



FIREWALL USER GUIDE



¹Access

REVISION HISTORY

Date	Author/s	Version	Change Reference
27/06/2017	Neil Wilson	4.0	Branding updates

CONTENTS

- Virtual1 Firewall FortiGate Firewalls.....6
 - Co-Management.....6
 - Planning Your Policy6
 - Logging-on to your firewall8
 - Firewall Policy.....9
 - How list order affects policy matching.....9
- Create/Edit Firewall Objects.....9
 - Address.....9
 - New Address10
 - New Group.....10
 - Service.....11
 - Virtual Addresses / Network Address Translation.....11
- Create/Edit a Firewall Policy.....12
 - Source Interface/Zone13
 - Source Address.....13
 - Destination Interface/Zone14
 - Destination Address.....14
 - Schedule.....14
- Creating a Firewall Policy Example.....14
 - Create address objects for YouTube and Facebook.....15
 - Create the schedule to limit access to between 12 noon and 2 pm.....15
 - Create security policies.....16
 - Reposition the security policies.....16
 - Results.....17
- Web Filtering.....18
 - Types of filtering:.....18
 - Web Category Filtering18

Web Content Filtering.....	18
Web URL Filtering.....	20
Google HTTP Searches Still Showing Images.....	20
Static DNS entries.....	20
Users change their local DNS settings to bypass the DNS rewriting on the FortiGate..	21
Google HTTPS Searches bypass the web filter (SSL Inspection).....	22
Antivirus.....	22
Profile page.....	22
New Antivirus Profile page.....	23
Anti-Spam.....	24
Email Filter Profiles.....	24
New Email Filter Profile page.....	25
Filter Precedence.....	26
For SMTP:.....	26
For POP3 and IMAP:.....	27
Spam checking Types:.....	27
IP Address.....	27
URL Checking.....	27
Checksum.....	28
Spam Submission.....	28
HELO DNS.....	29
Return Email DNS Check.....	29
IP Black/White List (BWL) Checking.....	29
Email Address Black/White List (BWL) Checking.....	30
Banned Word Checking.....	31
Adding words to a banned word list.....	31
VPN.....	33
Configuring user accounts and SSL VPN user groups.....	33
To create a user account in the Local domain.....	34

To create a user group	34
Configuring user accounts and SSL VPN user groups.....	34
IPsec Layer 2 Tunnelling Protocol (L2TP).....	35
Creating the IPsec profile on the Firewall.....	36
Configuring the Windows PC	39
SSL VPN's.....	43
Web-Only mode.....	43
Tunnel mode	43
FortiGate SSL VPN dialup client.....	44
DHCP.....	44
Setting-up Users to be able to VPN before login:.....	46
VPN Split-Tunnelling.....	48
VPN Tunnels (Site-to-Site).....	48
EXPORTING THE POLICY.....	49
Exporting the Policy using the GUI.....	49
Exporting the Policy using the CLI.....	49
Exporting the Policy from a different type of firewall.....	49

VIRTUAL1 FIREWALL FORTIGATE FIREWALLS

This guide is designed as a quick introduction to the FortiGate Firewalls that Virtual1 provides as either the **Enhanced Shared Firewall** product or the **Dedicated Firewall** device. The primary distinction between the two is that the Shared variant is delivered as a single Virtual Domain (VDOM) per customer, whereas the dedicated device usually has a single customer domain for the entire device.

Co-Management

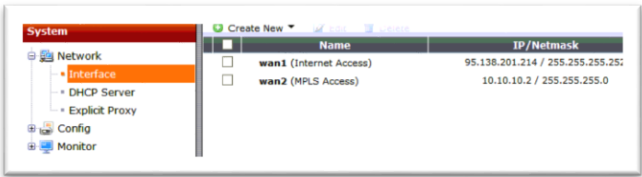
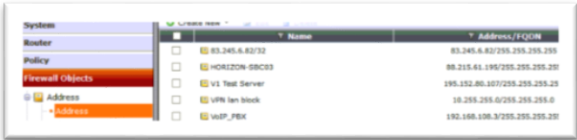
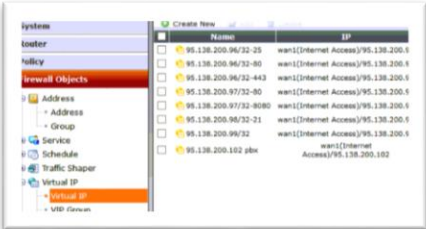
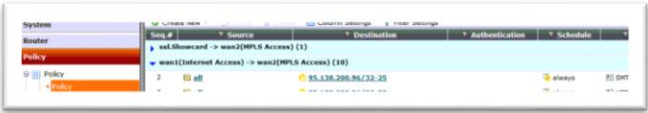
One issue that often exists with shared or managed firewall device is the inability of a skilled end-user to make changes to their policy without having to wait for the service provider. To overcome this, Virtual1 has introduced the "Co-Managed" concept. The partner can update their firewall policy and inform Virtual1, via changerequest@virtual1.com, of the changes made or they can raise a request in the usual way. Changes made without notifying Virtual1 may be overridden if the partner later asks for the policy to be rolled-back.

Please note Virtual1 reserves the right to adjust policy changes made by the partner where there is obvious detriment to the security of the device or the network it is protecting or adverse effect on other customers.

Planning Your Policy

The firewall is in its simplest incarnation, a router, passing network traffic between two or more networks, make decisions as to which traffic to selectively discard and amending the traffic headers if required. The main elements to consider are outlined in the table below.

You may also need to consider User and VPN configuration or amend the default Unified Threat Management (UTM) configuration but the above elements will provide a secure gateway to your network with the least amount of configuration required.

<p>Interfaces</p>	<p>These are the network ports on the firewall and are usually called wan1, wan2, etc. And need to be appropriately labelled.</p> 
<p>Address Objects</p>	<p>Before you can write rules on how to manipulate or filter traffic, you need to define the objects that are important. This makes it easier if for example, you change your mail server IP address, as you would only change it in one place rather than have to rewrite the whole policy. It also makes the policy much more readable</p> 
<p>Virtual Address Objects</p>	<p>Also known as Network Address Translation or NAT. This re-writes the source and destination addresses of a packet and is most commonly used to allow multiple devices INSIDE a firewall to share a single public Internet address on the OUTSIDE network. It can translate all traffic or just work on one port.</p> 
<p>Services</p>	<p>Types of application traffic, normally assigned to a specific port number.</p>
<p>Policy Rules</p>	<p>The rules within the Policy are where you define what traffic is and is not allowed to pass through the firewall.</p> 

Logging-on to your firewall

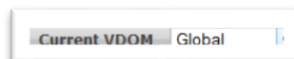
The Virtual1 Provisioning team will provide you with the address of your firewall, along with a username and password. Keep this safe. If you forget it, raise a support request via support@virtual1.co.uk or via 1 Portal.

Use a web-browser to connect to your firewall using https:\\

Login with the username and password provided



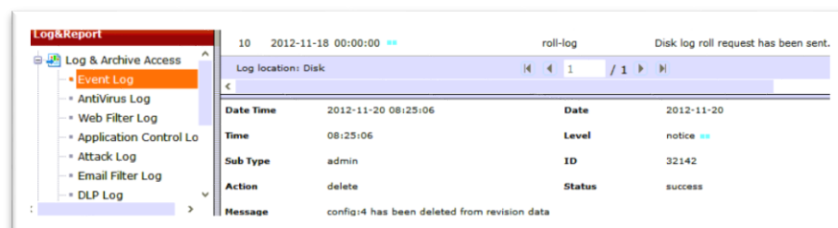
- On the Shared platform, you should be dropped directly into your own VDOM, if it is a dedicated device, choose the relevant VDOM from the list in the



bottom left.

- The VDOM usually bears your company name. The VDOMs, root, Global and Maint are standard VDOMs with specific purposes not covered in the document.

You can review recent log activity to see if there are any issues that need addressing or use one of the other menus on the left to start configuring your firewall



Firewall Policy

Firewall policies control all traffic attempting to pass through the Firewall unit, between Firewall interfaces, zones and VLAN sub interfaces.

Firewall policies are instructions the Firewall unit uses to decide connection acceptance and packet processing for traffic attempting to pass through. When the firewall receives a connection packet, it analyses the packet's source address, destination address, and service (by port number), and attempts to locate a firewall policy matching the packet.

Firewall policies can contain many instructions for the Firewall unit to follow when it receives matching packets. Some instructions are required, such as whether to drop or accept and process the packets, while other instructions, such as logging and authentication, are optional.

How list order affects policy matching

Each time a Firewall unit receives a connection attempting to pass through one of its interfaces, the unit searches its firewall policy list for a matching firewall policy. The search begins at the top of the policy list and progresses in order towards the bottom. The Firewall unit evaluates each policy in the firewall policy list for a match until a match is found. When the Firewall unit finds the first matching policy, it applies the matching policy's specified actions to the packet, and disregards subsequent firewall policies. Matching firewall policies are determined by comparing the firewall policy and that of the packet:

- source and destination interfaces
- source and destination firewall addresses
- services
- time/schedule.

If no policy matches, the connection is dropped. As a general rule, you should order the firewall policy list from most specific to most general because of the order in which policies are evaluated for a match, and because only the *first* matching firewall policy is applied to a connection.

