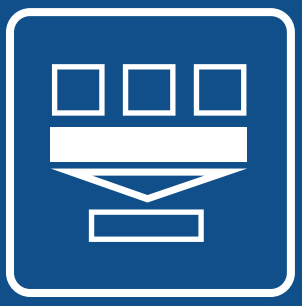
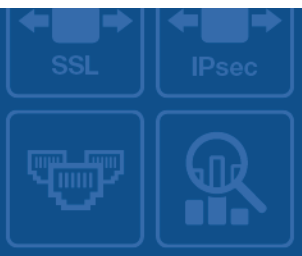


FORTINET
High Performance Network Security

FortiOS™ Handbook - Virtual Domains

VERSION 5.4.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

Tuesday, March 07, 2017

FortiOS™ Handbook - Virtual Domains

01-540-188666-20170307

TABLE OF CONTENTS

Change Log

Date	Change Description
March 7, 2017	Fixed some typos and minor errors.
Aug 31, 2016	Updated "What's new in FortiOS 5.4" on page 8 and "Using a VDOM in NAT/Route mode" on page 26
Aug 10, 2016	Updated "Benefits of Virtual Domains" on page 12 and "Enabling and accessing Virtual Domains" on page 14.
Apr 8, 2016	Initial Release.

Introduction

This guide explains how to set up and use Virtual Domains (VDOMs) with a FortiGate. It contains the following sections:

- Virtual Domains Overview: information about the basic concepts and rules for using VDOMs.
- Virtual Domains in NAT/Route mode: detailed explanations and examples for configuring VDOM features for a FortiGate in NAT/Route mode.
- Virtual Domains in Transparent modedetailed explanations and examples for configuring VDOM features for a FortiGate in Transparent mode.
- Inter-VDOM routing: concepts and scenarios for inter-VDOM routing.
- Troubleshooting Virtual Domains: diagnostic and troubleshooting information for some potential VDOM issues.

Before you begin using this guide, take a moment to note the following:

- By default, most FortiGate units support 10 VDOMs. Many FortiGate models support purchasing a license key to increase the maximum number
- This guide uses a FortiGate unit with interfaces named port1 through port4 for examples and procedures. The interface names on some models will vary. Where possible aliases for these ports are indicated to show their intended purpose and to help you determine which ports to use if your ports are labelled differently.
- Administrators are assumed to be super_admin administrators unless otherwise specified. Some restrictions will apply to other administrators.

What's new in FortiOS 5.4

The following new features have been added for Virtual Domains (VDOMs) in FortiOS 5.4:

Stackable VDOM licenses

VDOM licenses are now stackable, allowing you to buy additional licenses and stack them on top existing licenses to increase the number of VDOMs you can have.

Support execution of global CLI commands from within VDOMs

A new CLI command, `sudo`, allows the running of global commands from within the vdom context of the CLI.This means that the user no longer has to:

1. exit from the VDOM
2. enter global
3. run the command
4. return to the previous VDOM

The syntax for the command is:

```
sudo {global | vdom-name} {diagnose | execute | show | get}
```

These commands will only work if the user already has permissions to run the command. Unlike the the sudo command in some other operating systems like Linux, this command does not allow the user to run programs with the privileges of another user.

GUI features can now be enabled and disabled per VDOM

When VDOMs are enabled, most of the items in the Features section of the menu are moved to a similar menu section within the VDOM menu and are now customizable on a per VDOM basis. Some items such as IPv6 and Certificates are still configured on a global basis.

From the GUI, you can enable or disable GUI features from **System > Feature Select**.

Improvements and changes to per-VDOM certificates

The CA and local certificate configuration is now available per-VDOM. When an admin uploads a certificate to a VDOM, it will only be accessible inside that VDOM. When an admin uploads a certificate to global, it will be accessible to all VDOMs and global.

There are factory default certificates such as Fortinet_CA_SSL, Fortinet_SSL, PositiveSSL_CA, Fortinet_Wifi, and Fortinet_Factory, these certificates are moved to per-VDOM and automatically generated when a new VDOM is created.

The Fortinet_Firmware certificate has been removed and all the attributes that use Fortinet_Firmware now use Fortinet_Factory.

CLI Changes

Two new attributes `range` and `source` have been added:

`range` can be global or per-VDOM, if the certificate file is imported from global, it is a global certificate. If the certificate file is imported from a VDOM, it is VDOM certificate.

`source` can be `factory`, `user` or `fortiguard`:

`factory`: The factory certificate file with FortiOS version, this includes: Fortinet_CA_SSL, Fortinet_SSL, PositiveSSL_CA, Fortinet_Wifi, Fortinet_Factory.

`user`: Certificate file imported by the user.

`fortiguard`: Certificate file imported from FortiGuard.

```
config certificate local
   edit Fortinet_Factory
      set range global/vdom
      set source factory/user/fortiguard
   end
end
```

GUI Changes

Global and per-VDOM certificate configuration includes ***view details***, ***download***, ***delete***, and ***import*** certificate.

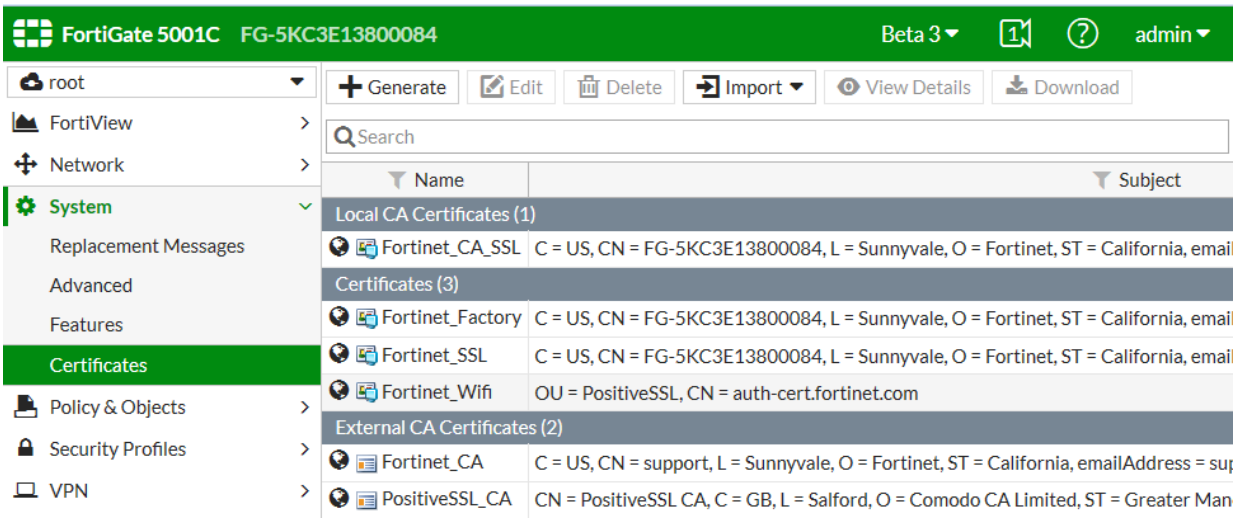
A ***Source*** and a ***Status*** columns have been added.

A global icon for ***Name*** column when VDOMs are enabled is added to show that the certificate is global.

A new VDOM now has the following default certificates: Fortinet_CA_SSL, Fortinet_Factory, Fortinet_SSL, Fortinet_Wifi, Fortinet_CA, and PositiveSSL_CA. These certificates are created automatically when the VDOM is created and every VDOM will have its own individual versions of these certificates.

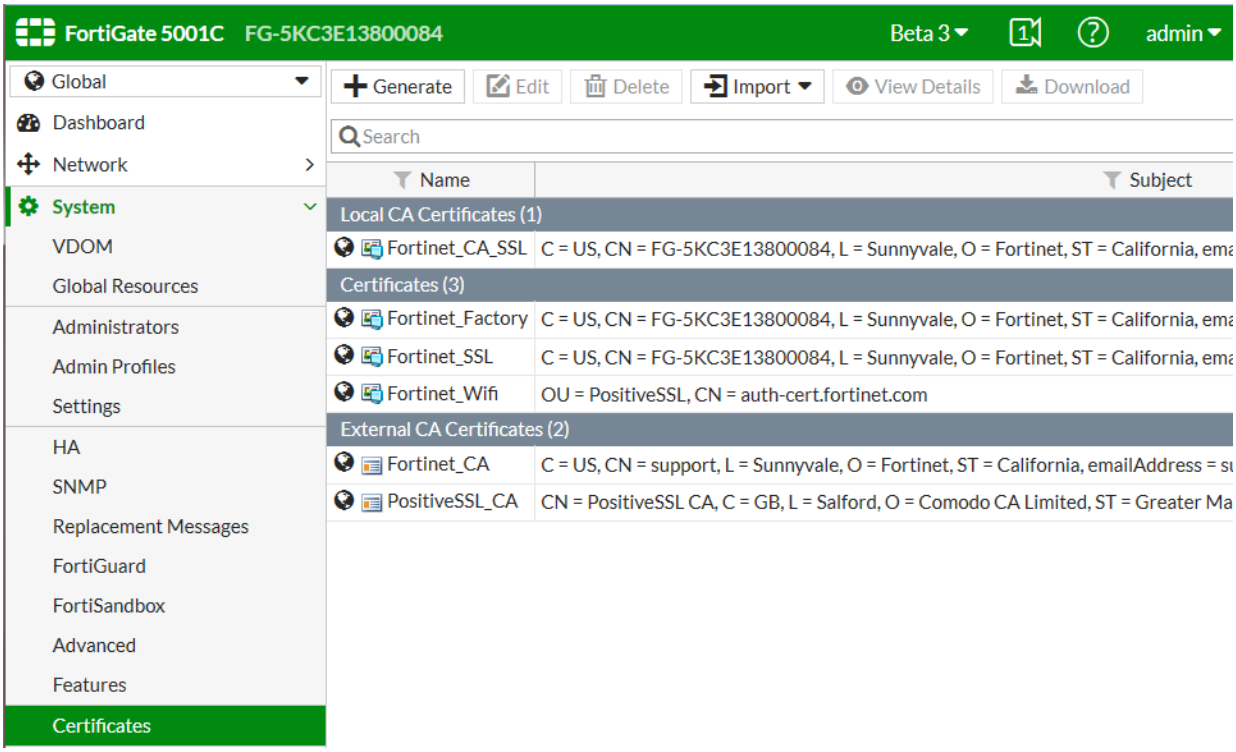
The Fortinet_firmware certificate has been removed. All default configurations that formerly used the Fortinet_ firmware certificate now use the Fortinet_Factory certificate.

Default root VDOM certificates



Certificates with the same names are also available from the global configuration. These are generated with you turn on VDOMs.

Default global certificates



Adding certificates to VDOMs and to the global configuration

If an administrator adds a certificate to a VDOM the certificate will only be available for that VDOM. If an administrator adds a certificate to the global configuration it will available for all VDOMs.

Adding option for VDOM logs through management VDOM

FortiOS supports the definition of per VDOM FortiAnalyzers. However it is required that each VDOM logs independently to its FortiAnalyzer server.

A new option, `use-management-vdom`, has been added to the CLI.

```
config vdom
   edit xxx
      config log fortianalyzer override-setting
         set use-management-vdom enable/disable
      end
   end
end
```

If this option is enabled, source-ip will become hidden and when FortiGate sends logs to FortiAnalyzer, it uses management vdom ip setting as source ip. Also if IPsec is enabled, the tunnel is created in management vdom and source ip belongs to management vdom.

Virtual Domains Overview

Virtual domains (VDOMs) are a method of dividing a FortiGate unit into two or more virtual units that function as multiple independent units. VDOMs can provide separate firewall policies and, in NAT/Route mode, completely separate configurations for routing and VPN services for each connected network or organization.

This chapter will cover the basics of VDOMs, how they change your FortiGate unit, and how to work with VDOMs.

VDOMs let you split your physical FortiGate unit into multiple virtual units. The resulting benefits range from limiting Transparent mode ports to simplified administration, to reduced space and power requirements.

In FortiOS 5.4.1, multiple VDOM support is disabled when Cooperative Security Fabric is enabled.

When VDOMs are disabled on any FortiGate unit, there is still one VDOM active: the root VDOM. It is always there in the background. When VDOMs are disabled, the root VDOM is not visible but it is still there.

The root VDOM must be there because the FortiGate unit needs a management VDOM for management traffic among other things. It is also why when you enable VDOMs, all your configuration is preserved in the root VDOM- because that is where you originally configured it.

This section includes:

Benefits of Virtual Domains

VDOMs provide the following benefits:

Easier administration

VDOMs provide separate security domains that allow separate zones, user authentication, firewall policies, routing, and VPN configurations. VDOMs separate security domains and simplify administration of complex configurations—you do not have to manage as many settings at one time.

By default, each FortiGate unit has a VDOM named root. This VDOM includes all of the unit's physical interfaces, modem, VLAN subinterfaces, zones, firewall policies, routing settings, and VPN settings.

Also, you can optionally assign an administrator account restricted to one VDOM. If the VDOM is created to serve an organization, this feature enables the organization to manage its own configuration.

In order to connect to a VDOM, an admin must log in using an interface belonging to that VDOM. This allows for proper authentication and restricts that admin's access to a single VDOM.

Each physical FortiGate unit requires a FortiGuard license to access security updates. VDOMs do not require any additional FortiGuard licenses, or updating — all the security updates for all the VDOMs are performed once per update at the global level. Combined this can be a potentially large money and time saving feature in your network.

Management systems such as SNMP, logging, alert email, FDN-based updates, and NTP-based time setting use addresses and routing in the management VDOM to communicate with the network. They can connect only to network resources that communicate with the management VDOM. Using a separate VDOM for management traffic enables easier management of the FortiGate unit global settings, and VDOM administrators can also manage their VDOMs more easily.

Continued security

When a packet enters a VDOM, it is confined to that VDOM and is subject to any firewall policies for connections between VLAN subinterfaces or zones in that VDOM, just like those interfaces on a FortiGate unit without VDOMs enabled.

To travel between VDOMs, a packet must first pass through a firewall policy on a physical interface. The packet then arrives at another VDOM on that same FortiGate unit, but on a different interface, where it must pass through another firewall before entering. It doesn't matter if the interface is physical or virtual — inter-VDOM packets still require the same security measures as when passing through physical interfaces.

VDOMs provide an additional level of security because regular administrator accounts are specific to one VDOM — an administrator restricted to one VDOM cannot change information on other VDOMs. Any configuration changes and potential errors will apply only to that VDOM and limit any potential down time. Using this concept, you can farther split settings so that the management domain is only accessible by the super_admin and does not share any settings with the other VDOMs.

Savings in physical space and power

To increase the number of physical FortiGate units, you need more rack space, cables, and power to install the new units. You also need to change your network configuration to accommodate the new physical units. In the future, if you need fewer physical units you are left with expensive hardware that is idle.

Increasing VDOMs involves no additional hardware, no additional cabling, and very few changes to existing networking configurations. VDOMs save physical space and power. You are limited only by the size of the VDOM license you buy and the physical resources on the FortiGate unit.

For example, if you are using one FortiGate 620B unit with 10 VDOMs instead of 10 physical units, over a year you will save an estimated 18,000 kWh. You could potentially save ten times that amount with a 100 VDOM license.

By default, most FortiGate units support 10 VDOMs. Many FortiGate models support purchasing a license key to increase the maximum number.

Improving Transparent mode configuration

When VDOMs are not enabled and you put your FortiGate unit into Transparent mode, all the interfaces on your unit become broadcast interfaces. The problem with this is that there are no interfaces free to do anything else.

With multiple VDOMs you can have one of them configured in Transparent mode, and the rest in NAT/Route mode. In this configuration, you have an available transparent mode FortiGate unit you can drop into your network for troubleshooting, and you also have the standard NAT for networking.

More flexible MSSP configurations

If you are a managed security and service provider (MSSP), VDOMs are fundamental to your business. As a service provider you have multiple customers, each with their own needs and service plans. VDOMs allow you to have a separate configuration for each customer, or group of customers; with up to 500 VDOMs configured per FortiGate unit on high end models.

Not only does this provide the exact level of service needed by each customer, but administration of the FortiGate unit is easier as well - you can provide uninterrupted service generally with immediate changes as required. Most importantly, it allows you to only use the resources that each customer needs. Inter-VDOM links allow you to customize the level of interaction you need between each of your customers and your administrators.

Enabling and accessing Virtual Domains

While Virtual Domains are essentially the same as your regular FortiGate unit for menu configuration, CLI command structure, and general task flow, there are some small differences.

After first enabling VDOMs on your FortiGate unit, you should take the time to familiarize yourself with the interface. This section will help walk you through virtual domains.

This section includes:

Enabling Virtual Domains

Using the default admin administration account, you can enable or disable VDOM operation on the FortiGate unit.

To enable VDOM configuration - web-based manager:

1. Log in with a super_admin account.
2. Go to the **Dashboard**.
3. In the **System Information** widget, locate **Virtual Domain**. Select **Enable** and confirm your selection.

The FortiGate unit logs off all sessions. You can now log in again as admin.

To enable VDOM configuration - CLI:

```
config system global
   set vdom-admin enable
end
```

Changes to the web-based manager and CLI

When Virtual Domains are enabled, your FortiGate unit will change. The changes will be visible in both the web-based manager and CLI, just the web-based manager, or just the CLI.

When enabling VDOMs, the web-based manager and the CLI are changed as follows:

- Global and per-VDOM configurations are separated. This is indicated in the Online Help by Global and VDOM icons.
- Only admin accounts using the super_admin profiles can view or configure global options
- Admin accounts using the super_admin profile can configure all VDOM configurations.
- All other administrator accounts can configure only the VDOM to which they are assigned.

The following changes are specific to the web-based manager:

- In the Global view, the System section of the left-hand menu is renamed to Global, and includes a VDOM sub-menu.
- The Log Config menu is moved from Log & Report into the new Global section.
- For admin accounts using the super_admin profile, a new section called Virtual Domains is added at the bottom of the left-hand menu. It lists all the individual VDOMs as expandable menus, with all VDOM specific options in that menu, which allows you to easily select which VDOM to configure, including the root VDOM.

