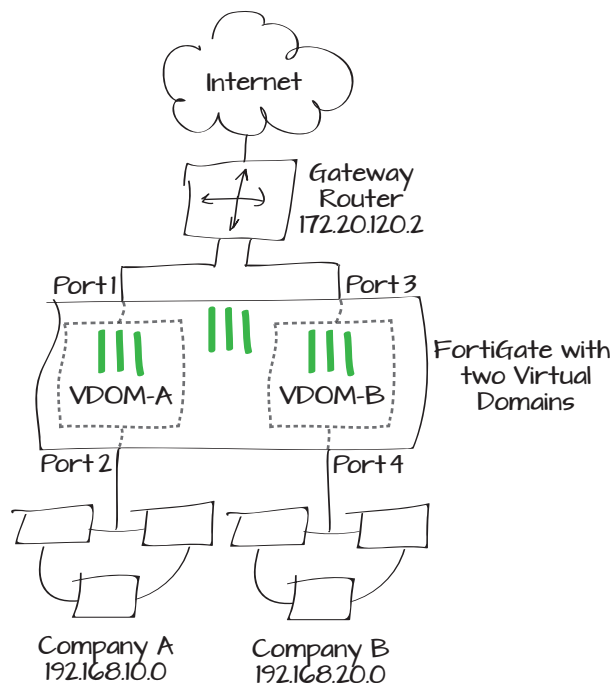


Using VDOMs to host two FortiOS instances on a single FortiGate unit

Virtual Domains (VDOMs) can be used to divide a single FortiGate unit into two or more virtual instances of FortiOS that function as independent FortiGate units. This example simulates an ISP that provides Company A and Company B with distinct Internet services. Each company has its own VDOM, IP address, and internal network.

1. Switching to VDOM mode and creating two VDOMS
2. Assigning interfaces to each VDOM
3. Creating administrators for each VDOM
4. Creating a basic configuration for VDOM-A
5. Creating a basic configuration for VDOM-B
6. Connecting the gateway router
7. Results



Switching to VDOM mode and creating two VDOMS

Go to **System > Dashboard > Status**.

In the **System Information** widget, find **Virtual Domain** and select **Enable**.



You will be required to re-login after enabling **Virtual Domain** due to the GUI menu options changing.

Go to **Global > VDOM > VDOM**.

Create two VDOMS: *VDOM-A* and *VDOM-B*. Leave both VDOMs as **Enabled**, with **Operation Mode** set to **NAT**.

System Information	
Host Name	FG100D3G12812324 [Change]
Serial Number	FG100D3G12812324
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Wed Oct 30 06:28:30 2013 (FortiGuard) [Change]
Firmware Version	v5.0,build0246 (Interim) [Update] [Details]
System Configuration	[Backup] [Restore] [Revisions]
Current Administrator	admin [Change Password] /1 in Total [Details]
Uptime	2 day(s) 0 hour(s) 46 min(s)
Virtual Domain	Disabled [Enable]

Name	<input type="text" value="VDOM-A"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Name	<input type="text" value="VDOM-B"/>
Enable	<input checked="" type="checkbox"/>
Operation Mode	<input type="button" value="NAT"/>
Comments	<input type="text" value="Write a comment..."/> 0/255

Assigning interfaces to each VDOM

Go to **Global > Network > Interfaces**.

Edit **port1** and add it to VDOM-A. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, 172.20.120.10/255.255.255.0).

Edit **port2** and add it to VDOM-A. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, 192.168.10.1/255.255.255.0), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.

Edit **port3** and add it to VDOM-B. Set **Addressing Mode** to **Manual** and assign an **IP/Network Mask** to the interface (in the example, 172.20.120.20/255.255.255.0).

Name port1(00:09:0F:B0:EB:F0)
Alias
Link Status Down
Type Physical Interface
Virtual Domain VDOM-A

Addressing mode Manual DHCP PPPoE One-Arm Sniffer Dedicate to FortiA
IP/Network Mask
IPv6 Address

Name port2(00:09:0F:B0:EB:F1)
Alias
Link Status Down
Type Physical Interface
Virtual Domain VDOM-A

Addressing mode Manual DHCP PPPoE Dedicate to FortiAP/FortiSwitch
IP/Network Mask
IPv6 Address

Administrative Access HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET FCT-Access
IPv6 Administrative Access HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET

DHCP Server Enable
Address Range

Create New	Edit	Delete
Starting IP	End IP	
192.168.10.2	192.168.10.254	

Netmask

Name port3(00:09:0F:B0:EB:F2)
Alias
Link Status Down
Type Physical Interface
Virtual Domain VDOM-B

Addressing mode Manual DHCP PPPoE One-Arm Sniffer Dedicate to FortiAP/F
IP/Network Mask
IPv6 Address

Edit **port4** and add it to VDOM-B. Set **Addressing Mode** to **Manual**, assign an **IP/Network Mask** to the interface (in the example, 192.168.20.1/255.255.255.0), and set **Administrative Access** to **HTTPS**, **PING**, and **SSH**. Enable **DHCP Server**.

Creating administrators for each VDOM

Go to **Global > Admin > Administrators**.

Create an administrator for VDOM-A, called *a-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.

Create an administrator for VDOM-B, called *b-admin*. Set **Type** to **Regular**, set a password, and set **Admin Profile** to **prof_admin**.



Make sure to remove the **root** VDOM from both administrator accounts.

