

The Wayback Machine - <https://web.archive.org/web/20160828235831/http://cookbook.fortinet.com:...>

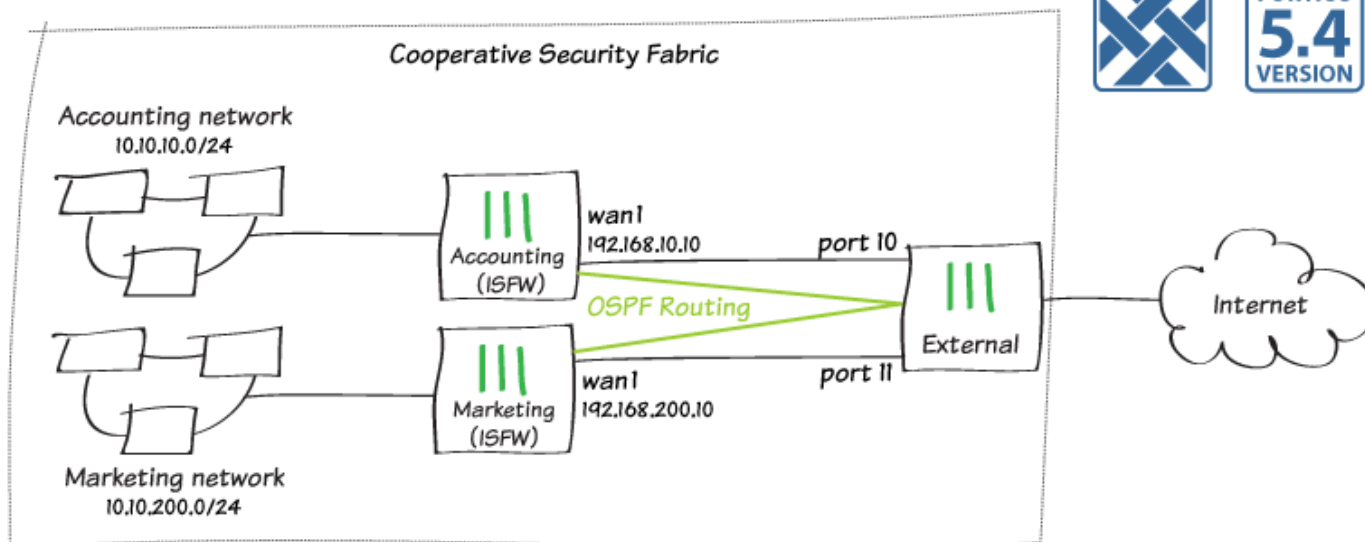


THE FORTINET COOKBOOK

COOPERATIVE SECURITY FABRIC / FORTIGATE / FORTIOS 5.4.1 / GETTING STARTED

Installing internal FortiGates and enabling a security fabric

Posted on June 8, 2016 by [Victoria Martin](#)



In this example, you will install two Internal Segmentation Firewalls (ISFWs) behind your External FortiGate. One of these FortiGates will be used to protect your Accounting team's network, while the other will be used for the Marketing team. You will also enable a [Cooperative Security Fabric](#) (CSF) and use OSPF routing between these FortiGates.

This recipe is part of the [Cooperative Security Fabric collection](#). It can also be used as a standalone recipe.



Watch the video

1. Configuring External to connect to Accounting

In this example, the External FortiGate's port 10 will connect to the Accounting FortiGate's wan1.

On the External FortiGate, go to **Network > Interfaces** and edit **port 10**.

Set an **IP/Network Mask** for the interface (in the example, 192.168.10.2).

Configure **Administrative Access** to allow **FortiTelemetry**, required for communication between FortiGate in the CSF. Configure other services as required.

Interface Name	port10 (90:6C:AC:45:6C:64)				
Alias	Accounting				
Link Status	Up				
Type	Physical Interface				
Role	LAN				
Address					
Addressing mode	Manual	DHCP	Dedicated to FortiSwitch		
IP/Network Mask	192.168.10.2/255.255.255.0				
Restrict Access					
Administrative Access	☒ HTTPS	☒ PING	☐ FMG-Access	☐ CAPWAP	☒ SSH
	☐ SNMP	☐ RADIUS Accounting	☒ FortiTelemetry		

Go to **Policy & Objects > IPv4 Policy** and create a policy for traffic from the Accounting FortiGate to the Internet.

Enable **NAT**.

Name	Accounting Internet
Incoming Interface	Accounting (port10) ▼
Outgoing Interface	Internet (port9) ▼
Source	all ✕
Destination Address	all ✕
Schedule	always ▼
Service	ALL ✕
Action	☒ ACCEPT ☐ DENY ☐ LEARN

Firewall / Network Options

NAT ☒

Fixed Port ☐

IP Pool Configuration ☒ Use Outgoing Interface Address ☐ Use Dynamic IP Pool

Connect the FortiGates.

2. Configuring the Accounting FortiGate

On the Accounting FortiGate, go to **Network > Interfaces** and edit **wan1**.