In the CLI, admin accounts using the super_admin profile must specify either the global or a VDOM-specific shell before entering commands:

- To change FortiGate unit system settings, from the top level you must first enter the following CLI before entering commands:

  ```
  config global
  ```

- To change VDOM settings, from the top level you must first enter the following CLI before entering commands for that VDOM:

  ```
  config vdom
     edit <vdom_name>
  ```

Settings configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus settings, and some logging settings. In general, any unit settings that should only be changed by the top level administrator are global settings.

Settings configured configwithin a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging, and reporting.

Viewing the VDOM list

The VDOM list shows all virtual domains, their status, and which VDOM is the management VDOM. It is accessible if you are logged in on an administrator account with the super_admin profile such as the “admin” administrator account.

In the VDOM list you can create or delete VDOMs, edit VDOMs, change the management VDOM, and enable or disable VDOMs.

You can access the VDOM list when viewing by going to **Global > System > VDOM**.

The root domain cannot be disabled, even if it is not the management VDOM.

Global and per-VDOM settings

Settings configured outside of a VDOM are called global settings. These settings affect the entire FortiGate unit and include areas such as interfaces, HA, maintenance, some antivirus, and some logging. In general, any unit settings that should only be changed by the top level administrator are global settings.

Settings configured within a VDOM are called VDOM settings. These settings affect only that specific VDOM and include areas such as operating mode, routing, firewall, VPN, some antivirus, some logging settings, and reporting.

When Virtual Domains are not enabled, the entire FortiGate unit is effectively a single VDOM. Per-VDOM limits apply. For some resource types, the global limit cannot be reached with only one VDOM.

Resource settings

Your FortiGate unit has a limited amount of hardware resources such as memory, disk storage, CPU operations. When Virtual Domains are disabled, this limit is not a major concern because all sessions, users, and other processes share all the resources equally.

When using Virtual Domains, hardware resources can be divided differently between Virtual Domains as they are needed. Minimum levels of resources can be specified for each VDOM, so that no Virtual Domain will suffer a complete lack of resources.

For example, if one VDOM has only a web server and logging server connected, and a second VDOM has an internal network of 20 users, these two VDOMs will require different levels of resources. The first VDOM will require many sessions but no user accounts. This compares to the second VDOM where user accounts and management resources are required, but fewer sessions.

Using the global and per-VDOM resource settings, you can customize the resources allocated to each VDOM to ensure the proper level of service is maintained on each VDOM.

Global resource settings

Global Resources apply to the whole FortiGate unit. They represent all of the hardware capabilities of your unit. By default the values are set to their maximum values. These values vary by your model due to each model having differing hardware capabilities.

It can be useful to change the maximum values for some resources to ensure there is enough memory available for other resources that may be more important to your configuration.

To use the earlier example, if your FortiGate unit is protecting a number of web servers and other publicly accessible servers you would want to maximize the available sessions and proxies while minimizing other settings that are unused such as user settings, VPNs, and dial-up tunnels.

Global Resources are only configurable at the global level, and only the admin account has access to these settings. To view the resource list, go to **Global > System > Global Resources**. You can also use the following CLI command:

```
config global
   config system resource-limits
   get
```

Note that global resources, such as the log disk quota resource, will only be visible if your FortiGate unit hardware supports those resources, such as having a hard disk to support the log disk resource.

For explicit proxies, when configuring limits on the number of concurrent users, you need to allow for the number of users based on their authentication method. Otherwise you may run out of user resources prematurely.

Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSAE, local database etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.

For all other situations, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.

Per-VDOM resource settings

While Global resources apply to resources shared by the whole FortiGate unit, per-VDOM resources are specific to only one Virtual Domain.

By default all the per-VDOM resource settings are set to no limits. This means that any single VDOM can use up all the resources of the entire FortiGate unit if it needs to do so. This would starve the other VDOMs for resources to the point where they would be unable to function. For this reason, it is recommended that you set some maximums on resources that are most vital to your customers.

Each Virtual Domain has its own resource settings. These settings include both maximum, and minimum levels. The maximum level is the highest amount of that resource that this VDOM can use if it is available on the FortiGate unit. Minimum levels are a guaranteed level that this minimum level of the resource will always be available no matter what the other VDOMs may be using.

For example, consider a FortiGate unit that has ten VDOMs configured. vdom1 has a maximum of 5000 sessions and a minimum of 1000 sessions. If the FortiGate unit has a global maximum of 20,000 sessions, it is possible that vdom1 will not be able to reach its 5000 session upper limit. However, at all times vdom1 is guaranteed to have 1000 sessions available that it can use. On the other hand, if the remaining nine VDOMs use only 1000 sessions each, vdom1 will be able to reach its maximum of 5000.

To view per-VDOM resource settings - web-based manager:

1. Select **Global > System > VDOM**.
2. Select the `root` VDOM, and select **Edit**.
3. Adjust the settings in the **Resource Usage** section of the page.
4. Select **OK**.

To view per-VDOM resource settings - CLI:

```
config global
   config system vdom-property
      edit root
   get
```

Virtual Domain Licensing

For select FortiGate models in the 1U category and higher, you can purchase a license key to increase the maximum number of VDOMs. Most Enterprise and Large Enterprise (2U) models can support up to 500 VDOMs. Chassis-based models can support over 500 VDOMs. For specific information, see the product data sheet.

Configuring 500 or more VDOMs will result in reduced system performance. See Troubleshooting Virtual Domains.

Your FortiGate unit has limited resources that are divided among all configured VDOMs. These resources include system memory and CPU. Running security features on many VDOMs at once can limit resources available for basic processing. If you require many VDOMs, all with active security features, it is recommended to upgrade to a more powerful FortiGate unit.

It is important to backup your configuration before upgrading the VDOM license on your FortiGate unit or units, especially with FortiGate units in HA mode.

To obtain a VDOM license key

1. Log in with a super_admin account.
2. Go to the **Dashboard**.
3. Record your FortiGate unit serial number as shown in **System Information** widget.
4. In the **License Information** widget, locate **Virtual Domain** and select **Purchase More**.

If you do not see the **Purchase More** option on the System Dashboard, your FortiGate model does not support more than 10 VDOMs.

5. You will be taken to the Fortinet customer support website where you can log in and purchase a license key for 25, 50, 100, 250, 500, or more VDOMs.
6. When you receive your license key, go to the Dashboard and select **Upload License** under **License Information**, **Virtual Domains**.
7. In the **Input License Key** field, enter the 32-character license key you received from Fortinet customer support.
8. Select **Apply**.

To verify the new VDOM license, in global configuration go to **System > Dashboard**. Under **License Information**, **Virtual Domains** the maximum number of VDOMs allowed is shown.

VDOMs created on a registered FortiGate unit are recognized as real devices by any connected FortiAnalyzer unit. The FortiAnalyzer unit includes VDOMs in its total number of registered devices. For example, if three FortiGate units are registered on the FortiAnalyzer unit and they contain a total of four VDOMs, the total number of registered FortiGate units on the FortiAnalyzer unit is seven. For more information, see the FortiAnalyzer Administration Guide.

Logging in to VDOMs

Management services communicate using the management VDOM, which is the root VDOM by default.

Management traffic requires an interface that has access to the Internet. If there is no interface assigned to the VDOM containing the management traffic, services including updates will not function.

Accessing a VDOM if you are the FortiGate's Administrator - web-based manager:

1. Log in with a super_admin account.
2. In the **Virtual Domains** menu on the left-hand side, select the VDOM to configure.
   The menu will expand to show the various pages and settings for that VDOM.
3. When you have finished configuring the VDOM, you can
   - open the **Global** menu to return to global configuration
   - log out

Accessing a VDOM if you are the FortiGate's Administrator - CLI:

With the super_admin, logging into the CLI involves also logging into the specific VDOM. If you need a reminder, use `edit ?` to see a list of existing VDOMs before you editing a VDOM.

If you misspell a VDOM you are trying to switch to, you will create a new VDOM by that name. Any changes you make will be part of the new VDOM, and not the intended VDOM. If you are having problems where your changes aren't visible, back up to the top level and use `edit ?` to see a list of VDOMs to ensure this has not happened. If it has happened, see Enabling and accessing Virtual Domains.

```
config vdom
   edit ?
   edit <chosen_vdom>
      ..
      <enter vdom related commands>
      ..
   end
exit
```

Accessing a VDOM if you are the VDOM's Administrator - web-based manager:

1. Connect to the FortiGate unit using an interface that belongs to the VDOM to be configured.
2. Log in using an administrator account that has access to the VDOM.
   The main web-based manager page opens. The interface is largely the same as if the device has VDOMs disabled. From here you can access VDOM-specific settings.

Accessing a VDOM if you are the VDOM's Administrator - CLI:

A non-super_admin account has access to only one VDOM and must log in through an interface that belongs to the same VDOM, but the process is the same as logging into a non-VDOM unit.

```
Login: regular_admin
Password: <password>
..
<enter vdom related commands>
..
exit
```

Configuring Virtual Domains

Only a super_admin administrator account such as the default “admin” account can create, disable, or delete VDOMs. That account can create additional administrators for each VDOM.

This section includes:

Creating a Virtual Domain

Once you have enabled Virtual Domains on your FortiGate unit, you can create additional Virtual Domains beyond the default root Virtual Domain.

By default new Virtual Domains are set to NAT/Route operation mode. If you want a Virtual Domain to be in Transparent operation mode, you must manually change it.

You can name new Virtual Domains as you like with the following restrictions:

- only letters, numbers, “-”, and “_” are allowed
- no more than 11 characters are allowed
- no spaces are allowed
- VDOMs cannot have the same names as interfaces, zones, switch interfaces, or other VDOMs.

When creating large numbers of VDOMs you should not enable advanced features such as proxies, web filtering, and antivirus due to limited FortiGate unit resources. Also when creating large numbers of VDOMs, you may experience reduced performance for the same reason.

To create a VDOM - web-based manager:

1. Log in with a super_admin account.
2. Select **Global > System > VDOM**.
3. Select **Create New**.
4. Enter a unique name for your new VDOM.
5. Enter a short and descriptive comment to identify this VDOM.
6. Select **OK**.

Repeat Steps 3 through 6 to add additional VDOMs.

To create a VDOM - CLI:

```
config vdom
   edit <new_vdom_name>
end
```

If you want to edit an existing Virtual Domain in the CLI, and mistype the name a new Virtual Domain will be created with this new misspelled name. If you notice expected configuration changes are not visible, this may be the reason. You should periodically check your VDOM list to ensure there are none of these misspelled VDOMs present.

Disabling a Virtual Domain

The status of a VDOM can be Enabled or Disabled.

Active status VDOMs can be configured. Active is the default status when a VDOM is created. The management VDOM must be an Active VDOM.

Disabled status VDOMs are considered “offline”. The configuration remains, but you cannot use the VDOM, and only the super_admin administrator can view it. You cannot delete a disabled VDOM without first enabling it, and removing references to it like usual—there is no **Delete** icon for disabled status VDOMs. You can assign interfaces to a disabled VDOM.

The following procedures show how to disable a VDOM called “test-vdom”.

To disable a VDOM - web-based manager:

1. Go to **Global > System > VDOM**.
2. Open the VDOM for editing.
3. Ensure **Enable** is not selected and then select **OK**.
   The VDOM’s Enable icon in the VDOM list is a grey X.

To disable a VDOM - CLI:

```
config vdom
   edit test-vdom
      config system settings
         set status disable
      end
end
```

To enable a VDOM - web-based manager:

1. Go to **Global > System > VDOM**.
2. Open the VDOM for editing.
3. Ensure **Enable** is selected and then select **OK**.
   The VDOM's Enable icon in the VDOM list is a green checkmark.

To enable a VDOM - CLI:

```
config vdom
   edit test-vdom
      config system settings
         set status enable
      end
end
```

Deleting a VDOM

Deleting a VDOM removes it from the FortiGate unit configuration.

Before you can delete a VDOM, all references to it must be removed, including any per-VDOM objects. If there are any references to the VDOM remaining, you will see an error message and not be able to delete the VDOM.

A disabled VDOM cannot be deleted. You can also not delete the root VDOM or the management VDOM.

Before deleting a VDOM, a good practice is to reset any interface referencing that VDOM to its default configuration, with "root" selected as the Virtual Domain.

The following procedures show how to delete the `test-vdom` VDOM.

To delete a VDOM - web-based manager:

1. Go to **Global > System > VDOM**.
2. Select the check box for the VDOM and then select the **Delete** icon.

   If the **Delete** icon is not active, there are still references to the VDOM that must first be removed. The **Delete** icon is available when all the references to this VDOM are removed.

3. Confirm the deletion.

To delete a VDOM - CLI:

```
config vdom
   delete test-vdom
end
```

Removing references to a VDOM

When you are going to delete a VDOM, all references to that VDOM must first be removed. It can be difficult to find all the references to the VDOM. This section provides a list of common objects that must be removed before

a VDOM can be deleted, and a CLI command to help list the dependencies.

Interfaces are an important part of VDOMs. If you can move all the interfaces out of a VDOM, generally you will be able to delete that VDOM.

Common objects that refer to VDOMs

When you are getting ready to delete a VDOM check for, and remove the following objects that refer to that VDOM or its components:

- Routing - both static and dynamic routes
- Firewall addresses, policies, groups, or other settings
- Security Features/Profiles
- VPN configuration
- Users or user groups
- Logging
- DHCP servers
- Network interfaces, zones, custom DNS servers
- VDOM Administrators

Administrators in Virtual Domains

When Virtual Domains are enabled, permissions change for administrators. Administrators are now divided into per-VDOM administrators, and `super_admin` administrators. Only `super_admin` administrator accounts can create other administrator accounts and assign them to a VDOM.

Administrator VDOM permissions

Different types of administrator accounts have different permissions within VDOMs. For example, if you are using a super_admin profile account, you can perform all tasks. However, if you are using a regular admin account, the tasks available to you depend on whether you have read only or read/write permissions. The following table shows what tasks can be performed by which administrators.

Administrator VDOM permissions

Tasks	Regular administrator account		Super_admin profile administrator account
	Read only permission	Read/write permission	
View global settings	yes	yes	yes
Configure global settings	no	no	yes
Create or delete VDOMs	no	no	yes
Configure multiple VDOMs	no	no	yes
Assign interfaces to a VDOM	no	no	yes

Tasks	Regular administrator account		Super_admin profile administrator account
	Read only permission	Read/write permission	
Revision Control Backup and Restore	no	no	yes
Create VLANs	no	yes - for 1 VDOM	yes - for all VDOMs
Assign an administrator to a VDOM	no	no	yes
Create additional admin accounts	no	yes - for 1 VDOM	yes - for all VDOMs
Create and edit protection profiles	no	yes - for 1 VDOM	yes - for all VDOMs

The only difference in admin accounts when VDOMs are enabled is selecting which VDOM the admin account belongs to. Otherwise, by default the administration accounts are the same as when VDOMs are disabled and closely resemble the `super_admin` account in their privileges.

Creating administrators for Virtual Domains

Using the admin administrator account, you can create additional administrator accounts and assign them to VDOMs.

The newly-created administrator can access the FortiGate unit only through network interfaces that belong to their assigned VDOM or through the console interface. The network interface must be configured to allow management access, such as HTTPS and SSH. Without these in place, the new administrator will not be able to access the FortiGate unit and will have to contact the super_admin administrator for access.

The following procedure creates a new Local administrator account called `admin_sales` with a password of `fortinet` in the `sales` VDOM using the `admin_prof` default profile.

To create an administrator for a VDOM - web-based manager:

1. Log in with a super_admin account.
2. Go to **System > Administrators**.
3. Select **Create New**.
4. Select **Regular** for Type, as you are creating a Local administrator account.
5. Enter the necessary information about the administrator: email, password, etc.
6. If this admin will be accessing the VDOM from a particular IP address or subnet, enable **Restrict this Admin Login from Trusted Hosts Only** and enter the IP in **Trusted Host #1**.
7. Select `prof_admin` for the **Admin Profile**.
8. Select `sales` from the list of **Virtual Domains**.
9. Select **OK**.

To create administrators for VDOMs - CLI:

```
config global
   config system admin
      edit <new_admin_name>
         set vdom <vdom_for_this_account>
         set password <pwd>
         set accprofile <an_admin_profile>
         ...
      end
```

Virtual Domain administrator dashboard display

When administrators logs into their virtual domain, they see a different dashboard than the global administrator will see. The VDOM dashboard displays information only relevant to that VDOM — no global or other VDOM information is displayed.

VDOM dashboard information

Information	per-VDOM	Global
System Information	read-only	yes
License Information	no	yes
CLI console	yes	yes
Unit Operation	read-only	yes
Alert Message Console	no	yes
Top Sessions	limited to VDOM sessions	yes
Traffic	limited to VDOM interfaces	yes
Statistics	yes	yes

Virtual Domains in NAT/Route mode

By default, a Virtual Domain (VDOM) uses NAT/Route mode. In this mode, the VDOM is installed as a gateway or router between two networks. In most cases, it is used between a private network and the Internet. This allows the VDOM to hide the IP addresses of the private network using network address translation (NAT).

Each VDOM on a FortiGate can be configured for NAT/Route mode or Transparent mode, regardless of the operation mode of other VDOMs on the FortiGate. For more information about Transparent mode, see "Virtual Domains in Transparent mode" on page 45.

This chapter contains the following sections:

Using a VDOM in NAT/Route mode

Once you have enabled virtual domains and created one or more VDOMs, you need to configure them. Configuring VDOMs on your FortiGate unit includes tasks such as the ones listed here; while you may not require all for your network topology, it is recommended that you perform them in the order given:

Changing the management virtual domain

The management virtual domain is the virtual domain where all the management traffic for the FortiGate unit originates. This management traffic needs access to remote servers, such as FortiGuard services and NTP, to perform its duties. It needs access to the Internet to send and receive this traffic.

Management traffic includes, but is not limited to

- DNS lookups
- logging to FortiAnalyzer or syslog
- FortiGuard service
- sending alert emails
- Network time protocol traffic (NTP)
- Sending SNMP traps
- Quarantining suspicious files and email.

By default the management VDOM is the root domain. When other VDOMs are configured on your FortiGate unit, management traffic can be moved to one of these other VDOMs.

Reasons to move the management VDOM include selecting a non-root VDOM to be your administration VDOM, or the root VDOM not having an interface with a connection to the Internet.

You cannot change the management VDOM if any administrators are using RADIUS authentication.

