance Vector

Routers share information with direct neighbors.

Use metrics to determine the best path.

Link State

Routers share information about direct connections with all routers in the network.

Construct a complete network map.

Calculate best path using algorithms

Faster convergence and more scalable.

OSPF Protocol

Distance Vector

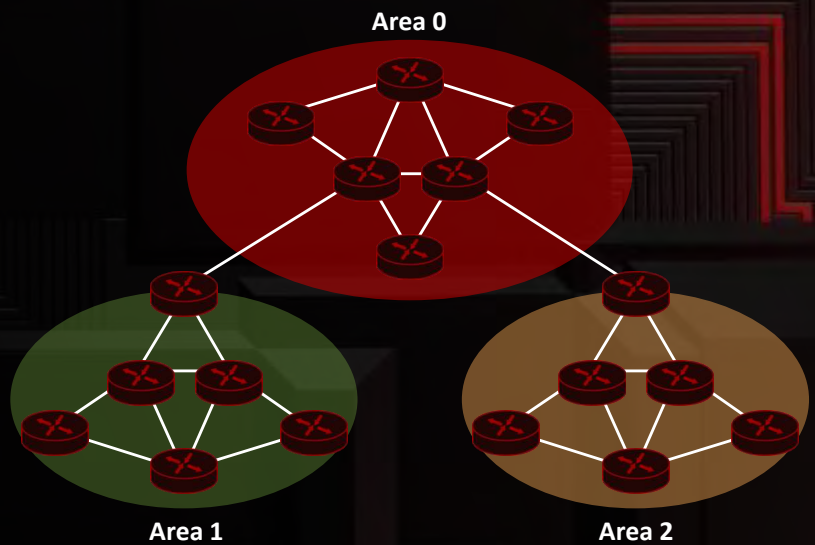
Only know about neighboring routers

RIPv1 & RIPv2

Link State

Share information about the entire network topology, allowing for optimal route calculation.

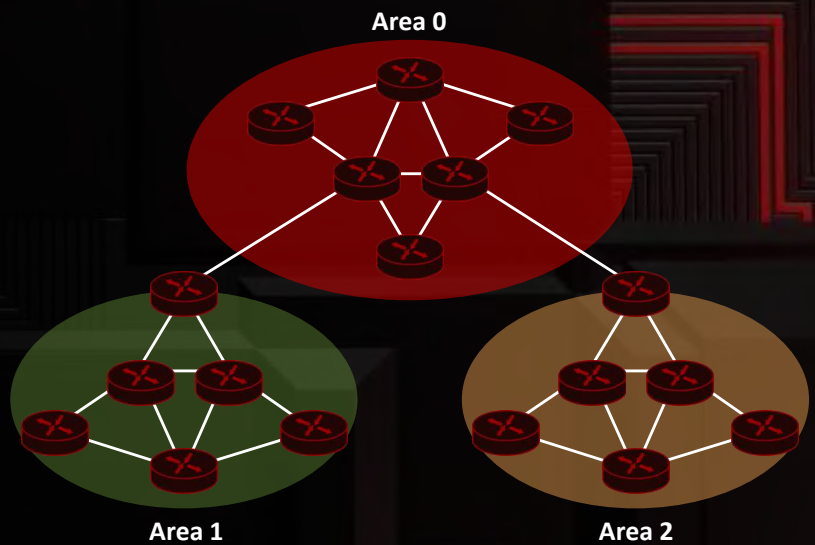
OSPF and ISIS



OSPF Multi-Area Design

Breaks down a big network into smaller, manageable pieces called areas

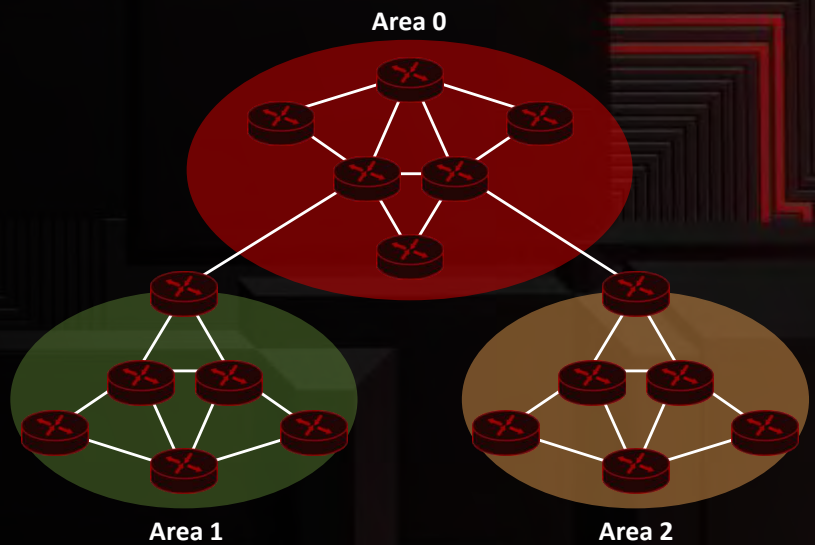
Makes the network easier to handle, speeds up route calculations, and cuts down on unnecessary data traffic between routers.



OSPF Multi-Area Design

OSPF Area Design **requires** that Area 0 sits at the top as a Backbone Area

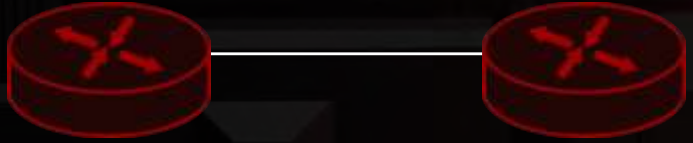
All other areas **must** connect to Area 0 in order to communicate



Common OSPF Network Types

Point to Point

2 routers



Common OSPF Network Types

Broadcast (Most commonly used)

Multiple routers

Can send multicast

Hello packets sent to
224.0.0.5 (all Devices)

224.0.0.6 (DR)



Common OSPF Network Types

Point-to-multipoint

Multiple routers

Does not support multicast



OSPF Adjacency

Relationship formed between OSPF routers within the same network segment, allowing them to exchange routing information.



OSPF – Steps to Adjacency

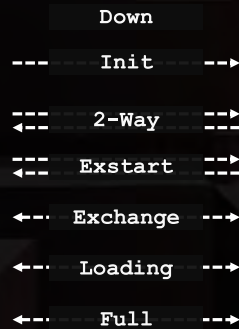
When OSPF is **started** on interfaces between 2 routers, the following occurs...

Routers send and receive a **series** of OSPF Packet Types

Routers **decide** on DR and BDR per interface

Possible States are...

Down	
Attempt	- seen in NBMA networks
Init	- Hello sent using RID - Not seeing your RID yet
2-Way	- Hello with your RID is seen - DR/BDR election started
Exstart	- Master/Slave - higher RID selected
Exchange	- DBD (DB Descriptor) LSA Headers exchanged to see if more are needed
Loading	- LSR and LSU containing all LSAs occurs
Full	- Steady state - Full LSDB synch has occurred



Requirements for OSPF Adjacencies

Matching:

- Area ID
- Area Type
- Authentication
- MTU
- Network Type
- Subnet
- Timers

Unique:

- Router IDs

```
Config router ospf
  set router-id 0.0.0.5
  config area
    edit 0.0.0.0
    next
  end
  config network
    edit 1
    set prefix 10.10.10.0 255.255.255.0
    set area 0.0.0.0
  end
end
```

Requirements for OSPF Adjacencies

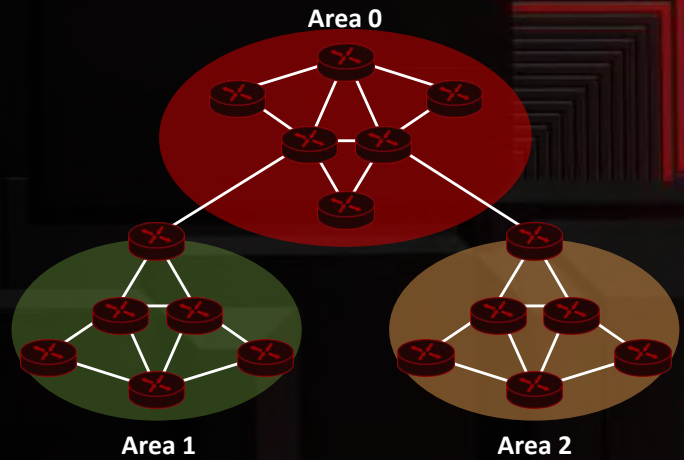
Matching:

Area ID

Helps in identifying and differentiating areas within the OSPF domain.

```
config area
```

```
edit 0.0.0.0  
next
```



Requirements for OSPF Adjacencies

Matching:

Area Type

Regular: Connects to backbone, all LSAs allowed.

Backbone Area (Area 0): Central hub, connects other areas.

Stub Area: No external LSAs, uses default route to exit.

Not-So-Stubby Area (NSSA): External LSAs allowed, can import external routes.

```
config area
```

```
edit 0.0.0.1  
set type stub
```

NOTE: If you setup are as 0.0.0.0 (backbone) then you will not have an option to set area.

Requirements for OSPF Adjacencies

Matching:

Authentication

Verify OSPF routers' identity to maintain routing information integrity and confidentiality.

```
config router key-chain
  edit <name>
    config key
      edit <id>
        ...
        set algorithm {md5 | hmac-sha1 |
                      hmac-sha256 | hmac-sha384 | hmac-sha512}
      next
    end
  next
end
```

Requirements for OSPF Adjacencies

Matching:

MTU (Maximum Transmission Unit)

largest size packet or frame that can be sent, measured in bytes.

```
config ospf-interface
  edit "NAME"
    set mtu <value>
```

Requirements for OSPF Adjacencies

Matching:

Network Type

Broadcast: Uses multicast for communication on Ethernet networks.

Non-Broadcast Multi-Access (NBMA): Manually configured neighbors, typically on Frame Relay.

Point-to-Point: Direct link between two routers.

Point-to-Multipoint: Treats links as a collection of point-to-point connections.

Point-to-Multipoint Non-Broadcast: Similar to Point-to-Multipoint but requires manual neighbor configuration.

```
config ospf-interface
edit port1
set network-type broadcast
```


Requirements for OSPF Adjacencies

Matching:

Subnet

```
config network
edit 1
set prefix 10.10.10.0 255.255.255.0
```

Requirements for OSPF Adjacencies

Matching:

Timers

Hello

Dead

Wait

```
config ospf-interface
  edit "NAME"
    set interface "port1"
    set priority 255
    set dead-interval 40
    set hello-interval 10
    set authentication message-digest
  next
```

Requirements for OSPF Adjacencies

Unique:

Router IDs

Chosen from the highest IP address on any of the router's active interfaces

OR

manually configured.

The router with the highest Router ID becomes the DR.

```
Config router ospf  
set router-id 0.0.0.5
```

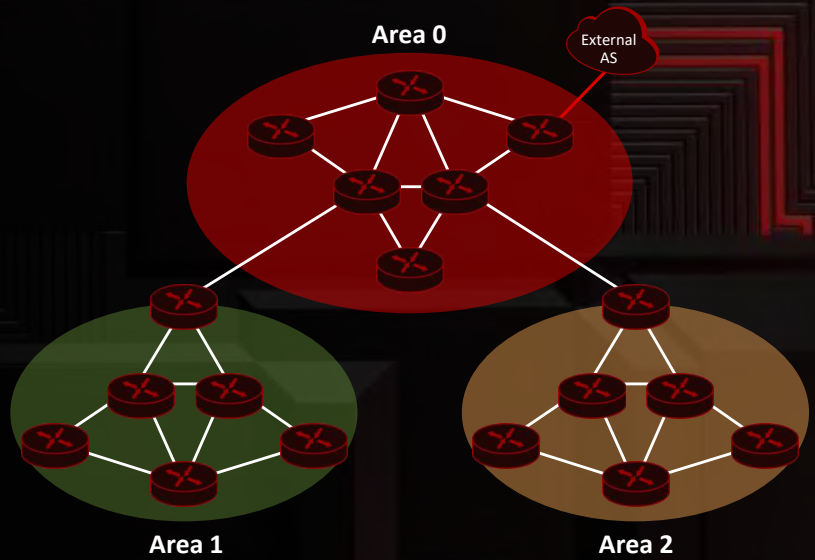
Router Types

Internal Router

Backbone Router

Area Border Router (ABR)

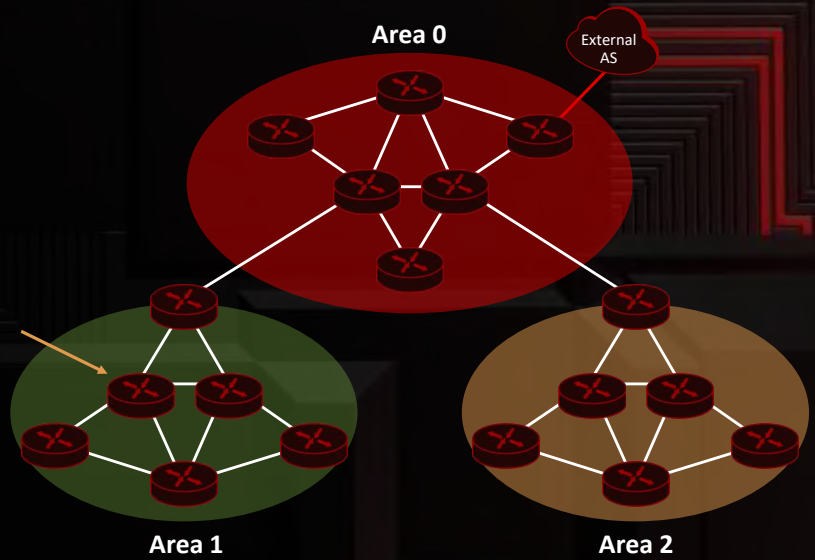
Autonomous System Boundary Router (ASBR)



Router Types

Internal Router

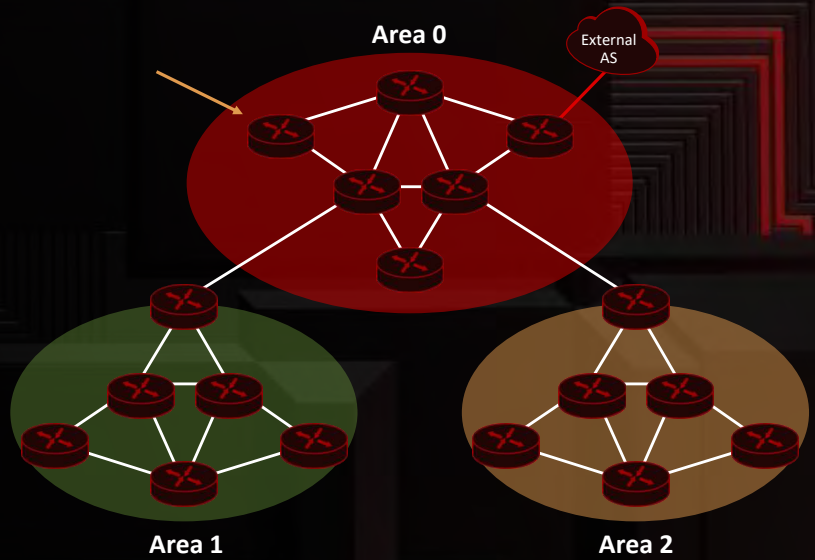
All interfaces belong to the same area.



Router Types

Backbone Router

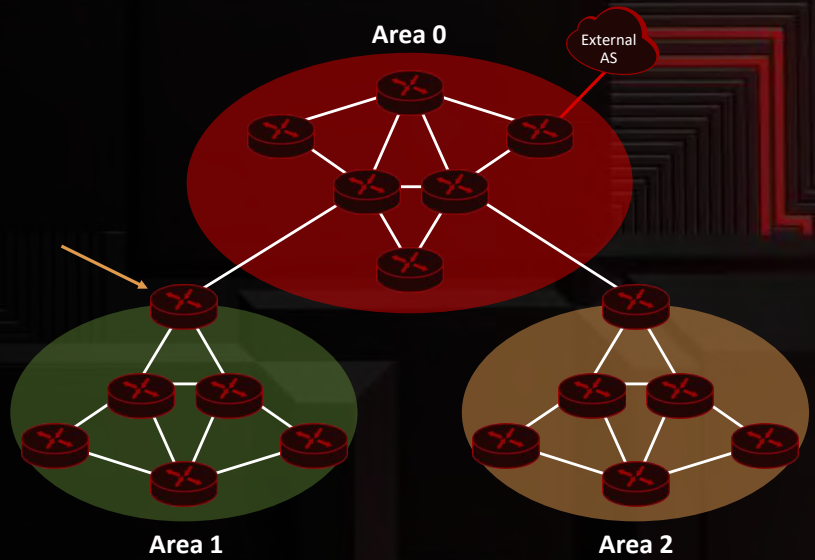
Has at least one interface in the backbone area (Area 0).