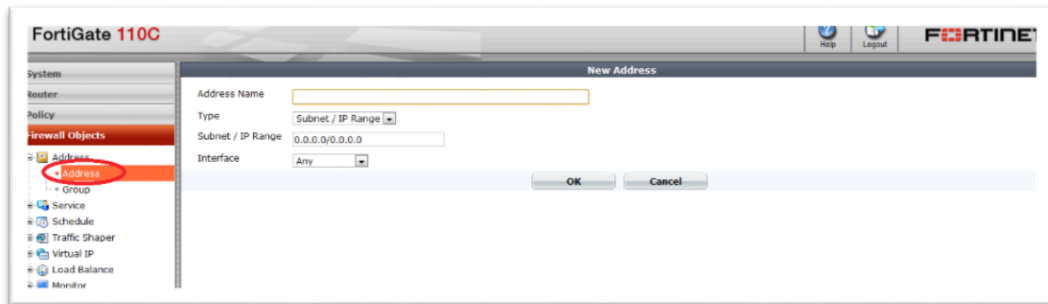
CREATE/EDIT FIREWALL OBJECTS

An object is a device or group of addresses – such as IP addresses – which are used to simplify writing your firewall policies. Examples of objects include servers (eg your mail server), or your LAN. Policies can be written without objects, but it can quickly become confusing if you are working with a large number of addresses.

Address

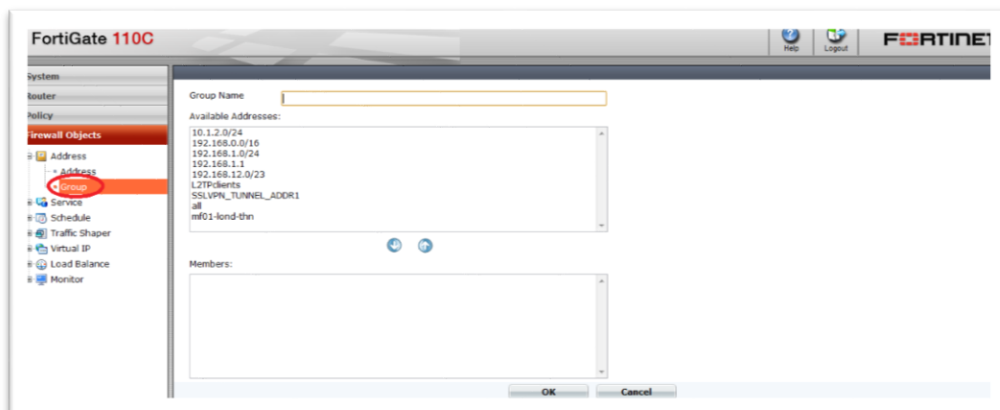
- Go into the Firewall Objects on the left hand side drop downs. Choose to create either a single address or group then click the create new button or select the edit icon beside an existing address or group

New Address



1. Type in address name
2. Select type: Subnet/IP range, FQDN and geography
3. Type in IP address
4. Select Interface

New Group



1. Type in group name
2. Select the addresses required for the group from the list
3. You can add and remove addresses using the blue arrow buttons

4. Click ok to confirm



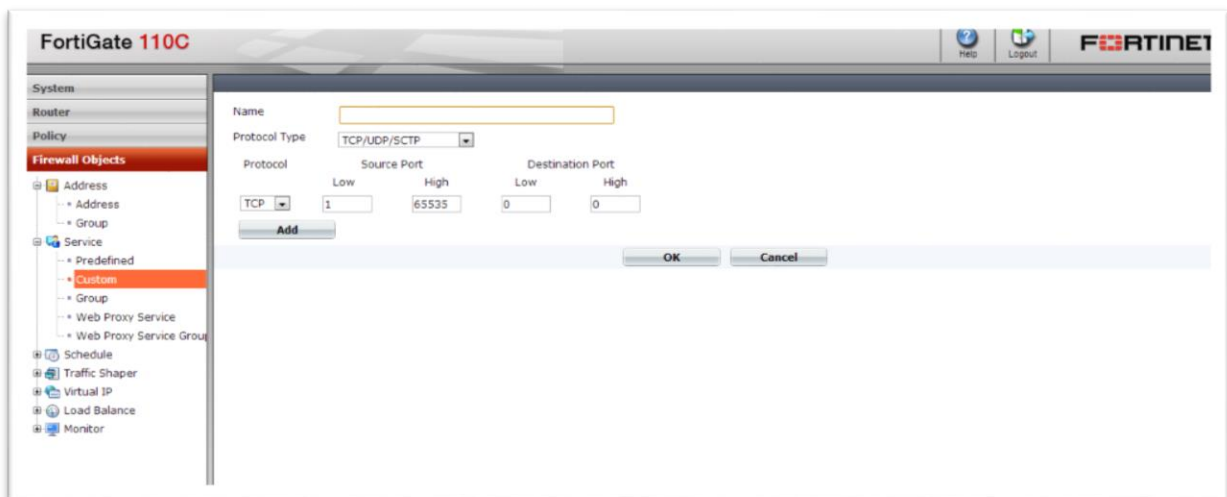
The screenshot shows the FortiGate 110C management interface. On the left, a tree view shows 'Firewall Objects' expanded to 'Service'. The main area displays a table of predefined services with columns for Name and Detail.

Name	Detail
AFS3	TCP/7000-7009 UDP/7000-7009
AH	IP/51
ANY	ALL
AOL	TCP/5190-5194
BGP	TCP/179
CVSPSEVER	TCP/2401 UDP/2401
DCE-RPC	TCP/135 UDP/135
DHCP	UDP/67-68
DHCP6	UDP/546,547
DNS	TCP/53 UDP/53
ESP	IP/50
FINGER	TCP/79
FTP	TCP/21
FTP_GET	TCP/21
FTP_PUT	TCP/21
GOPHER	TCP/70
GRE	IP/47
H323	TCP/1720,1503 UDP/1719
HTTP	TCP/80
HTTPS	TCP/443

Service

Services represent typical traffic types and application packets that pass through the Firewall unit. Firewall services define one or more protocols and port numbers associated with each service. Security policies use service definitions to match session types. You can organize related services into service groups to simplify your security policy list.

Many well-known traffic types have been predefined in firewall services. These predefined services are defaults, and cannot be edited or removed. However, if you require different services, you can create custom services.



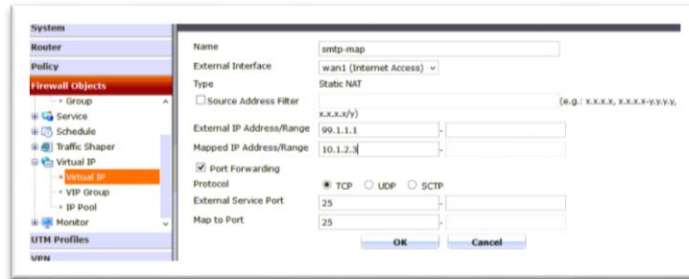
The screenshot shows the configuration page for a custom service in the FortiGate 110C. The 'Name' field is empty. The 'Protocol Type' is set to 'TCP/UDP/SCTP'. Below, the 'Protocol' is set to 'TCP', and the 'Source Port' range is from 1 to 65535, and the 'Destination Port' range is from 0 to 0. There are 'Add', 'OK', and 'Cancel' buttons.

Virtual Addresses / Network Address Translation

NAT uses a public address makes packets appear to come from a different address that they originated. Most typically this is used to map between internal and public Internet addresses to conserve public IP address space or for "security through obscurity". NAT can be configured to:

- Map a single IP public address to a single private IP address
- Map a range of address between external and internal interfaces

- Map one or more ports in a public address to different private devices (for example one public IP address may have port 25 going to one internal server and port 80 going to a different one whilst appearing to be a single host on



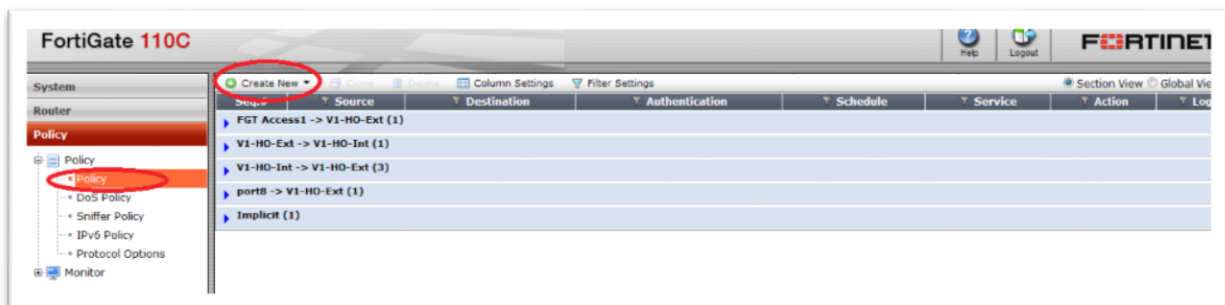
the public Internet)

To edit an existing mapping, double-click it or use the create icon on the top line to create a new one.