The following procedure will change the management VDOM from the default `root` to a VDOM named `mgmt_vdom`. It is assumed that `mgmt_vdom` has already been created and has an interface that can access the Internet.

To change the management VDOM - web-based manager:

1. Select **Global > System > VDOM.**
2. Select the checkbox next to the required VDOM.
3. Select **Switch Management.**
   The current management VDOM is shown in square brackets, “[root]” for example.

To change the management VDOM - CLI:

```
config global
   config system global
      set management-vdom mgmt_vdom
   end
```

Management traffic will now originate from `mgmt_vdom`.

Configuring interfaces

A VDOM must contain at least two interfaces to be useful. These can be physical interfaces or VLAN interfaces. By default, all physical interfaces are in the root VDOM. When you create a new VLAN, it is in the root VDOM by default.

When there are VDOMs on the FortiGate unit in both NAT and Transparent operation modes, some interface fields will be displayed as “-” on **Network > Interfaces**. Only someone with a super_admin account can view all the VDOMs.

When moving an interface to a different VDOM, firewall IP pools and virtual IPs for this interface are deleted. You should manually delete any routes that refer to this interface. Once the interface has been moved to the new VDOM, you can add these services to the interface again.

When configuring VDOMs on FortiGate units with accelerated interfaces you must assign both interfaces in the pair to the same VDOM for those interfaces to retain their acceleration. Otherwise they will become normal interfaces.

This section includes the following topics:

Adding a VLAN to a NAT/Route VDOM

The following example shows one way that multiple companies can maintain their security when they are using one FortiGate unit with VLANs that share interfaces on the unit.

This procedure will add a VLAN interface called `client1-v100` with a VLAN ID of 100 to an existing VDOM called `client1` using the physical interface called `port2`.

The physical interface does not need to belong to the VDOM that the VLAN belongs to.

To add a VLAN subinterface to a VDOM - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	client1-v100
Interface	port2
VLAN ID	100
Virtual Domain	Client1
Addressing mode	Manual
IP/Netmask	172.20.120.110/255.255.255.0
Administrative Access	HTTPS, SSH

You will see an expand arrow added to the port2 interface. When the arrow is expanded, the interface shows the `client1-v100` VLAN subinterface.

To add a VLAN subinterface to a VDOM - CLI:

```
config global
   config system interface
      edit client1-v100
         set type vlan
         set vlanid 100
         set vdom Client1
         set interface port2
         set ip 172.20.120.110 255.255.255.0
         set allowaccess https ssh
```

```
end
```

Moving an interface to a VDOM

Interfaces belong to the root VDOM by default. Moving an interface is the same procedure no matter if its moving from the root VDOM or a any other VDOM.

If you have an accelerated pair of physical interfaces both interfaces must be in the same VDOM or you will lose their acceleration.

The following procedure will move the port3 interface to the Client2 VDOM. This is a common action when configuring a VDOM. It is assumed that the Client2 VDOM has already been created. It is also assumed that your FortiGate unit has a port3 interface. If you are using a different model, your physical interfaces may not be named `port2`, `external` or `port3`.

To move an existing interface to a different VDOM - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** for the port3 interface.
3. Select `Client2` as the new **Virtual Domain**.
4. Select **OK**.

To move an existing interface to a different VDOM - CLI:

```
config global
   config system interface
      edit port3
         set vdom Client2
      end
```

Deleting an interface

Before you can delete a virtual interface, or move an interface from one VDOM to another, all references to that interface must be removed. For a list of objects that can refer to an interface see Virtual Domains Overview.

The easiest way to be sure an interface can be deleted is when the Delete icon is no longer greyed out. If it remains greyed out when an interface is selected, that interface still has objects referring to it, or it is a physical interface that cannot be deleted.

To delete a virtual interface - web-based manager:

1. Ensure all objects referring to this interface have been removed.
2. Select **Global > Network > Interfaces**.
3. Select the interface to delete.
4. Select the delete icon.

Adding a zone to a VDOM

Grouping interfaces and VLAN subinterfaces into zones simplifies policy creation. You can configure policies for connections to and from a zone, but not between interfaces in a zone.

Zones are VDOM-specific. A zone cannot be moved to a different VDOM. Any interfaces in a zone cannot be used in another zone. To move a zone to a new VDOM requires deleting the current zone and re-creating a zone in the new VDOM.

The following procedure will create a zone called `accounting` in the `client2` VDOM. It will not allow intra-zone traffic, and both `port3` and `port2` interfaces belong to this zone. This is a method of grouping and isolating traffic over particular interfaces—it is useful for added security and control within a larger network.

To add a zone to a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Network > Interfaces**.
3. Select **Create New > Zone**.
4. Enter the following information and select **OK**:

Zone Name	accounting
Block intra-zone traffic	Select
Interface Members	port3, port2

To add a zone to a VDOM - CLI:

```
config vdom
   edit client2
      config system zone
         edit accounting
            set interface port3 port2
            set intrazone deny
         end
   end
```

Configuring VDOM routing

Routing is VDOM-specific. Each VDOM should have a default static route configured as a minimum. Within a VDOM, routing is the same as routing on your FortiGate unit without VDOMs enabled.

When configuring dynamic routing on a VDOM, other VDOMs on the FortiGate unit can be neighbors. The following topics give a brief introduction to the routing protocols, and show specific examples of how to configure dynamic routing for VDOMs. Figures are included to show the FortiGate unit configuration after the successful completion of the routing example.

Default static route for a VDOM

The routing you define applies only to network traffic entering non-ssl interfaces belonging to this VDOM. Set the administrative distance high enough, typically 20, so that automatically configured routes will be preferred to the default.

In the following procedure, it is assumed that a VDOM called “Client2” exists. The procedure will create a default static route for this VDOM. The route has a destination IP of 0.0.0.0, on the port3 interface. It has a gateway of 10.10.10.1, and an administrative distance of 20.

The values used in this procedure are very standard, and this procedure should be part of configuring all VDOMs.

To add a default static route for a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Network > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port2
Gateway	10.10.10.1
Distance	20

To add a default static route for a VDOM - CLI:

```
config vdom
   edit client2
      config router static
         edit 4
            set device port2
            set dst 0.0.0.0 0.0.0.0
            set gateway 10.10.10.1
            set distance 20
         end
   end
```

Dynamic Routing in VDOMs

Dynamic routing is VDOM-specific, like all other routing. Dynamic routing configuration is the same with VDOMs as with your FortiGate unit without VDOMs enabled, once you are at the routing menu. If you have multiple VDOMs configured, the dynamic routing configuration between them can become quite complex.

VDOMs provide some interesting changes to dynamic routing. Each VDOM can be a neighbor to the other VDOMs. This is useful in simulating a dynamic routing area or AS or network using only your FortiGate unit.

You can separate different types of routing to different VDOMs if required. This allows for easier troubleshooting. This is very useful if your FortiGate unit is on the border of a number of different routing domains.

For more information on dynamic routing in FortiOS, see the Advanced Routing handbook.

Inter-VDOM links must have IP addresses assigned to them if they are part of a dynamic routing configuration. Inter-VDOM links may or may not have IP addresses assigned to them. Without IP addresses, you need to be careful how you configure routing. While the default static route can be assigned an address of 0.0.0.0 and rely instead on the interface, dynamic routing almost always requires an IP address.

RIP

The RIP dynamic routing protocol uses hop count to determine the best route, with a hop count of 1 being directly attached to the interface and a hop count of 16 being unreachable. For example if two VDOMs on the same FortiGate unit are RIP neighbors, they have a hop count of 1.

OSPF

OSPF communicates the status of its network links to adjacent neighbor routers instead of the complete routing table. When compared to RIP, OSPF is more suitable for large networks, it is not limited by hop count, and is more complex to configure. For smaller OSPF configurations its easiest to just use the backbone area, instead of multiple areas.

BGP

BGP is an Internet gateway protocol (IGP) used to connect autonomous systems (ASes) and is used by Internet service providers (ISPs). BGP stores the full path, or path vector, to a destination and its attributes which aid in proper routing.

Configuring security policies

Security policies are VDOM-specific. This means that all firewall settings for a VDOM, such as firewall addresses and security policies, are configured within the VDOM.

In VDOMs, all firewall related objects are configured per-VDOM including addresses, service groups, security profiles, schedules, traffic shaping, and so on. If you want firewall addresses, you will have to create them on each VDOM separately. If you have many addresses, and VDOMs this can be tedious and time consuming. Consider using a FortiManager unit to manage your VDOM configuration — it can get firewall objects from a configured VDOM or FortiGate unit, and push those objects to many other VDOMs or FortiGate units. See the FortiManager Administration Guide.

You can customize the **Policy** display by including some or all columns, and customize the column order onscreen. Due to this feature, security policy screenshots may not appear the same as on your screen.

Configuring a security policy for a VDOM

Your security policies can involve only the interfaces, zones, and firewall addresses that are part of the current VDOM, and they are only visible when you are viewing the current VDOM. The security policies of this VDOM filter the network traffic on the interfaces and VLAN subinterfaces in this VDOM.

A firewall service group can be configured to group multiple services into one service group. When a descriptive name is used, service groups make it easier for an administrator to quickly determine what services are allowed by a security policy.

In the following procedure, it is assumed that a VDOM called `Client2` exists. The procedure will configure an outgoing security policy. The security policy will allow all HTTPS, SSH, and DNS traffic for the `SalesLocal` address group on VLAN_200 going to all addresses on port3. This traffic will be scanned and logged.

To configure a security policy for a VDOM - web-based manager:

1. In **Virtual Domains**, select the client2 VDOM.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Name	Client2-outgoing
Incoming Interface	VLAN_200
Outgoing Interface	port3
Source Address	SalesLocal
Destination Address	any
Schedule	always
Service	HTTPS, SSH, DNS
Action	ACCEPT
Log Allowed Traffic	enable

To configure a security policy for a VDOM - CLI:

```
config vdom
   edit Client2
      config firewall policy
         edit 12
            set srcintf VLAN_200
            set srcaddr SalesLocal
            set dstintf port3(dmz)
            set dstaddr any
            set schedule always
            set service HTTPS SSH
            set action accept
            set status enable
            set logtraffic enable
         end
   end
```

Changing the inspection mode

If you wish to change the inspection mode for a VDOM, go to **System > VDOM** and edit the VDOM you want to configure. Set **Inspection Mode** to either **Proxy** or **Flow-based**.

VDOMs on the same FortiGate can use different inspection modes.

Configuring security profiles

In NAT/Route VDOMs, security profiles are exactly like regular FortiGate unit operation with one exception. In VDOMs, there are no default security profiles.

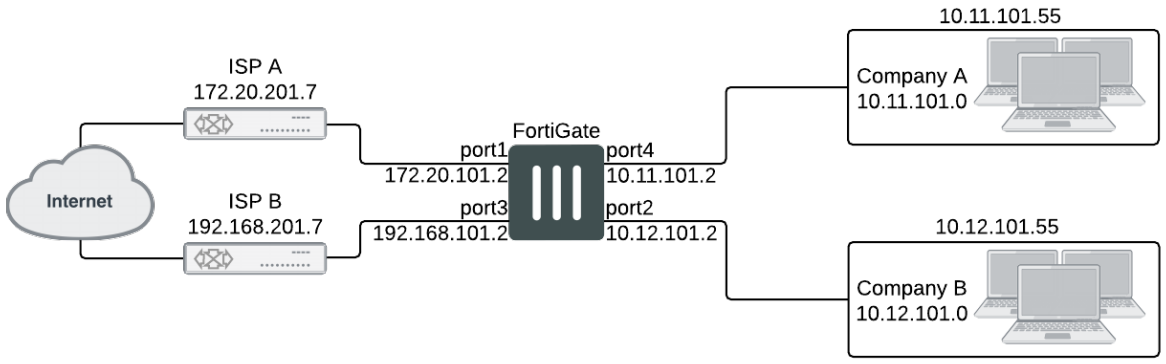
If you want security profiles in VDOMs, you must create them yourself. If you have many security profiles to create in each VDOM, you should consider using a FortiManager unit. It can get existing profiles from a VDOM or FortiGate unit, and push those profiles down to multiple other VDOMs or FortiGate units. See the FortiManager Administration Guide.

When VDOMs are enabled, you only need one FortiGuard license for the physical unit, and download FortiGuard updates once for the physical unit. This can result in a large time and money savings over multiple physical units if you have many VDOMs.

Configuring VPNs for a VDOM

Virtual Private Networking (VPN) settings are VDOM-specific, and must be configured within each VDOM. Configurations for IPsec Tunnel, IPsec Interface, PPTP and SSL are VDOM-specific. However, certificates are shared by all VDOMs and are added and configured globally to the FortiGate unit.

Example configuration: VDOM in NAT/Route mode



Company A and Company B each have their own internal networks and their own ISPs. They share a FortiGate unit that is configured with two separate VDOMs, with each VDOM running in NAT/Route mode enabling separate configuration of network protection profiles. Each ISP is connected to a different interface on the FortiGate unit.

This network example was chosen to illustrate one of the most typical VDOM configurations.

This example has the following sections:

- Network topology and assumptions
- General configuration steps
- Creating the VDOMs
- Configuring the FortiGate interfaces
- Configuring the vdomA VDOM
- Configuring the vdomB VDOM
- Testing the configuration

Network topology and assumptions

Both companies have their own ISPs and their own internal interface, external interface, and VDOM on the FortiGate unit.

For easier configuration, the following IP addressing is used:

- all IP addresses on the FortiGate unit end in ".2" such as 10.11.101.2.
- all IP addresses for ISPs end in ".7", such as 172.20.201.7.
- all internal networks are 10.*.*.* networks, and sample internal addresses end in ".55".

The IP address matrix for this example is as follows.

Address	Company A	Company B
ISP	`172.20.201.7`	`192.168.201.7`
Internal network	`10.11.101.0`	`10.012.101.0`
FortiGate / VDOM	`172.20.201.2 (port1)` `10.11.101.2 (port4)`	`192.168.201.2 (port3)` `10.012.101.2 (port2)`

The Company A internal network is on the 10.11.101.0/255.255.255.0 subnet. The Company B internal network is on the 10.12.101.0/255.255.255.0 subnet.

There are no switches or routers required for this configuration.

There are no VLANs in this network topology.

The interfaces used in this example are port1 through port4. Different FortiGate models may have different interface labels. port1 and port3 are used as external interfaces. port2 and port4 are internal interfaces.

The administrator is a super_admin account. If you are a using a non-super_admin account, refer to "Global and per-VDOM settings" to see which parts a non-super_admin account can also configure.

When configuring security policies in the CLI always choose a policy number that is higher than any existing policy numbers, select `services` before `profile-status`, and `profile-status` before `profile`. If these commands are not entered in that order, they may not be available to enter.

General configuration steps

For best results in this configuration, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the FortiGate interfaces
3. Configuring the vdomA VDOM, and Configuring the vdomB VDOM
4. Testing the configuration

Creating the VDOMs

In this example, two new VDOMs are created — vdomA for Company A and vdomB for Company B. These VDOMs will keep the traffic for these two companies separate while enabling each company to access its own ISP.

To create two VDOMs - web-based manager:

1. Log in with a super_admin account.
2. Go to **Global > System > VDOM**, and select **Create New**.

3. Enter `vdomA` and select **OK**.
4. Select **OK** again to return to the VDOM list.
5. Select **Create New**.
6. Enter `vdomB` and select **OK**.

To create two VDOMs - CLI:

```
config vdom
   edit vdomA
   next
   edit vdomB
end
```

Configuring the FortiGate interfaces

This section configures the interfaces that connect to the companies' internal networks, and to the companies' ISPs.

All interfaces on the FortiGate unit will be configured with an IP address ending in ".2" such as 10.11.101.2. This will simplify network administration both for the companies, and for the FortiGate unit global administrator. Also the internal addresses for each company differ in the second octet of their IP address - Company A is 10.11.*, and Company B is 10.12.*.

This section includes the following topics:

- Configuring the vdomA interfaces
- Configuring the vdomB interfaces

If you cannot change the VDOM of an network interface it is because something is referring to that interface that needs to be deleted. Once all the references are deleted the interface will be available to switch to a different VDOM. For example a common reference to the external interface is the default static route entry. See Example configuration: VDOM in NAT/Route mode.

Configuring the vdomA interfaces

The `vdomA` VDOM includes two FortiGate unit interfaces: port1 and external.

The port4 interface connects the Company A internal network to the FortiGate unit, and shares the internal network subnet of 10.11.101.0/255.255.255.0.

The external interface connects the FortiGate unit to ISP A and the Internet. It shares the ISP A subnet of 172.20.201.0/255.255.255.0.

To configure the vdomA interfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port1 interface.
3. Enter the following information and select **OK**:

Virtual Domain	vdomA

Addressing mode	Manual
IP/Netmask	172.20.201.2/255.255.255.0

4. Select **Edit** on the port4 interface.
5. Enter the following information and select **OK**:

Virtual Domain	vdomA
Addressing mode	Manual
IP/Netmask	10.11.101.2/255.255.255.0

To configure the vdomA interfaces - CLI:

```
config global
   config system interface
      edit port1
         set vdom vdomA
         set mode static
         set ip 172.20.201.2 255.255.255.0
      next
      edit port4
         set vdom ABCDomain
         set mode static
         set ip 10.11.101.2 255.255.255.0
      end
```

Configuring the vdomB interfaces

The `vdomB` VDOM uses two FortiGate unit interfaces: port2 and port3.

The port2 interface connects the Company B internal network to the FortiGate unit, and shares the internal network subnet of 10.12.101.0/255.255.255.0.

The port3 interface connects the FortiGate unit to ISP B and the Internet. It shares the ISP B subnet of 192.168.201.0/255.255.255.0.

To configure the vdomB interfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** on the port3 interface.
3. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	192.168.201.2/255.255.255.0

4. Select **Edit** on the port2 interface.
5. Enter the following information and select **OK**:

Virtual domain	vdomB
Addressing mode	Manual
IP/Netmask	10.12.101.2/255.255.255.0

To configure the vdomB interfaces - CLI:

```
config global
   config system interface
      edit port3
         set vdom vdomB
         set mode static
         set ip 192.168.201.2 255.255.255.0
      next
      edit port2
         set vdom vdomB
         set mode static
         set ip 10.12.101.2 255.255.255.0
   end
```

Configuring the vdomA VDOM

With the VDOMs created and the ISPs connected, the next step is to configure the vdomA VDOM.