Router Types

Area Border Router (ABR)

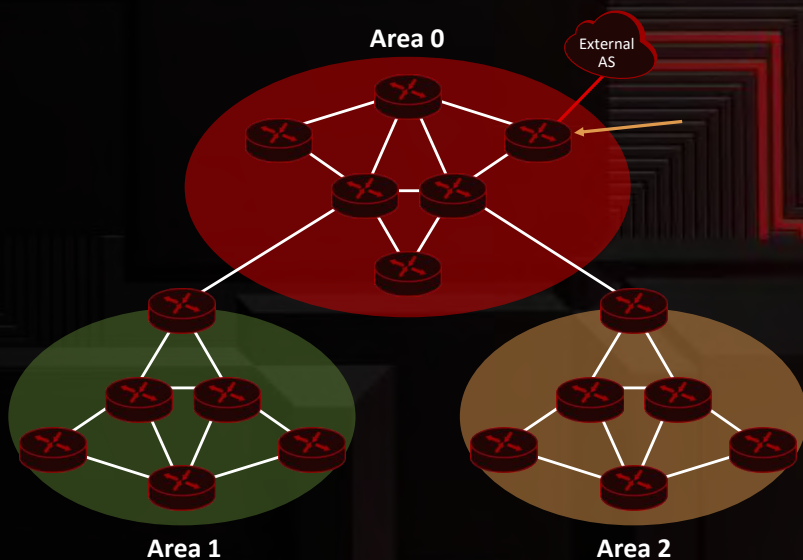
Connects and shares information between areas, has interfaces in multiple areas.



Router Types

Autonomous System Boundary Router (ASBR)

Exchanges information with routers outside the OSPF autonomous system.



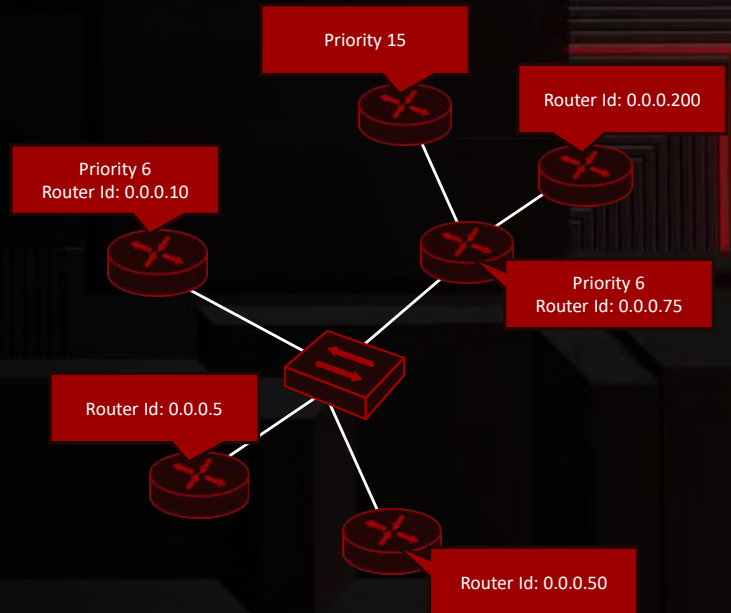
Router Types Within a Multi-Access Environment

The routers will be assigned one of three roles when multiple OSPF routers are attached to a multi-access environment (switch).

Designated Router (DR)

Backup Designated Router (BDR)

DROther

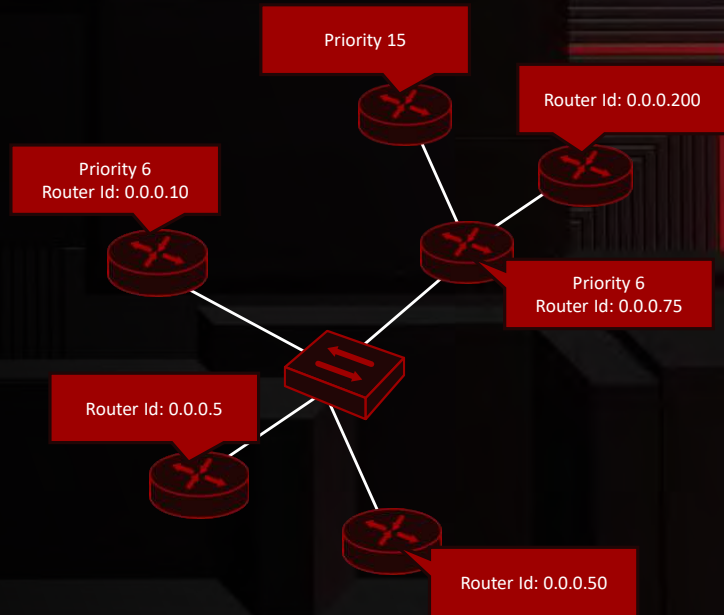


Router Types Within a Multi-Access Environment

Designated Router (DR):

Elected router on a multi-access network segment in OSPF to reduce the amount of OSPF traffic. Manages link-state information.

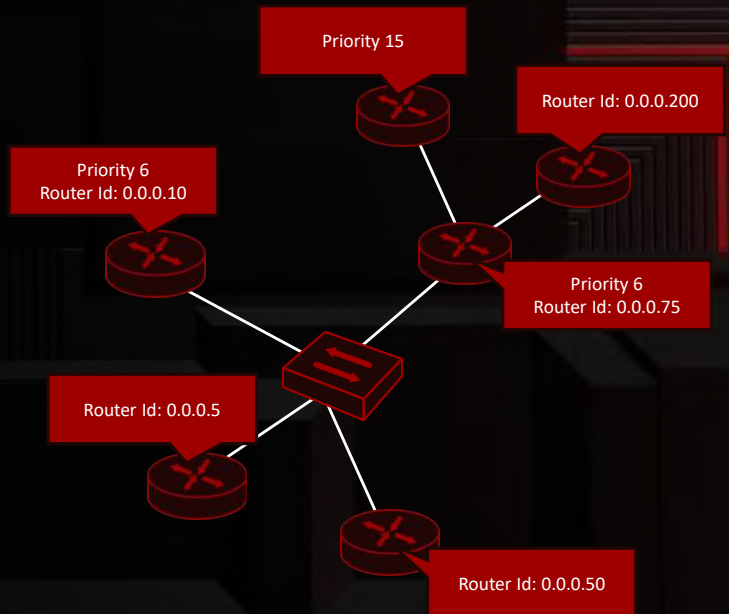
Forms full adjacency with all routers on its multi-access network segment.



Router Types Within a Multi-Access Environment

The DR is assigned based off of the following:

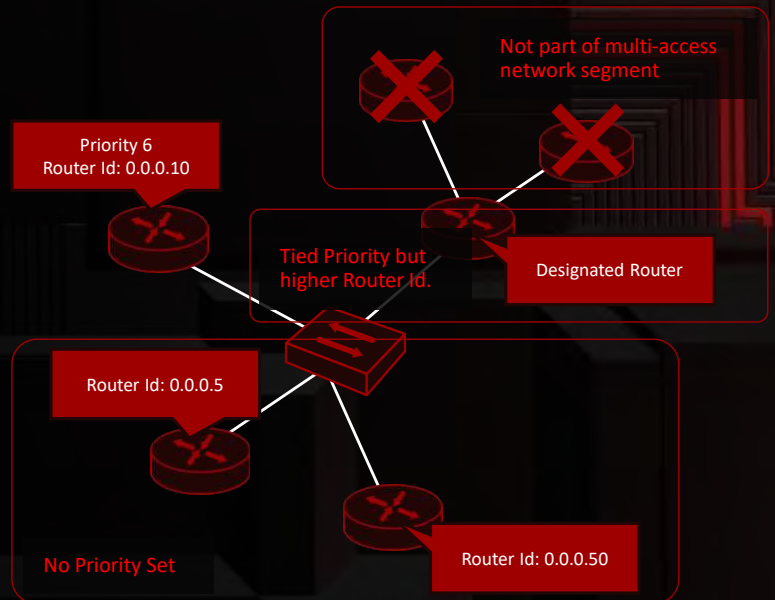
1. Highest Priority
If tie
2. Highest Router ID
If tie
3. Highest Interface IP



Key OSPF Router Types: Managing LSAs

The DR is assigned based off of the following:

1. Highest Priority
If tie
2. Highest Router ID
If tie
3. Highest Interface IP

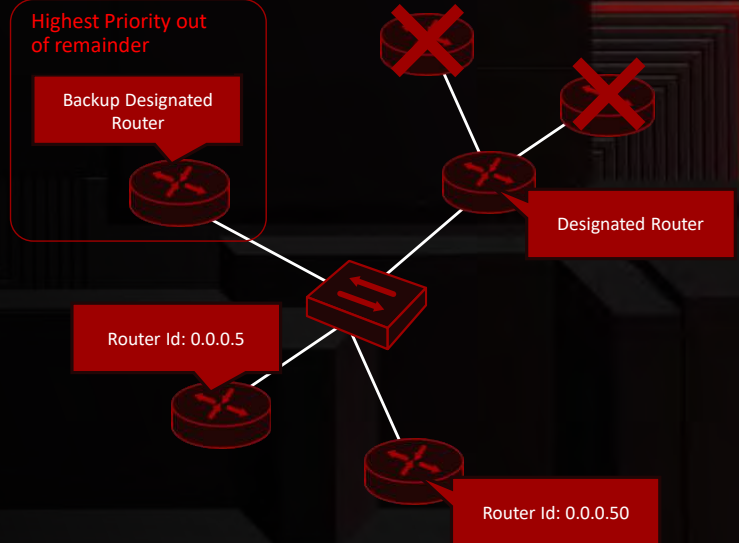


Key OSPF Router Types: Managing LSAs

Backup Designated Router (BDR):

Secondary router that takes over if the DR fails. It receives the same link-state information as the DR.

Forms full adjacency with all routers on its network segment.

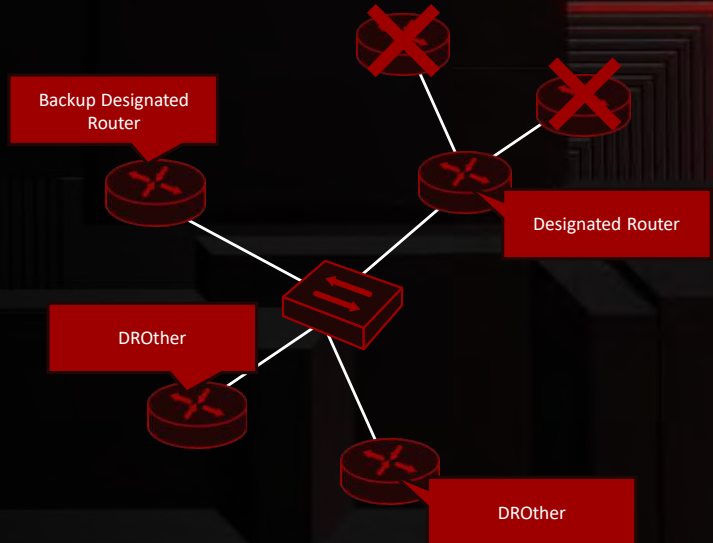


Key OSPF Router Types: Managing LSAs

DROther:

All other OSPF routers on the network segment that are not DR or BDR. They form adjacencies with the DR and BDR.

Forms full adjacency only with the DR and BDR, not with other DROthers.



Key OSPF Router Types: Managing LSAs

DR

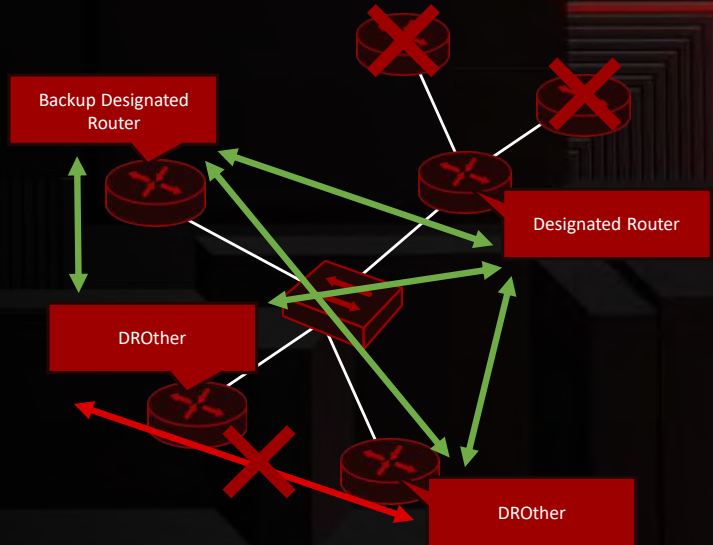
Full adjacency with all

BDR

Full adjacency with all

DROther:

Full adjacency only with the DR and BDR



Link-State Advertisement (LSA)

Data packet within the OSPF protocol.

Contains information about network links and the state of those links.

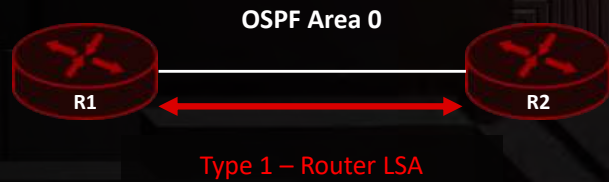
Used by OSPF routers to exchange topology information.

Each OSPF router uses received LSAs to build up a database of the network's topology, known as the Link-State Database (LSDB).

LSA Types

Router LSAs (Type 1)

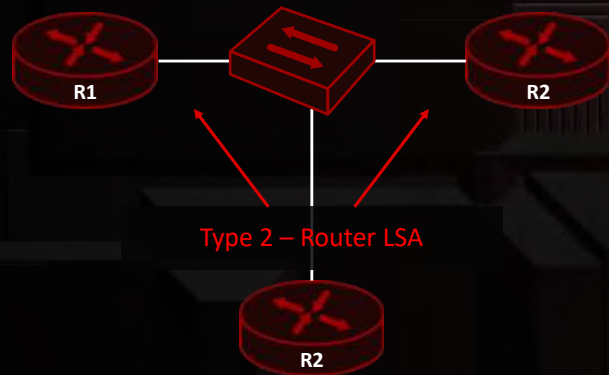
Generated by all routers, describe the local state of a router (its directly attached links).



LSA Types

Network LSAs (Type 2)

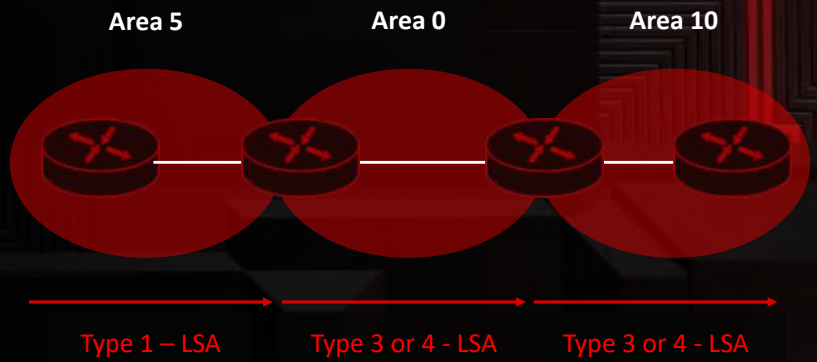
Generated by Designated Routers, describe which routers are connected to the network.



LSA Types

Summary LSAs (Type 3 and 4)

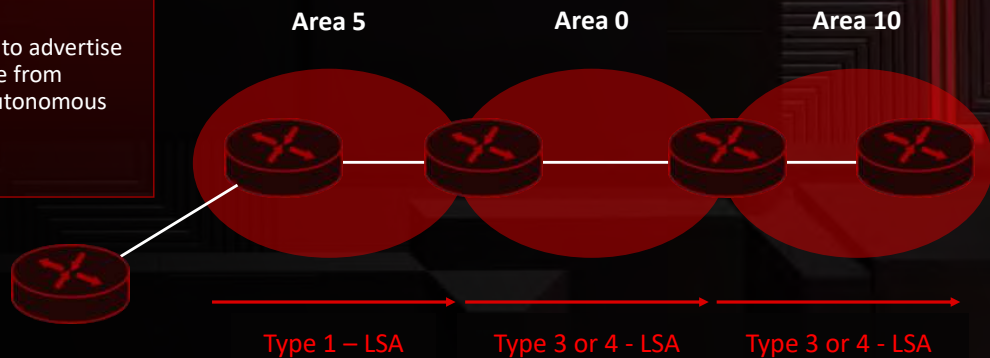
Generated by Area Border Routers, provide information about inter-area routes.