Name: port4(00:09:0F:B0:EB:F3)
 Alias:
 Link Status: Down ⬮
 Type: Physical Interface
 Virtual Domain: VDOM-B

Addressing mode: Manual DHCP PPPoE One-Arm Sniffer Dedicate to FortiAP/FortiSwitch
 IP/Network Mask:
 IPv6 Address:

Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET FCT-Access
 IPv6 Administrative Access: HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET

DHCP Server: Enable
 Address Range:

Starting IP	End IP
192.168.20.2	192.168.20.254

Netmask:

Administrator:
 Type: Regular Remote PKI
 Password:
 Confirm Password:
 Comments: 0/255

Admin Profile: prof_admin ⌵
 Virtual Domain: VDOM-A ✕ +

Administrator:
 Type: Regular Remote PKI
 Password:
 Confirm Password:
 Comments: 0/255

Admin Profile: prof_admin ⌵
 Virtual Domain: VDOM-B ✕ +

Creating a basic configuration for VDOM-A

Go to **Virtual Domains** and select **VDOM-A**.

Go to **Router > Static > Static Routes**.






Add a default route for the VDOM. Set **Destination IP/Mask** to *0.0.0.0/0.0.0.0*, set **Device** to **port1**, and set **Gateway** to the IP of the gateway router (in the example, 172.20.120.2).

Connect a PC to port2. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-A using the a-admin account (in the example, <https://192.168.10.1>).

Go to **Policy > Policy > Policy**.

Create a policy to allow Internet access. Set **Incoming Interface** to **port2** and **Outgoing Interface** to **port1**. Select **Enable NAT**.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="port1"/>
Gateway	<input type="text" value="172.20.120.2"/>

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	<input type="text" value="port2"/> 
Source Address	<input type="text" value="all"/> 
Outgoing Interface	<input type="text" value="port1"/> 
Destination Address	<input type="text" value="all"/> 
Schedule	<input type="text" value="always"/>
Service	<input type="text" value="ALL"/> 
Action	<input type="text" value="ACCEPT"/>
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	<input type="text" value="Click to add..."/>

Creating a basic configuration for VDOM-B

If you have logged out of the FortiGate unit, log back in.

Go to **Virtual Domains** and select **VDOM-B**. Go to **Router > Static > Static Routes**.

Add a default route for the VDOM. Set **Destination IP/Mask** to `0.0.0.0/0.0.0.0`, set **Device** to **port3**, and set **Gateway** to the IP of the gateway router (in the example, `172.20.120.2`).

Connect a PC to port4. Using HTTPS protocol, browse to the IP set for port2 and log into VDOM-B using the b-admin account (in the example, `https://192.168.20.1`).

Go to **Policy > Policy > Policy**.

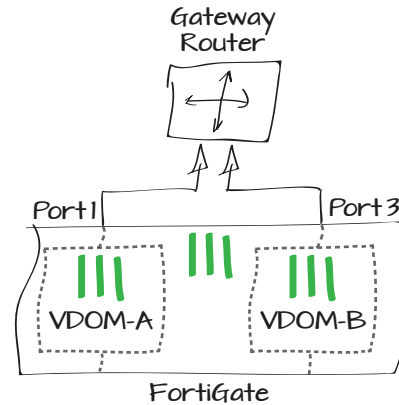
Create a policy to allow Internet access. Set **Incoming Interface** to **port4** and **Outgoing Interface** to **port3**. Select **Enable NAT**.

Destination IP/Mask	<input type="text" value="0.0.0.0/0.0.0.0"/>
Device	<input type="text" value="port3"/>
Gateway	<input type="text" value="172.20.120.2"/>

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	<input type="text" value="port4"/> +
Source Address	<input type="text" value="all"/> +
Outgoing Interface	<input type="text" value="port3"/> +
Destination Address	<input type="text" value="all"/> +
Schedule	<input type="text" value="always"/> -
Service	<input type="text" value="ALL"/> +
Action	<input type="text" value="ACCEPT"/> -
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	<input type="text" value="Click to add..."/>
<input type="radio"/> Use Central NAT Table	

Connecting the gateway router

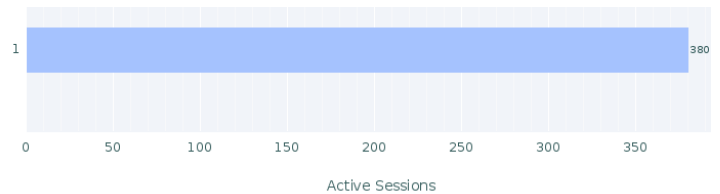
Connect port1 and port3 of the FortiGate unit to the gateway router to allow Internet traffic to flow.



Results

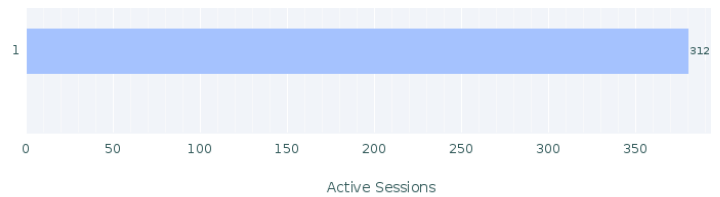
Connect to the Internet from the company A and company B networks and then log into the FortiGate unit.

Go to **Virtual Domains** and select **VDOM-A**. Go to **Policy > Policy > Monitor** to view the sessions being processed on VDOM-A.



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions
1	port2	port1	✓	380

Go to **Virtual Domains** and select **VDOM-B**. Go to **Policy > Policy > Monitor** to view the sessions being processed on VDOM-B.



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions
1	port4	port3	✓	312