Name	Give the new mapping a unique name.
External Interface	Usually the Public Internet interface
External IP Address	Put the public Internet address in here
Mapped IP Address	Put the private (RFC1918) address in here
Port-forwarding	Select this tick box to define a specific port, or leave unticked to map all ports

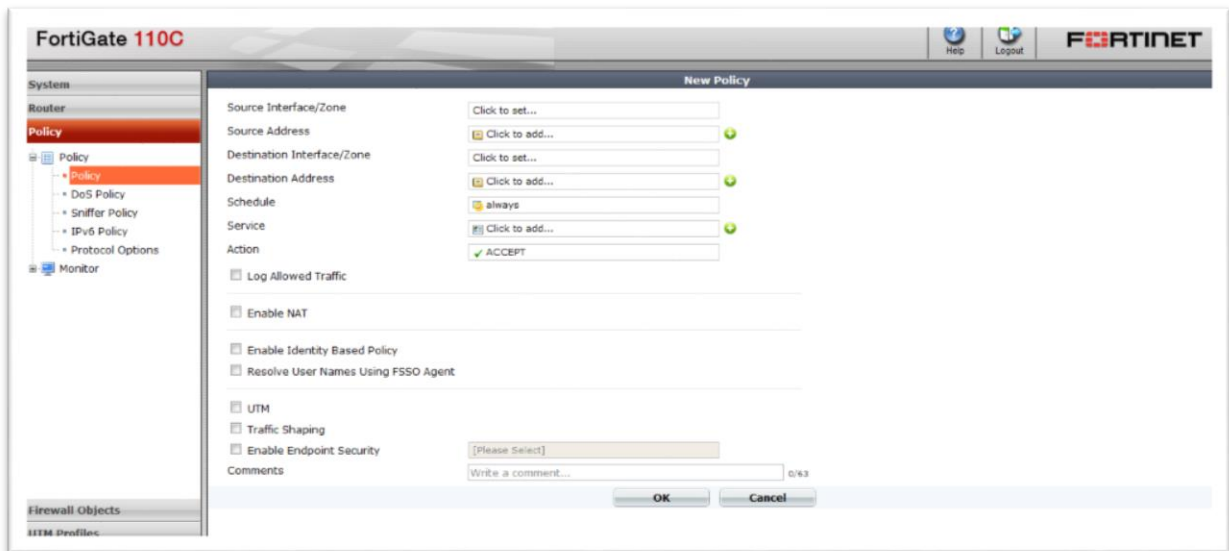
CREATE/EDIT A FIREWALL POLICY

- Go into the Policy tab on the left hand side drop downs, then click the create



new button or select the edit icon beside an existing policy

2. Configure the settings as described in the following table and in the



references to specific features then select *OK*.

Source Interface/Zone

The Interfaces on the firewall have standard names suffixed with 'int', 'ext' or 'dmz', dependent on their function. If you select *Any* as the source interface, the policy matches all interfaces as source. If *Action* is set to IPsec, the interface is associated with the local private network. If *Action* is set to SSL-VPN, the interface is associated with connections from remote SSL-VPN clients.

Source Address

Select the name of an address to associate with the Source Interface/Zone. Only packets whose header contains an IP address matching the selected address will be subject to this policy. You can also create firewall addresses by selecting *Create New* from this list.

If you want to associate multiple addresses or address groups with the Source Interface/Zone, from *Source Address*, select *Multiple*. In the dialog box, move the addresses or address groups from the *Available Addresses* section to the *Members* section, then select *OK*.

If *Action* is set to IPsec, the address is the private IP address of the host, server or network behind the Firewall unit.

If *Action* is set to SSL-VPN and the policy is for web-only mode clients, select *all*.

If *Action* is set to SSL-VPN and the policy is for tunnel mode clients, select the name of the address that you reserved for tunnel mode clients.

Destination Interface/Zone

Select the name of the Firewall network interface, or zone to which IP packets are forwarded. Interfaces and zones are configured on the System Network page

If you select *Any* as the destination interface, the policy matches all interfaces as destination.

If *Action* is set to *IPSEC*, the interface is associated with the entrance to the VPN tunnel.

If *Action* is set to *SSL-VPN*, the interface is associated with the local private network.

Destination Address

Select the name of an address to associate with the Destination Interface/Zone. Only packets whose header contains an IP address matching the selected address will be subject to this policy.

You can also create addresses by selecting *Create New* from this list.

If you want to associate multiple addresses or address groups with the Destination Interface/Zone, from Destination Address, select *Multiple*.

In the dialog box, move the addresses or address groups from the *Available Addresses* section to the *Members* section, then select *OK*.

If you select a virtual IP, the Firewall unit applies NAT or PAT. The applied translation varies by the settings specified in the virtual IP, and whether you select the 'enable NAT' tick box, below.

If *Action* is set to *IPSec*, the address is the private IP address to which packets may be delivered at the remote end of the VPN tunnel. If *Action* is set to *SSL-VPN*, select the name of the IP address that corresponds to the host, server, or network that remote clients need to access behind the Firewall unit.

Schedule

Select a one-time or recurring schedule or a schedule group that controls when the policy is in effect.

You can also create schedules by selecting *Create New* from this list.

CREATING A FIREWALL POLICY EXAMPLE

Limit Facebook and Youtube access to between 12pm and 2pm

Create a firewall schedule that allows access to YouTube and Facebook between 12 and 2. Create a new security policy that includes the schedule. This policy will be independent of the current Internet browsing policy.

This procedure presumes the following configurations are already complete:

- Users that connect to the Firewall unit for access to the Internet.
- Security policies to allow traffic to and from the Internet. For simplicity, this example uses a wide open policy for all other Internet browsing.

These following steps are required to complete this procedure:

Create firewall address entries for YouTube and Facebook.

- Create a recurring schedule that allows access to these sites.
- Create a security policy that references these sites and the schedule.
- Ensure the security is at the top of the policy list.

Create address objects for YouTube and Facebook

1 Go to *Firewall Objects > Address > Address* and select *Create New* and complete the following:

Address Name	YouTube
Type	FQDN
FQDN	www.youtube.com
Interface	XXXX-ext

2 Select *OK*.

3 Select *Create New* and complete the following:

Address Name	Facebook
Type	FQDN
FQDN	www.facebook.com
Interface	XXXX-ext

4. Select *OK*.

Create the schedule to limit access to between 12 noon and 2 pm

1. Go to *Firewall Objects > Schedule > Recurring* and select *Create New* and complete the following:

Name	Lunch Access
Day of the Week	Monday, Tuesday, Wednesday, Thursday, Friday
Start Time	Hour 12

	Minute 00
Stop Time	Hour 14 Minute 00

2 Select *OK*.

Create security policies

Create a security policy that uses the new schedule. For this example as well, you will create a security policy that blocks the use of the two sites outside of the scheduled allowed time.

1 Go to *Policy > Policy > Policy* and select *Create New* to add the security policy that restricts Internet access to between 12 and 2:

Source Interface/Zone	Internal
Source Address	All
Destination Interface/Zone	XXXX-ext
Destination Address	YouTube Facebook
Schedule	Lunch Access
Service	Any
Action	Accept

2 Select *OK*.

3 Select *Create New* to add a security policy that restricts access to YouTube and Facebook:

Source Interface/Zone	Internal
Source Address	All
Destination Interface/Zone	XXXX-ext
Destination Address	YouTube Facebook
Schedule	Always
Service	Any
Action	Deny

4 Select *OK*.

Reposition the security policies

In this example, there are two new security policies. The Firewall unit reads policies top down. When conditions are satisfied, it stops reading any further policies. Therefore, to ensure this policy activates when needed, you need to move the

specific policies above the general, *Allow All* policy. In this case, move the *Deny* policy to the top of the list, followed by the *Lunch Access* policy.

Results

With these policies in place, a user trying to access YouTube or Facebook, will not be able to connect. Once the allotted time occurs, access is allowed. The best way to test this is to try to connect to YouTube. It won't connect. Change either the system time on the Firewall unit or the schedule time to be within the current time, to see that access to the site is allowed.

WEB FILTERING

Types of filtering:

- FortiGuard Web Category Filtering provides many additional categories you can use to filter web traffic.
- Web Content Filtering blocks web pages containing words or patterns that you specify.
- URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources.

Web Category Filtering

Fortinet maintains a category database of websites and you can block access to sites by category. This is the easiest way to enable filtering of the majority of undesirable websites.

To enable a web filter, follow these steps:

- Under Security Profiles, choose Web Filter
- Use the + on the top right to create a new profile (rather than use the default one offered)
- Tick the Categories you want to block
- Tick "Enable Safe Search" and "Search Engine Safe Search"
- Under Ratings tick the options you want. We recommend at least "Rate Images by URL"
- Under Proxy Options Ratings tick the options you want. We recommend at least "Provide Details..."
- Return to Policy & Objects > Policy > IPv4. Double-click the relevant (Internal to External) policy and under the "Web Filter" column, choose the filter you just created.

Web Content Filtering

Allow or block access to specific keywords by adding them to the Web Content filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs.

To enable a web content filter, follow these steps:

- Under Security Profiles, choose Web Filter and select the filter profile you created above (if you have not done this, follow the steps above)

- Under Static URL Filter, choose “Enable Web Content Filter”
- Add entries for the patterns you wish to block.

Web URL Filtering

Allow or block access to specific URLs by adding them to the URL filter list. Add patterns using text and regular expressions (or wildcard characters) to allow or block URLs.

To enable a web URL filter, follow these steps:

- Under Security Profiles, choose Web Filter and select the filter profile you created above (if you have not done this, follow the steps above)
- Under Static URL Filter, choose “Enable URL Filter”
- Add entries for the sites you wish to block.

Google HTTP Searches Still Showing Images

The “Safe search” function in the web filter forces searches to Google to be turned into “safe searches”, even if it is turned-off by the user. For this to work, the FortiGate must be the DNS server for the LAN. If a different DNS server is used, this will not work.

Without forcing safesearching, even when a web filter is in place, Google’s caching behaviour may make it possible to view cached images from websites that are themselves blocked.