Configuring the vdomA includes the following:

- Adding vdomA firewall addresses
- Adding the vdomA security policy
- Adding the vdomA default route

Adding vdomA firewall addresses

You need to define the addresses used by Company A's internal network for use in security policies. This internal network is the 10.11.101.0/255.255.255.0 subnet.

The FortiGate unit provides one default address, "all", that you can use when a security policy applies to all addresses as the source or destination of a packet.

To add the vdomA firewall addresses - web-based manager:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Policy & Objects > Addresses**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Ainternal
Type	Subnet / IP Range
Subnet / IP Range	10.11.101.0/255.255.255.0
Interface	port4

To add the ABCDomain VDOM firewall addresses - CLI:

```
config vdom
   edit vdomA
      config firewall address
         edit Ainternal
            set type ipmask
            set subnet 10.11.101.0 255.255.255.0
      end
   end
```

Adding the vdomA security policy

You need to add the `vdomA` security policy to allow traffic from the internal network to reach the external network, and from the external network to internal as well. You need two policies for this domain.

To add the vdomA security policy - web-based manager:

1. In **Virtual Domains**, select **vdomA**.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Name	VDOMA-internal-to-external
Incoming Interface	port4
Outgoing Interface	port1
Source Address	Ainternal
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

5. Select **Create New**.
6. Enter the following information and select **OK**:

Name	VDOMA-external-to-internal
Incoming Interface	port1
Outgoing Interface	port4
Source Address	all
Destination Address	Ainternal
Schedule	Always

Service	ANY
Action	ACCEPT

To add the vdomA security policy - CLI:

```
config vdom
   edit vdomA
      config firewall policy
         edit 1
            set srcintf port4
            set srcaddr Ainternal
            set dstintf port1
            set dstaddr all
            set schedule always
            set service ANY
            set action accept
            set status enable
         next
         edit 2
            set srcintf port1
            set srcaddr all
            set dstintf port4
            set dstaddr Ainternal
            set schedule always
            set service ANY
            set action accept
            set status enable
         end
```

Adding the vdomA default route

You also need to define a default route to direct packets from the Company A internal network to ISP A. Every VDOM needs a default static route, as a minimum, to handle traffic addressed to external networks such as the Internet.

The administrative distance should be set slightly higher than other routes. Lower admin distances will get checked first, and this default route will only be used as a last resort.

To add a default route to the vdomA - web-based manager:

1. For **Virtual Domains**, select **vdomA**
2. Go to **Network > Static Routes**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port1
Gateway	172.20.201.7
Distance	20

To add a default route to the vdomA - CLI:

```
config vdom
   edit vdomA
      config router static
         edit 1
            set device port1
            set gateway 172.20.201.7
         end
```

Configuring the vdomB VDOM

In this example, the vdomB VDOM is used for Company B. Firewall and routing settings are specific to a single VDOM.

vdomB includes the FortiGate port2 interface to connect to the Company B internal network, and the FortiGate port3 interface to connect to ISP B. Security policies are needed to allow traffic from port2 to external and from external to port2 interfaces.

This section includes the following topics:

Adding the vdomB firewall address

You need to define addresses for use in security policies. In this example, the vdomB VDOM needs an address for the port2 interface and the “all” address.

To add the vdomB firewall address - web-based manager:

1. In **Virtual Domains**, select **vdomB**.
2. Go to **Policy & Objects > Addresses**.
3. Select **Create New**.
4. Enter the following information and select **OK**:

Address Name	Binternal
Type	Subnet / IP Range
Subnet / IP Range	10.12.101.0/255.255.255.0
Interface	port2

To add the vdomB firewall address - CLI:

```
config vdom
   edit vdomB
      config firewall address
         edit Binternal
            set type ipmask
            set subnet 10.12.101.0 255.255.255.0
         end
```

```
end
```

Adding the vdomB security policy

You also need a security policy for the Company B domain. In this example, the security policy allows all traffic.

To add the vdomB security policy - web-based manager:

1. Log in with a super_admin account.
2. In **Virtual Domains**, select vdomB.
3. Go to **Policy & Objects > IPv4 Policy**
4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VDOMB-internal-to-external
Incoming Interface	port2
Outgoing Interface	port3
Source Address	Binternal
Destination Address	all
Schedule	Always
Service	ANY
Action	ACCEPT

6. Select **Create New**.
7. Enter the following information and select **OK**:

Name	VDOMB-external-to-internal
Incoming Interface	port3
Outgoing Interface	port2
Source Address	all
Destination Address	Binternal
Schedule	Always
Service	ANY
Action	ACCEPT

To add the vdomB security policy - CLI:

```
config vdom
   edit vdomB
      config firewall policy
         edit 1
```

```
            set srcintf port2
            set dstintf port3
            set srcaddr Binternal
            set dstaddr all
            set schedule always
            set service ANY
            set action accept
            set status enable
        edit 1
            set srcintf port3
            set dstintf port2
            set srcaddr all
            set dstaddr Binternal
            set schedule always
            set service ANY
            set action accept
            set status enable
        end
    end
```

Adding a default route to the vdomB VDOM

You need to define a default route to direct packets to ISP B.

To add a default route to the vdomB VDOM - web-based manager:

1. Log in as the super_admin administrator.
2. In **Virtual Domains**, select vdomB.
3. Go to **Network > Static Routes**.
4. Select **Create New**.
5. Enter the following information and select **OK**:

Destination IP/Mask	0.0.0.0/0.0.0.0
Device	port3
Gateway	192.168.201.7
Distance	20

To add a default route to the vdomB VDOM - CLI:

```
config vdom
   edit vdomB
      config router static
         edit 1
            set dst 0.0.0.0/0
            set device external
            set gateway 192.168.201.7
         end
   end
```

Testing the configuration

Once you have completed configuration for both company VDOMs, you can use diagnostic commands, such as `tracert` in Windows, to test traffic routed through the FortiGate unit. Alternately, you can use the `traceroute` command on a Linux system with similar output.

Possible errors during the traceroute test are:

- "`* * * Request timed out`" - the trace was not able to make the next connection towards the destination fast enough
- "`Destination host unreachable`" - after a number of timed-out responses the trace will give up

Possible reasons for these errors are bad connections or configuration errors.

For additional troubleshooting, see Troubleshooting Virtual Domains.

Testing traffic from the internal network to the ISP

In this example, a route is traced from the Company A internal network to ISP A. The test was run on a Windows PC with an IP address of 10.11.101.55.

The output here indicates three hops between the source and destination, the IP address of each hop, and that the trace was successful.

From the Company A internal network, access a command prompt and enter this command:

```
C:\>tracert 172.20.201.7
Tracing route to 172.20.201.7 over a maximum of 30 hops:
  1   <10 ms   <10 ms   <10 ms  10.11.101.2
  2   <10 ms   <10 ms   <10 ms  172.20.201.2
  3   <10 ms   <10 ms   <10 ms  172.20.201.7
Trace complete.
```

Virtual Domains in Transparent mode

A VDOM in Transparent mode is installed between the internal network and the router. In this mode, the VDOM does not make any changes to IP addresses and only applies security scanning to traffic. When a VDOM is added to a network in Transparent mode, no network changes are required, except to provide the VDOM with a management IP address.

Each VDOM on a FortiGate can be configured for NAT/Route mode or Transparent mode, regardless of the operation mode of other VDOMs on the FortiGate. For more information about NAT/Route mode, see "Virtual Domains in NAT/Route mode" on page 26.

This chapter includes the following sections:

Transparent Mode Overview

In transparent mode, a VDOM becomes a layer-2 IP forwarding bridge. This means that Ethernet frames are forwarded based on destination MAC address, and no other routing is performed. All incoming traffic that is accepted by the firewall, is broadcast out on all interfaces.

In transparent mode the VDOM is a forwarding bridge, not a switch. A switch can develop a port table and associated MAC addresses, so that it can bridge two ports to deliver the traffic instead of broadcasting to all ports. In transparent mode, the VDOM does not following this switch behavior, but instead is the forwarding bridge that broadcasts all packets out over all interfaces, subject to security policies.

Differences between NAT/Route and Transparent mode

The differences between NAT/Route mode and Transparent mode include:

Differences between NAT/Route and Transparent modes

Features	NAT/Route mode	Transparent mode
Specific Management IP address required	No	Yes
Perform Network Address Translation (NAT)	Yes	Yes
Stateful packet inspection	Yes	Yes
Layer-2 forwarding	Yes	Yes

Features	NAT/Route mode	Transparent mode
Layer-3 routing	Yes	No
Unicast Routing / Policy Based routing	Yes	No
DHCP server	Yes	No
IPsec VPN	Yes	Yes
PPTP/L2TP VPN	Yes	No
SSL VPN	Yes	No
Security features	Yes	Yes
VLAN support	Yes	Yes - limited to VLAN trunks.
Ping servers (dead gateway detection)	Yes	No

To provide administrative access to a FortiGate unit or VDOM in Transparent mode, you must define a management IP address and a gateway. This step is not required in NAT/Route mode where you can access the FortiGate unit through the assigned IP address of any interface where administrative access is permitted.

If you incorrectly set the Transparent mode management IP address for your FortiGate unit, you will be unable to access your unit through the web-based manager. In this situation, you will need to connect to the FortiGate unit using the console cable and change the settings so you can access the unit. Alternately, if your unit has an LCD panel, you can change the operation mode and interface information through the LCD panel.

Operation mode differences in VDOMs

A VDOM, such as root, can have a maximum of 255 interfaces in Network Address Translation (NAT) mode or Transparent mode. This includes VLANs, other virtual interfaces, and physical interfaces. To have more than a total of 255 interfaces configured, you need multiple VDOMs with multiple interfaces on each.

In Transparent mode without VDOMs enabled, all interfaces on the FortiGate unit act as a bridge — all traffic coming in on one interface is sent back out on all the other interfaces. This effectively turns the FortiGate unit into a two interface unit no matter how many physical interfaces it has. When VDOMs are enabled, this allows you to determine how many interfaces to assign to a VDOM running in Transparent mode. If there are reasons for assigning more than two interfaces based on your network topology, you are able to. However, the benefit of VDOMs in this case is that you have the functionality of Transparent mode, but you can use interfaces for NAT/Route traffic as well.

You can add more VDOMs to separate groups of VLAN subinterfaces. When using a FortiGate unit to serve multiple organizations, this configuration simplifies administration because you see only the security policies and settings for the VDOM you are configuring.

One essential application of VDOMs is to prevent problems caused when a FortiGate unit is connected to a layer-2 switch that has a global MAC table. FortiGate units normally forward ARP requests to all interfaces, including VLAN subinterfaces. It is then possible for the switch to receive duplicate ARP packets on different VLANs. Some

layer-2 switches reset when this happens. As ARP requests are only forwarded to interfaces in the same VDOM, you can solve this problem by creating a VDOM for each VLAN.

For more information about Transparent mode, see the Transparent Mode & Internal Segmentation Firewall (ISFW) handbook.

Using a VDOM in Transparent mode

The essential steps to configure a VDOM in Transparent mode are:

- Switching to Transparent mode
- Adding VLAN subinterfaces
- Creating security policies

You can also configure the security profiles that manage antivirus scanning, web filtering and spam filtering.

In Transparent mode, you can access the web-based manager by connecting to an interface configured for administrative access and using HTTPS to access the management IP address. In the following examples, administrative access is enabled by default on the internal interface and the default management IP address is `10.11.0.1`.

Switching to Transparent mode

A VDOM is in NAT/Route mode by default when it is created. You must switch it to Transparent mode, and add a management IP address so you can access the VDOM from your management computer.

Before applying the change to Transparent mode, ensure the VDOM has administrative access on the selected interface, and that the selected management IP address is reachable on your network.

Switching the VDOM to Transparent mode cannot be done through the GUI. It must be done through the CLI only.

To switch the VDOM to Transparent mode - CLI:

```
config vdom
   edit <name>
      config system settings
         set opmode transparent
         set mangeip 10.11.0.99 255.255.255.0
      end
   end
```

Adding VLAN subinterfaces

There are a few differences when adding VLANs in Transparent mode compared to NAT/Route mode.

In Transparent mode, VLAN traffic is trunked across the VDOM. That means VLAN traffic cannot be routed, changed, or inspected. For this reason when you assign a VLAN to a Transparent mode VDOM, you will see the **Addressing Mode** section of the interface configuration disappear in from the web-based manager. It is

because with no routing, inspection, or any activities able to be performed on VLAN traffic the VDOM simply re-broadcasts the VLAN traffic. This requires no addressing.

Also any routing related features such as dynamic routing or Virtual Router Redundancy Protocol (VRRP) are not available in Transparent mode for any interfaces.

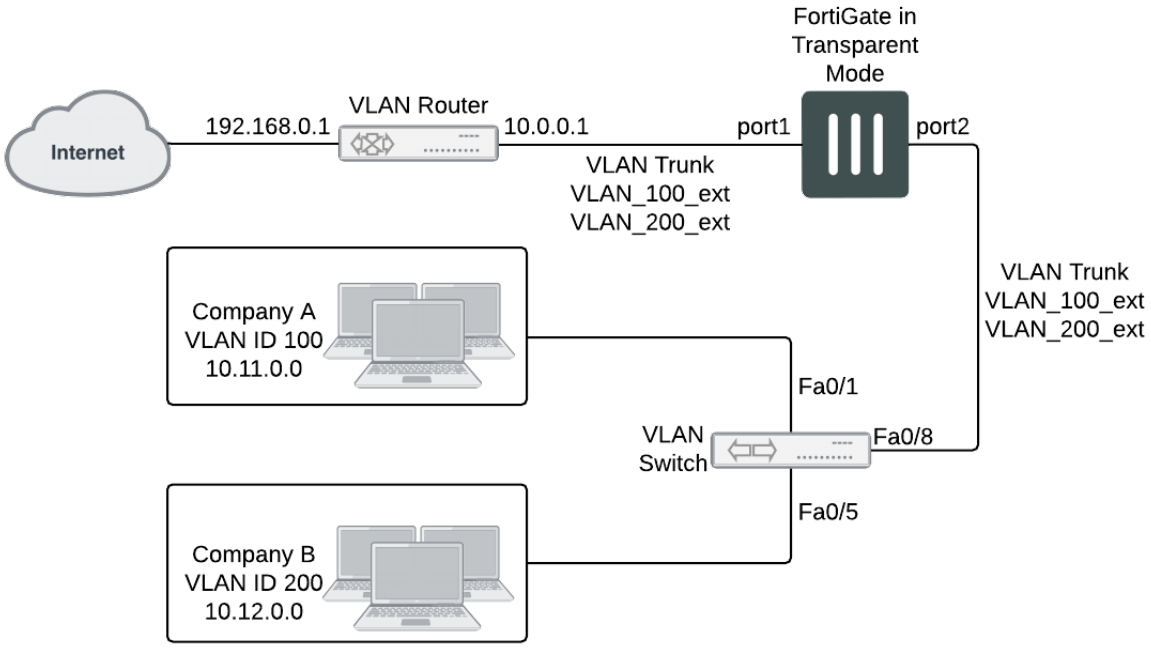
Creating security policies

Security policies permit communication between the FortiGate unit's network interfaces based on source and destination IP addresses. Typically you will also limit communication to desired times and services for additional security.

In Transparent mode, the FortiGate unit performs antivirus and antispam scanning on each packet as it passes through the unit. You need security policies to permit packets to pass from the VLAN interface where they enter the unit to the VLAN interface where they exit the unit. If there are no security policies configured, no packets will be allowed to pass from one interface to another.

For more information, see the Firewall handbook.

Example configuration: VDOM in Transparent mode



In this example, the FortiGate unit provides network protection to two organizations — Company A and Company B. Each company has different policies for incoming and outgoing traffic, requiring three different security policies and protection profiles.

VDOMs are not required for this configuration, but by using VDOMs the profiles and policies can be more easily managed on a per-VDOM basis either by one central administrator or separate administrators for each company. Also future expansion is simply a matter of adding additional VDOMs, whilst not disrupt the existing VDOMs.

For this example, firewalls are only included to deal with web traffic. This is to provide an example without making configuration unnecessarily complicated.

This example includes the following sections:

Network topology and assumptions

Each organization's internal network consists of a different range of IP addresses:

- 10.11.0.0/255.255.0.0 for Company A.
- 10.12.0.0/255.255.0.0 for Company B.

For the procedures in this section, it is assumed that you have enabled VDOM configuration on your FortiGate unit. For more information, see Virtual Domains Overview.

The VDOM names are similar to the company names for easy recognition. The root VDOM cannot be renamed and is not used in this example.

Interfaces used in this example are port1 and port2. Some FortiGate models may not have interfaces with these names. port1 is an external interface. port2 is an internal interface.

General configuration steps

The following steps summarize the configuration for this example. For best results, follow the procedures in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Configuring common items
2. Creating virtual domains
3. Configuring the Company_A VDOM
4. Configuring the Company_B VDOM
5. Configuring the VLAN switch and router
6. Testing the configuration

Configuring common items

Both VDOMs require you configure security profiles. These will be configured the same way, but need to be configured in both VDOMs.

The relaxed profile allows users to surf websites they are not allowed to visit during normal business hours. Also a quota is in place to restrict users to one hour of access to these websites to ensure employees do not take long and unproductive lunches.

To create a strict web filtering profile - web-based manager:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter**.
2. Select **Create New**.
3. Enter `strict` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for all Categories except Business Oriented, and Other.
5. Block all Classifications except Cached Content, and Image Search.
6. Ensure **FortiGuard Quota** for all Categories and Classifications is Disabled.
7. Select **OK**.

To create a strict web filtering profile - CLI:

```
config vdom
   edit <vdom_name>
      config webfilter profile
         edit strict
            config ftgd-wf
               set allow g07 g08 g21 g22 c01 c03
               set deny g01 g02 g03 g04 g05 g06 c02 c04 c05 c06 c07
            end
            set web-ftgd-err-log enable
         end
```

To create a relaxed web filtering profile - web-based manager:

1. Go to the proper VDOM, and select **Security Profiles > Web Filter**.
2. Select **Create New**.
3. Enter `relaxed` for the **Name**.
4. Expand FortiGuard Web Filtering, and select block for Potentially Security Violating Category, and Spam URL Classification.
5. Enable FortiGuard Quotas to allow 1 hour for all allowed Categories and Classifications.