LSA Types

External LSA (Type 5)

Generated by ASBR to advertise routes that originate from outside the OSPF autonomous system.



Self-Originated LSAs

Display LSAs that the router has originated.

```
NGFW-1 # get router info ospf database self-originate
```

```
OSPF Router with ID (0.0.0.1) (Process ID 0, VRF 0)
```

```
Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Flag	Link count
0.0.0.1	0.0.0.1	317	80000005	66d2	0031	1

```
Net Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Flag
10.1.0.254	0.0.0.1	307	80000003	53ef	0031

LSA Details

Key Input:

LSA ID, sequence
number, router ID, age

```
NGFW-1 # get router info ospf database router lsa
OSPF Router with ID (0.0.0.1) (Process ID 0, VRF 0)

Router Link States (Area 0.0.0.0)

LS age: 400
Options: 0x2 (*)+--+--+([4])
Flags: 0x0
LS Type: router LSA
Link State ID: 0.0.0.1
Advertising Router: 0.0.0.1
LS Seq Number: 0x000005
Checksum: 0x66d2
Length: 36
Number of Links: 1

Link connected to: a Transit Network
(Link ID) Designated Router address: 10.1.0.254
(Link Data) Router Interface address: 10.1.0.254
Number of TOS metrics: 0
TOS 0 Metric: 1

LS age: 313
Options: 0x2 (*)+--+--+([4])
Flags: 0x0
LS Type: router LSA
Link State ID: 0.0.0.2
Advertising Router: 0.0.0.2
LS Seq Number: 0x000006
Checksum: 0x941c
Length: 48
Number of Links: 2

Link connected to: a Transit Network
(Link ID) Designated Router address: 10.1.0.254
(Link Data) Router Interface address: 10.1.0.190
Number of TOS metrics: 0
TOS 0 Metric: 1

Link connected to: Stub Network
(Link ID) Network/subnet number: 10.1.4.0
(Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
TOS 0 Metric: 1

LS age: 360
Options: 0x2 (*)+--+--+([4])
Flags: 0x0
LS Type: router LSA
Link State ID: 0.0.0.3
Advertising Router: 0.0.0.3
LS Seq Number: 0x000007
Checksum: 0x5179
Length: 48
Number of Links: 2

Link connected to: a Transit Network
(Link ID) Designated Router address: 10.1.0.254
(Link Data) Router Interface address: 10.1.0.1
Number of TOS metrics: 0
TOS 0 Metric: 1

Link connected to: Stub Network
(Link ID) Network/subnet number: 10.1.10.0
(Link Data) Network Mask: 255.255.255.0
Number of TOS metrics: 0
TOS 0 Metric: 1
```

Conclusions

OSPF Review

Adjacencies

Router Types

LSA



OSPF Configuration & Troubleshooting

OSPF Configuration - CLI

STEPS

- 1 Set Algorithm for authentication
- 2 BASIC OSPF SETTINGS
- 3 NETWORK
- 4 OSPF INTERFACE

OSPF Configuration

Setting Algorithm

Only MD5 supported Prior to 7.0.1

```
config router key-chain
  edit <name>
    config key
      edit <id>
        ...
        set algorithm {md5 | hmac-sha1 | hmac-sha256 | hmac-sha384 | hmac-sha512}
      next
    end
  next
end
```

OSPF Configuration

Basic OSPF settings

Router-id

Area

Authentication

```
Config router ospf
set router-id 0.0.0.5
config area
  edit 0.0.0.0
  set authentication message-digest
  next
end
```

OSPF Configuration

Network

```
Config router ospf
config network
edit 1
    set prefix 10.10.10.0 255.255.255.0
    set area 0.0.0.0
    set network type broadcast
end
end
```

OSPF Configuration

Interface

```
config ospf-interface
edit "NAME"
  set interface "port1"
  set priority 255
  set dead-interval 40
  set hello-interval 10
  set authentication message-digest
next
edit "NAME"
  set interface "port2"
  set dead-interval 40
  set hello-interval 10
  set authentication message-digest
next
```

FortiManager

Device & Groups -> Network -> OSPF
Add Areas, Networks and Router ID





High Availability and Quick Recovery

OSPF Equal-cost multi-path routing (ECMP)

Allows for multiple paths with equal cost to a destination to be installed in the routing table.

Disabled by default

```
Config router ospf
  set rfc1583-compatible enable
end
```


OSPF Bidirectional Forwarding Detection (BFD)

Provides rapid failure detection times

Configure on each OSPF Router and each interface

```
config router ospf
  set bfd enable
end

config system interface
  edit "port number"
  set bfd enable
  next
end
```

OSPF Graceful Restart Mode

A mechanism allowing OSPF routers to continue forwarding traffic during a short interruption of OSPF service.

Helps maintain continuous network operation during software upgrades or minor hardware changes.

```
Config router ospf
  set restart-mode graceful-restart
  set restart-period <SECONDS>
  set restart-on-topology-change {enable | disable}
end
end
```



Troubleshooting OSPF

Troubleshooting BFD

Check status with:

Get router info bfd neighbor

```
NGFW-1 # get router info bfd neighbor
```

OurAddress	NeighAddress	State	Interface	LDesc/RDesc
10.1.0.254	10.1.0.100	UP	port3	2/2
10.1.0.254	10.1.0.1	UP	port3	1/2

OSPF Status

Quickly view OSPF operation and troubleshoot OSPF issues.

OSPF Router ID

OSPF Administrative status

OSPF operational status

```
NGFW-1 # get router info ospf status
Routing Process "ospf 0" with ID 0.0.0.1
Process uptime is 32 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Do not support Restarting
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
External LSA database is unlimited.
Number of LSA originated 2
Number of LSA received 8
Number of areas attached to this router: 1
Area 0.0.0.0 (BACKBONE)
  Number of interfaces in this area is 1(1)
  Number of fully adjacent neighbors in this area is 2
  Area has no authentication
  SPF algorithm last executed 00:27:56.440 ago
  SPF algorithm executed 6 times
  Number of LSA 4. Checksum 0x01e852
```

OSPF Neighbor

State

Full/DROther

Full/Backup

Full/ -

Broadcast network

Interface

ToRemote

Typically a VPN

```
NGFW-1 # get router info ospf neighbor
```

OSPF process 0, VRF 0:

Neighbor ID	Pri	State	Dead Time	Address	Interface
0.0.0.3	1	Full/DROther	00:00:37	10.1.0.1	port3
0.0.0.2	1	Full/Backup	00:00:39	10.1.0.100	port3
0.0.0.9	1	Full/ -	00:00:34	10.1.0.5	ToRemote

OSPF Interface

Area 0.0.0.0

Area port is apart in, in this instance backbone network.

Router ID 0.0.0.1

Router ID of current Fortigate

Designated Router

Neighbor count

```
NGFW-1 # get router info ospf interface
port3 is up, line protocol is up
Internet Address 10.1.0.254/24, Area 0.0.0.0, MTU 1500
Process ID 0, VRF 0, Router ID 0.0.0.1, Network Type BROADCAST, Cost:
1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 0.0.0.1, Interface Address 10.1.0.254
Backup Designated Router (ID) 0.0.0.2, Interface Address 10.1.0.100
Timer intervals configured, Hello 10.000, Dead 40, Wait 40, Retransmit
5
Hello due in 00:00:02
Neighbor Count is 2, Adjacent neighbor count is 2
Crypt Sequence Number is 345
Hello received 366 sent 204, DD received 9 sent 8
LS-Req received 2 sent 2, LS-Upd received 10 sent 11
LS-Ack received 11 sent 5, Discarded 2
BFD enabled
```

OSPF LSDB

Summary of the OSPF link-state database (LSDB)

```
NGFW-1 # get router info ospf database brief
```

```
OSPF Router with ID (0.0.0.1) (Process ID 0, VRF 0)
```

```
Router Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Flag	Link count
0.0.0.1	0.0.0.1	231	80000005	66d2	0031	1
0.0.0.2	0.0.0.2	143	80000006	941c	0012	2
0.0.0.3	0.0.0.3	200	80000007	9179	0012	2

```
Net Link States (Area 0.0.0.0)
```

Link ID	ADV Router	Age	Seq#	CkSum	Flag
10.1.0.254	0.0.0.1	221	80000003	53ef	0031

Sniffer with OSPF

diagnose sniffer packet any
"proto 89" 4

Tell if OSPF HELLO packets are
sent/received

```
interfaces=[any]
filters=[proto 89]
0.748972 internal out 10.160.0.106 -> 224.0.0.5: ip-proto-89 48
4.796492 internal in 10.161.0.58 -> 224.0.0.5: ip-proto-89 44
```

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-tips-for-FortiOS-routing-RIP-OSPF-BGP-static/ta-p/198593>

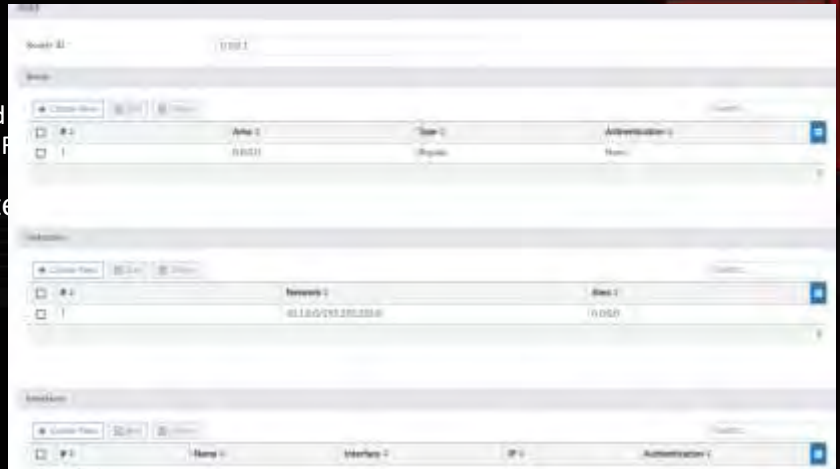
DEMO - Configuring OSPF

Configure OSPF with FortiManager

Device & Groups -> Managed
FortiGate -> Network -> OSPF

Configure OSPF on FortiGate

Route filter



Conclusions

Configuration

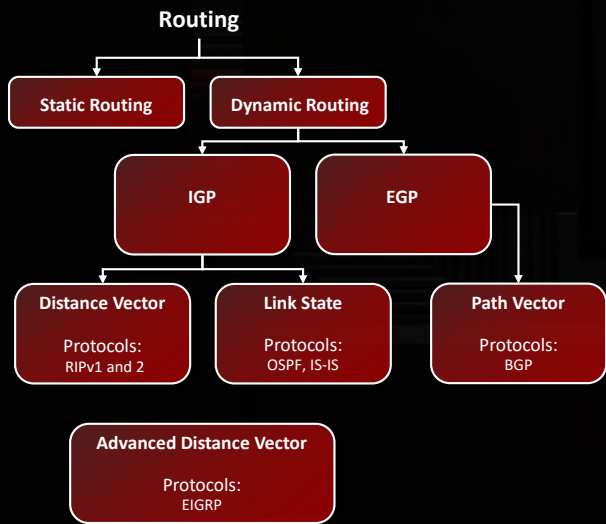
Expediting recovery

Troubleshooting



BGP

Routing Options



IGP (Interior Gateway Protocol)

Used within an autonomous system (AS).

Examples: OSPF, IS-IS, RIP.

Focus on optimal path and speed.

EGP (Exterior Gateway Protocol)

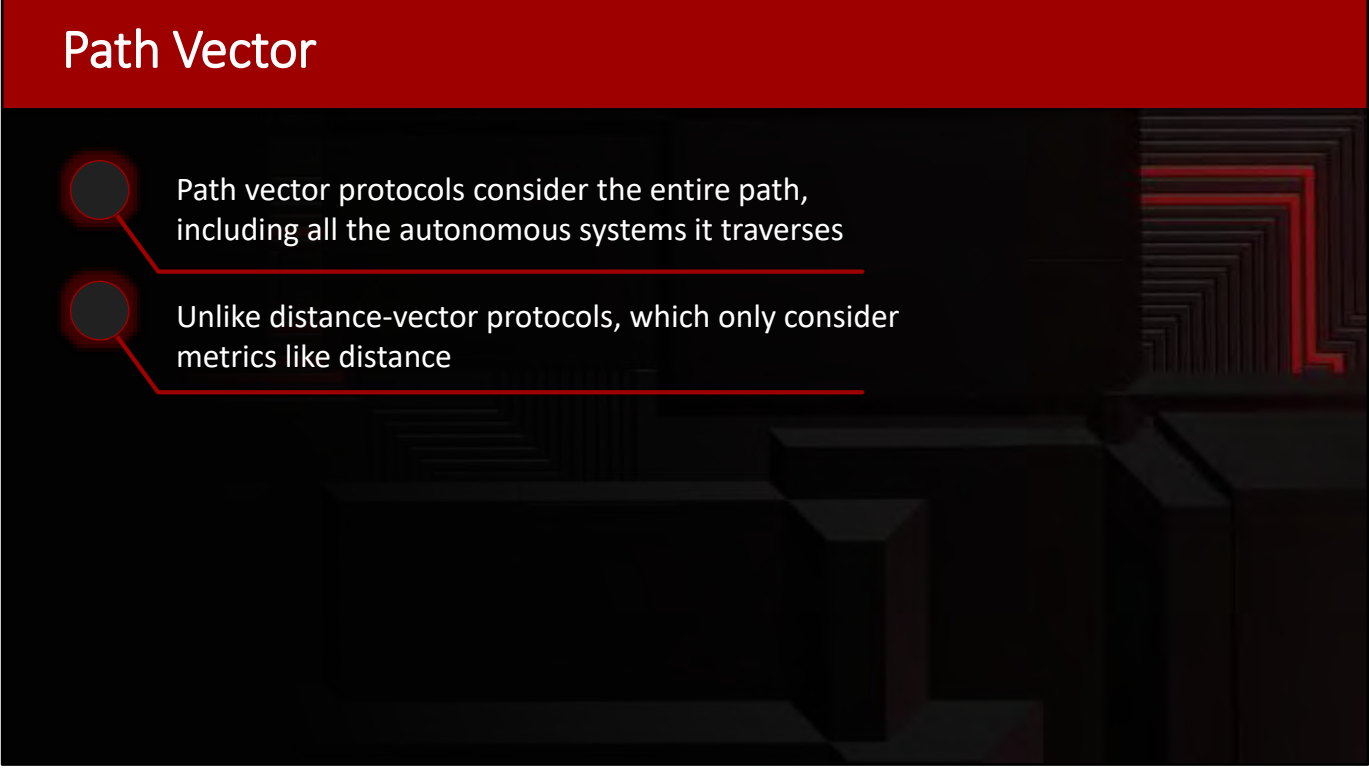
Used between different AS

Example: BGP.

Focus on policy enforcement and scalability.

AS: Single administrative network domain (think of different companies ISP)

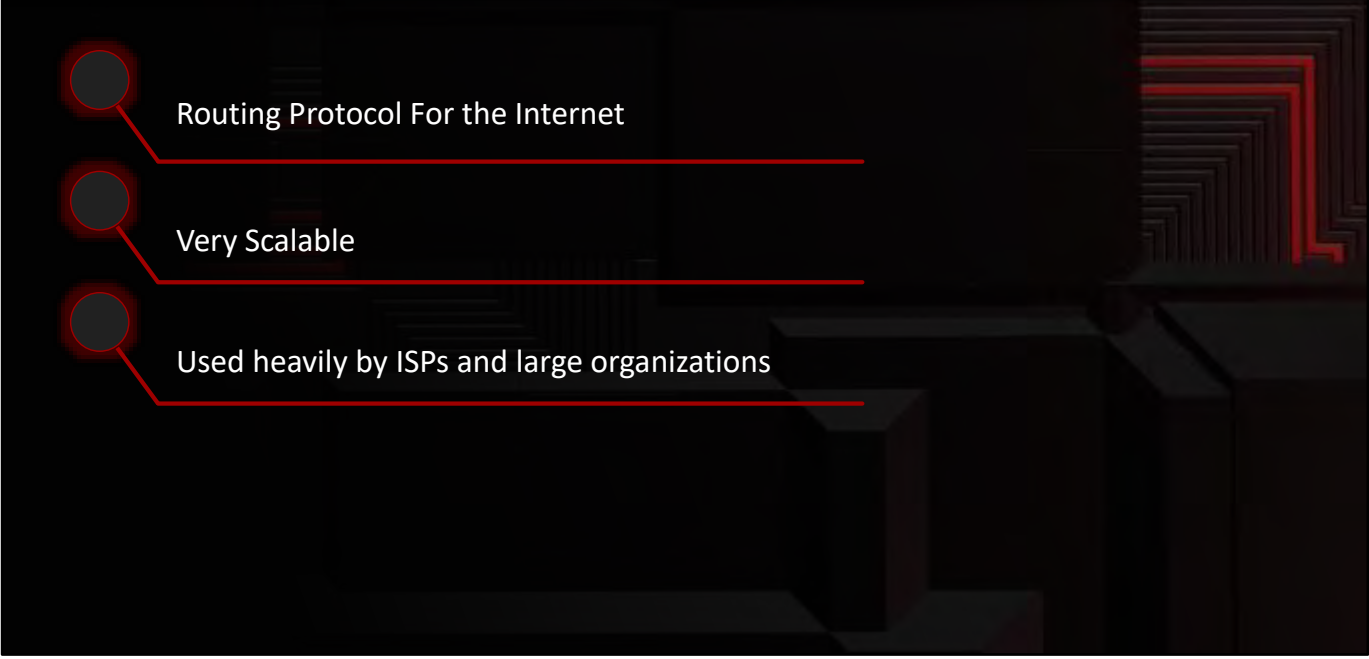
Path Vector



Path vector protocols consider the entire path, including all the autonomous systems it traverses

Unlike distance-vector protocols, which only consider metrics like distance

Border Gateway Protocol

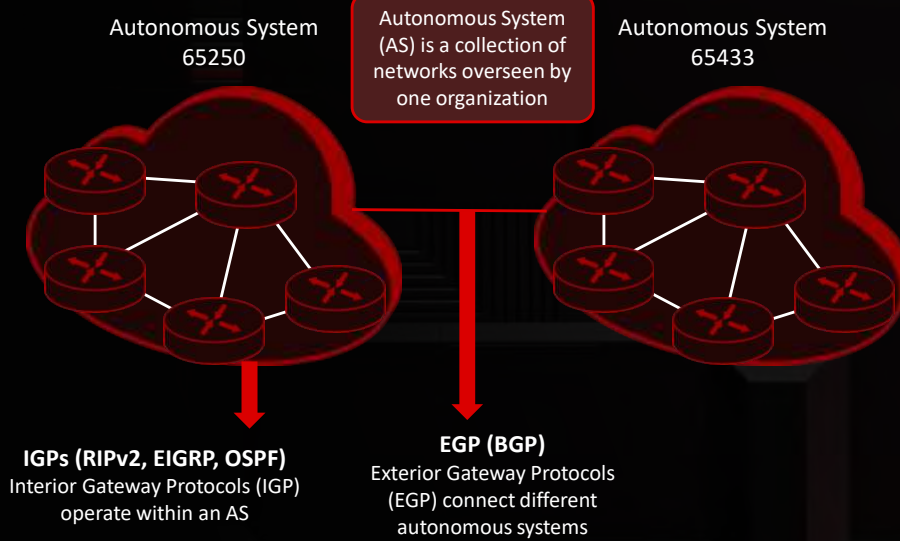


Routing Protocol For the Internet

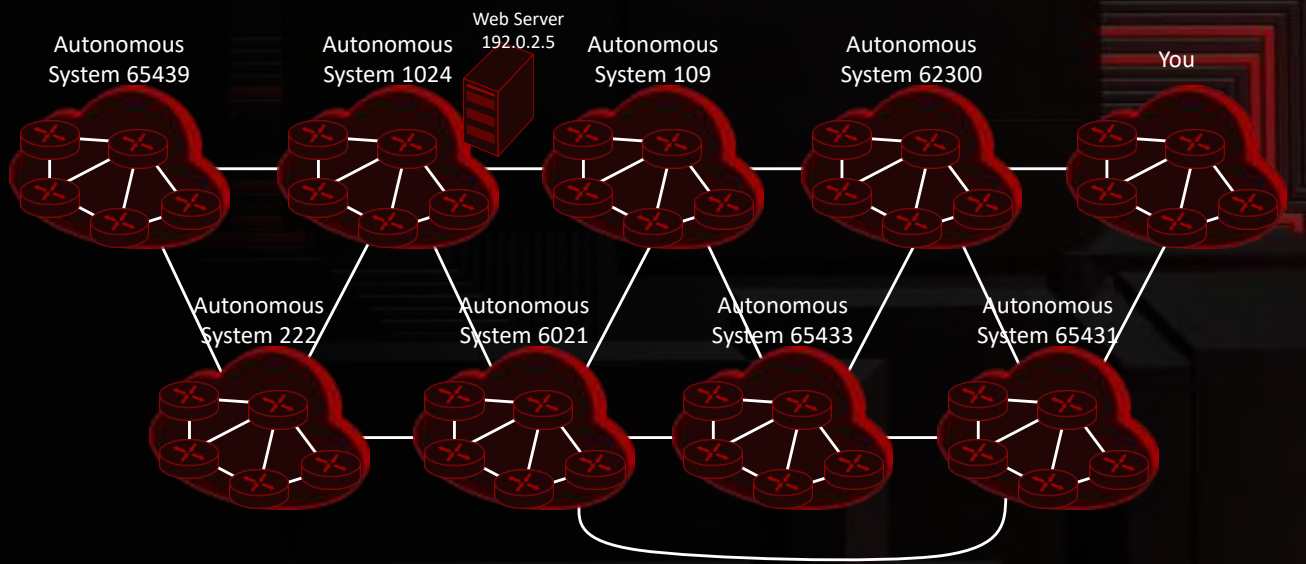
Very Scalable

Used heavily by ISPs and large organizations

BGP Autonomous Systems (AS)



BGP Autonomous Systems (AS)



Autonomous System Numbers

Public – Assigned By IANA through RIRs and ISPs

2 byte original range 1 to 65535

4 byte new range 65536 to 4294967295

Private – Assigned By You

64512 to 65534

4200000000 to 4294967294

BGP Basics

- Uses TCP port 179
client/server
- Classified as:
Path Vector (similar to D.V.)
- Forms neighborships
- Advertises NLRI
Prefix
Advertises Path Attributes (PA)

eBGP vs iBGP



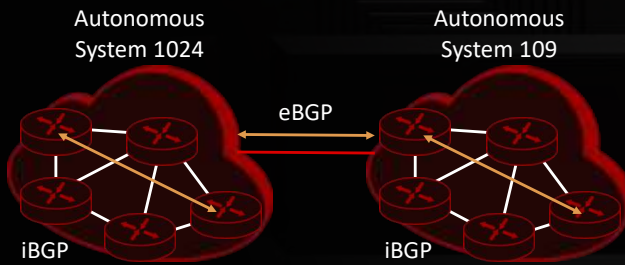
eBGP

Peering between directly connected routers in different AS, AD of 20



iBGP

Peering between any routers in same AS, AD of 200



BGP Messages

Open

Used to establish peering by exchanging basic parameters such as AS number and authentication values

Keepalive

Sent periodically to maintain peering

Update

Used to exchange path attributes and prefixes when adding and withdrawing routes

Notification

Signals BGP issues and errors, typically causes BGP peering to reset



Routing Information Bases



Data structures that hold the router's route information.

RIB-In:

Stores routes learned from all BGP peers.

Local RIB:

Contains the best routes selected from the RIB-In.

Installed in the routing table

RIB-out:

Stores all routes that are advertised to all BGP peers.

BGP Attributes

AS-Path:

Loop prevention and path selection

Local Preference:

Used internally within an AS to prefer one exit point over others

Next Hop:

Specifies the next hop IP address.
Must be reachable

Multi-Exit Discriminator (MED)

External path preference

Lower value suggests a more preferred path when multiple entry points exist into an AS

Community:

Tag for custom path decisions.

Allows for flexible policy settings.
Can be used to signal certain route preferences.

BGP Route Selection

When a BGP router has multiple paths for the same destination, it considers these attributes in the given order:

Local Preference:

Used for choosing an exit point from the AS. Higher value preferred.

AS-Path:

Shorter paths are chosen next.

Origin:

Preference is given to routes learned from an IGP, then EGP, and lastly incomplete origins.

MED:

Lower value is more preferred. Considered when all else is equal.

Route Age:

Older routes are considered more stable and are preferred when all else is equal.

Configuring BGP