- If the FortiGate is used as the DNS server, add static DNS entries to force the safesearch functionality manually for Google and any other search engines. (see next section).
- If another DNS server is used, make sure it is re-writing google.com and google.co.uk to return forcesafesearch.google.com instead. See your DNS Server documentation on how to do this. In Windows for example, create a new forward lookup zone for www.google.com with the necessary CNAME and A record required.
- The FortiGate can alternatively inspect all traffic, find DNS responses and re-write them to prevent the DNS server doing the work but it is very CPU-intensive and subsequently only supported on Dedicated Firewalls. We recommend this method is **not** followed, but if it is needed, read the section called “method 2” on this page:

<http://cookbook.fortinet.com/blocking-adultmature-content-google-safesearch/>

Static DNS entries

When acting as the DNS server, the FortiGate can rewrite entries to make a DNS query return a different result than is normally returned by the Internet servers. This is

usually used to force Google.com and Google.co.uk to use the safe search equivalents (as mentioned above).

Make Google.com visitors instead go to forcesafesearch.google.com:

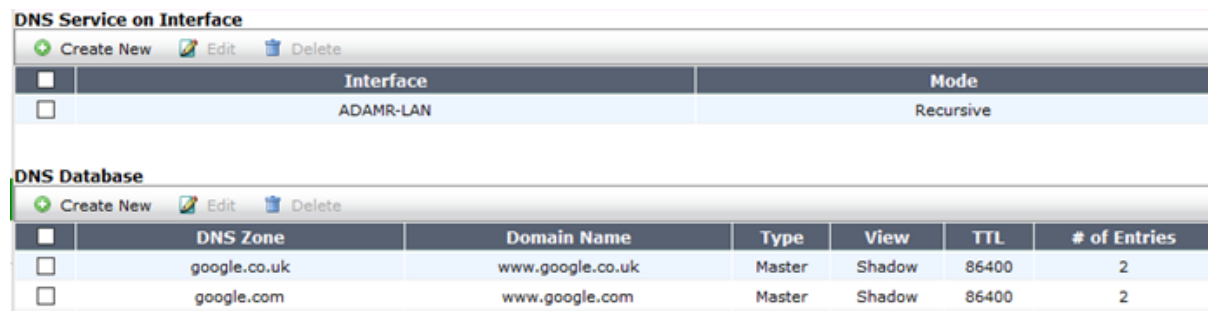
- System> Network> DNS Server
- Add a new Zone "google.com"
- Set domain name to "www.google.com"¹
- Set Authoritative to "Enable"
- Add a CNAME entry for www.google.com to forcesafesearch.google.com
- Add an A entry for forcesafesearch.google.com to 216.239.30.120

Example DNS Server entry for Google.com:

Make sure you do the same with google.co.uk and any other of the google search domains you want to rewrite. A list of all the Google domains can be found here for example:

https://www.google.com/supported_domains

If you have created entries for .co.uk and .com, your system>Network>DNS Server entry should look like this:



The screenshot shows the FortiGate configuration interface for DNS. The top section is titled "DNS Service on Interface" and contains a table with two columns: "Interface" and "Mode". The interface is set to "ADAMR-LAN" and the mode is "Recursive". Below this is the "DNS Database" section, which contains a table with columns: "DNS Zone", "Domain Name", "Type", "View", "TTL", and "# of Entries".

DNS Service on Interface	
Interface	Mode
ADAMR-LAN	Recursive

DNS Database						
DNS Zone	Domain Name	Type	View	TTL	# of Entries	
google.co.uk	www.google.co.uk	Master	Shadow	86400	2	
google.com	www.google.com	Master	Shadow	86400	2	

Set the TTL to the desired time for the DNS to refresh. 86400 is the default and fine for most situations.

Users change their local DNS settings to bypass the DNS rewriting on the FortiGate

To resolve this issue, we recommend employing a rule to block access to other DNS resolvers (port 53) to prevent users attempting to use a third-party DNS server instead.

¹ If you set the domain to "google.com" it will prevent access to other google hosts such as maps and mail. Set it to www.google.com so that only the search engine page is intercepted.

Google HTTPS Searches bypass the web filter (SSL Inspection)

When a user logs into a Google account and switches to HTTPS searches, the web filter may be bypassed. If this is a problem, SSL inspection needs to be enabled. The FortiGate guide on how to do this is here:

Please read this knowledge base article:

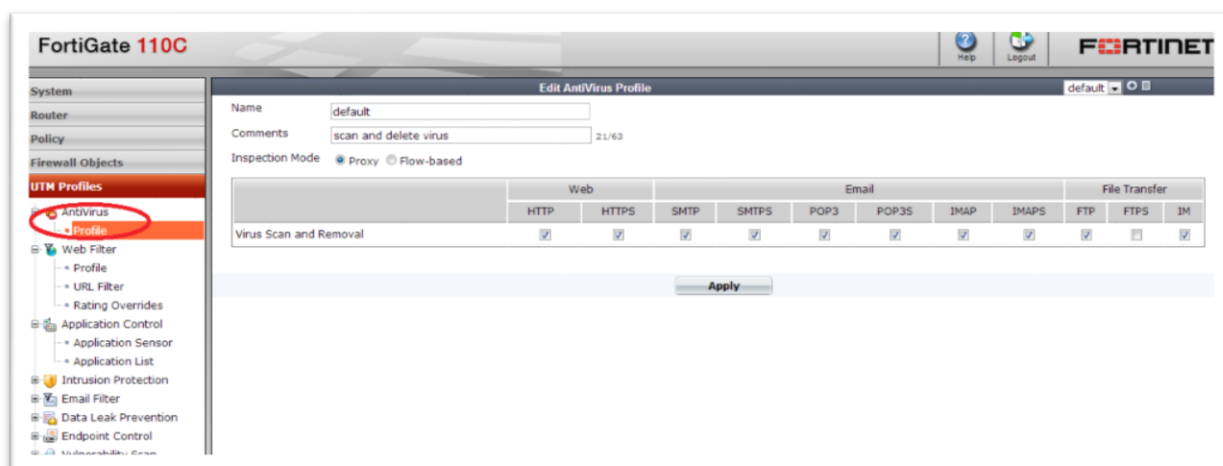
<http://kb.fortinet.com/kb/documentLink.do?externalID=FD35257>

Note that some sites may then create certificate issues. This may be unavoidable, but those sites could be excluded from the SSL inspection if required. A guide on how to do that can be found here:

<http://cookbook.fortinet.com/preventing-certificate-warnings/>

ANTIVIRUS

Profile page



On this page, you can edit, delete or create a new antivirus profile.

- Create New: Creates a new antivirus profile. When you select Create New, you are automatically redirected to the New Antivirus Profile page.
- Edit: Modifies settings within the antivirus profile. When you select Edit, you are automatically redirected to the Edit Antivirus Profile page.
- Delete: Removes an antivirus profile from the list on the Profile page.

To remove multiple antivirus profiles from within the list, on the Antivirus Profile page, in each of the rows of the profiles you want to remove, select the check box and then select Delete.

To remove all antivirus profiles in the list, on the Antivirus Profile page, select the check box in the check box column, and then select Delete.

- Name: The name of the antivirus profile.
- Comments: A description for the antivirus profile.

New Antivirus Profile page

This page also allows you to configure quarantine settings for including a virus sender to the Banned User List.

This page appears when you select Create New on the Edit Antivirus Profile page. If you are on the Profile page, and you select Create New, you will be redirected to the New Antivirus Profile page.

Note: Logging is enabled in the CLI.

- **Name:** Enter a name for the profile. If you are editing an existing antivirus profile and want to change the name, enter a new name in this field. You must select OK to save these changes.
- **Comments:** Enter a description for the profile; this is optional. If you are editing an existing antivirus profile and want to change the description, enter the changes in this field. You must select OK to save the changes.
- **Virus Scan and Removal:** Select any of the following to have the unit scan for viruses when the available protocols are used for web (Internet activity, for example HTTP), email (for example, POP3 or POP3S), and transferring files (for example, FTP).
- **Quarantine:** Select to enable the quarantine of detected viruses. Quarantined information is available in Log&Report > Log & Archive Access.

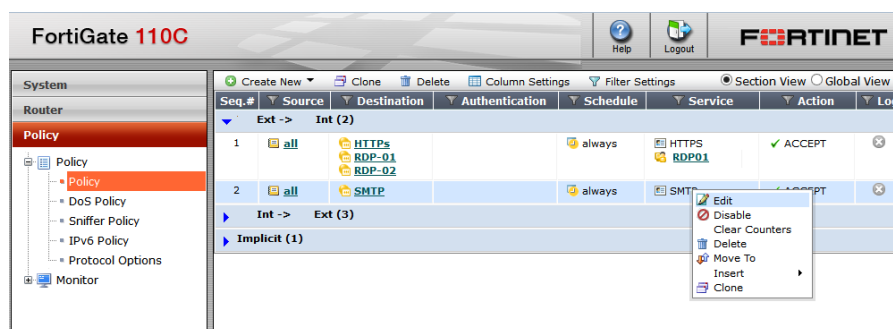
ANTI-SPAM

Email Filter Profiles

Usually you will have an email profile created for you and assigned as the standard inbound email policy. To check which one is in use:

Policy > Policy > Policy

Find the entry for the inbound rule to your mail server, right-click and choose Edit