Creating virtual domains

The FortiGate unit supports 10 virtual domains. Root is the default VDOM. It cannot be deleted or renamed. The root VDOM is not used in this example. New VDOMs are created for Company A and Company B

To create the virtual domains - web-based manager:

1. With VDOMs enabled, select **Global > System > VDOM**.
2. Select **Create New**.
3. Enter `Company_A` for Name, and select **OK**.
4. Select **Create New**.
5. Enter `Company_B` for Name, and select **OK**.

To create the virtual domains - CLI:

```
config system vdom
   edit Company_A
   next
   edit Company_B
end
```

Configuring the Company_A VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company_A VDOM.

This section includes the following topics:

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the port2 interface and another one on the port1 interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_100_int
Interface	port2
VLAN ID	100
Virtual Domain	Company_A

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_100_ext
Interface	port1
VLAN ID	100
Virtual Domain	Company_A

To add the VLAN subinterfaces - CLI:

```
config system interface
   edit VLAN_100_int
      set interface port2
```

```
      set vlanid 100
      set vdom Company_A
   next
   edit VLAN_100_ext
      set interface port1
      set vlanid 100
      set vdom Company_A
   end
```

Creating the Lunch schedule

Both organizations have the same lunch schedule, but only Company A has relaxed its security policy to allow employees more freedom in accessing the Internet during lunch. Lunch schedule will be Monday to Friday from 11:45am to 2:00pm (14:00).

To create a recurring schedule for lunchtime - web-based manager:

1. In Company_A VDOM, go to **Policy & Objects > Schedules**.
2. Select **Create New**.
3. Enter `Lunch` as the name for the schedule.
4. Select **Mon**, **Tues**, **Wed**, **Thu**, and **Fri**.
5. Set the **Start** time as `11:45` and set the **Stop** time as `14:00`.
6. Select **OK**.

To create a recurring schedule for lunchtime - CLI:

```
config vdom
   edit Company_A
      config firewall schedule recurring
         edit Lunch
            set day monday tuesday wednesday thursday friday
            set start 11:45
            set end 14:00
         end
```

Configuring Company_A firewall addresses

For Company A, its networks are all on the 10.11.0.0 network, so restricting addresses to that domain provides added security.

To configure Company_A firewall addresses - web-based manager:

1. In the Company_A VDOM, go to **Policy & Objects > Addresses**.
2. Select **Create New**.
3. Enter `CompanyA` in the **Address Name** field.
4. Type 10.11.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure vdomA firewall addresses - CLI:

```
config firewall address
   edit CompanyA
      set type ipmask
```

```
    set subnet 10.11.0.0 255.255.0.0
end
```

Creating Company_A security policies

A security policy can include varying levels of security feature protection. This example only deals with web filtering. The following security policies use the custom security `strict` and `relaxed` profiles configured earlier.

For these security policies, we assume that all protocols will be on their standard ports, such as port 80 for http traffic. If the ports are changed, such as using port 8080 for http traffic, you will have to create custom services for protocols with non-standard ports, and assign them different names.

The firewalls configured in this section are:

- internal to external — always allow all, security features - web filtering: strict
- internal to external — Lunch allow all, security features - web filtering:relaxed

Security policies allow packets to travel between the internal VLAN_100 interface to the external interface subject to the restrictions of the protection profile. Entering the policies in this order means the last one configured is at the top of the policy list, and will be checked first. This is important because the policies are arranged so if one does not apply the next is checked until the end of the list.

To configure Company_A security policies - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	CompanyA-lunch
Incoming Interface	VLAN_100_int
Outgoing Interface	VLAN_100_ext
Source Address	CompanyA
Destination Address	all
Schedule	Lunch
Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	relaxed

This policy provides relaxed protection during lunch hours — going from strict down to scan for protocol options and web filtering. AntiVirus and Email Filtering remain at strict for security — relaxing them would not provide employees additional access to the Internet and it would make the company vulnerable.

1. Select **Create New**.

2. Enter the following information and select **OK**:

Name	CompanyA-strict
Incoming Interface	VLAN_100_int
Outgoing Interface	VLAN_100_ext
Source Address	CompanyA
Destination Address	all
Schedule	always
Service	all
Action	ACCEPT
Security Features	enable
Web Filtering	strict

This policy enforces strict scanning at all times, while allowing all traffic. It ensures company policies are met for network security.

4. Verify that the policy list arranged **By Sequence** to make sure the CompanyA-lunch policy is located above the CompanyA-strict policy. If necessary, rearrange the policies so that the appropriate policy is applied to outgoing traffic.

To configure Company_A security policies - CLI:

```
config vdom
   edit Company_A
      config firewall policy
         edit 1
            set name "CompanyA-lunch"
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule Lunch
            set webfiltering relaxed
         next
         edit 2
            set name "CompanyA-strict"
            set srcintf VLAN_100_int
            set dstintf VLAN_100_ext
            set srcaddr all
            set dstaddr all
            set action accept
            set schedule always
            set webfiltering strict
         end
```

Configuring the Company_B VDOM

This section describes how to add VLAN subinterfaces and configure security policies for the Company B VDOM.

This section includes the following topics:

Adding VLAN subinterfaces

You need to create a VLAN subinterface on the internal interface and another one on the external interface, both with the same VLAN ID.

To add VLAN subinterfaces - web-based manager:

1. Go to **Network > Interfaces**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	VLAN_200_int
Interface	port2
VLAN ID	200
Virtual Domain	Company_B

4. Select **Create New**.
5. Enter the following information and select **OK**:

Name	VLAN_200_ext
Interface	port1
VLAN ID	200
Virtual Domain	Company_B

To add the VLAN subinterfaces - CLI:

```
config system interface
   edit VLAN_200_int
      set interface internal
      set vlanid 200
      set vdom Company_B
   next
   edit VLAN_200_ext
      set interface external
      set vlanid 200
      set vdom Company_B
```

```
end
```

Creating Company_B service groups

Company_B does not want its employees to use any online chat software except NetMeeting, which the company uses for net conferencing. To simplify the creation of a security policy for this purpose, you create a service group that contains all of the services you want to restrict. A security policy can manage only one service or one group.

To create a chat service group - web-based manager:

1. Go to **Policy & Objects > Services** and select **Create New > Service Group**.
2. Enter `Chat` in the **Group Name** field.
3. For each of IRC, AOL, SIP-MSNmessenger and TALK, select the service in the **Available Services** list and select the right arrow to add it to the **Members** list.

If a particular service does not appear in the **Available Services** list, see the list in **Policy & Objects > Services**. Some services do not appear by default unless edited.

4. Select **OK**.

To create a games and chat service group - CLI:

```
config firewall service group
   edit Chat
      set member IRC SIP-MSNmessenger AOL TALK
   end
```

Configuring Company_B firewall addresses

Company B's network is all in the 10.12.0.0 network. Security can be improved by only allowing traffic from IP addresses on that network.

To configure Company_B firewall address - web-based manager:

1. In the Company_B VDOM, go to **Policy & Objects > Addresses.**
2. Select **Create New**.
3. Enter `new` in the **Address Name** field.
4. Type 10.12.0.0/255.255.0.0 in the **Subnet / IP Range** field.
5. Select **OK**.

To configure Company_B firewall addresses - CLI:

```
config vdom
   edit Company_B
      config firewall address
         edit all
            set type ipmask
            set subnet 10.12.0.0 255.255.0.0
         end
```

Configuring Company_B security policies

Security policies allow packets to travel between the internal and external VLAN_200 interfaces subject to the restrictions of the protection profile.

To configure Company_B security policies - web-based manager:

1. Go to **Policy & Objects > IPv4 Policy**.
2. Select **Create New**.
3. Enter the following information and select **OK**:

Name	CompanyB-deny-games-chat
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	BusinessDay
Service	games-chat
Action	DENY

This policy prevents the use of network games or chat programs (except NetMeeting) during business hours.

4. Enter the following information and select **OK**:

Name	CompanyB-lunch
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	Lunch
Service	HTTP, DNS
Action	ACCEPT
Security Features	enable
Web Filter	relaxed

This policy relaxes the web category filtering during lunch hour.

5. Select **Create New**.
6. Enter the following information and select **OK**:

Name	CompanyB-strict

Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	BusinessDay
Service	HTTP, DNS
Action	ACCEPT
Security Profiles	enabled
Web Filter	strict

This policy provides rather strict web category filtering during business hours.

7. Select **Create New**.
8. Enter the following information and select **OK**:

Name	CompanyB-after-hours
Incoming Interface	VLAN_200_int
Outgoing Interface	VLAN_200_ext
Source Address	all
Destination Address	all
Schedule	always
Service	ANY
Action	ACCEPT
Security Profiles	enabled
Web Filter	relaxed

Because it is last in the list, this policy applies to the times and services not covered in preceding policies. This means that outside of regular business hours, the Relaxed protection profile applies to email and web browsing, and online chat and games are permitted. Company B needs this policy because its employees sometimes work overtime. The other companies in this example maintain fixed hours and do not want any after-hours Internet access.

To configure Company_B security policies - CLI:

```
config firewall policy
   edit 1
      set name "CompanyB-deny-games-chat"
      set srcintf VLAN_200_int
      set srcaddr all
```

```
    set dstintf VLAN_200_ext
    set dstaddr all
    set schedule BusinessDay
    set service Games
    set action deny
next
edit 2
    set name "CompanyB-lunch"
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule Lunch
    set service HTTP
    set profile_status enable
    set profile Relaxed
next
edit 3
    set name "CompanyB-strict"
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule BusinessDay
    set service HTTP
    set profile_status enable
    set profile BusinessOnly
next
edit 4
    set name "CompanyB-after-hours"
    set srcintf VLAN_200_int
    set srcaddr all
    set dstintf VLAN_200_ext
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set profile_status enable
    set profile Relaxed
end
```

Configuring the VLAN switch and router

The Cisco switch is the first VLAN device internal passes through, and the Cisco router is the last device before the Internet or ISP.

This section includes the following topics:

- Configuring the Cisco switch
- Configuring the Cisco router

Configuring the Cisco switch

On the Cisco Catalyst 2900 ethernet switch, you need to define the VLANs 100, 200 and 300 in the VLAN database, and then add configuration files to define the VLAN subinterfaces and the 802.1Q trunk interface.

Add this file to Cisco VLAN switch:

```
!
interface FastEthernet0/1
switchport access vlan 100
!
interface FastEthernet0/5
switchport access vlan 300
!
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
!
```

Switch 1 has the following configuration:

Port 0/1	VLAN ID 100
Port 0/3	VLAN ID 200
Port 0/6	802.1Q trunk

Configuring the Cisco router

The configuration for the Cisco router in this example is the same as in the basic example, except we add VLAN_ 300. Each of the three companies has its own subnet assigned to it.

The IP addressees assigned to each VLAN on the router are the gateway addresses for the VLANs. For example, devices on VLAN_100 would have their gateway set to 10.11.0.1/255.255.0.0.

```
!
interface FastEthernet0/0
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/0.1
 encapsulation dot1Q 100
 ip address 10.11.0.1 255.255.0.0
!
interface FastEthernet0/0.3
 encapsulation dot1Q 200
 ip address 10.12.0.1 255.255.0.0
!
```

The router has the following configuration:

Port 0/0.1	VLAN ID 100
Port 0/0.3	VLAN ID 200
Port 0/0	802.1Q trunk

Testing the configuration

Use diagnostic commands, such as tracert, to test traffic routed through the network.

You should test traffic between the internal VLANs as well as from the internal VLANs to the Internet to ensure connectivity.

For additional troubleshooting, see Troubleshooting Virtual Domains.

This section includes the following topics:

- Testing traffic from VLAN_100 to the Internet
- Testing traffic from VLAN_100 to VLAN_200

Testing traffic from VLAN_100 to the Internet

In this example, a route is traced from VLANs to a host on the Internet. The route target is www.example.com.

From a host on VLAN_100, access a command prompt and enter this command:

```
C:\>tracert www.example.com
Tracing route to www.example.com [208.77.188.166]
over a maximum of 30 hops:
 1 <10 ms <10 ms <10 ms 10.100.0.1
...
14 172 ms 141 ms 140 ms 208.77.188.166
Trace complete.
```

The number of steps between the first and the last hop, as well as their IP addresses, will vary depending on your location and ISP. However, all successful tracerts to www.example.com will start and end with these lines.

Repeat the tracert for VLAN_200.

The tracert for each VLAN will include the gateway for that VLAN as the first step. Otherwise, the tracert should be the same for each VLAN.

Testing traffic from VLAN_100 to VLAN_200

In this example, a route is traced between two internal networks. The route target is a host on VLAN_200. The Windows traceroute command `tracert` is used.

From VLAN_100, access a Windows command prompt and enter this command:

```
C:\>tracert 10.12.0.2
Tracing route to 10.12.0.2 over a maximum of 30 hops:
1 <10 ms <10 ms <10 ms 10.100.0.1
2 <10 ms <10 ms <10 ms 10.12.0.2
Trace complete.
```

You can repeat this for different routes in the topology. In each case the IP addresses will be the gateway for the starting VLAN, and the end point at the ending VLAN.

Inter-VDOM routing

Inter-VDOM routing changes this allows VDOMs to communicate internally without using additional physical interfaces, using VDOM links. VDOM links are virtual interfaces that connect VDOMs. A VDOM link contains a pair of interfaces with each one connected to a VDOM, and forming either end of the inter-VDOM connection.

This chapter contains the following sections:

Benefits of inter-VDOM routing

Inter-VDOM routing has a number of advantages over independent VDOM routing. These benefits include:

Freed-up physical interfaces

Tying up physical interfaces on the FortiGate unit presents a problem. With a limited number of interfaces available, configuration options for the old style of communication between VDOMs are very limited. VLANs can be an answer to this, but they have some limitations.

For example, the FortiGate-800 has 8 physical ethernet ports. If they are assigned 2 per VDOM (one each for external and internal traffic) there can only be 4 VDOMs at most configured, not the 10 VDOMs the license will allow. Adding even one additional interface per VDOM to be used to communicate between VDOMs leaves only 2 VDOMs for that configuration, since it would required 9 interfaces for 3 VDOMs. Even using one physical interface for both external traffic and inter-VDOM communication would severely lower the available bandwidth for external traffic on that interface.

With the introduction of inter-VDOM routing, traffic can travel between VDOMs internally, freeing up physical interfaces for external traffic. Using the above example we can use the 4 VDOM configuration and all the interfaces will have their full bandwidth.

More speed than physical interfaces

Internal interfaces are faster than physical interfaces. Their speed depends on the FortiGate unit CPU and its load. That means that an inter-VDOM link interface will be faster than a outbound physical interface connected to another inbound physical interface.

However, while one virtual interface with normal traffic would be considerably faster than on a physical interface, the more traffic and more internal interfaces you configure, the slower they will become until they are slower than the physical interfaces. CPU load can come from other sources such as AV or content scanning. This produces the same effect—internal interfaces such as inter-VDOM links will be slower.

Continued support for secure firewall policies

VDOMs help to separate traffic based on your needs. This is an important step in satisfying regulations that require proof of secure data handling. This is especially important to health, law, accounting, and other businesses that handle sensitive data every day.

By keeping things separate, traffic has to leave the FortiGate unit and re-enter to change VDOMs. This forces traffic to go through the firewall when leaving and enter through another firewall, keeping traffic secure.

With inter-VDOM routing, the need for the physical interfaces is greatly reduced. However, firewall policies still need to be in place for traffic to pass through any interface, physical or virtual, and thus provide the same level of security both internally and externally. Configuration of firewall policies is the same for inter-VDOM links as for any other interface, and your data will continue to have the high level of security.

Configuration flexibility

A typical VDOM uses at least two interfaces, typically physical interfaces, one for internal and one for external traffic. Depending on the configuration, more interfaces may be required. This means that the maximum number of VDOMs configurable on a FortiGate unit using physical interfaces is the number of interfaces available divided by two. VLANs can increase the number by providing multiple virtual interfaces over a single physical interface, but VLANs have some limitations. Using physical interfaces for inter-VDOM communication therefore limits the number of possible configurations on your FortiGate unit.

To overcome this limitation, inter-VDOM links can be created within the FortiGate unit. Using virtual interfaces, inter-VDOM links free up the physical interfaces for external traffic. Using VDOM links on a FortiGate unit with 8 physical interfaces, you can have 4 VDOMs communicating with each other (meshed configuration) and continue to have 2 physical interfaces each for internal and external connections. This configuration would have required 20 physical interfaces without inter-VDOM routing. With inter-VDOM routing it only requires 8 physical interfaces, with the other 12 interfaces being internal VDOM links.

Inter-VDOM routing allows you to make use of standalone VDOMs, Management VDOMs, and Meshed VDOMs without being limited by the number of physical interfaces on your FortiGate unit. For more information about these types of VDOMs, see "Inter-VDOM configurations" on page 63.

Inter-VDOM configurations

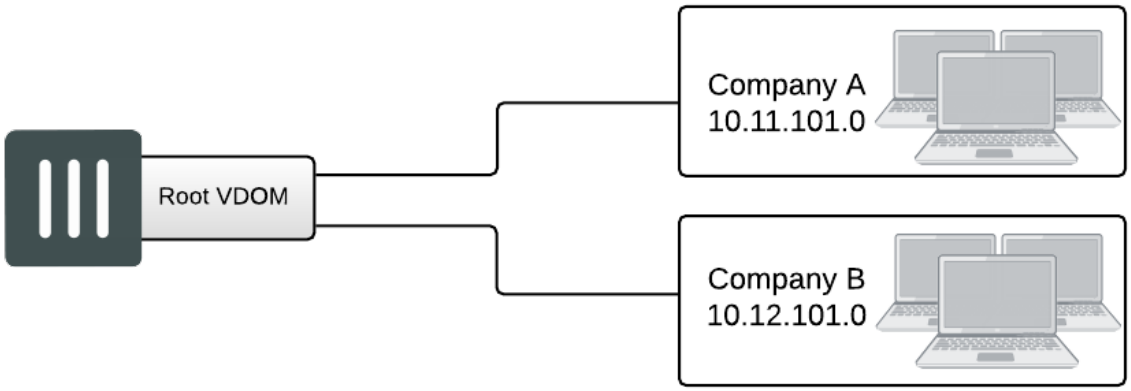
By using fewer physical interfaces to inter-connect VDOMs, inter-VDOM links provide you with more configuration options.