```
Config router bgp
  set as [AS NUMBER]
  set router-id [router ip]
  config neighbor
    edit [IP ADDRESS]
      set remote-as 200
    next
  end
end
```

Route Reflectors (RR)

Adds ability to share routes from iBGP peers to other iBGP peers.

Reduces amount of iBGP connections needed.

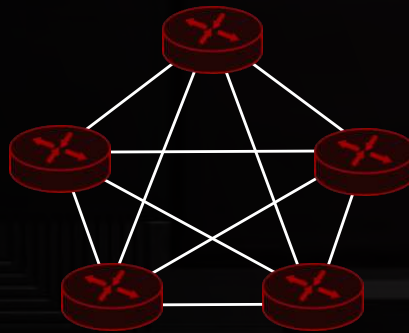


```
Config router bgp
  config neighbor
    edit [ip address]
      set route-reflector-
        client enable
    next
  end
end
```

Route Reflectors (RR)

Adds ability to share routes from iBGP peers to other iBGP peers.

Reduces amount of iBGP connections needed.



Full Mesh



Redistribution

Inject statics into its BGP routing process.

These routes will then be advertised to all BGP peers



```
Config router bgp
  config redistribute static
  set status enable
end
```



Filtering

Filtering

Access-list

Control routing updates or filter specific routes based on IP address or subnet.

Prefix-list

Allow more granular control as you can match on both the network prefix and the prefix length.

Route-map

Used in conjunction with access-lists or prefix-lists to manipulate attributes of routes

Access-List

```
config router access-list
  edit BGP_SUBNET_FILTER
    config rule
      edit 1
        set prefix 10.17.0.0/16
        set action deny
      next
      edit 2
        set prefix 10.0.0.0/8
        set action permit
      next
    end
  end
end
```



```
config router bgp
  config neighbor
    edit 100.64.1.254
      set distribute-list-in
        BGP_SUBNET_FILTER
    next
  end
end
```



Prefix-list

```
config router prefix-list
  edit BGP_SUBNET_FILTER
    config rule
      edit 1
        set prefix 10.17.0.0/16
        set action deny
      next
      edit 2
        set prefix 10.0.0.0/8
        set action permit
        set ge 16
      next
    end
  end
end
```



```
config router bgp
  config neighbor
    edit 100.64.1.254
      set prefix-list-in
        BGP_SUBNET_FILTER
      next
    end
  end
end
```



Route-map

```
config router route-map
  edit change-weight
    config rule
      edit 1
        set match-origin igp
        set set-weight 40000
      next
    end
  next
```



```
config router bgp
  config neighbor
    edit 100.64.1.254
      set route-map-in change-weight
    next
  end
end
```



Combining Route-maps with Access-lists and Prefix-lists

```
config router access-list
  edit BGP_SUBNET_FILTER
    config rule
      edit 1
        set prefix 10.17.0.0/16
        set action deny
      next
      edit 2
        set prefix 10.0.0.0/8
        set action permit
      next
    end
  end
end
```



```
config router route-map
  edit set-tag
    config rule
      edit 1
        set match-ip-address
        BGP_SUBNET_FILTER
        set set-route-tag 10
      next
    end
  next
end
```



Network-import-check

When enabled

Router checks routing table for matching IGP route.

Match Found

Router will continue to advertise that network to its BGP peers

Match Not Found

Router will withdraw the advertisement for that network from BGP

Config router bgp

set as [AS NUMBER]

set router-id [router ip]

set network-import-check enable

config neighbor

edit [IP ADDRESS]

set remote-as 200

next

end

end

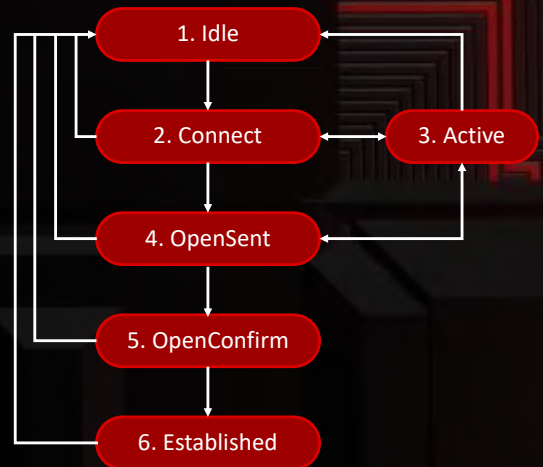




Troubleshooting

BGP neighbor states

1. **Idle:**
Initial state, no resources allocated, and it's willing to establish a connection.
2. **Connect:**
TCP connection attempts are made in this state.
3. **Active:**
The router is trying to initiate a TCP session with its peer.
4. **OpenSent:**
An OPEN message has been sent, and the router is waiting for an OPEN message from its peer.
5. **OpenConfirm:**
The router received an OPEN message and responded with a KEEPALIVE message.
6. **Established:**
The routers are exchanging UPDATE messages. This is the final, operational state.



BGP Neighbors

Check bgp neighbor status Connectivity time

NGFW-1 # get router info bgp neighbor

VRF 0 neighbor table:

BGP neighbor is 100.64.1.254, remote AS 100, local AS 65100, external link

BGP version 4, remote router ID 100.64.1.254

BGP state = Established, up for 00:01:34

Last read 00:00:34, hold time is 180, keepalive interval is 60 seconds

Configured hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received (old and new)

Address family IPv4 Unicast: advertised and received

Address family VPNv4 Unicast: advertised

Received 5 messages, 0 notifications, 0 in queue

Sent 4 messages, 0 notifications, 0 in queue

Route refresh request: received 0, sent 0

NLRIs treated as withdraw: 0

Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast

BGP table version 1, neighbor version 1

Index 1, Offset 0, Mask 0x2

Community attribute sent to this neighbor (both)

1 accepted prefixes, 1 prefixes in rib

1 announced prefixes

For address family: VPNv4 Unicast

BGP table version 1, neighbor version 1

Index 1, Offset 0, Mask 0x2

Community attribute sent to this neighbor (both)

0 accepted prefixes, 0 prefixes in rib

0 announced prefixes

For address family: IPv6 Unicast

BGP table version 1, neighbor version 1

Index 1, Offset 0, Mask 0x2

Community attribute sent to this neighbor (both)

0 accepted prefixes, 0 prefixes in rib

0 announced prefixes

Connections established 1; dropped 0

Local host: 100.64.1.1, Local port: 179

Foreign host: 100.64.1.254, Foreign port: 44258

Egress interface: 3

Nexthop: 100.64.1.1

Nexthop interface: port1

Nexthop global: fe80::9fff:fe00:602

Nexthop local: ::

BGP connection: non shared network

BGP neighbor is 100.64.2.254, remote AS 100, local AS 65100, external link

BGP version 4, remote router ID 100.64.1.254

BGP state = Established, up for 00:01:34

Last read 00:00:34, hold time is 180, keepalive interval is 60 seconds

Configured hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:

Route refresh: advertised and received (old and new)

Address family IPv4 Unicast: advertised and received

Address family VPNv4 Unicast: advertised

Address family IPv6 Unicast: advertised

Received 5 messages, 0 notifications, 0 in queue

Sent 4 messages, 0 notifications, 0 in queue

Route refresh request: received 0, sent 0

NLRIs treated as withdraw: 0

Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast

BGP table version 1, neighbor version 1

Index 2, Offset 0, Mask 0x4

Community attribute sent to this neighbor (both)

2 accepted prefixes, 2 prefixes in rib

1 announced prefixes

For address family: VPNv4 Unicast

BGP table version 1, neighbor version 1

Index 2, Offset 0, Mask 0x4

Community attribute sent to this neighbor (both)

0 accepted prefixes, 0 prefixes in rib

0 announced prefixes

For address family: IPv6 Unicast

BGP table version 1, neighbor version 1

Index 2, Offset 0, Mask 0x4

Community attribute sent to this neighbor (both)

0 accepted prefixes, 0 prefixes in rib

0 announced prefixes

Connections established 1; dropped 0

Local host: 100.64.2.1, Local port: 179

Foreign host: 100.64.2.254, Foreign port: 52958

Egress interface: 4

Nexthop: 100.64.2.1

Nexthop interface: port2

Nexthop global: fe80::9fff:fe00:702

Nexthop local: ::

BGP connection: non shared network

BGP Summary

```
NGFW-1 # get router info bgp summary
```

```
VRF 0 BGP router identifier 172.16.1.254, local AS number 65100
```

```
BGP table version is 1
```

```
2 BGP AS-PATH entries
```

```
0 BGP community entries
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd		
100.64.1.254	4	100	5		4		1	0	0	00:01:27	1
100.64.2.254	4	100	5		4		1	0	0	00:01:27	2

BGP Summary

v:
The BGP version that the BGP speaker (neighbor) is using.