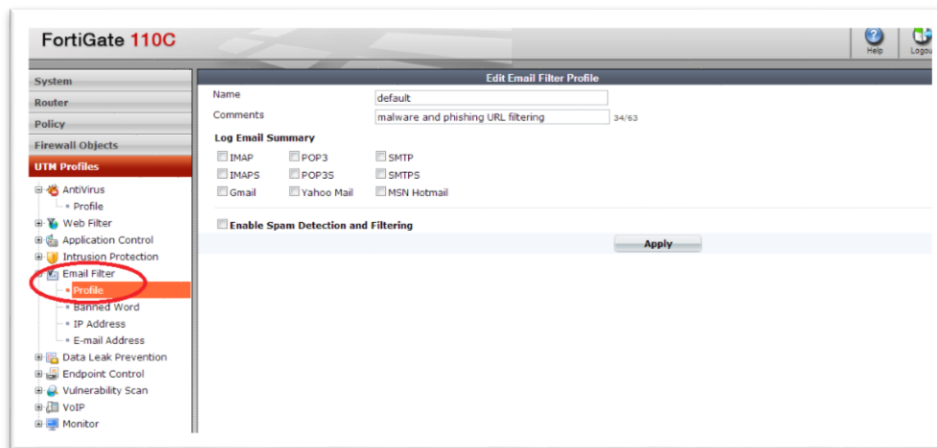


Now look at the UTM options. UTM should be ticked as should “Enable Email Filter”

The name of the active filter will be listed

<input checked="" type="checkbox"/> UTM	
<input type="checkbox"/> Enable AntiVirus	default
<input type="checkbox"/> Enable Web Filter	default
<input type="checkbox"/> Enable Application Control	default
<input type="checkbox"/> Enable IPS	default
<input checked="" type="checkbox"/> Enable Email Filter	Default
<input type="checkbox"/> Enable DLP Sensor	default

New Email Filter Profile page



This provides settings for configuring multiple email filter profiles. If you are editing an email filter profile, you are automatically redirected to the Edit Email Filter Profile page.

This page appears when you select Create New on the Edit Email Filter Profile page. If you are on the Profile page, and you select Create New, you will be redirected to the New Email Filter Profile page.

Name: Enter a name for the email filter profile.

If you are editing an existing email profile and want to change the name, enter the new name in the Name field and then select Apply to save the changes.

Comments: Enter a description about the email filter profile. This is optional.

If you are editing an existing email profile and want to change the description, enter the new description in the Comments field and then select Apply to save the changes.

Log Email Summary: Select to log specific information about the spam email activity on protocols such as IMAP or web mail such as Yahoo Mail.

This feature does not record all email filtering activity, only IMAP, POP3, SMTP, Yahoo Mail, and MSN Hotmail spam detected email messages. If you want to log all email filtering activity, you must enable it in the CLI.

Enable Spam Detection and Filtering: Select to enable specific settings for detecting and filtering spam email messages for IMAP, POP3 and SMTP as well as IMAPS, POP3S and SMTPS.

Spam Action: Select to either tag or discard email that the unit determines to be spam. Tagging adds the text in the Tag Format field to the subject line or header of an email message that is identified as spam. Discard is available only for SMTP.

Note: When you enable virus scanning for SMTP and SMTPS in an antivirus profile, scanning in splice mode is also called streaming mode and is enabled automatically. When scanning in splice mode, the unit scans and streams the traffic to the destination at the same time, terminating the stream to the destination if a virus is selected.

When virus scanning is enabled for SMTP, the unit can only discard spam email if a virus is detected. Discarding immediately drops the connection. If virus scanning is not enabled, you can choose to either tag or discard SMTP spam.

Tag Location: Select to add the tag to the subject or MIME header of email identified as spam. If you select to add the tag to the subject line, the unit converts the entire subject line, including the tag, to UTF-8 format. This improves display for some email clients that cannot properly display subject lines that use more than one encoding.

To add the tag to the MIME header, you must enable spamhdrcheck in the CLI for each protocol (IMAP, POP3 and SMTP).

Tag Format: Enter a word or phrase with which to tag email identified as spam. When typing a tag, use the same language as the unit's current administrator language setting. Tag text using other encodings may not be accepted. For example, when entering a spam tag that uses Japanese characters, first verify that the administrator language settings is Japanese; the unit will not accept a spam tag written in Japanese characters while the administrator language setting is English.

Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the Firewall administrator language setting.

FortiGuard Spam Filtering [optional add on]

Appears only when Enable Spam Detection and Filtering is enabled. Select to enable FortiGuard spam filtering.

Local Spam Filtering

Appears only when Enable Spam Detection and Filtering is enabled. Select to enable local spam filtering. Select the various check boxes beside the options you want included in the profile.

When you enable local spam filtering, you can apply email address and IP address black and white lists, as well as a banned word list to the profile.

Filter Precedence

The order in which incoming emails pass through the spam filter is determined by the protocol used to transfer email.

For SMTP:

1. Verification BWL (Black / White List) IP address with the last IP hop.
2. Verification RBL (Real-time Blackhole List) & ORDBL (Open Relay Database List) IP address FortiGuard check, HELO DNS lookup through.

3. BWL check the email address.
4. Checking the MIME header (Multipurpose Internet Mail Extensions).
5. BWL check the IP address (for IPs extracted from the headers received).
6. Return DNS check emails, check FortiGuard – AntiSpam (for IPs extracted from the headers and URLs received in email content).
7. Verification of banned words in the subject email.
8. Verification of banned words in the email content.

For POP3 and IMAP:

1. BWL check the email address.
2. MIME header check, verification of the IP address BWL.
3. Return DNS check emails, check FortiGuard – AntiSpam RBL & ORDBL verification.
4. Verification of banned words in the subject email.
5. Verification of banned words in the email content.

If SMTP, POP3 and IMAP filters need to ask a server (service FortiGuard-AntiSpam DNSBL / ORDBL) a response is executed simultaneously; to avoid delays, the questions are sent while other filters are running, the first response to a trigger is an action that takes effect as soon as the response is received. Each email goes to the next filter if no matches or problems are found.

The results of all the filter tests are added together to give a score as to whether the mail is spam. The default trigger value is 10. This can be raised to mark less email as spam and lowered to apply a greater scrutiny.

Spam checking Types:

IP Address

The FortiGate unit will submit the IP address of the client to the FortiGuard service for checking. If the IP address exists in the FortiGuard IP address black list, your FortiGate unit will treat the message as spam

URL Checking

The FortiGate unit will submit all URLs appearing in the email message body to the FortiGuard service for checking. If a URL exists in the FortiGuard URL black list, your FortiGate unit will treat the message as spam.

Checksum

The FortiGate unit will submit a checksum of each email message to the FortiGuard service for checking. If a checksum exists in the FortiGuard checksum black list, your FortiGate unit will treat the message as spam.

Spam Submission

When you enable FortiGuard email checksum checking, the FortiGate unit will append a link to the end of every message detected as spam. This link allows email users to “correct” the FortiGuard service by informing it that the message is not spam.

Note: Carefully consider the use of the Spam submission option on email leaving your network. Users not familiar with the feature may click the link on spam messages because they are curious. This will reduce the accuracy of the feature.

HELO DNS

Whenever a client opens an SMTP session with a server, the client sends a HELO command with the client domain name. When you enable HELO DNS lookup, the FortiGate unit will take the domain the client submitted as part of the HELO greeting and send it to the configured DNS. If the domain does not exist, the FortiGate unit will treat all messages the client delivers as spam. The HELO DNS lookup is available only for SMTP traffic.

Return Email DNS Check

The FortiGate unit will take the domain in the reply-to email address and send it to the configured DNS. If the domain does not exist, the FortiGate unit will treat the message as spam.

IP Black/White List (BWL) Checking

The FortiGate unit will compare the client IP address with the IP address black/white list specified. If the client IP address exists, the FortiGate unit acts according to the action configured for the IP address in the list: allow the message, reject it, or mark it as spam

Each IP address black/white list contains a number of IP addresses, each having a specified action. When the FortiGate unit accepts mail from a client with an IP address on the IP address black/white list specified in the active protection profile, it performs the action specified for the address.

To add an address to an IP address black/white list

1. Go to UTM > Email Filter > IP Address.
2. Select the Edit icon of the list to which you want to add an address.
3. Select Create New.
4. Enter the address or netmask in the IP/netmask field.
5. Select the action:
 - Mark as Clear: Messages from clients with matching IP addresses will be allowed, bypassing further email filtering.
 - Mark as Reject: Messages from clients with matching IP addresses will be rejected. The FortiGate unit will return a reject message to the client.

- Mark as Spam: Messages from clients with matching IP addresses will be treated as spam, subject to the action configured in the applicable protection profile.

Email Address Black/White List (BWL) Checking

The FortiGate unit will compare the sender email address with the email address black/white list specified in the protection profile. If the sender email address exists, the FortiGate unit acts according to the action configured for the email address in the list: allow the message or mark it as spam.

Each email address black/white list contains a number of email addresses, each having a specified action. When the FortiGate unit accepts an email message from a client with a reply-to address on the email address black/white list specified in the active protection profile, it performs the action specified for the address.

To add an address to an email address black/white list

1. Go to UTM > Email Filter > E-mail Address.
2. Select the Edit icon of the list to which you want to add an address.
3. Select Create New.
4. Enter the email address in the Email Address field.
5. If you need to enter a pattern in the Email Address field, select whether to use wildcards or regular expressions to specify the pattern.

Wildcard uses an asterisk ("*") to match any number of any character. For example, *@example.com will match all addresses ending in @example.com.

Regular expressions use Perl regular expression syntax. See <http://perldoc.perl.org/perlretut.html> for detailed information about using Perl regular expressions.