None of these configurations use VLANs to reduce the number of physical interfaces. It is generally assumed that an internal or client network will have its own internal interface and an external interface to connect to its ISP and the Internet.

These inter-VDOM configurations can use any FortiGate model with possible limitations based on the number of physical interfaces. VLANs can be used to work around these limitations.

There are four different types of inter-VDOM configurations:

Standalone VDOM



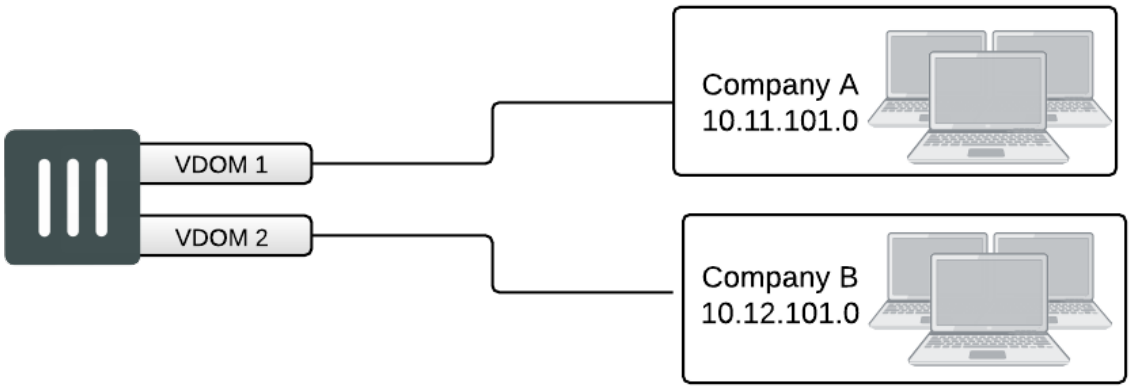
The standalone VDOM configuration uses a single VDOM on your FortiGate unit — the root VDOM that all FortiGate units have by default. This is the VDOM configuration you are likely familiar with. It is the default configuration for FortiGate units before you create additional VDOMs.

The configuration shown above has no VDOM inter-connections and requires no special configurations or settings.

The standalone VDOM configuration can be used for simple network configurations that only have one department or one company administering the connections, firewalls and other VDOM-dependent settings.

However, with this configuration, keeping client networks separate requires many interfaces, considerable firewall design and maintenance, and can quickly become time consuming and complex. Also, configuration errors for one client network can easily affect other client networks, causing unnecessary network downtime.

Independent VDOMs



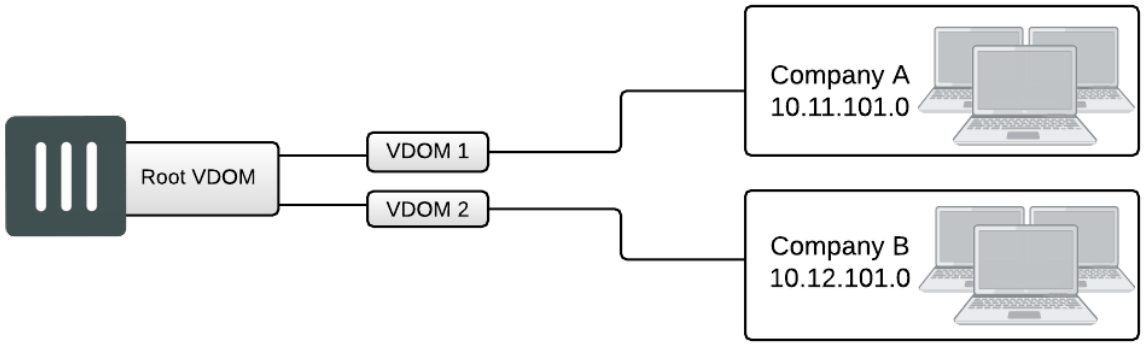
The independent VDOMs configuration uses multiple VDOMs that are completely separate from each other. This is another common VDOM configuration.

This configuration has no communication between VDOMs and apart from initially setting up each VDOM, it requires no special configurations or settings. Any communication between VDOMs is treated as if communication is between separate physical devices.

The independent inter-VDOM configuration can be used where more than one department or one company is sharing the FortiGate unit. Each can administer the connections, firewalls and other VDOM-dependent settings for only its own VDOM. To each company or department, it appears as if it has its own FortiGate unit. This configuration reduces the amount of firewall configuration and maintenance required by dividing up the work.

However, this configuration lacks a management VDOM for VDOMs 1, 2, and 3. This is illustrated in Figure 50. This management VDOM would enable an extra level of control for the FortiGate unit administrator, while still allowing each company or department to administer its own VDOM.

Management VDOM



In the management VDOM configuration, the root VDOM is the management VDOM. The other VDOMs are connected to the management VDOM with inter-VDOM links. There are no other inter-VDOM connections.

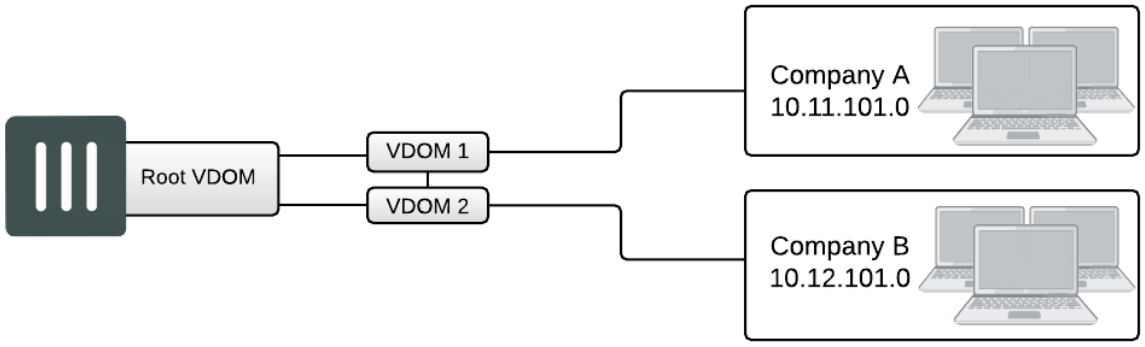
The inter-VDOM links connect the management VDOM to the other VDOMs. This does not require any physical interfaces, and the bandwidth of inter-VDOM links can be faster than physical interfaces, depending on the CPU workload.

Only the management VDOM is connected to the Internet. The other VDOMs are connected to internal networks. All external traffic is routed through the management VDOM using inter-VDOM links and firewall policies between the management VDOM and each VDOM. This ensures the management VDOM has full control over access to the Internet, including what types of traffic are allowed in both directions. There is no communication directly between the non-root VDOMs. Security is greatly increased with only one point of entry and exit. Only the management VDOM needs to be fully managed to ensure network security in this case. Each client network can manage its own configuration without compromising security or bringing down another client network.

The management VDOM configuration is ideally suited for a service provider business. The service provider administers the management VDOM with the other VDOMs as customers. These customers do not require a dedicated IT person to manage their network. The service provider controls the traffic and can prevent the customers from using banned services and prevent Internet connections from initiating those same banned services. One example of a banned service might be Instant Messaging (IM) at a company concerned about intellectual property. Another example could be to limit bandwidth used by file-sharing applications without banning that application completely. Firewall policies control the traffic between the customer VDOM and the management VDOM and can be customized for each customer.

The management VDOM configuration is limited in that the customer VDOMs have no inter-connections. In many situations this limitation is ideal because it maintains proper security. However, some configurations may require customers to communicate with each other, which would be easier if the customer VDOMs were inter-connected.

Meshed VDOM



The meshed VDOMs configuration, including partial and full mesh, has VDOMs inter-connected with other VDOMs. There is no special feature to accomplish this—they are just complex VDOM configurations.

Partial mesh means only some VDOMs are inter-connected. In a full mesh configuration, all VDOMs are inter-connected to all other VDOMs. This can be useful when you want to provide full access between VDOMs but handle traffic differently depending on which VDOM it originates from or is going to.

With full access between all VDOMs being possible, it is extra important to ensure proper security. You can achieve this level of security by establishing extensive firewall policies and ensuring secure account access for all administrators and users.

Meshed VDOM configurations can become complex very quickly, with full mesh VDOMs being the most complex. Ensure this is the proper solution for your situation before using this configuration. Generally, these configurations are seen as theoretical and are rarely deployed in the field.

Configuring VDOM links

Once VDOMs are configured on your FortiGate unit, configuring inter-VDOM routing and VDOM-links is very much like creating a VLAN interface. VDOM-links are managed through the web-based manager or CLI. In the web-based manager, VDOM link interfaces are managed in the network interface list.

This section includes the following topics:

Creating VDOM links

VDOM links connect VDOMs together to allow traffic to pass between VDOMs as per firewall policies. Inter-VDOM links are virtual interfaces that are very similar to VPN tunnel interfaces except inter-VDOM links do not require IP addresses.

To create a VDOM link, you first create the point-to-point interface, and then bind the two interface objects associated with it to the virtual domains.

In creating the point-to-point interface, you also create two additional interface objects by default. They are called `vlink10` and `vlink11` - the interface name you chose with a 1 or a 0 to designate the two ends of the link.

Once the interface objects are bound, they are treated like normal FortiGate interfaces and need to be configured just like regular interfaces.

The assumptions for this example are as follows:

- Your FortiGate unit has VDOMs enabled and you have 2 VDOMs called `customer1` and `customer2` already configured. For more information on configuring VDOMs see Configuring Virtual Domains.
- You are using a super_admin account.

To configure an inter-VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Create New > VDOM link**, enter the following information, and select **OK**.

Name	vlink1 (The name can be up to 11 characters long. Valid characters are letters, numbers, “-”, and “_”. No spaces are allowed.)
Interface #0	

	Virtual Domain	customer1
	IP/Netmask	10.11.12.13/255.255.255.0
	Administrative Access	HTTPS, SSL
Interface #1		
	Virtual Domain	customer2
	IP/Netmask	172.120.100.13/255.255.255.0
	Administrative Access	HTTPS, SSL

To configure an inter-VDOM link - CLI:

```
config global
   config system vdom-link
      edit vlink1
      end
   config system interface
      edit vlink10
         set vdom customer1
      next
      edit vlink11
         set vdom customer2
      end
```

Once you have created and bound the interface ends to VDOMs, configure the appropriate firewall policies and other settings that you require. To confirm the inter-VDOM link was created, find the VDOM link pair and use the expand arrow to view the two VDOM link interfaces. You can select edit to change any information.

IP addresses and inter-VDOM links

Besides being virtual interfaces, here is one main difference between inter-VDOM links and regular interfaces—default inter-VDOM links do not require IP addresses. IP addresses are not required by default because an inter-VDOM link is an internal connection that can be referred to by the interface name in firewall policies, and other system references. This introduces three possible situations with inter-VDOM links that are:

- **unnumbered** - an inter-VDOM link with no IP addresses for either end of the tunnel
- **half numbered** - an inter-VDOM link with one IP address for one end and none for the other end
- **full numbered** - an inter-VDOM link with two IP addresses, one for each end.

Not using an IP address in the configuration can speed up and simplify configuration for you. Also you will not use up all the IP addresses in your subnets if you have many inter-VDOM links.

Half or full numbered interfaces are required if you are doing NAT, either SNAT or DNAT as you need an IP number on both ends to translate between.

You can use unnumbered interfaces in static routing, by naming the interface and using `0.0.0.0` for the gateway. Running traceroute will not show the interface in the list of hops. However you can see the interface when you are sniffing packets, which is useful for troubleshooting.

Deleting VDOM links

When you delete the VDOM link, the two link objects associated with it will also be deleted. You cannot delete the objects by themselves. The example uses a VDOM routing connection called “vlink1”. Removing vlink1 will also remove its two link objects vlink10 and vlink11.

Before deleting the VDOM link, ensure all policies, firewalls, and other configurations that include the VDOM link are deleted, removed, or changed to no longer include the VDOM link.

To remove a VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Delete** for the VDOM link **vlink1**.

To remove a VDOM link - CLI:

```
config global
   config system vdom-link
      delete vlink1
   end
```

NAT to Transparent VDOM links

Inter-VDOM links can be created between VDOMs in NAT mode and VDOMs in Transparent mode, but it must be done through the CLI, as the VDOM link type must be changed from the default PPP to Ethernet for the two VDOMs to communicate. The below example assumes one vdom is in NAT mode and one is Transparent.

An IP address must be assigned to the NAT VDOM’s interface, but no IP address should be assigned to the Transparent VDOM’s interface.

To configure a NAT to Transparent VDOM link - CLI:

```
config global
   config system vdom-link
      edit vlink1
      set type ethernet
      end
   config system interface
      edit vlink10
         set vdom (interface 1 name)
         set ip (interface 1 ip)
      next
      edit vlink11
         set vdom (interface 2 name)
      end
```

Ethernet-type is not recommended for standard NAT to NAT inter-VDOM links, as the default PPP-type link does not require the VDOM links to have addresses, while Ethernet-type does. VDOM link addresses are explained in IP addresses and inter-VDOM links.

Dynamic routing over inter-VDOM links

BGP is supported over inter-VDOM links. Unless otherwise indicated, routing works as expected over inter-VDOM links.

If an inter-VDOM link has no assigned IP addresses to it, it may be difficult to use that interface in dynamic routing configurations. For example BGP requires an IP address to define any BGP router added to the network.

In OSPF, you can configure a router using a router ID and not its IP address. In fact, having no IP address avoids possible confusing between which value is the router ID and which is the IP address. However for that router to become adjacent with another OSPF router it will have to share the same subnet, which is technically impossible without an IP address. For this reason, while you can configure an OSPF router using an IP-less inter-VDOM link, it will likely be of limited value to you.

In RIP the metric used is hop count. If the inter-VDOM link can reach other nodes on the network, such as through a default route, then it may be possible to configure a RIP router on an inter-VDOM link. However, once again it may be of limited value due to limitations.

As stated earlier, BGP requires an IP address to define a router — an IP-less inter-VDOM link will not work with BGP.

In Multicast, you can configure an interface without using an IP address. However that interface will be unable to become an RP candidate. This limits the roles available to such an interface.

HA virtual clusters and VDOM links

FortiGate HA is implemented by configuring two or more FortiGate units to operate as an HA cluster. To the network, the HA cluster appears to function as a single FortiGate unit, processing network traffic and providing normal security services such as firewall, VPN, IPS, virus scanning, web filtering, and spam filtering.

Virtual clustering extends HA features to provide failover protection and load balancing for a FortiGate unit operating with virtual domains. A virtual cluster consists of a cluster of two FortiGate units operating with virtual domains. Traffic on different virtual domains can be load balanced between the cluster units.

With virtual clusters (vclusters) configured, inter-VDOM links must be entirely within one vcluster. You cannot create links between vclusters, and you cannot move a VDOM that is linked into another virtual cluster. If your FortiGate units are operating in HA mode, with multiple vclusters when you create the vdom-link, the CLI command `config system vdom-link` includes an option to set which vcluster the link will be in.

What is virtual clustering?

Virtual clustering is an extension of the FGCP for FortiGate units operating with multiple VDOMS enabled. Virtual clustering operates in active-passive mode to provide failover protection between two instances of a VDOM operating on two different cluster units. You can also operate virtual clustering in active-active mode to use HA load balancing to load balance sessions between cluster units. Alternatively, by distributing VDOM processing between the two cluster units you can also configure virtual clustering to provide load balancing by distributing sessions for different VDOMs to each cluster unit.

Virtual clustering and failover protection

Virtual clustering operates on a cluster of two (and only two) FortiGate units with VDOMs enabled. Each VDOM creates a cluster between instances of the VDOMs on the two FortiGate units in the virtual cluster. All traffic to and from the VDOM stays within the VDOM and is processed by the VDOM. One cluster unit is the primary unit for each VDOM and one cluster unit is the subordinate unit for each VDOM. The primary unit processes all traffic for the VDOM. The subordinate unit does not process traffic for the VDOM. If a cluster unit fails, all traffic fails over to the cluster unit that is still operating.

Virtual clustering and heartbeat interfaces

The HA heartbeat provides the same HA services in a virtual clustering configuration as in a standard HA configuration. One set of HA heartbeat interfaces provides HA heartbeat services for all of the VDOMs in the cluster. You do not have to add a heartbeat interface for each VDOM.

Virtual clustering and HA override

For a virtual cluster configuration, override is enabled by default for both virtual clusters when you:

- Enable VDOM portioning from the web-based manager by moving virtual domains to virtual cluster 2
- Enter set vcluster2 enable from the CLI config system ha command to enable virtual cluster 2.

Usually you would enable virtual cluster 2 and expect one cluster unit to be the primary unit for virtual cluster 1 and the other cluster unit to be the primary unit for virtual cluster 2. For this distribution to occur override must be enabled for both virtual clusters. Otherwise you will need to restart the cluster to force it to renegotiate.

Virtual clustering and load balancing or VDOM partitioning

There are two ways to configure load balancing for virtual clustering. The first is to set the HA mode to active-active. The second is to configure VDOM partitioning. For virtual clustering, setting the HA Mode to active-active has the same result as active-active HA for a cluster without virtual domains. The primary unit receives all sessions and load balances them among the cluster units according to the load balancing schedule. All cluster units process traffic for all virtual domains.

Note: If override is enabled the cluster may renegotiate too often. You can choose to disable override at any time. If you decide to disable override, for best results, you should disable it for both cluster units.

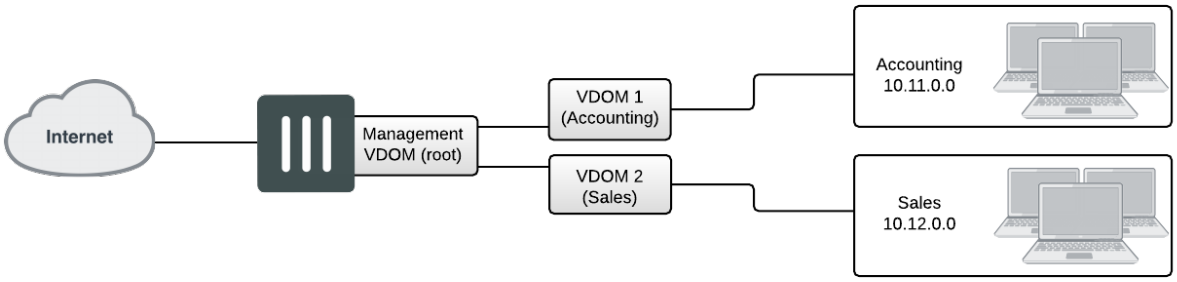
In a VDOM partitioning virtual clustering configuration, the HA mode is set to active-passive. Even though virtual clustering operates in active-passive mode you can configure a form of load balancing by using VDOM partitioning to distribute traffic between both cluster units. To configure VDOM partitioning you set one cluster unit as the primary unit for some virtual domains and you set the other cluster unit as the primary unit for other virtual domains. All traffic for a virtual domain is processed by the primary unit for that virtual domain. You can control the distribution of traffic between the cluster units by adjusting which cluster unit is the primary unit for each virtual domain.