AS:
The autonomous system number of the neighbor.

MsgRcvd and MsgSent:
The number of BGP messages received and sent to each neighbor.

TblVer:
The version number of the BGP routing table.

InQ and OutQ:
The number of updates queued to be sent (OutQ) and the number of updates received but not yet processed (InQ).

Up/Down:
The length of time the connection has been established (up) or the time since the connection was lost (down).

State/PfxRcd:
The state of the BGP connection and the number of prefixes received from each neighbor.
If State is Established you will just see prefix received

Clearing BGP

Clear all current BGP sessions
Tears down and reestablish BGP peer connections

```
NGFW-1 # execute router  
clear bgp all
```

Enabling Debugs

```
diagnose ip router bgp all enable
```

Enables logs for all bgp operations

```
diagnose ip router bgp level info
```

Adds informational messages in the logs

Debug Filters

Diagnose debug flow filter

```
diagnose debug flow filter port 179
```

```
diagnose debug flow filter addr <IP_Address>
```

```
diagnose debug flow filter
```

```
addr <IP_Address1> <IP_Address2> { and | or }
```

DEMO - Configuring BGP

Configure BGP with FortiManager

Policy & Objects -> Managed FortiGate -> Network -> BGP

(Feature Visibility could have it off)

Configure BGP on FortiGate



Conclusions

BGP configuration

Route Reflectors

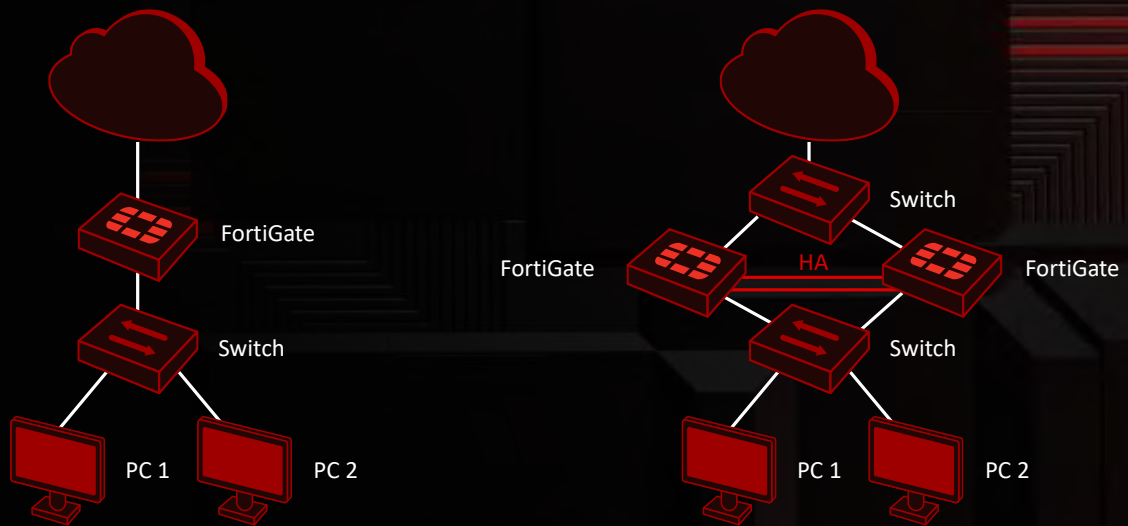
Filtering

Troubleshooting



High Availability

High Availability



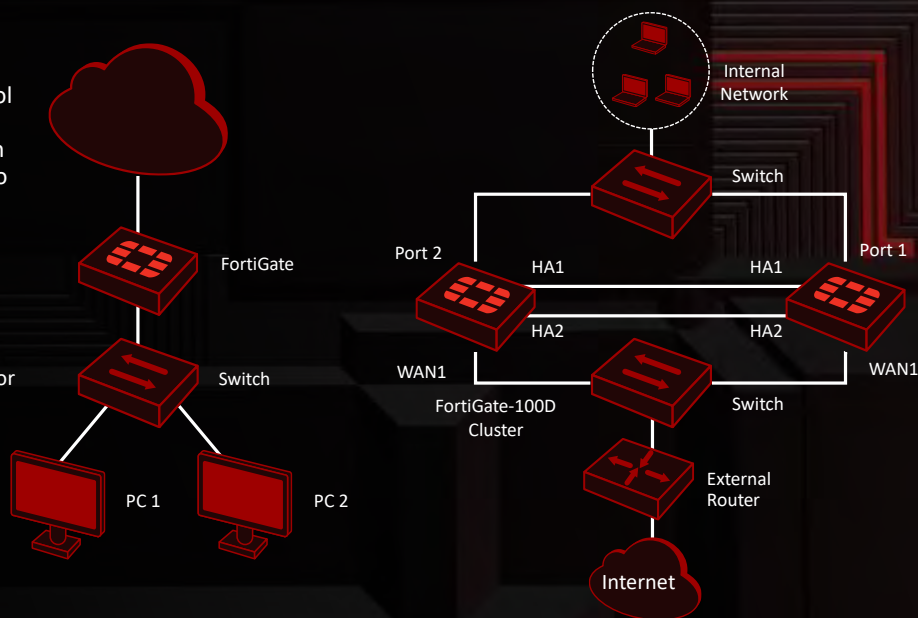
High Availability (HA)

The FortiGate Clustering Protocol (FGCP) is a proprietary HA solution whereby FortiGates can find other member FortiGates to negotiate and create a cluster.

FGCP uses TCP/703

Focuses on minimizing system downtime.

Provides failover capabilities for critical systems.



How Failover Happens

1

Link fails

Before triggering a failover when a link fails, the administrator must ensure that monitor interfaces are configured.

Normally, the internal interface that connects to the internal network, and an outgoing interface for traffic to the internet or outside the network, should be monitored.

Any of those links going down will trigger a failover.

How Failover Happens

2 Loss of power for active unit.

When an active (master) unit loses power, a backup (slave) unit automatically becomes the master.

The impact on traffic is minimal.

There are no settings for this kind of fail over.

How Failover Happens

3

SSD failure

HA failover can be triggered by an SSD failure.

To enable an SSD failure triggering HA fail over;

```
config system ha
    set ssd-failover enable
end
```

HA Requirements

Same:

Model

Firmware

Licenses

Master

Highest priority

Slave

No configuration other than ha

Lower priority

```
config system ha
  set mode {a-a / a-p}
  set group-name <name>
  set group-id <ID>
  set password <password>
  set hbdev <"interface name"> <integer>
  set priority <priority>
  set link-failed-signal enable
end
```

HA Mode

Mode

Active-Active

Both devices handle traffic

Active-Passive

One device handles traffic while other waits in standby

```
config system ha
  set mode {a-a / a-p}
  set group-name <name>
  set group-id <ID>
  set password <password>
  set hbdev <"interface name"> <integer>
  set priority <priority>
  set link-failed-signal enable
end
```

HA MAC-Address

The virtual MAC address is determined based on following formula 00-09-0f-09-<group-id_hex>

To prevent virtual mac conflicts select different Group ID for each HA cluster

Ref: [Technical Tip: HA Cluster virtual MAC addresses - Fortinet Community](#)

```
config system ha
  set mode {a-a / a-p}
  set group-name <name>
  set group-id <ID>
  set password <password>
  set hbdev <"interface name"> <integer>
  set priority <priority>
  set link-failed-signal enable
end
```

HA Heartbeat

Set interfaces where heartbeat
keepalives will send out of

Recommended two
interfaces

```
config system ha
  set mode {a-a / a-p}
  set group-name <name>
  set group-id <ID>
  set password <password>
  set hbdev <"interface name"> <integer>
  set priority <priority>
  set link-failed-signal enable
end
```

HA Link-failed-signal

Shuts down the interface for one second during failover

Causes switches to clear mac table

Without this some switches may still forward to wrong FortiGate

```
config system ha
  set mode {a-a / a-p}
  set group-name <name>
  set group-id <ID>
  set password <password>
  set hbdev <"interface name"> <integer>
  set priority <priority>
  set link-failed-signal enable
end
```


Check HA Sync Status

Can be viewed in the GUI

Widget on the Dashboard
On the System > HA page.

It can also be confirmed through the CLI.

When a cluster is out of sync, administrators should correct the issue as soon as possible as it affects the configuration integrity and can cause issues to occur.



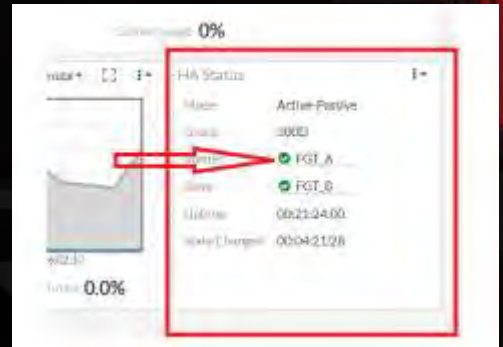
HA Sync in the GUI

Dashboard widget;

Following HA setup, the HA Status widget can be added to the Dashboard.

The widget shows the HA sync status by displaying a green checkmark next to each member in sync.

A red mark indicates the member is out of sync.



HA Sync in the GUI



The same set of icons will be displayed on the System > HA page to indicate if the member is in sync



HA Sync Status in the CLI



You can type **get sys ha status** to see if the cluster is in sync.

The sync status is reported under Configuration Status.

```
FortiFirewall-VM64-KVM # get sys ha status
HA Health Status: OK
Model: FortiFirewall-VM64-KVM
Mode: HA-A-A
Group Name: HA-FAILOVER
Group ID: 5
Debug: 0
Cluster Uptime: 0 days 0:6:0
Cluster state change time: 2023-08-01 17:43:05
Primary selected using:
<2023/08/01 17:43:05> vcluster-1: FFVMEVFECASAT3F9 is selected as the primary because its override priority is larger than peer member FFVMEVOD-VZVCUA6.
<2023/08/01 17:40:55> vcluster-1: FFVMEVFECASAT3F9 is selected as the primary because it's the only member in the cluster.
ses_pickup: disable
load_balance: disable
load_balance_udp: disable
schedule: Round robin.
upgrade_mode: set
override: disable
Configuration Status:
FFVMEVFECASAT3F9(updated 4 seconds ago): in-sync
FFVMEVFECASAT3F9 checksum dump: 69 da 2d 7d f9 b2 c4 2f 56 54 12 2b d3 b4 b0 56
FFVMEVOD-VZVCUA6(updated 4 seconds ago): in-sync
FFVMEVOD-VZVCUA6 checksum dump: 69 da 2d 7d f9 b2 c4 2f 56 54 12 2b d3 b4 b0 56
System Usage Stats:
FFVMEVFECASAT3F9(updated 4 seconds ago):
  sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/97%, memory=49%
FFVMEVOD-VZVCUA6(updated 4 seconds ago):
  sessions=2, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=49%
HBDEV stats:
FFVMEVFECASAT3F9(updated 4 seconds ago):
  port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=585777/1620/0/0, tx=1252980/2407/0/0
FFVMEVOD-VZVCUA6(updated 4 seconds ago):
  port2: physical/1000auto, up, rx-bytes/packets/dropped/errors=1250723/2395/0/0, tx=585261/1624/0/0
Primary : FortiFirewall-VM64-KVM, FFVMEVFECASAT3F9, HA cluster index = 1
Secondary : FortiFirewall-VM64-KVM, FFVMEVOD-VZVCUA6, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FFVMEVFECASAT3F9, HA operating index = 0
Secondary: FFVMEVOD-VZVCUA6, HA operating index = 1
```

Troubleshooting

```
FortiFirewall-VM64-KVM # get system ha
group-id          : 5
group-name        : HA_FAILOVER
mode              : a-a
sync-packet-balance : disable
password          : *
hbdev             : "port2" 1
session-sync-dev  :
route-ttl         : 10
route-wait        : 0
route-hold        : 10
multicast-ttl     : 600
evpn-ttl          : 60
sync-config       : enable
encryption        : disable
authentication     : disable
hb-interval       : 2
hb-interval-in-milliseconds: 100ms
hb-lost-threshold : 20
hello-holddown    : 20
gratuitous-arps   : enable
arps              : 5
arps-interval     : 8
session-pickup    : disable
link-failed-signal : enable
uninterruptible-upgrade: enable
uninterruptible-primary-wait: 30
ha-mgmt-status    : disable
ha-eth-type       : 8899
hc-eth-type       : 8891
lzep-eth-type     : 8893
ha-uptime-diff-margin: 300
schedule          : round-robin
override          : disable
priority          : 10
monitor           :
pingserver-monitor-interface:
vcluster:
ssd-failover      : disable
memory-compatible-mode: disable
memory-based-failover: disable
failover-hold-time : 0
load-balance-all : disable
```

Troubleshooting

```
FortiFirewall-VM64-KVM # diag hardware deviceinfo nic port2
Name: port2
Driver: e1000
Version: 7.3.21-k8-NAPI
Bus: 0000:00:04.0
Hwaddr: 00:09:0f:00:05:01
Permanent Hwaddr: 00:c4:fc:f9:00:01
State: up
Link: up
Mtu: 1500
Supported: auto 10half 10full 100half 100full 1000full
Advertised: auto 10half 10full 100half 100full 1000full
Speed: 1000full
Auto: enabled
RX Ring: 256
TX Ring: 256
Rx packets: 357
Rx bytes: 127793
Rx compressed: 0
Rx dropped: 0
Rx errors: 0
  Rx Length err: 0
  Rx Buf overflow: 0
  Rx Crc err: 0
  Rx Frame err: 0
  Rx Fifo overrun: 0
  Rx Missed packets: 0
Tx packets: 1131
Tx bytes: 521163
Tx compressed: 0
Tx dropped: 0
Tx errors: 0
  Tx Aborted err: 0
  Tx Carrier err: 0
  Tx Fifo overrun: 0
  Tx Heartbeat err: 0
  Tx Window err: 0
Multicasts: 251
Collisions: 0
```

Troubleshooting

```
FortiFirewall-VM64-KVM # diagnose sys session list
```

```
session info: proto=6 proto_state=01 duration=311 expire=3588 timeout=3600 flags=00000000 socktype=0 sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=local may_dirty nosyn_ses
statistic(bytes/packets/allow_err): org=1144/14/1 reply=576/10/1 tuples=2
tx speed(Bps/kbps): 3/0 rx speed(Bps/kbps): 1/0
origin->sink: org pre->in, reply out->post dev=20->19/19->20 gw=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 169.254.0.1:5950->169.254.0.2:703(0.0.0.0:0)
hook=post dir=reply act=noop 169.254.0.2:703->169.254.0.1:5950(0.0.0.0:0)
pos/(before,after) 0/(0,0), 0/(0,0)
misc=0 policy_id=4294967295 pol_uuid_idx=0 auth_info=0 chk_client_info=0 vd=1
serial=000000096 tos=ff/ff app_list=0 app=0 url_cat=0
rpidb_link_id=00000000 ngfwid=n/a
npu_state=00000000
```

Troubleshooting

diagnose debug application hataalk -1

```
FortiWeb # (ha_hb.c : 176) : mem-table[0]:
(ha_hb.c : 61) : member name : wasp
(ha_hb.c : 62) : member pcnt : 0
(ha_hb.c : 63) : member pri : 5
(ha_hb.c : 64) : member sn : FV-1KC3R11700136
(ha_hb.c : 65) : member age : 11209
(ha_hb.c : 66) : member role : 1
(intf_check.c : 273) : clicfg->monitor_count : 1, count : 1
(ha_hb_send.c : 85) : sock : 26, sendlen : 264(head: 88, mem(2) 88)
(ha_hb_send.c : 104) : Send HB buf success.
(ha_hb.c : 83) : Enter Function : get_master_sn
(ha_hb.c : 756) : =====
(ha_hb.c : 760) : ==> HB..., I'am (Master) master is : FV-1KC3R11700094
(ha_hb.c : 637) : update my status info : FV-1KC3R11700094
(ha_hb.c : 871) : Enter Fun : hb_packet_check
(ha_hb.c : 897) : mysn : FV-1KC3R11700094(0), comesn : FV-1KC3R11700136(1)
(ha_hb_recv.c : 446) : Got an valid HB packet(port3), len : 176
(ha_hb_recv.c : 451) : come from : FV-1KC3R11700136
(ha_hb_recv.c : 104) : fill ha member to local
(ha_hb_recv.c : 251) : slave (FV-1KC3R11700136) arrived ...
(ha_hb_recv.c : 342) : An exist slave device arrive...
(ha_hb_recv.c : 512) : sockfd1 : 200(UP), sockfd2 : 0(DOWN)
(ha_hb.c : 159) : Enter Function : print_member_tab
(ha_hb.c : 166) : total cnt : 2
```


Conclusions

High Availability

Configuration

Troubleshooting



VPN Setup and Troubleshooting

IPsec VPN Overview

Securely transmits data over untrusted networks

Combines three protocols into a cohesive security framework

Provides encryption, integrity, and authentication

Applicable in Site-to-Site or Remote Access scenarios

IKE/IKEv2

Provides a framework for policy negotiation and key management

AH

Provides an encapsulation for authentication of user traffic. Mostly obsolete.