6. Select the action:
 - Mark as Spam: Messages with matching reply-to email addresses will be treated as spam, subject to the action configured in the applicable protection profile.
 - Mark as Clear: Messages with matching reply-to addresses will be allowed, bypassing further email filtering.

Banned Word Checking

FortiGate unit will examine the email message for words appearing in the banned word list specified in the protection profile. If the total score of the banned word discovered in the email message exceeds the threshold value set in the protection profile, the FortiGate unit will treat the message as spam.

When determining the banned word score total for an email message, each banned word score is added once no matter how many times the word appears in the message.

Every time the banned word filter detects a pattern in an email message, it adds the pattern score to the sum of scores for the message. You set this score when you create a new pattern to block content. The score can be any number from zero to 99999. Higher scores indicate more offensive content. When the total score equals or exceeds the threshold, the email message is considered as spam and treated according to the spam action configured in the protection profile.

The score for each pattern is counted only once, even if that pattern appears many times in the email message. The default score for banned word patterns is 10 and the default threshold is 10. This means that by default, an email message is blocked by a single match.

A pattern can be part of a word, a whole word, or a phrase. Multiple words entered as a pattern are treated as a phrase. The phrase must appear as entered to match. You can also use wildcards or regular expressions to have a pattern match multiple words or phrases.

Adding words to a banned word list

Each banned word list contains a number of words, each having a score, and specifying whether the email FortiGate unit will search for the word in the message subject, message body, or both.

When the FortiGate unit accepts an email message containing one or more words in the banned word list specified in the active protection profile, it totals the scores of the banned words in the email message.

If the total is higher than the threshold set in the protection profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal.

The score of a banned word present in the message will be counted toward the score total only once, regardless of how many times the word appears in the message

To add words to a banned word list

1. Go to UTM > Email Filter > Banned Word.
2. Select the Edit icon of the list to which you want to add a word.
3. Select Create New.
4. Enter the word or the pattern in the Pattern field.
5. In the Pattern Type field, select whether you use wildcards or regular expressions.

Wildcard uses an asterisk ("*") to match any number of any character. For example, re* will match all words starting with "re".

Regular expressions use Perl regular expression syntax. See <http://perldoc.perl.org/perlretut.html> for detailed information about using Perl regular expressions.

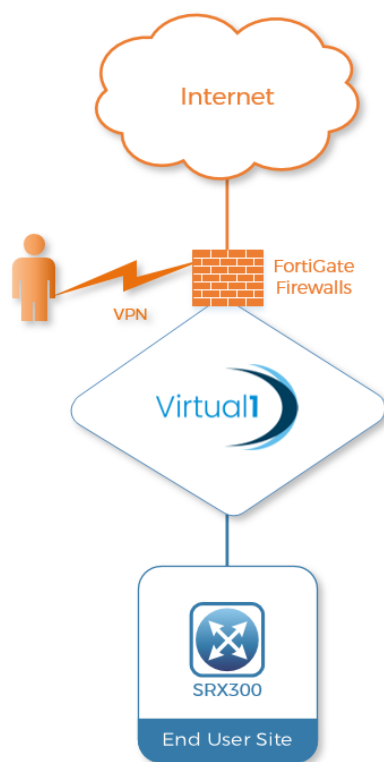
6. In the Language field, select the language.
7. Select where the FortiGate unit will check for the banned word. The options are the message body, the subject, or All, which combines the other two options.
8. Enter a score. If the word appears in the message as determined by the Where setting, the score is added to the scores of all the other banned words appearing in the email message. If the score total is higher than the threshold set in the protection profile, the email message will be detected as spam. If the total score is lower than the threshold, the message will be allowed to pass as normal

VPN

Virtual Private Network (VPN) technology enables remote users to connect to their private Virtual1 network to gain access to their resources in a secure way. For example, an employee traveling or working from home can use a VPN to securely access the office network through the Internet.

The use of a VPN ensures that authorized parties can access the office network from anywhere with an Internet connection and any of the information that is exchanged between the employee and the office is secured and cannot be intercepted.

The firewall supports SSL (using the Fortinet SSL clients), L2TP/IPSec (using the MS Windows client) and GRE/IPSec (Cisco Client). The "Forticlient SSLVPN" client is a simple SSL VPN connectivity client up to version 4.0.2267 (). Fortinet also provide a client called Fortiguard that additionally provides local anti-virus protection for the client. We tend to recommend the former for simplicity.



Configuring user accounts and SSL VPN user groups

Remote users must be authenticated before they can request services and/or access network resources through the web portal. The authentication process relies on FortiGate user group definitions, which can optionally use established authentication mechanisms such as RADIUS and LDAP to authenticate remote clients. (For information about this, we recommend the Fortiguard Admin guide, chapter 7: <http://docs.forticare.com/fos40hlp/43/wwhelp/wwhimpl/js/html/wwhelp.htm>)

You can choose to use a plain text password for authentication through the FortiGate unit (Local domain) or forward authentication requests to an external RADIUS or LDAP server. If password protection will be provided through a RADIUS or

LDAP server, you must configure the FortiGate unit to forward authentication requests to the RADIUS or LDAP server. The following procedures explain how to create a user account and user group in the Local domain.

To create a user account in the Local domain

- Go to User > Local and select Create New.
- In the User Name field, type a name for the remote user (for example, User_1).
- Select Password to have the user authenticated using a password stored on the FortiGate unit.
- In the Password field, type the password to associate with the user account.
- Select OK.
- Repeat this procedure for each remote user.

To create a user group

1. Go to User > User Group and select Create New.
2. In the Group Name field, type a name for the group (for example, Web-only group).
3. From the Type drop-down list, select SSL VPN.
4. One at a time, select user names from the Available Users list, and select the right-pointing arrow to move them to the Members list.
5. Select the blue triangle to expand the SSL-VPN User Group Options.
6. Select Enable SSL-VPN Tunnel Service If the remote clients associated with the user group need to establish an SSL VPN tunnel with the FortiGate unit.

Note: If a user has been configured to use tunnel-mode only, when they log in, the tunnel is brought up automatically.

Configuring user accounts and SSL VPN user groups

To enable client-integrity checking options, select from the following:

- Check FortiClient AV Installed and Running
- Check FortiClient FW Installed and Running
- Check for Third Party AV Software
- Check for Third Party Firewall Software

The client-integrity checking options determine whether the FortiClient™ Host Security application or other antivirus/firewall applications are running on the client computer before a tunnel is established.

If there are no applications installed and enabled on the client computer, the connection is refused. Currently supported AV clients are Norton (Symantec) AntiVirus or McAfee VirusScan.

1. To activate the split tunnel feature, select *Enable Split Tunnelling*. Split tunnelling ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route.(for more on split-tunnelling, see later in this guide)
2. To override the Tunnel IP range defined in VPN > SSL > Config, enter the starting and ending IP address range for this group in the Restrict Tunnel IP range for this group fields.
3. If the user group requires web-only-mode access, select *Enable Web Application* and then select the web applications and/or network file services that the user group needs. The corresponding server applications can be running on the network behind the FortiGate unit or accessed remotely through the Internet.
4. To enable the FortiGate unit to remove residual information from the remote client computer (for example, from the web browser cache) just before the SSL VPN session ends, select *Enable Cache Clean*. When this feature is enabled, if the client's browser cannot install and run the cache cleaner, the user is not allowed to access the SSL-VPN portal.

Note: If you configure a user group and define Restrict tunnel IP range for this group, the group range is used in the SSL VPN configuration. If you do not define a range of global IP addresses, you must define a group range. If you define both IP address ranges, the group level range is applied to the configuration.

5. To have the FortiGate unit display a second HTML page in a popup window when the web portal home page is displayed, type the URL of the web page into the Redirect URL field.
6. To display a custom web portal home page caption for this group, enter the message in the Customize portal message for this group field.
7. Select OK

Note: This custom message overrides the portal message configured in VPN > SSL > Config.

IPsec Layer 2 Tunnelling Protocol (L2TP)

L2TP is a tunnelling protocol published in 1999 that is used with VPNs, as the name suggests. Microsoft Windows operating system has a built-in L2TP client starting

since Windows 2000. Mac OS X 10.3 system and higher also have a built-in client. VPN Clients contact the remote FortiGate Firewall to request the VPN tunnel.

Microsoft Windows Client

Features:

- Standard L2TP/IPSec dialup
- Uses built in Windows client
- No split tunnelling

Configuration Parameters (provided by Virtual1):

- Shared Key
- Username
- Password
- IP address

Creating the IPSec profile on the Firewall

To configure FortiGate unit VPN settings to support FortiClient users, you need to:

- configure the FortiGate Phase 1 VPN settings
- configure the FortiGate Phase 2 VPN settings
- add the firewall policy

1. At the local FortiGate unit, define the phase 1 configuration needed to establish a secure connection with the FortiClient peer:

Name	Enter a name to identify the VPN tunnel. This name appears in phase 2 configurations, firewall policies and the VPN monitor
Remote Gateway	Select Dialup User
Local Interface	Select the interface through which clients connect to the FortiGate unit.
Mode	Select Main (ID Protection).
Authentication Method	Select Pre-shared Key. Enter the pre-shared key. This must be the same pre-shared key provided to the FortiClient users.
Peer option	Select Accept any peer ID.
Enable IPSec Interface	You must select Advanced to see this setting. If IPSec Interface Mode is enabled, the FortiGate unit creates a virtual IPSec interface for a route-based VPN. Disable this option if you want to create a policy-based VPN.

2. Define the phase 2 parameters needed to create a VPN tunnel with the FortiClient

peer.