Set an **IP/Network Mask** for the interface that is on the same **subnet** as the External FortiGate's port 10 (in the example, 192.168.10.10).

Configure **Administrative Access** to allow **FortiTelemetry**.

Interface Name	wan1 (08:5B:0E:35:40:70)		
Alias			
Link Status	Up		
Type	Physical Interface		
Role	WAN ▼		
Estimated Bandwidth	0 Kbps Upstream	0 Kbps Downstream	
Address			
Addressing mode	☒ Manual	☐ DHCP	☐ PPPoE
IP/Network Mask	192.168.10.10/255.255.255.0		
Restrict Access			
Administrative Access	☒ HTTPS ☒ SSH ☒ FortiTelemetry	☒ PING ☐ SNMP	☒ HTTP ☐ RADIUS Accounting
		☒ FMG-Access	☐ CAPWAP

Edit the **lan** interface.

Set **Addressing Mode** to **Manual** and set the **IP/Netmask** to a private **IP address** (in the example, 10.10.10.1). Configure **Administrative Access** to allow **FortiTelemetry**.

Under **Networked Devices**, enable **Device Detection**.

Interface Name	lan				
Type	VLAN Switch				
VLAN ID	0				
Physical Interface Members	port1 port2 port3 port4 port5 port6 port7 port8 port9 port10				
Role	LAN				
Address					
Addressing mode	Manual DHCP PPPoE Dedicated to FortiSwitch				
IP/Network Mask	10.10.10.1/255.255.255.0				
Restrict Access					
Administrative Access	☐ HTTPS ☒ PING ☐ FMG-Access ☐ CAPWAP ☒ SSH ☐ SNMP ☐ RADIUS Accounting ☒ FortiTelemetry				
DHCP Server					
Address Range					
+ Create New Edit Delete					
<table><thead><tr><th>Starting IP</th><th>End IP</th></tr></thead><tbody><tr><td>10.10.10.2</td><td>10.10.10.254</td></tr></tbody></table>		Starting IP	End IP	10.10.10.2	10.10.10.254
Starting IP	End IP				
10.10.10.2	10.10.10.254				
Netmask	255.255.255.0				
Default Gateway	Same as Interface IP Specify				
DNS Server	Same as System DNS Same as Interface IP Specify				
Advanced...					
Networked Devices					
Device Detection	☒				
Active Scanning	☒				

Go to **Policy & Objects > IPv4 Policy** and create a policy to allow users on the Accounting network to access the Internet.

Because OSPF routing will be used, make sure **NAT** is not enabled.

Name	Internet
Incoming Interface	lan
Outgoing Interface	wan1
Source	all
Destination Address	all
Schedule	always
Service	ALL
Action	☒ ACCEPT ☐ DENY ☐ LEARN

Firewall / Network Options

NAT ☐

3. Installing and configuring the Marketing FortiGate

Connect and configure the Marketing FortiGate using the same method as the Accounting FortiGate. Make sure to include the following:

On External

- Configure an interface to connect to the Marketing FortiGate (this example uses *port 11* with the IP 192.168.200.2)
- Create a policy for traffic from the Marketing FortiGate to the Internet

On Marketing

- Configure **wan1** to connect to the External FortiGate (example IP: 192.168.200.10)
- Configure the **lan** interface for the Marketing Network (example IP: 10.10.200.1)
- Create a policy to allow users on the Marketing network to access the Internet

4. Configuring OSPF routing between the FortiGates

On the External FortiGate, go to **Network > OSPF**. Set

Router ID

Advanced Options(Default, Redistribution)
 Default Information ☐ None ☐ Regular ☒ Always

Apply

Router ID to 0.0.0.1 and select **Apply**.

Expand the **Advanced Options** and set **Default Information** to **Always**, to make sure the default route is broadcast from External to the ISFW FortiGates.

In **Areas**, select **Create New**. Set **Area** to 0.0.0.0, **Type** to **Regular**, and **Authentication** to **None**.

Area	0.0.0.0	(IP)
Type	Regular	
Authentication	None	

In **Networks**, select **Create New**. Set **IP/Netmask** to 192.168.10.0/255.255.255.0 (the subnet that includes Accounting's wan1) and **Area** to 0.0.0.0.

IP/Netmask	192.168.10.0/255.255.255.0
Area	0.0.0.0

Create a second entry with the **IP/Netmask** set to 192.168.200.0/255.255.255.0 (the subnet that includes Marketing's wan1).

On the Accounting FortiGate, configure OSPF routing as shown.

The **Networks** in this configuration are the subnet that includes Accounting's wan1 and the subnet for the Accounting Network.