ESP

Provides an encapsulation for encryption and authentication of user traffic

IKEv1 vs IKEv2

IKEv1

Two Phases

Phase 1: Establishes Secure Channel

Main Mode (6 steps) or Aggressive Mode (3 steps)

Negotiates encryption, hash, DH group, lifetime

Phase 2: Negotiates IPSec SA parameters

Quick Mode; builds on Phase 1's security

Negotiates encryption, hash, lifetime for data traffic

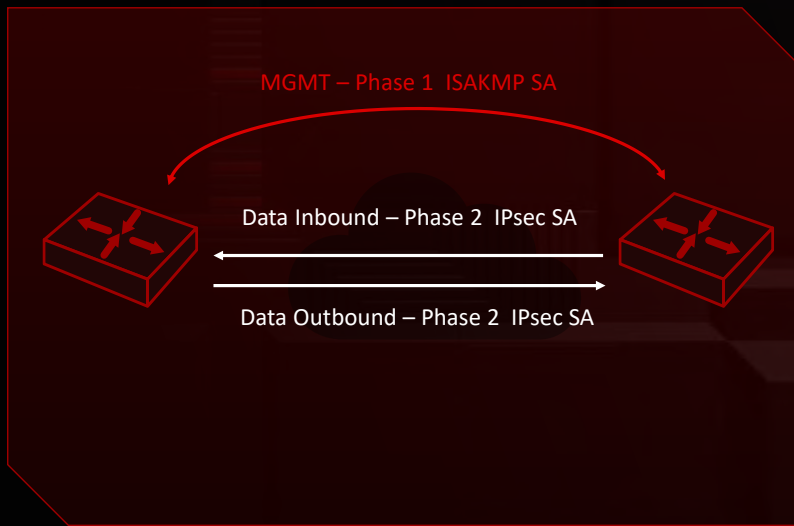
IKEv2

Combines Phase 1 and 2 into a single exchange

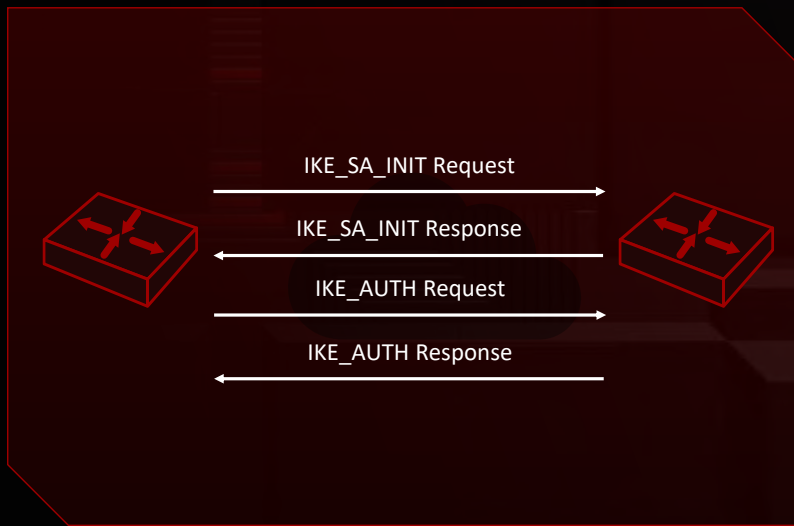
More efficient and flexible than IKEv1

Simplified negotiation with fewer messages

IKE v1 Flow



IKE v1 Flow



IKEv1 Phase 1 Requirements

Hashing

Data integrity

Authentication

Digital signature (RSA-Sig)

Pre-shared key (PSK)

Group (Diffie-Helman group)

Lifetime

Encryption

Hash Methods

Hash Functions

Used to ensure integrity and verify data
Produces a fixed-size output (hash) from input data

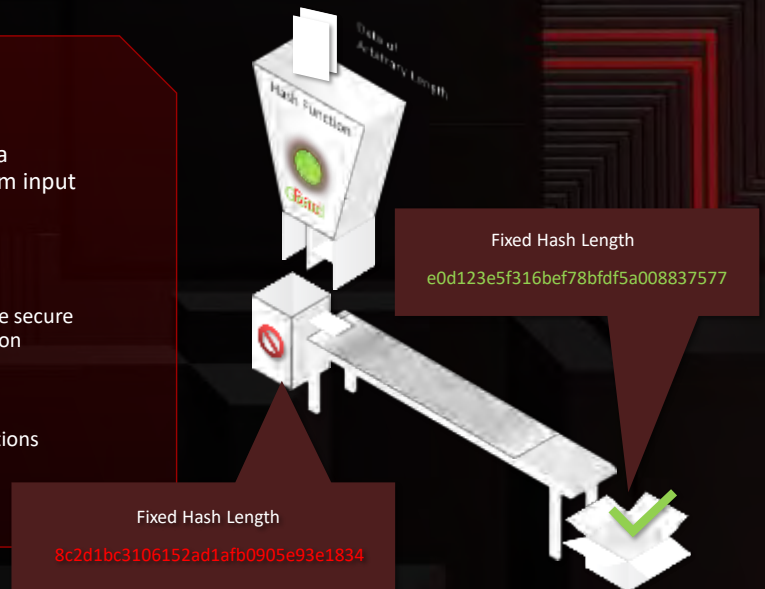
Common Hash Algorithms in IPsec

SHA-1

160-bit hash output
Slower than MD5 but considered more secure
Suitable for general integrity verification

MD5

128-bit hash output
Faster but less secure than SHA-1
Less common in modern implementations



Authentication Methods

Pre-shared Key: This is a form of symmetric encryption where the same key is used to both encrypt and decrypt the data. The key must be known to both parties before communication can take place.

Certificates: These are digital documents that bind a public key to an entity. The certificate is digitally signed by a trusted third party, ensuring that the public key belongs to the stated owner.

Authentication Methods

XAUTH

XAuth provides additional security by requiring VPN users to authenticate themselves before they're granted access to the network.

This method of authentication can be used in combination with both pre-shared key and certificate authentication.

Groups

Diffie-Hellman Groups

Key exchange algorithm enabling secure communication

Allows two parties to generate a shared secret over an insecure channel

Different groups represent different "strengths" or sizes of keys

Common Groups

Group 1: 768-bit key (now considered weak)

Group 2: 1024-bit key (common but being phased out)

Group 5: 1536-bit key (stronger, more common in modern implementations)

Group 14: 2048-bit key (even stronger, recommended for most applications)

Selection based on balance between security needs and performance considerations

Lifetime

Defines how long a particular set of security associations (SAs) remains active

Time-based (e.g., 8 hours) or traffic-based (e.g., after 10GB of data)

Shorter lifetimes increase security by forcing frequent renegotiation

Longer lifetimes improve performance by reducing renegotiation overhead

Often configured differently for Phase 1 and Phase 2

Must be agreed upon between both VPN endpoints

Encryption Algorithms

Encryption

- Used to ensure confidentiality by encrypting data

- Makes data unreadable without the correct key

Common Encryption Algorithms in IPSec

AES (Advanced Encryption Standard)

- Various key lengths (128, 192, 256 bits)

- Considered very secure and widely adopted

- Good balance of security and performance

DES (Data Encryption Standard)

- 56-bit key

- Now considered weak due to key length; often avoided

3DES (Triple DES)

- Applies DES three times with different keys

- More secure than DES but less efficient than AES

Configuring IPsec VPN

Steps to Configuring IPsec VPN

Define Phase 1: Set interface, proposal, PSK or Certs

Define Phase 2: Set protocols (ESP, AH), encryption and hash

Define policies: Link Phase 1 and 2; apply to traffic

Assign users/groups to VPN if needed

Configuring IPsec VPN

Phase 1 Configuration:

Defines the "to_HQ2" IPsec VPN connection.

Interface Selection:

Utilizes "port1" for the VPN connection.

Encryption and Hashing:

Proposes AES and SHA algorithms.

Remote Gateway:

Connects to IP address 172.16.202.1.

Authentication:

Employs a Pre-Shared Key (PSK) labeled "sample."

```
config vpn ipsec phase1-interface
edit "to_HQ2"
set interface "port1"
set peertype any
set net-device enable
set proposal aes128-sha256 aes256-sha256
aes128-sha1 aes256-sha1
set remote-gw 172.16.202.1
set psksecret sample
next
end
```

Configuring IPsec VPN

Phase 2 Configuration:

Defines the "to_HQ2" IPsec VPN connection.

Linked to Phase 1:

Associates with Phase 1 configuration named "to_HQ2."

Encryption and Hashing:

Proposes various AES algorithms and SHA hashing.

Auto-Negotiation:

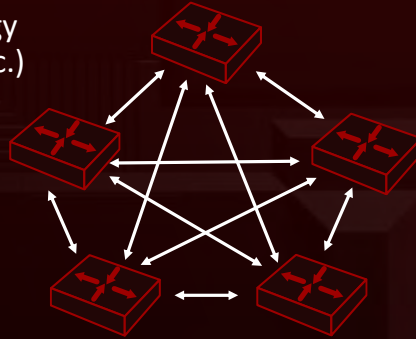
Enables automatic negotiation of parameters.

```
config vpn ipsec phase2-interface
edit "to_HQ2"
    set phase1name "to_HQ2"
    set proposal aes128-sha1 aes256-sha1 aes128-
sha256 aes256-sha256 aes128gcm aes256gcm
chacha20poly1305
    set auto-negotiate enable
next
end
```


VPN Community

Manages multiple VPNs across devices

Easily define VPN topology
(hub-spoke, full mesh, etc.)



VPN Community - Lab

FortiManager

Core -> VPN Manager -> IPsec VPN ->
VPN Communities.

Add Devices to VPN Community

Right click name set -> Add Managed
Gateway

Assign Role and Device

Install VPN Configuration

Add & Install Policies



Anti-replay

Prevents replay attacks by rejecting old packets

Important in scenarios with high-security requirements

Options

Disable:

No protection against replay attacks, vulnerable to SYN floods.

Loose:

Checks packet sequence and ICMP replay, with specific criteria for SYN, FIN, RST bits, ICMP error packets, and RST sequence number if check-reset-range is strict.

Strict:

Includes all loose checks plus verifies TCP sequence number in SYN packets for new sessions, helps prevent SYN flooding, drops failed checks.

Default

```
config system global
set anti-replay {disable | loose | strict}
```

IKE NAT-T

IKE NAT-T (NAT Traversal) allows IPSec traffic to pass through NAT or PAT devices

Encapsulates IPSec packets in UDP to traverse NAT

Negotiated during Phase 1

```
set nat traversal enable  
#Default is enable
```

AutoDiscovery VPN (ADVPN)

IPSec VPN

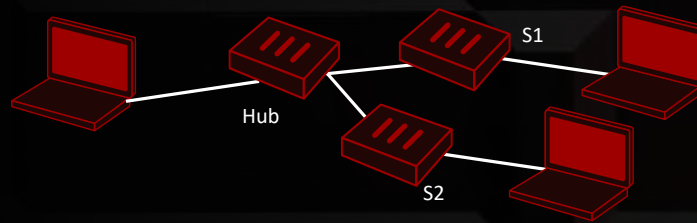
Establish secure communication between two known endpoints.

Use for fixed point-to-point connections.

ADVPN

Dynamic establishment of VPN tunnels between spokes in a hub-and-spoke network, reducing latency.

Use for dynamic networks with varying paths (like in SD-WAN).



Configure ADVPN

Use the easy configuration keys.



Troubleshooting IPsec VPN

1 **Tunnel Name:** 'to10.174.0.182'

2 **Remote IP:** 10.174.0.182 with port 0

(the port being 0 usually means it's the default or not specified)

3 **Selectors:**

Total Selectors: 1

Active/Up Selectors: 1

4 **Receive Statistics (rx):**

Packets (pkt): 1921

Errors (err): 0

5 **Transmit Statistics (tx):**

Packets (pkt): 69

Errors (err): 2

```
get vpn ipsec tunnel summary
```

```
'to10.174.0.182' 10.174.0.182:0 selectors(total,up): 1/1 rx(pkt,err): 1921/0 tx(pkt,err): 69/2  
'to10.189.0.182' 10.189.0.182:0 selectors(total,up): 1/0 rx(pkt,err): 0/0 tx(pkt,err): 0/0
```

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-IPsec-VPNs-tunnels/ta-p/195955>

Troubleshooting IPsec VPN

Gateways and IKE Mode:

Local and remote gateways specified (<SIDE A IP>, <SIDE B IP>), using IKEv2 mode.

Interface Details:

'Port1' with Rx/Tx packet statistics.

Tunnel Mode:

Configured in tunnel mode with broad selectors.

Security Association (SA):

Details including lifetime/rekey, MTU, encryption (AES), and authentication (SHA256).

Additional Features:

Dead Peer Detection (DPD), replay enabled, no NPU acceleration.

```
NGFW-1 # get vpn ipsec tunnel details
```

```
gateway
name: <NAME>
local-gateway: <SIDE A IP> (static)
remote-gateway: <SIDE B IP> (dynamic)
dpd-link: on
mode: ike-v2
interface: 'port1' (3)
rx packets: 0 bytes: 0 errors: 0
tx packets: 0 bytes: 0 errors: 0
dpd: on-demand/negotiated idle: 2000ms retry: 3 count:
selectors
name: <NAME>
auto-negotiate: disable
mode: tunnel
src: 0:0:0:0:0-255.255.255.255:0
dst: 0:0:0:0:0-255.255.255.255:0
SA
lifetime/rekey: 1800/1644
mtu: 1280
tx-esp-sea: 1
replay: enabled
qat: 0
inbound
spi: 25cf01b6
enc: aes-cb1 a9d64alcacae8e37707e605ac0112d7
auth: sha256 a6fef2cd8f6b931b0a98cb94b12eb27f245c77dbf80ea0780d90b3f04de752f
outbound
spi: 10e0c092
enc: aes-cb 69a37ac2418a423b2a4992d3a1d751f4
auth: sha256 0f10c47e14d3f294449d1f8415775f9ea4d7df119e11addf1bc8a0c72b7584de
NPU acceleration: none
```


Troubleshooting IPsec

Tunnel Information:

Version 2, with source and destination IPs, tunnel IDs, MTU, and DPD (Dead Peer Detection) enabled.

Binding and Mode:

Bound to interface 3, with static layer and automatic mode, primary role.

Dead-on-Demand (DoD) and NAT

Traversal (NATT):

DoD mode on-demand, NATT mode none.

Proxy and Security Association (SA) Details:

Proxy ID, SA options, MTU, expiration, and replay window of 2048.

Encryption and Decryption (enc/dec) Details:

Specifies AES and SHA256 keys for both enc and dec, along with NPU information.

```
Spoke-2 # diagnose vpn tunnel list name <NAME>
list ipsec tunnel by names in vd 0
```

```
-----
name=<NAME> ver=2 serial=1 <Source IP>-><dst ip> tun id=100.64.1.1 tun id6=::100.64.1.1 dst
mtu=65535 dpd-link=on weight=1
bound if=3 lwy=static/1 tun=intf mode=auto/1 encap=none/552 options [0228]=npu frag-ffc run state=0
role=primary accept traffic=1 overlay id=0
```

```
proxyid num=1 child num=0 refcnt=5 ilast=42951037 olast=42951037 ad=/0
stat: r*0=0 +x0=0 rxb=0 txb=0
```

```
dod: mode=on-demand on=1 idle=20000ms retry=3 count=0 seano=0
```

```
natt: mode=none draft=0 interval=0 remote port=0
```

```
fec: egress=0 ingress=0
```

```
proxyid=<NAME> 0 proto=0 sa=1 ref=2 serial=1
```

```
Src: 0:0:0:0:0:255:255:255:255:0
```

```
Dst: 0:0:0:0:0:255:255:255:255:0
```

```
SA: ref=3 options=30202 type=00 soft=0 mtu=65470 expire=1661/08 replaywin=2048
```

```
seano=1 esn=0 replaywin lastseq=00000000 aat=192 rekey=0 hash search len=1
```

```
life: type=01 bytes=0/0 timeout=1767/1800
```

```
dec: spi=10e0c092 esp=aes key=16 69a37ac2418a42362a4992d3ald751f4
```

```
ah=sha256 key=32 0f10c47e14d3f294449d1f8415775f9ea4d7df119e11adff1bc8a0c7267584de
```

```
enc: spi=25cf01b6 esp=aes key=16 1a9d64alcacae8e37707e605ac0112d7
```

```
ah=sha256 key=32 a6fefdc2d8f6b931b0a98cb94b12eb27f245c77dbf80ea0780d90b3f04de752f
```

```
dec:pkts/bytes=0/0, enc:pkts/bytes=0/0
```

```
npu flag=00 npu rowy=100.64.1.1 npu low=100.64.5.1 npu selid=0 dec npuid=0 enc npuid=0
run tally=0
```

Troubleshooting IPsec VPNs

IKE Realtime Debug provides a live view of the negotiation process between VPN peers during tunnel establishment.