Name	Enter a name to identify this phase 2 configuration.
Phase 1	Select the name of the phase 1 configuration that you defined.
Advanced	Select to configure the following optional setting; DHCP-IPsec Select if you provide virtual IP addresses to clients using DHCP.

3. Define names for the addresses or address ranges of the private networks that the VPN links. These addresses are used in the firewall policies that permit communication between the networks.

- Define an address name for the individual address or the subnet address that the dialup users access through the VPN.
- If FortiClient users are assigned virtual IP addresses, define an address name for the subnet to which these VIPs belong

4. Define firewall policies to permit communication between the private networks through the VPN tunnel. Route-based and policy-based VPNs require different firewall policies.

Policy-based VPN firewall policy

Define an IPSec firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Source Address Name	Select the address name that you defined in Step 3 for the private network behind this FortiGate unit.
Destination Interface/Zone	Select the FortiGate unit's public interface.
Destination Address Name	If FortiClient users are assigned VIPs, select the address name that you defined in Step 3 for the VIP subnet. Otherwise, select All.
Action	Select IPSEC.
VPN Tunnel	Select the name of the phase 1 configuration that you created in Step 1. Select Allow inbound to enable traffic from the remote network to initiate the tunnel. Select Allow Outbound if you want to allow hosts on the private network to initiate communications with the FortiClient users after the tunnel is established.

Route-based VPN firewall policies

Define an ACCEPT firewall policy to permit communications between the source and destination addresses. Enter these settings in particular:

Source Interface/Zone	Select the VPN Tunnel (IPSec Interface) you configured in Step 1.
Source Address Name	Select All.
Destination Interface/Zone	Select the interface that connects to the private network behind this FortiGate unit.
Destination Address Name	Select All.
Action	Select ACCEPT.
NAT	Disable.

If you want to allow hosts on the private network to initiate communications with the FortiClient users after the tunnel is established, you need to define a firewall policy for communication in that direction. Enter these settings in particular:

5. Place VPN policies in the policy list above any other policies having similar source and destination addresses.

Configuring the Windows PC

The Fortinet suite of security products affords a VPN client application called FortiClient. The software is available for free download from the following location: -

<http://www.forticlient.com/>

By default, an IPsec VPN connection is available to a Virtual Firewall without additional licencing. Additional security features such as client Antivirus, Web Security and SSL VPNs are available with supplementary licences.

[Windows XP]

Configuration of the Windows PC for a VPN connection to the FortiGate unit consists of the following:

- In Network Connections, configure a Virtual Private Network connection to the FortiGate unit.
- Ensure that the IPSEC service is running.
- Ensure that IPsec has not been disabled for the VPN client.

The instructions in this section are based on Windows XP SP3. Other versions of Windows may vary slightly.

To configure the network connection:

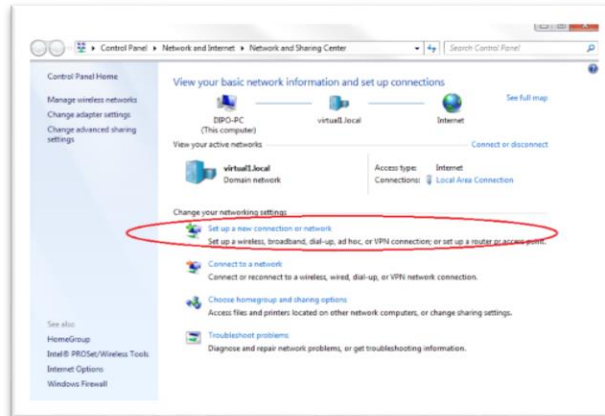
- Open *Network Connections*.
- This is available through the Control Panel.
- Double-click *New Connection Wizard* and *Select Next*.
- Select *Connect to the network at my workplace*.
- Select *Next*.
- Select *Virtual Private Network connection* and then select *Next*.
- In the *Company Name* field, enter a name for the connection and then select *Next*.
- Select *Do not dial the initial connection* and then select *Next*.
- Enter the public IP address or FQDN of the FortiGate unit and then select *Next*.
- Optionally, select *Add a shortcut to this connection to my desktop*.
- Select *Finish*. The *Connect* dialog opens on the desktop.
- Select *Properties* and then select the *Security* tab.
- Select *IPSec Settings*.
- Select *Use pre-shared key for authentication*, enter the pre-shared key that you have been allocated for your VPN, and select *OK*.
- Select *OK*.

To check that the IPSEC service is running:

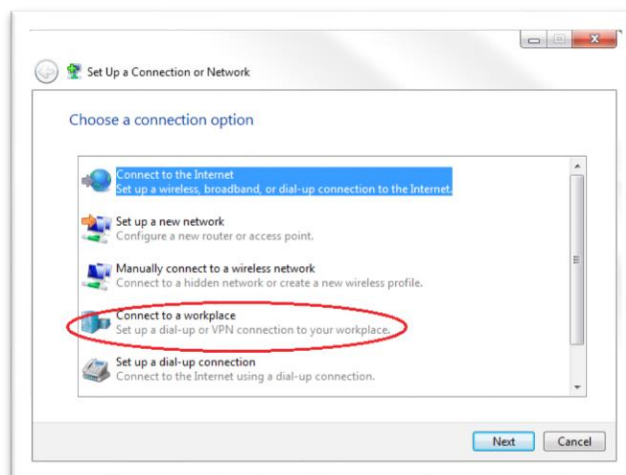
- Open *Administrative Tools*.
- This is available through the Control Panel.
- Double-click *Services*.
- Look for IPSEC Services. Confirm that the *Startup Type* is *Automatic* and *Status* is set to *Started*. If needed, double-click *IPSEC Services* to change these settings.

[Windows 7, 10, 10.1]

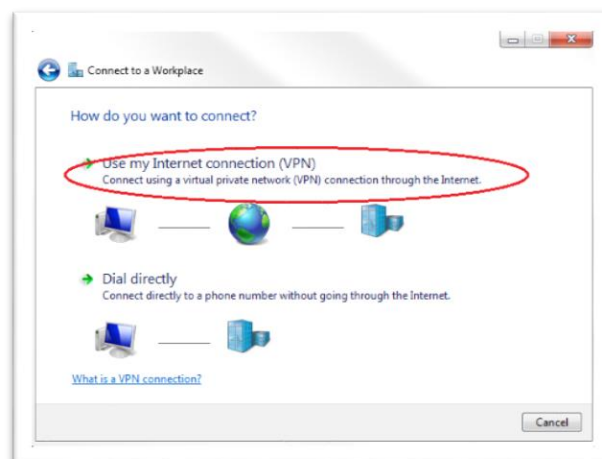
Open up *network and sharing centre* from Control Panel, and choose *Set up a new connection or network*.



Choose *connect to a workplace*



Choose *use my Internet connection*



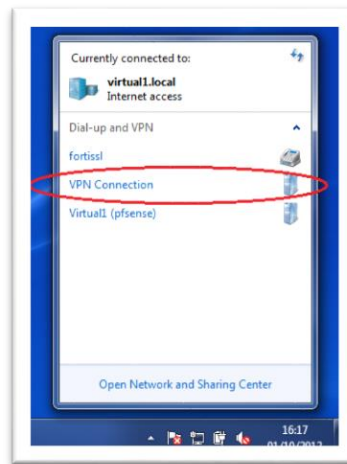
Type in your IP Address and name the connection in the destination name box and click Next

The screenshot shows a Windows dialog box titled "Connect to a Workplace". The main heading is "Type the Internet address to connect to". Below this, it says "Your network administrator can give you this address." There are two input fields: "Internet address:" with a placeholder "[Example:Contoso.com or 157.54.0.1 or 3ffe1234-1111]" and "Destination name:" with the text "VPN Connection". At the bottom, there are three checkboxes: "Use a smart card" (unchecked), "Allow other people to use this connection" (unchecked) with a sub-note "This option allows anyone with access to this computer to use this connection.", and "Don't connect now; just set it up so I can connect later" (checked). "Next" and "Cancel" buttons are at the bottom right.

Type in your username and password details and click create

The screenshot shows the same "Connect to a Workplace" dialog box, but at a different step. The heading is "Type your user name and password". It features three input fields: "User name:", "Password:", and "Domain (optional):". Between the "Password:" and "Domain (optional):" fields are two checkboxes: "Show characters" (unchecked) and "Remember this password" (unchecked). "Create" and "Cancel" buttons are located at the bottom right.

Your VPN is now ready to use. To launch it, simply click the small network icon on the system tray at the bottom right corner, and pick the new connection created from the popup list, and connect.



SSL VPN's

SSL (Secure Sockets Layer) VPNs use HTTPS which is supported by most web browsers for exchanging sensitive information securely between a web server and a client. SSL establishes an encrypted link, ensuring that all data passed between the FortiGate and the browser remains private and secure. SSL protection is initiated automatically when a user (client) connects to the FortiGate. Once the successful connection is established, the browser encrypts all the information before it leaves the computer. When the information reaches its destination, it is decrypted using a secret (private) key. Any data sent back is first encrypted, and is decrypted when it reaches the client.

Web-Only mode

Web-Only mode provides remote users with a fast and efficient way to access server applications from any thin client computer equipped with a web browser. Web-only mode offers true clientless network access using any web browser that has built-in SSL encryption and the Java runtime environment.

When the FortiGate unit provides services in web-only mode, a secure connection between the remote client and the FortiGate unit is established through the SSL VPN security in the FortiGate unit and the SSL security in the web browser. After the connection has been established, the FortiGate unit provides access to selected services and network resources through a web portal.