For example, you could have 4 VDOMs, two of which have a high traffic volume and two of which have a low traffic volume. You can configure each cluster unit to be the primary unit for one of the high volume VDOMs and one of the low volume VDOMs. As a result each cluster unit will be processing traffic for a high volume VDOM and a low volume VDOM, resulting in an even distribution of traffic between the cluster units. You can adjust the distribution at any time. For example, if a low volume VDOM becomes a high volume VDOM you can move it from one cluster unit to another until the best balance is achieved. From the web-based manager you configure VDOM partitioning by setting the HA mode to active-passive and distributing virtual domains between Virtual Cluster 1 and Virtual Cluster 2. You can also configure different device priorities, port monitoring, and remote link failover, for Virtual Cluster 1 and Virtual Cluster 2.

From the CLI you configure VDOM partitioning by setting the HA mode to a-p. Then you configure device priority, port monitoring, and remote link failover and specify the VDOMs to include in virtual cluster 1. You do the same for virtual cluster 2 by entering the config secondary-vcluster command.

Failover protection does not change. If one cluster unit fails, all sessions are processed by the remaining cluster unit. No traffic interruption occurs for the virtual domains for which the still functioning cluster unit was the primary unit. Traffic may be interrupted temporarily for virtual domains for which the failed unit was the primary unit while processing fails over to the still functioning cluster unit. If the failed cluster unit restarts and rejoins the virtual cluster, VDOM partitioning load balancing is restored.

Example configuration: Inter-VDOM routing



This example shows how to configure a FortiGate unit to use inter-VDOM routing.

This section contains the follow topics:

Network topology and assumptions

Two departments of a company, Accounting and Sales, are connected to one FortiGate 800 unit. To do its work, the Sales department receives a lot of email from advertising companies that would appear to be spam if the Accounting department received it. For this reason, each department has its own VDOM to keep firewall policies and other configurations separate. A management VDOM makes sense to ensure company policies are followed for traffic content.

The traffic between Accounting and Sales will be email and HTTPS only. It could use a VDOM link for a meshed configuration, but we will keep from getting too complex. With the configuration, inter-VDOM traffic will have a slightly longer path to follow than normal—from one department VDOM, through the management VDOM, and back to the other department VDOM. Since inter-VDOM links are faster than physical interfaces, this longer path should not be noticed.

Firewall policies will be in place. For added security, firewall policies will allow only valid office services such as email, web browsing, and FTP between either department and the Internet. Any additional services that are required can be added in the future.

The company uses a single ISP to connect to the Internet. The ISP uses DHCP to provide an IP address to the FortiGate unit. Both departments use the same ISP to reach the Internet.

Other assumptions for this example are as follows:

- Your FortiGate unit has interfaces labelled port1 through port4 and VDOMs are not enabled.
- You are using the super_admin account.
- You have the FortiClient application installed.
- You are familiar with configuring interfaces, firewalls, and other common features on your FortiGate unit.

General configuration steps

This example includes the following general steps. For best results, follow the steps in the order given. Also, note that if you perform any additional actions between procedures, your configuration may have different results.

1. Creating the VDOMs
2. Configuring the physical interfaces
3. Configuring the VDOM links
4. Configuring the firewall and Security Profile settings
5. Testing the configuration

Creating the VDOMs

This procedure enables VDOMs and creates the Sales and Accounting VDOMs.

To create the VDOMs - web-based manager:

1. Log in as the super_admin administrator.
2. Go to the **Dashboard** and locate the **System Information** widget. Enable **Virtual Domain**.
3. Log in again.
4. Go to **Global > System > VDOM**.
5. Select **Create New**, enter `Accounting` for the VDOM Name, and select **OK**.
6. Select **Create New**, enter `Sales` for the VDOM Name, and select **OK**.

To create the VDOMs - CLI:

```
config system global
   set vdom enable
end
config system vdom
   edit Accounting
   next
   edit Sales
   next
end
```

Configuring the physical interfaces

Next, the physical interfaces must be configured. This example uses three interfaces on the FortiGate unit - port2 (internal), port3(dmz), and port1(external). port2 and port3 interfaces each have a department's network connected. port1 is for all traffic to or from the Internet and will use DHCP to configure its IP address, which is common with many ISPs.

To configure the physical interfaces - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select **Edit** for the port2 interface, enter the following information, and select **OK.**

Alias	AccountingLocal
Virtual Domain	Accounting
Addressing mode	Manual
IP/Netmask	172.100.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the accounting department internal interface.

3. Select **Edit** for the port3 interface, enter the following information, and select **OK**.

Alias	SalesLocal
Virtual Domain	Sales
Addressing mode	Manual
IP/Netmask	192.168.1.1/255.255.0.0
Administrative Access	HTTPS, PING, SSH
Description	This is the sales department internal interface.

4. Select **Edit** for the port1 interface, enter the following information, and select **OK**.

Alias	ManagementExternal
Virtual Domain	root
Addressing Mode	DHCP
Distance	5
Retrieve default gateway from server	Enable
Override internal DNS	Enable

Administrative Access	HTTPS, SSH, SNMP
Description	This is the accounting department internal interface.

When the mode is set to DHCP or PPoE on an interface you can set the distance field. This is the administrative distance for any routes learned through the gateway for this interface. The gateway is added to the static route table with these values. A lower distance indicates a preferred route.

To configure the physical interfaces - CLI:

```
config global
   config system interface
      edit port2
         set alias AccountingLocal
         set vdom Accounting
         set mode static
         set ip 172.100.1.1 255.255.0.0
         set allowaccess https ping ssh
         set description "The accounting dept internal interface"
      next
      edit port3
         set alias SalesLocal
         set vdom Sales
         set mode static
         set ip 192.168.1.1 255.255.0.0
         set allowaccess https ping ssh
         set description "The sales dept. internal interface"
      next
      edit port1
         set alias ManagementExternal
         set vdom root
         set mode DHCP
         set distance 5
         set gwdetect enable
         set dns-server-override enable
         set allowaccess https ssh snmp
         set description "The systemwide management interface."
      end
```

Configuring the VDOM links

To complete the connection between each VDOM and the management VDOM, you need to add the two VDOM links; one pair is the Accounting - management link and the other is for Sales - management link.

When configuring inter-VDOM links, you do not have to assign IP addresses to the links unless you are using advanced features such as dynamic routing that require them. Not assigning IP addresses results in faster configuration, and more available IP addresses on your networks.

If you require them, or if you simply want to assign IP addresses for clarity can do so.

To configure the Accounting and management VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select the expand arrow to select **Create New > VDOM link**.
3. Enter the following information, and select **OK**.

Name		AccountVlnk
Interface #0		
	Virtual Domain	Accounting
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Accounting VDOM side of the link.
Interface #1		
	Virtual Domain	root
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Management VDOM side of the link.

To configure the Accounting and management VDOM link - CLI:

```
config global
   config system vdom-link
      edit AccountVlnk
      next
   end
   config system interface
      edit AccountVlnk0
         set vdom Accounting
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Accounting side of the VDOM link"
      next
      edit AccountVlnk1
         set vdom root
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Management side of the VDOM link"
      end
```

To configure the Sales and management VDOM link - web-based manager:

1. Go to **Global > Network > Interfaces**.
2. Select the expand arrow and select **Create New > VDOM link**.

3. Enter the following information, and select **OK**.

Name		SalesVlnk
Interface #0		
	Virtual Domain	Sales
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Sales VDOM side of the link.
Interface #1		
	Virtual Domain	root
	IP/Netmask	0.0.0.0/0.0.0.0
	Administrative Access	HTTPS, PING, SSH
	Description	The Management VDOM side of the link.

To configure the Sales and management VDOM link - CLI:

```
config global
   config system vdom-link
      edit SalesVlnk
   end
   config system interface
      edit SalesVlnk0
         set vdom Accounting
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Sales side of the VDOM link"
      next
      edit SalesVlnk1
         set vdom root
         set ip 0.0.0.0 0.0.0.0
         set allowaccess https ping ssh
         set description "Management side of the VDOM link"
      end
   end
```

Configuring the firewall and Security Profile settings

With the VDOMs, physical interfaces, and VDOM links configured the firewall must now be configured to allow the proper traffic. Firewalls are configured per-VDOM, and firewall objects must be created for each VDOM separately.

For this example, the firewall group of services allowed between the internal networks and the Internet are the basic services for web browsing, file transfer, and email. These include: HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, and SMTP.

The only services allowed between Sales and Accounting are secure web browsing (HTTPS) and email (POP3 and SMTP).

The limited number of services ensures security between departments. The list of services can be expanded in the future if needed.

Security profile settings will block all non-essential business websites while logging all web traffic, scan and file filter all web and email protocols, and block game and peer-to-peer applications using application control.

For added security, FortiClient is required on internal computers with AntiVirus scanning configured. This is enforced by **Endpoint NAC** in firewall policies.

Using firewall addresses makes the firewall policies easier to read. Also if any changes need to be made in the future, you can simply update the addresses without changing the firewall policies. The addresses required are:

- `AccountingLocal` - all traffic from the internal accounting network
- `AccountingVlnk` - all traffic from the VDOM link between accounting and management VDOMs
- `SalesLocal` - all traffic from the internal sales network
- `SalesVlnk` - all traffic from the VDOM link between sales and management VDOM.

The Accounting VDOM requires `AccountingLocal`, `AccountingVlnk`, and `SalesLocal`. The Sales VDOM requires `SalesLocal`, `SalesVlnk`, and `AccountingLocal`.

This section includes the following topics:

Configuring firewall service groups

Service groups are an easy way to manage multiple services, especially if the same services are used on different networks.

The two service groups used here are intended for normal office traffic to the Internet, and for restricted traffic between departments. In both cases network traffic will be limited to the services listed to prevent any potential security risks or bandwidth-robbing applications.

These service groups can be changed as needed to either include additional valid services that are being used on the network, or to exclude services that are not required. Also, custom services can be created as needed for applications that are not listed.

To configure two firewall service groups - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Policy & Objects > Services** and select **Create New > Service Group.**
3. Select **Create New**, enter the following information, and select **OK.**

Group Name	OfficeServices
Members	HTTP, HTTPS, SSL, FTP, DNS, NTP, POP3, PING, SMTP

4. Select **Create New**, enter the following information, and select **OK**.

Group Name	AccountingSalesServices
Members	HTTPS, POP3, PING, SMTP

To configure two firewall service groups - CLI:

```
config vdom
   edit Accounting
      config firewall service group
         edit OfficeServices
            set member HTTP HTTPS SSH FTP DNS NTP POP3 PING SMTP
         next
         edit AccountingSalesServices
            set member HTTPS POP3 PING SMTP
         end
   end
```

Configuring Security Profile settings for the Accounting VDOM

Security Profile settings include web filtering, antivirus, application control, and other features. This example just uses those three features to ensure that

- the business environment is free from viruses
- employees do not surf grossly inappropriate websites, and
- employees do not use games or peer-to-peer applications at work.

To configure web filtering for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Web Filter**.
3. Select **Create New**.
4. Enter `webStrict` for the **Name**.
5. Select the arrow to expand the **FortiGuard Web Filtering** section.
6. Block all **Categories** except Business Oriented, Other, and Unrated.
7. Block all **Classifications** except Image Search..
8. Log all **Categories** and **Classifications**.
9. Select **OK**.

To configure AntiVirus for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > AntiVirus**.
3. Select **Create New**.
4. Enter `avStrict` for the **Name**.
5. Set **Detect Virues** to **Block** and enable all **Inspected Protocols**.
6. Select **OK**.

To configure application control for the Accounting VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Application Control.**
3. Select **Create New** (+ button at top right of page).
4. Enter `appStrict` for **Name** and select OK.
5. Select **Create New**.
6. In **Filters**, set **Category** to **game**.
7. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

8. Select **Create New**.
9. In **Filters**, set **Category** to **p2p**.
10. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

11. Select **Apply**.

To configure application control for the Accounting VDOM - CLI:

```
config vdom
   edit Accounting
      config application list
         edit appStrict
            config entries
               edit 1
                  set category 2
               next
               edit 2
                  set category 8
               end
         end
   end
```

Configuring firewall settings for the Accounting VDOM

This configuration includes two firewall addresses and two firewall policies for the Accounting VDOM - one for the internal network, and one for the VDOM link with the management VDOM (root).

For added security, all traffic allowed will be scanned. Only valid office traffic will be allowed using the service group `OfficeServices`.

Note the spelling of `AccountVlnk` which is due to the eleven character limit on VDOM link names.

To configure firewall addresses - web-based manager:

1. Open the **Accounting** VDOM.
2. Select **Policy & Objects > Addresses**.
3. Select **Create New**, enter the following information, and select **OK**.

Address Name	AccountingLocal
Type	Subnet/ IP Range
Subnet / IP Range	172.100.0.0
Interface	port1

4. Select **Create New**, enter the following information, and select **OK**.

Address Name	AccountManagement
Type	Subnet/ IP Range
Subnet / IP Range	10.0.1.0
Interface	AccountVlnk

To configure firewall addresses - CLI:

```
config vdom
   edit Accounting
      config firewall address
         edit AccountingLocal
            set type iprange
            set subnet 172.100.0.0
            set associated-interface port1
         next
         edit AccountManagement
            set type iprange
            set subnet 10.0.1.0
            set associated-interface AccountVlnk
         end
      end
```

To configure the firewall policies from AccountingLocal to the Internet - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Policy & Objects > IPv4 Policy**.

3. Select **Create New**, enter the following information, and then select **OK**.

Name	Accounting-Local-to-Management
Incoming Interface	port2
Outgoing Interface	AccountVlnk
Source Address	AccountingLocal
Destination Address	AccountManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict

4. Open the **root** VDOM.
5. Go to **Policy & Objects > IPv4 Policy.**
6. Select **Create New**, enter the following information, and then select **OK**.

Name	Accounting-VDOM-to-Internet
Incoming Interface	AccountVlnk
Outgoing Interface	ManagementExternal
Source Address	AccountManagement
Destination Address	all
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Web Filtering	webStrict

AntiVirus Filtering	avStrict
Application Control	appStrict

To configure the firewall policies from AccountingLocal to Internet - CLI:

```
config vdom
   edit Accounting
      config firewall policy
         edit 1
            set name "Accounting-Local-to-Management"
            set srcintf port2
            set dstintf AccountVlnk
            set srcaddr AccountingLocal
            set dstaddr AccountManagement
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
            set av-profile avStrict
            set webfilter-profile webStrict
            set application-list appStrict
         end
   end
config vdom
   edit root
      config firewall policy
         edit 2
            set name "Accounting-VDOM-to-Internet"
            set srcintf AccountVlnk
            set dstintf port1
            set srcaddr AccountManagement
            set dstaddr all
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
            set av-profile scan
            set webfilter-profile scan
            set application-list AppControlList
         end
   end
```

To configure the firewall policies from Internet to AccountingLocal - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**, enter the following information, and select **OK**.

Name	Internet-access-to-Accounting-VDOM
Incoming Interface	port1
Outgoing Interface	AccountVlnk

Source Address	all
Destination Address	AccountManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict

4. Open the **Accounting** VDOM.
5. Go to **Policy & Objects > IPv4 Policy.**
6. Select **Create New**, enter the following information, and select **OK**.

Name	Management-access-to-Accounting-local
Incoming Interface	AccountVlnk
Outgoing Interface	port2
Source Address	AccountManagement
Destination Address	AccountingLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Enable NAT	enable
Security Features	enabled
Web Filtering	webStrict
AntiVirus Filtering	avStrict
Application Control	appStrict

To configure the firewall policies from Internet to AccountingLocal - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 3
```

```
            set name "Internet-access-to-Accounting-VDOM"
            set srcintf port1
            set dstintf AccountVlnk
            set srcaddr all
            set dstaddr AccountManagement
            set action accept
            set schedule always
            set service OfficeServices
            set nat enable
            set av-profile avStrict
            set webfilter-profile webStrict
            set application-list appstrict
         end
      end
   config vdom
      edit Accounting
         config firewall policy
            edit 4
               set name "Management-access-to-Accounting-local"
               set srcintf AccountVlnk
               set dstintf port2
               set srcaddr AccountManagement
               set dstaddr AccountingLocal
               set action accept
               set schedule always
               set service OfficeServices
               set nat enable
               set av-profile avStrict
               set webfilter-profile webStrict
               set application-list appstrict
            end
      end
```

Configuring Security Profile settings for the Sales VDOM

Security profile settings include web filtering, antivirus, application control, and other features. This example just uses those three features to ensure that

- the business environment is free from viruses
- employees do not surf grossly inappropriate websites, and
- employees do not use games or peer-to-peer applications at work.

Note that Sales web traffic is different from Accounting, and web filtering is different to account for this.

To configure web filtering for the Sales VDOM - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Security Profiles > Web Filter**.
3. Select **Create New**.
4. Enter `webStrict` for the **Name**.
5. In **FortiGuard Categories**, select all of the categories except **Bandwidth Consuming**, **General Interest - Business** and **Unrated**.
6. In **Change Action for Selected Categories** select **Block**.
7. Select **Apply**.

To configure web filtering for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config webfilter profile
         edit webStrict
            config ftgd-wf
               set allow g07 g08 g21 g22 c01 c03
               set deny g01 g02 g03 g04 g05 g06 c02 c04 c05 c06 c07
            end
            set web-ftgd-err-log enable
         end
   end
```

To configure AntiVirus for the Sales VDOM - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Security Profiles > AntiVirus**.
3. Select **Create New**.
4. Enter `avStrict` for the **Name**.
5. Set **Detect Virues** to **Block** and enable all **Inspected Protocols**.
6. Select **Apply**.