Information includes IKE phase 1 and 2 negotiation details, errors, authentication, and encryption information.

Failed authentication usually signifies issues with mismatched settings between VPN peers

IKE Debug

Enabling the debug:

```
diagnose debug application ike -1  
diagnose debug enable
```

Filtering

```
diagnose vpn ike log-filter  
list  
name  
    phase1 name  
src-addr4  
msrc-addr4  
    multiple addresses  
dst-addr4
```

*ensure correct address (NAT)

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-IPSEC-Tunnel-debugging-IKE/ta-p/190052>

```
ike 0: comes 192.168.175.153:500->192.168.175.152:500,ifindex=3....  
ike 0: IKEv1 exchange=Identity Protection id=ceb2556bb6a76a83/69eea84d4ce9b6c8 len=108  
ike 0: in  
CEB2556BB86A76A8369EEA84D4CE9B6C80510020100000000000006CCD04DA2FAF085808B8B0  
45C1AE7D3E8A9BECB21CD179AACD8965B038D50A5A97138CB6C53E5D18F6EE42EB77E8ADC08  
51783CBC676C7A93F30C0F9DCAC2E097A0E678A42D889777CAFC8DC0FC73C0E9F  
ike 0:Tunnel_1:30: responder: main mode get 3rd message...  
ike 0:Tunnel_1:30: dec  
CEB2556BB86A76A8369EEA84D4CE9B6C80510020100000000000006C7417465E8B8E5E10828E1  
60CB2ACED88EC9EC68E9C4B84E29743ED43E9723086CADD6EF04768A557744BADE51B4C1964  
5E35B56519BB56CA1800DB16533C40AE802554C8E295986F716B7B3C288704D83  
ike 0:Tunnel_1:30: parse error  
ike 0:Tunnel_1:30: probable pre-shared secret mismatch
```

IKE Debug

Order of Debug:

Phase 1

Xauth

IKE mode configuration

Phase 2

```
ike 0: comes 192.168.175.153:500->192.168.175.152:500,ifindex=3....
ike 0: IKEv1 exchange=Identity Protection id=ceb2556bb6a76a83/69eea84d4ce9b6c8 len=108
ike 0: in
CEB2556BB86A76A8369EEA84D4CE9B6C80510020100000000000006CCD04DA2FAF085808B8B0
45C1AE7D3E8A9BECB21CD179AACD8965B038D50A5A97138CB6C53E5D18F6EE42EB77E8ADC08
51783CBC676C7A93F30C0F9DCAC2E097A0E678A42D889777CAFC8DC0FC73C0E9F
ike 0:Tunnel_1:30: responder: main mode get 3rd message...
ike 0:Tunnel_1:30: dec
CEB2556BB86A76A8369EEA84D4CE9B6C80510020100000000000006C7417465E8B5E10828E1
60CB2ACED88EC9EC68E9C4B84E29743ED43E9723086CADD6EF04768A557744BADE51B4C1964
5E35B56519BB56CA1800DB16533C40AE802554C8E295986F716B7B3C288704D83
ike 0:Tunnel_1:30: parse error
ike 0:Tunnel_1:30: probable pre-shared secret mismatch
```

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-IPSEC-Tunnel-debugging-IKE/ta-p/190052>

Conclusions

IPSEC Basics

Configuring IPSEC VPN

ANTI-Replay

NAT-T

ADVPN

OCVPN

Troubleshooting commands

get vpn ipsec tunnel summary

get vpn ipsec tunnel details

diagnose vpn tunnel list name <NAME>

IKE debug

IKE Debug

Key things to check

What is the other device proposing?

Which side should change their settings to match

Common Failure Messages

probable pre-shared secret mismatch

negotiation failure

no SA proposal chosen



Web Filtering

Inspection Order

- 1 Static URL Filter
- 2 FortiGuard Web Filter
- 2 Web Content Filter
- 2 Advanced Options



Server Name Indication (SNI)

- Indicates the hostname the client is attempting to connect to at the start of the handshake process.
- This allows a server to present multiple certificates on the same IP address and TCP port number.

```
config firewall ssl-ssh-profile
edit <profile name>
config https
    set sni-server-cert-check [
enable* | strict | disable]
```

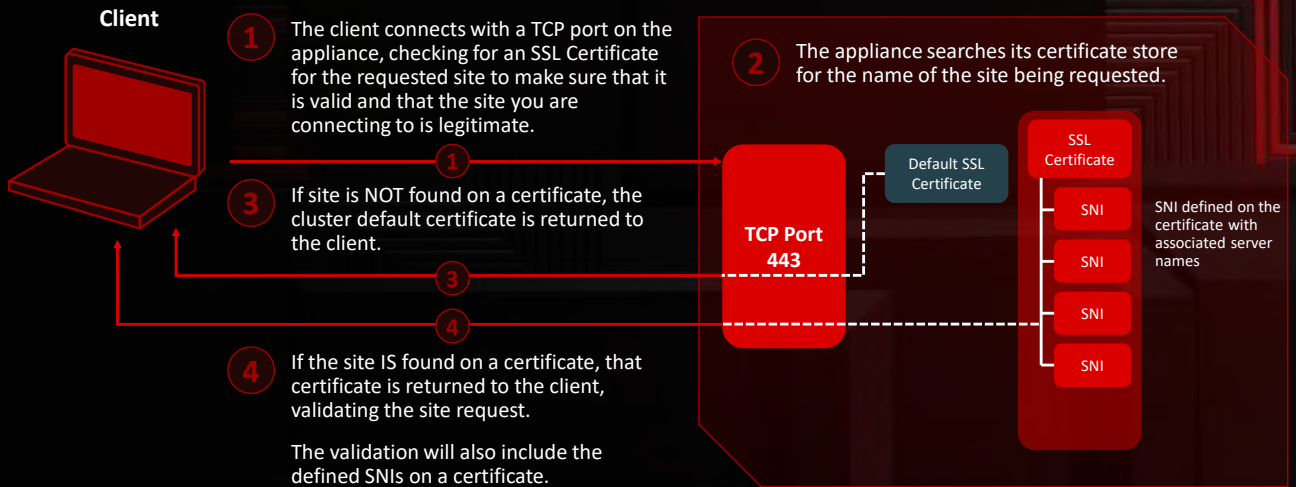
Server Name Indication (SNI)

- enable: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, use the CN in the server certificate to do URL filtering.
- strict: Check the SNI in the client hello message with the CN or SAN fields in the returned server certificate. If mismatched, close the connection.
- disable: Do not check the SNI in the client hello message with the CN or SAN fields in the returned server certificate.

```
config firewall ssl-ssh-profile
edit <profile name>
config https
    set sni-server-cert-check [
enable* | strict | disable]
```

SNI

https://help.fortinet.com/fadc/3-2-3/html-e/Content/Clusters/Server_Name_Indication.html



Inspect Encrypted Traffic



Methods

SSL Certificate Inspection

- Inspects only the header information of packets.

- Does not decrypt the payload of the packet.

- Allows for quick decision-making based on certificate details such as issuer and subject.

Full SSL Inspection

- Inspects both header information and payload of packets.

- Decrypts the payload for deep inspection, then re-encrypts it before forwarding.

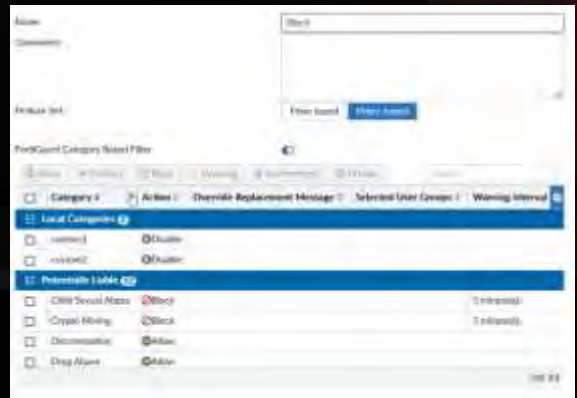
- More thorough but introduces additional latency due to decryption and re-encryption process.

DEMO – Web Filter

● Create & apply Web Filter

● Discuss the order of inspection

If site will be blocked or not



Web filtering Categories

get webfilter categories

g01 Potentially Liable:
1 Drug Abuse
3 Hacking
4 Illegal or Unethical
5 Discrimination
6 Explicit Violence
12 Extremist Groups
59 Proxy Avoidance
62 Plagiarism
83 Child Abuse
g02 Adult/Mature Content:
2 Alternative Beliefs
7 Abortion
8 Other Adult Materials
9 Advocacy Organizations
11 Gambling
13 Nudity and Risque
14 **bleep**ography
15 Dating
16 Weapons (Sales)
57 Marijuana
63 **bleep** Education
64 Alcohol
65 Tobacco
66 Lingerie and Swimsuit
67 Sports Hunting and War Games
g04 Bandwidth Consuming:
19 Freeware and Software Downloads
24 File Sharing and Storage
25 Streaming Media and Download
72 Peer-to-peer File Sharing
75 Internet Radio and TV
76 Internet Telephony
g05 Security Risk:
26 Malicious Websites
61 Phishing
86 Spam URLs
88 Dynamic DNS
90 Newly Observed Domain
91 Newly Registered Domain
g06 General Interest - Personal:
17 Advertising
18 Brokerage and Trading
20 Games
23 Web-based Email
28 Entertainment
29 Arts and Culture
30 Education
33 Health and Wellness
34 Job Search
35 Medicine
36 News and Media
37 Social Networking
38 Political Organizations
39 Reference
40 Global Religion
42 Shopping
44 Society and Lifestyles
46 Sports
47 Travel
48 Personal Vehicles
54 Dynamic Content
55 Meaningless Content
56 Folklore
68 Web Chat
69 Instant Messaging
70 Newsgroups and Message Boards
71 Digital Postcards
77 Child Education
78 Real Estate
79 Restaurant and Dining
80 Personal Websites and Blogs
82 Content Servers
85 Domain Parking
87 Personal Privacy
89 Auction
g07 General Interest - Business:
31 Finance and Banking
41 Search Engines and Portals
43 General Organizations
49 Business
50 Information and Computer Security
51 Government and Legal Organizations
52 Information Technology
53 Armed Forces
56 Web Hosting
81 Secure Websites
84 Web-based Applications
92 Charitable Organizations
98 Remote Access
94 Web Analytics
95 Online Meeting
g21 Unrated
0 Unrated
g22 Local Categories
140 custom1
141 custom2

Testing Block



<https://fortiguards.com/wftest/<categorynumber>.html>

Web Filter cache



Increase speed of web filtering by enabling cache

Set amount of time FortiGate will store blocked IP

```
config system fortiguard
  set webfilter-cache {enable | disable}
  set webfilter-cache-ttl <integer>
end
```


urlfilter

[illegible]

Diagnose Debug Rating

Weight

Priority of traffic

Increases based on lost packets

RTT

Round-trip time

Flags

Server Status

D

Found with DNS lookup

F

Failed

I

Last INIT request was sent

S

Rating requests can be sent

T

Timed

TZ

Time Zone difference between unit

```
# diagnose debug rating
```

```
Locale      : english
```

```
Service     : Web-filter
```

```
Status      : Enable
```

```
License     : Contract
```

```
Service     : Antispam
```

```
Status      : Disable
```

```
Service     : Virus Outbreak Prevention
```

```
Status      : Disable
```

```
-- Server List (Thu Oct 10 10:53:55 2019) --
```

IP	Weight	RTT	Flags	TZ	Packets	Curr	Lost	Total	Lost
62.209.40.73	0	28		1	1		0		0
62.209.40.72	0	29		1	1		0		0
209.222.147.43	10	0	DT	0	4		2		2

<https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGuard-Web-Filtering-problems/ta-p/196965>

FailOpen Mechanisms

Mechanisms:

IPS Failopen

Allows traffic to continue flowing through the FortiGate unit even if the IPS engine fails or encounters an error.

AV Failopen

Keeps traffic flowing if the anti-virus engine encounters a problem.

PRO:

Maintains connectivity

CON:

Traffic will not be inspected by IPS or AV during outage

Conclusions

Inspection Order

SNI

SSL Inspection

Demo - Configuring Web filter

get webfilter categories

Testing category block

web filter cache

diagnose debug application urlfilter

diagnose debug rating

failopen mechanisms



FortiGate IPS

Operates by inspecting traffic as it passes through the FortiGate unit and matching it against various attack signatures.

If a match is found, it takes the action specified in the matching IPS sensor (pass, block, reset, etc.).

Global IPS Configuration

Global IPS settings define the default IPS behavior, applicable when no specific rule or policy is present.

```
config ips global
  set fail-open {enable|disable*}
  set database {regular*|extended}
  set traffic-submit {enable*|disable}
  set anomaly-mode {periodical|continuous*}
  set session-limit-mode
    {accurate|heuristic*}
```

Fail-open

If enabled traffic will be allowed if IPS buffer is full.

```
config ips global
  set fail-open {enable|disable*}
  set database {regular|extended}
  set traffic-submit {enable|disable}
  set anomaly-mode {periodical|continuous}
  set session-limit-mode
    {accurate|heuristic}
```


Database

Regular protects against common attacks. Extended adds protection against legacy attacks.

```
config ips global
set fail-open [enable|disable]
set database [regular*|extended]
set traffic-submit [enable|disable]
set anomaly-mode [periodical|continuous]
set session-limit-mode
[accurate|heuristic]
```

Traffic-Submit

If enabled attack data will be sent to FortiGuard.

```
config ips global
  set fail-open [enable|disable]
  set database [regular|extended]
  set traffic-submit [enable*|disable]
  set anomaly-mode [periodical|continuous]
  set session-limit-mode
    [accurate|heuristic]
```

Anomaly-Mode

Periodical allows a set number of packets post-detection.

Continuous blocks all traffic once an anomaly is spotted

```
config ips global
  set fail-open [enable|disable]
  set database [regular|extended]
  set traffic-submit [enable|disable]
  set anomaly-mode [periodical|continuous*]
  set session-limit-mode
    [accurate|heuristic]
```

Session-limit mode

Accurate mode demands more resources to count concurrent sessions precisely.