Router ID Apply

▶ **Advanced Options**(Default, Redistribution)

Areas

[Create New](#) [Edit](#) [Delete](#)

	Area	Type	Authentication
☐	0.0.0.0	Regular	None

Networks

[Create New](#) [Edit](#) [Delete](#)

	Network	Area
☐	192.168.10.0/255.255.255.0	0.0.0.0
☐	10.10.10.0/255.255.255.0	0.0.0.0

Interfaces

[Create New](#) [Edit](#) [Delete](#)

	Name	Interface	Cost	IP	Authentication
No OSPF interface defined.					

In the example, the Marketing FortiGate is a 90D, a model that does not support OSPF configuration using the [GUI](#). To add OSPF routing, use the following [CLI](#) command:

```
config router ospf
  set router-id 0.0.0.3
  config area
    edit 0.0.0.0
    next
  end
  config network
    edit 1
      set prefix 192.168.200.0/255.255.255.0
    next
    edit 2
      set prefix 10.10.200.0/255.255.255.0
    next
  end
end
```

5. Enabling the Cooperative Security Fabric

On the External FortiGate, go to **System > Cooperative Security Fabric**. Enable **Cooperative Security Fabric (CSF)** and set a **Group name** and **Group password**.

☒ **Cooperative Security Fabric (CSF)**

Group name

Group password

Connect to upstream FortiGate ☐

On the Accounting FortiGate, go to **System > Cooperative Security Fabric**. Enable **Cooperative Security Fabric (CSF)** and enter the name and password for the fabric.

☒ **Cooperative Security Fabric (CSF)**

Group name

Group password

Connect to upstream FortiGate ☒

FortiGate IP

FortiTelemetry port

Enable **Connect to upstream FortiGate** and enter the IP address of External port 10.

Configure CSF on the Marketing FortiGate, using the IP address of External port 11.

6. Results

On the External FortiGate, go to **FortiView > Physical Topology**.



This dashboard shows a visualization of all access layer devices in the Cooperative Security Fabric.

On the External FortiGate, go to **FortiView > Logical Topology**.



This dashboard displays information about the interface (logical or physical) that each device in the CSF is connected to.

Go to **Monitor > Routing Monitor**. You will see both ISFW FortiGates listed, using OSPF routing.

Refresh		Route Lookup			
Type	Subtype	Network	Gateway	Interface	Up Time
Static		0.0.0.0/0	172.20.121.2	port9 (Internet)	
OSPF		10.10.10.0/24	192.168.10.1	port10 (Accounting)	0 00:07:15
OSPF		10.10.200.0/24	192.168.200.1	port11 (Marketing)	0 00:04:51

7. (Optional) Adding security profiles to the fabric

CSF configurations allow you to distribute security functions to different FortiGates in the security fabric. For example, you may want to implement virus scanning on the External FortiGate but add application control and web filtering to the ISFW FortiGates.

This results in distributed processing between the FortiGates in the CSF; reducing the load on each one. It also allows you to customize the web filtering and application control for the specific needs of the Accounting network as other internal networks may have different application control and web filtering requirements.

This configuration may result in threats getting through the External FortiGate which means you should very closely limit access to the network connections between the FortiGates in the CSF.

On the External FortiGate, go to **Policy & Objects > IPv4 Policy** and edit the policy allowing traffic from the Accounting FortiGate to the Internet.

Under **Security Profiles**, enable **AntiVirus** and select the **default** profile.

Do the same for the policy allowing traffic from the Marketing FortiGate to the Internet.

Security Profiles

AntiVirus	☒	AV default
Web Filter	☐	
DNS Filter	☐	
Application Control	☐	
CASI	☐	
IPS	☐	
Proxy Options		PRX default
SSL/SSH Inspection	☐	

On the Accounting FortiGates, go to **Policy & Objects > IPv4 Policy** and edit the policy allowing traffic from the Accounting Network to the Internet.

Under **Security Profiles**, enable **Web Filter** and **Application Control**. Select the **default** profiles for both.

Do the same on the Marketing FortiGate.

Security Profiles

AntiVirus	☐	
Web Filter	☒	WEB default
DNS Filter	☐	
Application Control	☒	APP default
CASI	☐	
Proxy Options		PRX default
SSL/SSH Inspection	☒	SSL certificate-inspection

Another strategy you could choose is to have flow-based inspection on the External FortiGate and proxy-based inspection used by the ISFW FortiGates. For more information, see [Inspecting traffic content using flow-based inspection](#).

About

Latest Posts



Victoria Martin

Technical Writer & Head Cookbook Chef at [Fortinet](#)

Victoria Martin works in Ottawa as part of the [FortiOS](#) technical documentation team. She graduated with a Bachelor's degree from Mount Allison University, after which she attended

Humber College's book publishing program, followed by the more practical technical writing program at Algonquin College. She does need glasses but also likes wearing them, since glasses make you look smarter.

Related posts:

- [ISFW and Cooperative Security Fabric \(Video\)](#)
- [Adding endpoint control to a security fabric](#)
- [Cooperative Security Fabric](#)

Share this recipe:



🔖 [AntiVirus, application control, CSF, FortiTelemetry, installation, interfaces, ISFW, OSPF, web filtering](#)