To configure AntiVirus for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config antivirus profile
         edit "avStrict"
            config http
               set options scan file-filter
            end
            config ftp
               set options scan file-filter
            end
            config imap
               set options scan file-filter
            end
            config pop3
               set options scan file-filter
            end
            config smtp
               set options scan file-filter
            end
            config nntp
               set options scan file-filter
            end
            config im
               set options scan file-filter
            end
            set filepattable 1
            set av-virus-log enable
            set av-block-log enable
         end
   end
```

To configure application control for the Sales VDOM - web-based manager:

1. Open the **Accounting** VDOM.
2. Go to **Security Profiles > Application Control.**
3. Select **Create New** (+ button at top right of page).
4. Enter `appStrict` for **Name** and select OK.
5. Select **Create New**.
6. In **Filters**, set **Category** to **game**.
7. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

8. Select **Create New**.
9. In **Filters**, set **Category** to **p2p**.
10. In **Applications/Settings**, enter the following, and select **OK**.

Action	Block
Packet Logging	Enable

11. Select **Apply**.

To configure application control for the Sales VDOM - CLI:

```
config vdom
   edit Sales
      config application list
         edit "appStrict"
            config entries
               edit 1
                  set category 2
               next
               edit 2
                  set category 8
               end
         end
   end
```

Configuring firewall settings for the Sales VDOM

Like the Accounting firewall settings, this configuration includes two firewall addresses and two firewall policies for the sales VDOM: one for the internal network, and one for the VDOM link with the management VDOM.

When entering the CLI commands, the number of the firewall policies must be high enough to be a new policy. Depending on the number of firewall policies on your FortiGate unit, this may require starting at a higher number than the 6 required for the default configuration. This number is added automatically when you configure firewall policies using the web manager interface.

The FortiClient application must be used on Sales network computers to ensure additional protection for the sensitive information and for protection against spam.

To configure firewall addresses - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Policy & Objects > Addresses**.
3. Select **Create New,** enter the following information, and select **OK**.

Address Name	SalesLocal
Type	Subnet / IP Range
Subnet / IP Range	172.100.0.0
Interface	port3

4. Go to **Policy & Objects > Addresses**.
5. Select **Create New**, enter the following information, and select **OK**.

Address Name	SalesManagement
Type	Subnet / IP Range
Subnet / IP Range	10.0.1.0
Interface	SalesVlnk

To configure the firewall addresses - CLI:

```
config vdom
   edit Sales
      config fireall address
         edit SalesLocal
            set type iprange
            set subnet 172.100.0.0
            set associated-interface port2
         next
         edit SalesManagement
            set type iprange
            set subnet 10.0.1.0
            set associated-interface SalesVlnk
         end
   end
```

To configure the firewall policies from SalesLocal to the Internet - web-based manager:

1. Open the **Sales** VDOM.
2. Go to **Policy & Objects > IPv4 Policy**.
3. Select **Create New**, enter the following information, and select **OK**.

Name	Sales-local-to-Management
Incoming Interface	port3
Outgoing Interface	SalesVlnk
Source Address	SalesLocal
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Log Allowed Traffic	enabled

4. Open the **root** VDOM.
5. Go to **Policy & Objects > IPv4 Policy.**
6. Select **Create New**, enter the following information, and select **OK**.

Name	Sales-VDOM-to-Internet
Incoming Interface	SalesVlnk
Outgoing Interface	ManagementExternal
Source Address	SalesManagement
Destination Address	all
Schedule	always
Service	OfficeServices
Action	ACCEPT
Log Allowed Traffic	enabled

To configure the firewall policies from SalesLocal to the Internet - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 6
            set name "Sales-local-to-Management"
            set srcintf port2
            set srcaddr SalesLocal
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service OfficeServices
            set action accept
            set logtraffic enable
         end
```

```
    end
  config vdom
    edit Sales
      config firewall policy
        edit 7
          set name "Sales-VDOM-to-Internet"
          set srcintf SalesVlnk
          set srcaddr SalesManagement
          set dstintf external
          set dstaddr all
          set schedule always
          set service OfficeServices
          set action accept
          set logtraffic enable
        end
    end
```

To configure the firewall policies from the Internet to SalesLocal - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy & Objects > IPv4 Policy.**
3. Select **Create New**, enter the following information, and select **OK**.

Name	Internet-access-to-Sales-VDOM
Incoming Interface	ManagementExternal
Outgoing Interface	SalesVlnk
Source Address	all
Destination Address	SalesManagement
Schedule	always
Service	OfficeServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled

4. Open the **Sales** VDOM.
5. Go to **Policy & Objects > IPv4 Policy.**
6. Select **Create New**, enter the following information, and select **OK**.

Name	Management-access-to-Sales-local
Incoming Interface	SalesVlnk
Outgoing Interface	port2

Source Address	SalesManagement
Destination Address	SalesLocal
Schedule	always
Service	OfficeServices
Action	ACCEPT
Log Allowed Traffic	enabled

To configure the firewall policies from the Internet to SalesLocal - CLI:

```
config vdom
   edit root
      config firewall policy
         edit 8
            set name "Internet-access-to-Sales-VDOM"
            set srcintf external
            set srcaddr all
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service OfficeServices
            set action accept
            set logtraffic enable
         end
   end
config vdom
   edit Sales
      config firewall policy
         edit 9
            set name "Management-access-to-Sales-local"
            set srcintf SalesVlnk
            set srcaddr SalesManagement
            set dstintf port2
            set dstaddr SalesLocal
            set schedule always
            set service OfficeServices
            set action accept
            set logtraffic enable
         end
   end
```

Configuring firewall settings between the Accounting and Sales VDOMs

Firewall policies are required for any communication between each internal network and the Internet. Policies are also required for the two internal networks to communicate with each other through the management VDOM.

The more limited AccountingSalesServices group of services will be used between Sales and Accounting to ensure the traffic is necessary business traffic only. These policies will result in a partially meshed VDOM configuration. The FortiClient application must be used to ensure additional protection for the sensitive accounting information.

Two firewall policies are required to allow traffic in both directions between Sales and Accounting.

To configure the firewall policy between Sales and Accounting on the management VDOM - web-based manager:

1. Open the **root** VDOM.
2. Go to **Policy & Objects > IPv4 Policy.**
3. Select **Create New**, enter the following information, and select **OK**.

Name	Sales-VDOM-to-Accounting-VDOM
Incoming Interface	SalesVlnk
Outgoing Interface	AccountVlnk
Source Address	SalesManagement
Destination Address	AccountingManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Protection Profile	scan
Log Allowed Traffic	enabled

4. Go to **Policy & Objects > IPv4 Policy.**
5. Select **Create New**, enter the following information, and select **OK**.

Name	Accounting-VDOM-to-Sales-VDOM
Incoming Interface	AccountVlnk
Outgoing Interface	SalesVlnk
Source Address	AccountingManagement
Destination Address	SalesManagement
Schedule	always
Service	AccountingSalesServices
Action	ACCEPT
Log Allowed Traffic	enabled

To configure the firewall policy between Sales and Accounting on the management VDOM - CLI:

```
config vdom
   edit root
      config system firewall policy
         edit 9
            set name "Sales-VDOM-to-Accounting-VDOM"
```

```
            set srcintf SalesVlnk
            set srcaddr SalesManagement
            set dstintf AccountVlnk
            set dstaddr AccountManagement
            set schedule always
            set service AccountingSalesServices
            set action accept
            set logtraffic enable
        next
        edit 10
            set name "Accounting-VDOM-to-Sales-VDOM"
            set srcintf AccountVlnk
            set srcaddr AccountManagement
            set dstintf SalesVlnk
            set dstaddr SalesManagement
            set schedule always
            set service AccountingSalesServices
            set action accept
            set logtraffic enable
        end
end
```

Testing the configuration

Once the inter-VDOM routing has been configured, tests must be conducted to confirm proper operation. If there are any problems, use the troubleshooting tips to resolve them.

This section includes the following topics:

- Testing connectivity
- Troubleshooting Tips

Testing connectivity

Testing connectivity ensures that physical networking connections as well as FortiGate unit interface configurations, including firewall policies, are properly configured.

The easiest way to test connectivity is to use the `ping` and `traceroute` commands to confirm the connectivity of different routes on the network. Include testing:

- from AccountingLocal to Internet
- from Internet to AccountingLocal
- from SalesLocal to Internet
- from Internet to SalesLocal
- from AccountingLocal to SalesLocal.

When using the commands on a Windows computer, go to a command line prompt and enter either `ping <IP address>` or `tracert <IP address>`.

When using the commands on a FortiGate unit, go to the CLI and enter either `exec ping <IP address>` or `exec traceroute <IP address>`.

Troubleshooting Tips

When there are problems with connectivity, the following troubleshooting tips will help resolve the issues.

- If a multiple hop test, such as traceroute, is not successful then reduce it to a single hop to simplify the test. Test each link of the path to see which hop is down. If all hops are up, check the FortiGate unit policies to ensure they allow basic traffic to flow as expected.
- If ping does not work, confirm that the FortiGate unit interfaces have Ping enabled and also ensure Ping is enabled in the firewall policies. Otherwise the Ping traffic will be blocked.
- If one protocol does not work but others do work, check the FortiGate unit firewall policies for that one protocol to ensure it is allowed.
- If there are unexplained connectivity problems, check the local computer to ensure it does not have a software firewall running that may be blocking traffic. MS Windows computers have a firewall running by default that can cause problems.

For additional troubleshooting, see Troubleshooting Virtual Domains.

Troubleshooting Virtual Domains

When you are configuring VDOMs you may run into some issues, with your VDOM configuration, your network configuration, or your device setup. This section addresses common problems and specific concerns that an administrator of a VDOM network may have.

This section includes:

VDOM admin having problems gaining access

With VDOMs configured, administrators have an extra layer of permissions and may have problems accessing their information.

Confirm the admin's VDOM

Each administrator account, other than the super_admin account, is tied to one specific VDOM. That administrator is not able to access any other VDOM. It may be possible they are trying to access the wrong VDOM.

Confirm the VDOM's interfaces

An administrator can only access their VDOM through interfaces that are assigned to that VDOM. If interfaces on that VDOM are disabled or unavailable there will be no method of accessing that VDOM by its local administrator. The super_admin will be required to either bring up the interfaces, fix the interfaces, or move another interface to that VDOM to restore access.

Confirm the VDOMs admin access

As with all FortiGate units, administration access on the VDOM's interfaces must be enabled for that VDOM's administrators to gain access. For example if SSH is not enabled, that is not available to administrators.

To enable admin access, the super_admin will go to the **Global > Network > Interfaces** page, and for the interface in question enable the admin access.

FortiGate unit running very slowly

You may experience a number of problems resulting from your FortiGate unit being overloaded. These problems may appear as:

- CPU and memory threshold limits exceeded on a continual basis
- AV failopen happening on a regular basis

- dropped traffic or sessions due to lack of resources

These problems are caused by a lack of system resources. There are a number of possible reasons for this.

Too many VDOMs

If you have configured many VDOMs on your system, past the default ten VDOMs, this could easily be your problem.

Each VDOM you create on your FortiGate unit requires system resources to function - CPU cycles, memory, and disk space. When there are too many VDOMs configured there are not enough resources for operation. This may be a lack of memory in the session table, or no CPU cycles for processing incoming IPS traffic, or even a full disk drive.

Go to **Global > System > VDOM** and see the number of configured VDOMs on your system. If you are running 500 or more VDOMs, you must have a FortiGate 5000 chassis. Otherwise you need to reduce the number of VDOMs on your system to fix the problem. Even if you have the proper hardware, you may encounter noticeably slow throughput if you are using advanced features such as security profiles or deep content inspection with many configured VDOMs.

One or more VDOMs are consuming all the resources

If you have sufficient hardware to support the number of VDOMs you are running, check the global resources on your FortiGate unit. At a glance it will tell you if you are running out of a particular resource such as sessions, or users. If this is the case, you can then check your VDOMs to see if one particular VDOM is using more than its share of resources. If that is the case you can change the resource settings to allow that VDOM (or those VDOMs) fewer resources and in turn allow the other VDOMs access to those resources.

Too many Security Features in use

It is likely that reducing the Security Features in use regardless of number of VDOMs will greatly improve overall system performance and should be considered as an option.

Finally it is possible that your FortiGate unit configuration is incorrect in some other area, which is using up all your resources. For example, forgetting that you are running a network sniffer on an interface will create significant amounts of traffic that may prevent normal operation.

General VDOM tips and troubleshooting

Besides ping and traceroute, there are additional tools for troubleshooting your VDOM configurations. These include packet sniffing and debugging the packet flow.

Perform a sniffer trace

When troubleshooting networks, it helps to look inside the headers of packets to determine if they are traveling along the route you expect that they are. Packet sniffing can also be called a network tap, packet capture, or logic analyzing.

If your FortiGate unit has NP interfaces that are offloading traffic, this will change the sniffer trace. Before performing a trace on any NP interfaces, you should disable offloading on those interfaces.

What sniffing packets can tell you

If you are running a constant traffic application such as ping, packet sniffing can tell you if the traffic is reaching the destination, what the port of entry is on the FortiGate unit, if the ARP resolution is correct, and if the traffic is being sent back to the source as expected.

Sniffing packets can also tell you if the Fortigate unit is silently dropping packets for reasons such as RPF (Reverse Path Forwarding), also called Anti Spoofing, which prevents an IP packet from being forwarded if its Source IP does not either belong to a locally attached subnet (local interface), or be part of the routing between the FortiGate and another source (static route, RIP, OSPF, BGP). Note that RPF can be disabled by turning on asymmetric routing in the CLI (`config system setting, set asymmetric enable`), however this will disable stateful inspection on the FortiGate unit and cause many features to be turned off.

If you configure virtual IP addresses on your Fortigate unit, it will use those addresses in preference to the physical IP addresses. You will notice this when you are sniffing packets because all the traffic will be using the virtual IP addresses. This is due to the ARP update that is sent out when the VIP address is configured.

How to sniff packets

When you are using VDOMs, you must be in a VDOM to access the `diag sniffer` command. At the global level, the command is not available. This is limit the packets only to the ones on your VDOM, and protects the privacy of other VDOM clients.

The general form of the internal FortiOS packet sniffer command is:

```
diag sniffer packet <interface_name> <'filter'> <verbose> <count>
```

To stop the sniffer, type `CTRL+C`.

<interface_name>	The name of the interface to sniff, such as “port1” or “internal”. This can also be “any” to sniff all interfaces.
<'filter'>	What to look for in the information the sniffer reads. `none` indicates no filtering, and all packets will be displayed as the other arguments indicate. The filter must be inside single quotes (‘).
<verbose>	The level of verbosity as one of: **1 -** print header of packets **2 -** print header and data from IP of packets **3 -** print header and data from Ethernet of packets
<count>	The number of packets the sniffer reads before stopping. If you don’t put a number here, the sniffer will run forever unit you stop it with <CTRL C>.

For a simple sniffing example, enter the CLI command `diag sniffer packet port1 none 1 3`. This will display the next 3 packets on the port1 interface using no filtering, and using verbose level 1. At this verbosity level you can see the source IP and port, the destination IP and port, action (such as ack), and sequence numbers.

In the output below, port 443 indicates these are HTTPS packets, and 172.20.120.17 is both sending and receiving traffic.

```
Head_Office_620b # diag sniffer packet port1 none 1 3
interfaces=[port1]
filters=[none]
0.545306 172.20.120.17.52989 -> 172.20.120.141.443: psh 3177924955 ack 1854307757

0.545963 172.20.120.141.443 -> 172.20.120.17.52989: psh 1854307757 ack 3177925808

0.562409 172.20.120.17.52988 -> 172.20.120.141.443: psh 4225311614 ack 3314279933
```

For a more advanced example of packet sniffing, the following commands will report packets on any interface travelling between a computer with the host name of `PC1` and the computer with the host name of `PC2`. With verbosity 4 and above, the sniffer trace will display the interface names where traffic enters or leaves the FortiGate unit. Remember to stop the sniffer, type `CTRL+C`. Note that `PC1` and `PC2` may be VDOMs.

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2>" 4
```

or

```
FGT# diagnose sniffer packet any "(host <PC1> or host <PC2>) and icmp" 4
```

The following sniffer CLI command includes the ARP protocol in the filter which may be useful to troubleshoot a failure in the ARP resolution (for instance PC2 may be down and not responding to the FortiGate ARP requests).

```
FGT# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4
```

Debugging the packet flow

Traffic should come in and leave the VDOM. If you have determined that network traffic is not entering and leaving the VDOM as expected, debug the packet flow.

Debugging can only be performed using CLI commands. Debugging the packet flow requires a number of debug commands to be entered as each one configures part of the debug action, with the final command starting the debug.

If your FortiGate unit has NP interfaces that are offloading traffic, this will change the packet flow. Before performing the debug on any NP interfaces, you should disable offloading on those interfaces.

The following configuration assumes that `PC1` is connected to the internal interface of the FortiGate unit and has an IP address of `10.11.101.200`. `PC1` is the host name of the computer.

To debug the packet flow in the CLI, enter the following commands:

```
FGT# diag debug enable
FGT# diag debug flow filter add <PC1>
FGT# diag debug flow show console enable
FGT# diag debug flow trace start 100
FGT# diag debug enable
```

The `start 100` argument in the above list of commands will limit the output to 100 packets from the flow. This is useful for looking at the flow without flooding your log or your display with too much information.

To stop all other debug activities, enter the command:

```
FGT# diag debug flow trace stop
```

The following is an example of debug flow output for traffic that has no matching Firewall Policy, and is in turn blocked by the FortiGate unit. The denied message indicates the traffic was blocked. Note that even with VDOMs not enabled, vd-root is still shown.

```
id=20085 trace_id=319 func=resolve_ip_tuple_fast line=2825 msg="vd-root received a
    packet(proto=6, 192.168.129.136:2854->192.168.96.153:1863) from port3."

id=20085 trace_id=319 func=resolve_ip_tuple line=2924 msg="allocate a new session-
    013004ac"

id=20085 trace_id=319 func=vf_ip4_route_input line=1597 msg="find a route: gw-
    192.168.150.129 via port1"

id=20085 trace_id=319 func=fw_forward_handler line=248 msg=" Denied by forward policy
    check"
```