Heuristic mode uses estimation for better performance, generally sufficient.

```
config ips global
  set fail-open [enable|disable]
  set database [regular|extended]
  set traffic-submit [enable|disable]
  set anomaly-mode [periodical|continuous]
  set session-limit-mode
    [accurate|heuristic*]
```

diagnose test application ipsmonitor

Test various aspects of the IPS monitor's operation and identify issues.

```
FortiFirewall-VM64-KVM # diagnose test application ipsmonitor
```

```
IPS Engine Test Usage:
```

- 1: Display IPS engine information
- 2: Toggle IPS engine enable/disable status
- 3: Display restart log
- 4: Clear restart log
- 5: Toggle bypass status
- 6: Submit attack characteristics now
- 10: IPS queue length
- 11: Clear IPS queue length
- 12: IPS I7 socket statistics
- 13: IPS session list
- 14: IPS NTurbo statistics
- 15: IPSA statistics
- 18: Display session info cache
- 19: Clear session info cache
- 21: Reload VSA malicious URL database
- 22: Reload allowlist URL database
- 24: Display Flow AV statistics
- 25: Reset Flow AV statistics
- 32: Reload certificate blocklist database
- 40: Display packet log statistics
- 41: Reset packet log statistics
- 42: IoT device notification statistics
- 43: AV exempt statistics
- 44: Dump IPS stack backtrace
- 96: Toggle IPS engines watchdog timer
- 97: Start all IPS engines
- 98: Stop all IPS engines
- 99: Restart all IPS engines and monitor

diagnose test application ipsmonitor

Common uses:

- 3: Display restart log
- 4: Clear restart log
- 5: Toggle bypass status
- 97: Start all IPS engines
- 98: Stop all IPS engines
- 99: Restart all IPS engines and monitor

FortiFirewall-VM64-KVM # diagnose test application ipsmonitor

IPS Engine Test Usage:

- 1: Display IPS engine information
- 2: Toggle IPS engine enable/disable status
- 3: Display restart log
- 4: Clear restart log
- 5: Toggle bypass status
- 6: Submit attack characteristics now
- 10: IPS queue length
- 11: Clear IPS queue length
- 12: IPS I7 socket statistics
- 13: IPS session list
- 14: IPS NTurbo statistics
- 15: IPSA statistics
- 18: Display session info cache
- 19: Clear session info cache
- 21: Reload VSA malicious URL database
- 22: Reload allowlist URL database
- 24: Display Flow AV statistics
- 25: Reset Flow AV statistics
- 32: Reload certificate blocklist database
- 40: Display packet log statistics
- 41: Reset packet log statistics
- 42: IoT device notification statistics
- 43: AV exempt statistics
- 44: Dump IPS stack backtrace
- 96: Toggle IPS engines watchdog timer
- 97: Start all IPS engines
- 98: Stop all IPS engines
- 99: Restart all IPS engines and monitor

Anomaly List

View the list of current anomaly signatures and their configurations

An anomaly signature helps detect traffic that deviates from what is considered normal

<https://community.fortinet.com/t5/FortiCare/Technical-Tip-Block-IP-address-with-DDoS-attacks-detection/tg-p/252839>

```
# diag ips anomaly list
```

```
list nids meter:
```

```
id=tcp_port_scan      ip=10.129.2.76 dos_id=1  
exp=2793 pps=13 freq=337
```

```
id=udp_scan           ip=10.129.2.76 dos_id=1  
exp=2570 pps=0 freq=10
```

Conclusions

Global ips configuration

diagnose test application
ipsmonitor

Anomaly List



Sessions

Understanding Session Entries

What is a Session Entry?

A session entry, also known as a session table entry, represents a single session in FortiGate.

It contains all the details of the session, including source and destination IP addresses, source and destination ports, protocol type, session state, and more.

Session entries enable the FortiGate firewall to keep track of each individual communication pathway, ensuring each session's data packets follow the correct pathway and abide by the firewall rules and policies.

Diagnose sys session stat

```
FortiFirewall-VM64-KVM # diagnose sys session stat
misc info:      session_count=3 setup_rate=0
exp_count=0 reflect_count=0 clash=0
memory_tension_drop=0 ephemeral=0/65526
removeable=0 extreme_low_mem=0
delete=0, flush=0, dev_down=1/2683 ses_walkers=0
TCP sessions:
    1 in ESTABLISHED state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ips_recv=00000000
policy_deny=0000000e
av_recv=00000000
fqdn_count=00000009
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0
rt6_limit=0
```

Display session and system statistics

Diagnose sys session stat

```
FortiFirewall-VM64-KVM # diagnose sys session stat
misc info:      session_count=3 setup_rate=0
exp_count=0 reflect_count=0 clash=0
memory_tension_drop=0 ephemeral=0/65526
removeable=0 extreme_low_mem=0
delete=0, flush=0, dev_down=1/2683 ses_walkers=0
TCP sessions:
    1 in ESTABLISHED state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ips_recv=00000000
policy_deny=0000000e
av_recv=00000000
fqdn_count=00000009
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0
rt6_limit=0
```

session_count=3
Active sessions

setup_rate=0
Sessions being setup per second

exp_count=0
Expired sessions

reflect_count=0
Sessions created in response to other sessions

clash=0
Sessions that tried to occupy the same slot

memory_tension_drop=0
Terminated session due to memory resources

Diagnose sys session stat

```
FortiFirewall-VM64-KVM # diagnose sys session stat
misc info:      session_count=3 setup_rate=0
exp_count=0 reflect_count=0 clash=0
memory_tension_drop=0 ephemeral=0/65526
removeable=0 extreme_low_mem=0
delete=0, flush=0, dev_down=1/2683 ses_walkers=0
TCP sessions:
    1 in ESTABLISHED state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ips_rcv=00000000
policy_deny=0000000e
av_rcv=00000000
fqdn_count=00000009
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0
rt6_limit=0
```

ephemeral=0/65526

Transient sessions

Have not been fully established

Process of being terminated

Diagnose sys session stat

```
FortiFirewall-VM64-KVM # diagnose sys session stat
misc info:      session_count=3 setup_rate=0
exp_count=0 reflect_count=0 clash=0
memory_tension_drop=0 ephemeral=0/65526
removeable=0 extreme_low_mem=0
delete=0, flush=0, dev_down=1/2683 ses_walkers=0
TCP sessions:
    1 in ESTABLISHED state
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ips_recv=00000000
policy_deny=0000000e
av_recv=00000000
fqdn_count=00000009
fqdn6_count=00000000
global: ses_limit=0 ses6_limit=0 rt_limit=0
rt6_limit=0
```

removeable=0

Sessions that can be removed due to inactivity

extreme_low_mem=0

Flag indicating low memory

delete=0, flush=0

Manually deleted or flushed

dev_down=1/2683

Records the number of times all firewall sessions were deleted related to an IPsec interface that was turned off administratively.

ses_walkers=0

tasks that go through the session table to clean up or maintain sessions

Diagnose sys session list

```
FortiFirewall-VM64-KVM # diagnose sys session list
```

```
session info: proto=2 proto_state=00 duration=303
expire=207 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/
vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=00/2/1
reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org out->post, reply pre->in dev=14-
>18/18->0 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 10.255.1.1:0-
>224.0.0.22:0(0.0.0.0:0)
hook=in dir=reply act=noop 224.0.0.22:0-
>10.255.1.1:0(0.0.0.0:0)
misc=0 policy_id=0 pol_uuid_idx=0 auth_info=0
chk_client_info=0 vd=0
serial=0000000000 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id=0000000000 ngfwid=n/a
np_u_state=0000000000
```

Displays current session table on FortiGate.

Shows all active sessions.

Details include:

source/destination addresses, ports, session state, and duration.

Diagnose sys session list

```
FortiFirewall-VM64-KVM # diagnose sys session list
```

```
session info: proto=2 proto_state=00 duration=303
expire=297 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/
vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=80/2/1
reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org out->post, reply pre->in dev=14-
>18/18->0 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 10.255.1.1:0-
>224.0.0.22:0(0.0.0.0:0)
hook=in dir=reply act=noop 224.0.0.22:0-
>10.255.1.1:0(0.0.0.0:0)
misc=0 policy_id=0 pol_uid_idx=0 auth_info=0
chk_client_info=0 vd=0
serial=000000000 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id=000000000 ngfwid=n/a
np_u_state=000000000
```

session info: Describes the basic properties of the session.

proto=2: Protocol number (e.g., 2 for TCP).

proto_state=00: Protocol state.

duration=303: Duration of the session in seconds.

expire=297: Time in seconds before the session expires.

timeout=0: Session timeout value.

flags=00000000: Specific flags related to the session.

Diagnose sys session list

```
FortiFirewall-VM64-KVM # diagnose sys session list
```

```
session info: proto=2 proto_state=00 duration=303
expire=297 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/
vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=00/2/1
reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
orgin->sink: org out->post, reply pre->in dev=14-
>18/18->0 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 10.255.1.1:0-
>224.0.0.22:0(0.0.0.0:0)
hook=in dir=reply act=noop 224.0.0.22:0-
>10.255.1.1:0(0.0.0.0:0)
misc=0 policy_id=0 pol_uid_idx=0 auth_info=0
chk_client_info=0 vd=0
serial=0000000000 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id=0000000000 ngfwid=n/a
np_u_state=0000000000
```

origin-shaper, reply-shaper, per_ip_shaper:
Shaping policies that may be applied to the session.

class_id, ha_id, policy_dir: Various IDs related to policy, High Availability, etc.

tunnel, vlan_cos: Information related to any tunneling or VLANs involved.

state=log local nds: The current state of the session.

statistic(bytes/packets/allow_err): Statistics about the session including bytes, packets, and errors.

Diagnose sys session list

```
FortiFirewall-VM64-KVM # diagnose sys session list
```

```
session info: proto=2 proto_state=00 duration=303
expire=297 timeout=0 flags=00000000 socktype=0
sockport=0 av_idx=0 use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/
vlan_cos=255/255
state=log local nds
statistic(bytes/packets/allow_err): org=80/2/1
reply=0/0/0 tuples=2
tx speed(Bps/kbps): 0/0 rx speed(Bps/kbps): 0/0
origin->sink: org out->post, reply pre->in dev=14-
>18/18->0 gwy=0.0.0.0/0.0.0.0
hook=out dir=org act=noop 10.255.1.1:0-
>224.0.0.22:0(0.0.0.0:0)
hook=in dir=reply act=noop 224.0.0.22:0-
>10.255.1.1:0(0.0.0.0:0)
misc=0 policy_id=0 pol_uuid_idx=0 auth_info=0
chk_client_info=0 vd=0
serial=00000000 tos=ff/ff app_list=0 app=0 url_cat=0
rpd_b_link_id=00000000 ngfwid=n/a
npu_state=00000000
```

tx speed, rx speed: Transmit and receive speeds.

origin->sink: The flow direction of the original and reply packets.

hook: Describes actions performed on the packet.

misc, policy_id, pol_uuid_idx, auth_info, chk_client_info, vd: Various other parameters and identifiers related to policies, authentication, etc.

serial, tos, app_list, app, url_cat: Additional information including serial number, type of service, applications, URLs.

rpd_b_link_id, ngfwid, npu_state: Hardware-related information.

FortiGate Session Commands

Command: "diagnose sys session list expectation"

list expectation sessions on the FortiGate device.

Expectation session is a session FortiGate expects to see in the future

Typically created by:

Session Helpers

Manages control and data sessions for complex protocols, creating expectation sessions to handle related data connections.

Application Layer Gateways (ALG)

Operates at the application layer to facilitate specific applications or protocols, working with expectation sessions to manage related connections.

Sniffing Traffic

```
FortiFirewall-VM64-KVM # diagnose sniff packet any
Using Original Sniffing Mode
interfaces=[any]
filters=[none]
0.256618 192.168.1.197 -> 192.168.1.2: icmp: echo request
0.256645 192.168.1.2 -> 192.168.1.197: icmp: echo reply
1.274610 192.168.1.197 -> 192.168.1.2: icmp: echo request
1.274635 192.168.1.2 -> 192.168.1.197: icmp: echo reply
2.292086 192.168.1.197 -> 192.168.1.2: icmp: echo request
2.292110 192.168.1.2 -> 192.168.1.197: icmp: echo reply
3.306696 192.168.1.197 -> 192.168.1.2: icmp: echo request
3.306724 192.168.1.2 -> 192.168.1.197: icmp: echo reply
4.181963 arp who-has 192.168.1.1 (ff:ff:ff:ff:ff:ff) tell
192.168.1.139
4.322415 192.168.1.197 -> 192.168.1.2: icmp: echo request
4.322439 192.168.1.2 -> 192.168.1.197: icmp: echo reply
5.337115 192.168.1.197 -> 192.168.1.2: icmp: echo request
5.337138 192.168.1.2 -> 192.168.1.197: icmp: echo reply
6.350750 192.168.1.197 -> 192.168.1.2: icmp: echo request
6.350774 192.168.1.2 -> 192.168.1.197: icmp: echo reply
^C
17 packets received by filter
0 packets dropped by kernel
```

Capture and display live packet data

Details:

interfaces=[any]

filters=[none]

Any filter information will be listed here

0 packets dropped by kernel

System kernel did not process some packets that matched your sniffing filter

Filtering Sniffing Traffic

```
FortiFirewall-VM64-KVM # diagnose sniffer packet any 'host 192.168.1.197 and (port 80 or 443)'
Using Original Sniffing Mode
interfaces=[any]
filters=[host 192.168.1.197 and (port 80 or 443)]
1.029779 192.168.1.197.63858 -> 192.168.1.2.80: syn 2561322230
1.029852 192.168.1.2.80 -> 192.168.1.197.63858: syn 887187054 ack 2561322231
1.030038 192.168.1.197.63858 -> 192.168.1.2.80: ack 887187055
1.030250 192.168.1.197.63858 -> 192.168.1.2.80: psh 2561322231 ack 887187055
1.030259 192.168.1.2.80 -> 192.168.1.197.63858: ack 2561322955
1.055181 192.168.1.2.80 -> 192.168.1.197.63858: 887187055 ack 2561322955
1.055485 192.168.1.2.80 -> 192.168.1.197.63858: psh 887188515 ack 2561322955
1.055730 192.168.1.197.63858 -> 192.168.1.2.80: ack 887188806
^C
8 packets received by filter
0 packets dropped by kernel
```

Dirty Flags

```
# config system settings
    set firewall-session-dirty { check-all | check-new |
check-policy-option }
End

# diagnose sys session list

session info: proto=1 proto_state=00 duration=2 expire=59
timeout=0 flags=00000000 socktype=0 sockport=0 av_idx=0
use=3
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan_cos=0/0
state=local may_dirty
statistic(bytes/packets/allow_err): org=180/3/1
reply=180/3/1 tuples=2
tx speed(Bps/kbps): 80/0 rx speed(Bps/kbps): 80/0
origin->sink: org pre->in, reply out->post dev=3->14/14->3
gwy=0.0.0.0/0.0.0.0
hook=pre dir=org act=noop 192.168.1.197:1-
>192.168.1.2:8(0.0.0.0:0)
hook=post dir=reply act=noop 192.168.1.2:1-
>192.168.1.197:0(0.0.0.0:0)
misc=0 policy_id=4294967295 pol_uuid_idx=0 auth_info=0
chk_client_info=0 vd=0
serial=0000000c tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id=00000000 ngfwid=n/a
npu_state=00000000
total session: 2
```

Indicates it needs reevaluation

HA

If marked dirty, the HA system knows that the session's information must be updated to ensure that all units have the correct, consistent information.

Dirty Flags

Marked Dirty:

- 1 Changes to a firewall policy
- 2 Routing Changes
- 3 Network config changes

Conclusions

Sessions

Commands

Diagnose sys session stat

Diagnose sys session list

Expectation

Sniffing

Dirty Flags



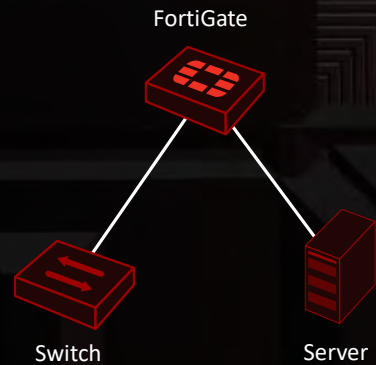
Automating Threat Responses with Automation Stitches

What are Automation Stitches?

Automatically manage a response to a detected event or threat

Example:

Set an automated email if server is unreachable.

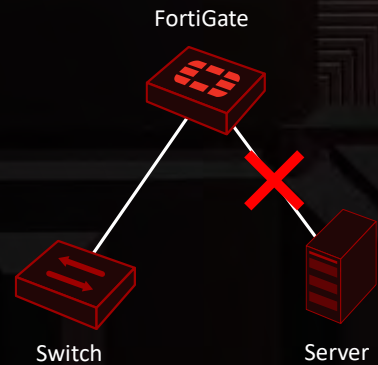


Core Components

Trigger:

Event or condition that initiates an automation stitch.

Can be based on a variety of sources, such as logs, system events, and security fabric alerts.



Core Components

Action:

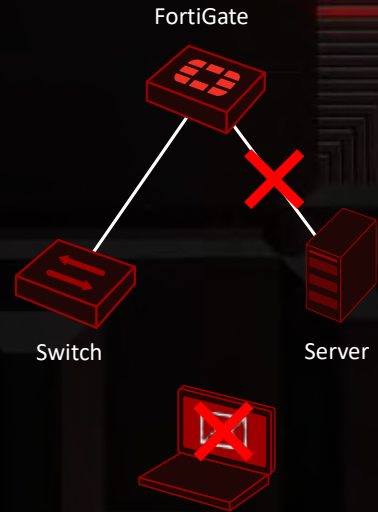
Once a trigger is activated, the automation stitch performs a specified action.

Examples:

Sending an email notification

Isolating a device from the network

Blocking an IP address



Core Components

Expiry Time:

This is the duration for which the action is effective.

After the expiry time, the action is reversed.

Example

If an IP address was blocked, it would be unblocked after the expiry time.

Conditions:

These are optional and allow the administrator to refine when the automation stitch is executed.

The automation stitch will only execute if the condition is met in addition to the trigger.

LAB - Configuring Automation Stitches

Configure an Automation Stitch on FortiGate



Conclusions

Automation Stitches

Core Components

Configuration