Tunnel mode

Tunnel mode offers remote users the freedom to connect to the internal network using the traditional means of web-based access from laptop computers.

The SSL VPN client encrypts all traffic from the remote client computer and sends it to the FortiGate unit through an SSL VPN tunnel over the HTTPS link between the web browser and the FortiGate unit.

Split tunnelling is an option which ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. This could potentially conserve bandwidth and alleviates bottlenecks.

In tunnel mode, remote clients connect to the FortiGate unit and the web portal login page using Microsoft Internet Explorer, Mozilla Foundation/Firefox, Mac OS, or Linux.

The FortiGate unit acts as a secure HTTP/HTTPS gateway and authenticates remote users as members of a user group. After successful authentication, the FortiGate unit redirects the web browser to the web portal home page dictated by the user group settings. If the user does not have the SSL VPN client installed, they will be prompted to download the SSL VPN client (an ActiveX or Java plugin) and install it using controls provided through the web portal.

FortiGate SSL VPN dialup client

When the user initiates a VPN connection with the FortiGate unit through the SSL VPN client, the FortiGate unit establishes a tunnel with the client and assigns the client a virtual IP address from a range of reserved addresses. The client uses the assigned IP address as its source address for the duration of the connection. After the tunnel has been established, the user can access the network behind the FortiGate unit.

Features

- Option to use Web Browser only or Slim line client
- Split tunnelling

Configuration Parameters

- Username
- Password
- URL

DHCP

Dynamic Host Configuration Protocol is a system used to assign IP addresses and other, related information to network clients. Usually a server on the customer LAN performs this role and the firewall simply has to refer request to it. If no such server exists, the firewall can perform the role itself. DHCP is especially important for VPN configurations.

Configuring DHCP service on the FortiGate unit

If the FortiClient dialup clients are configured to obtain a VIP address using DHCP, configure the FortiGate dialup server to either:

- relay DHCP requests to a DHCP server behind the FortiGate unit
- act as a DHCP server

To configure DHCP relay on the FortiGate unit

1. Go to System > DHCP > Service.
2. Expand the row that corresponds to the interface to the Internet (for example, external or wan1).

3. In the Relay row beneath the interface name, select the Edit icon.
4. Select DHCP Relay Agent Enable
5. For Type select IPSEC.
6. In the DHCP Server IP field, type the IP address of the DHCP server.
7. Select OK.
8. If a router is installed between the FortiGate unit and the DHCP server, define a static route to the DHCP server.

To configure a DHCP server on the FortiGate unit

1. Go to System > DHCP > Service.
2. Expand the row that corresponds to the interface to the Internet (for example, external or wan1).
3. In the Servers row beneath the interface name, select the Add DHCP Server icon (+).
4. In the Name field, type a name for the FortiGate DHCP server configuration.
5. Select IPsec, enter the information outlined in the table below and select OK:

IP Range	Enter the range of VIP addresses that the DHCP server can dynamically assign to dialup clients when they connect. As a precaution, do not assign VIP addresses that match the private network behind the FortiGate unit(for example, if the dialup clients need to access a host on local subnet 192.168.12.0/24, you could configure the DHCP server to assign any VIP address in the 10.254.254.100to 10.254.254.125range). If you need to exclude specific IP addresses from the range, you can define an exclusion range.
Network Mask	Enter the network mask of the IP addresses that you specified in the IP Range fields (for example, 255.255.255.0for a class C network).
Default Gateway	Enter the IP address of the default gateway that the DHCP server assigns to DHCP clients.
Domain	If you want the FortiGate unit to assign a domain name to dialup clients when they connect, enter the registered domain name
Lease Time	Specify a lease time:

Setting-up Users to be able to VPN before login:

Windows XP

Windows XP uses a feature called PLAP (Pre-Login Access Provider)

1. For information on creating Windows XP VPN connections, visit:
<http://support.microsoft.com/kb/314076>
2. The **Anyone's Use** tickbox must be selected when creating the VPN connection.

Logging on using PLAP

1. At the Log On to Windows dialogue box, fill in the User name and Password fields. Select your domain from the Log on to drop down. Then check the Log on using dial-up connection checkbox. (If they are hidden, click **Options** to reveal the Log on to drop down and dial-up checkbox.) Click OK.
2. The Network Connections dialog box will appear. Select your VPN connection from the drop down. Click Connect.

Windows 7, 10, 10.1

Windows uses a feature called SSO (Single Sign-on)

1. Logon on using the credentials of a local administrator on the computer:
2. Open the Network and Sharing Center and create your VPN connection, by clicking **Set Up A New Connection**



3. Choose **Connect To A Workplace**
4. On the next page, specify a FQDN or IP address for your shared firewall instance, and type a friendly name for this connection. **VERY IMPORTANT:** Also be sure to select the **Allow Other People To Use This Connection** checkbox as shown below.



Selecting that checkbox is important since it makes the System the owner of the VPN connection and not the user. Select the **Don't Connect Now** option which will

set up the new VPN connection but not initiate it until you manually choose to do so later.

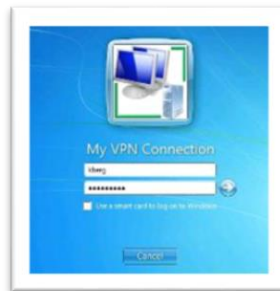
5. On the next wizard page, type the credentials that will be used for logging on to the domain.
6. Finish the wizard to set up the new VPN connection.

Logging On using VPN SSO

7. Turn on the computer and wait until the logon screen appears.
8. Press Ctrl+Alt+Del. Click **Switch User**
9. Click the blue button on the bottom-right near the usual Red button



A screen will open with the name entered as the VPN friendly name entered in step 4 of the procedure above. Type the username and password.



10. Once the VPN connection has been established, the credentials used will automatically be used to log on to the desktop of the computer.

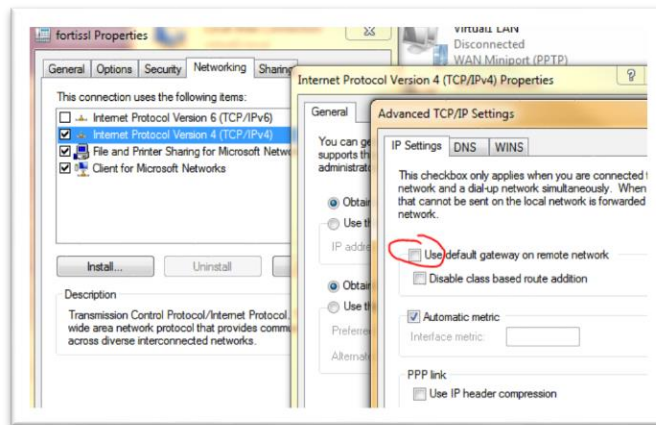
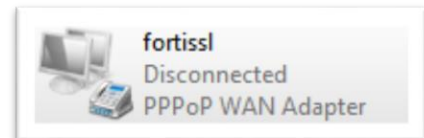
When Remote client has out of date cached credentials and cannot get on the domain:

1. Login to the laptop as a user that can get onto it (ie. cached credentials)
2. Run the VPN and connect as usual
3. In a CMD window type: "RUNAS /profile /user:DOMAIN\USER cmd"
4. Type in their correct password when prompted
5. The username/password will now be cached properly
6. Disconnect the VPN. Restart. Login as normal

VPN Split-Tunnelling

When the VPN user wants to access the Internet using a connection other than routing through the VPN tunnel they need to use "Split-tunnelling". This feature requires the use of the SSL client provided by FortiGate rather than the In-built Windows Client.

1. Install and configure the SSL client
2. Under Windows control Panel, navigate to **Network and Internet > Network Connections**
3. Right-click "fortissl" and select Properties
4. Untick the "Use default gateway on remote network" option. The SSL Client will not allow



for Windows Single Sign-on. So Split-tunnelling and SSO are mutually exclusive.

VPN Tunnels (Site-to-Site)

The FortiGate supports both route-based and policy-based tunnels. Route-based are generally easier to configure, but both have their benefits:

Policy-based	Route-based
Available in NAT/Route or Transparent mode	Available only in NAT/Route mode
Requires a firewall policy with IPSEC action that specifies the VPN tunnel. One policy controls connections in both directions.	Requires only a simple firewall policy with ACCEPT action. A separate policy is required for connections in each direction.
Supports DHCP over IPsec	Does not support DHCP over IPsec

Configuring site-to-site VPNs can be complicated and it is recommended you read the Fortinet manual, found here: <http://docs.fortinet.com/fgt/archives/3.0/techdocs>.

EXPORTING THE POLICY

If you have an existing FortiGate device, you may wish to export the policy so that you can examine it, make any edits and either upload it or use it as a basis for manually creating a new one.

Exporting the Policy using the GUI

(left hand side) System > Dashboard > Dashboard

(right hand side) System Information > System Configuration > Backup

Choose local PC, leave "Encrypt" unticked and don't set a password.

The result is a clear text firewall policy.

Exporting the Policy using the CLI

There is no CLI export commands but you can instead display the policy on the screen and capture the output to a text file (see the help file for your chosen terminal software for details). Here are the FortiGate commands to display the policy and related objects on-screen:

```
show firewall policy
show firewall address
show firewall addrgrp
```

Exporting the Policy from a different type of firewall

If the source firewall is not a FortiGate, we recommend using a tool such as Forticonverter. It is an expensive tool but useful if there are a lot of migrations to be done during the course of a year.

<https://www.fortinet.com/products-services/products/firewall/forticonverter.html>