WAN Optimization, Web Cache, Explicit Proxy, and WCCP

FortiOS™ Handbook v2
for FortiOS 4.0 MR2
### WAN optimization configuration examples

<table>
<thead>
<tr>
<th>Example: Basic peer-to-peer WAN optimization configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network topology and assumptions</td>
<td>55</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>56</td>
</tr>
<tr>
<td>Configuring basic peer-to-peer WAN optimization - web-based manager</td>
<td>56</td>
</tr>
<tr>
<td>Configuring basic peer-to-peer WAN optimization - CLI</td>
<td>58</td>
</tr>
<tr>
<td>Testing and troubleshooting the configuration</td>
<td>59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example: Active-passive WAN optimization</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network topology and assumptions</td>
<td>61</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>62</td>
</tr>
<tr>
<td>Configuring basic active-passive WAN optimization - web-based manager</td>
<td>62</td>
</tr>
<tr>
<td>Configuring basic active-passive WAN optimization - CLI</td>
<td>65</td>
</tr>
<tr>
<td>Testing and troubleshooting the configuration</td>
<td>67</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example: Adding secure tunneling to an active-passive WAN optimization configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network topology and assumptions</td>
<td>69</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>69</td>
</tr>
<tr>
<td>Configuring WAN optimization with secure tunneling - web-based manager</td>
<td>70</td>
</tr>
<tr>
<td>Configuring WAN optimization with secure tunneling - CLI</td>
<td>72</td>
</tr>
</tbody>
</table>

### Web caching

<table>
<thead>
<tr>
<th>Configuring Web Cache Only WAN optimization</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exempting web sites from web caching</td>
<td>76</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example: Web Cache Only WAN optimization</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network topology and assumptions</td>
<td>77</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Web Cache Only WAN optimization - web-based manager</td>
<td>78</td>
</tr>
<tr>
<td>Configuring Web Cache Only WAN optimization - CLI</td>
<td>79</td>
</tr>
<tr>
<td>Testing and troubleshooting the configuration</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring active-passive web caching</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Active-passive Web Caching</td>
<td>82</td>
</tr>
<tr>
<td>Network topology and assumptions</td>
<td>82</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>82</td>
</tr>
<tr>
<td>Configuring active-passive web caching - web-based manager</td>
<td>82</td>
</tr>
<tr>
<td>Configuring active-passive web caching - CLI</td>
<td>84</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuring peer-to-peer web caching</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Peer-to-peer web caching</td>
<td>86</td>
</tr>
<tr>
<td>Network topology and assumptions</td>
<td>86</td>
</tr>
<tr>
<td>General configuration steps</td>
<td>87</td>
</tr>
<tr>
<td>Configuring peer-to-peer web caching - web-based manager</td>
<td>87</td>
</tr>
<tr>
<td>Configuring peer-to-peer web caching - CLI</td>
<td>88</td>
</tr>
</tbody>
</table>
Changing web cache settings ................................................. 89

**Advanced configuration example** ................................. 93
Out-of-path WAN optimization with inter-VDOM routing ............... 93
  Network topology and assumptions .................................. 93
  Configuration steps ..................................................... 94
  Client-side configuration steps - web-based manager .............. 95
  Server-side configuration steps - web-based manager ............. 102
  Client-side configuration steps - CLI .................................. 105
  Server-side configuration steps - CLI .................................. 112

**SSL offloading for WAN optimization and web caching** .......... 115
Example: SSL offloading for a WAN optimization tunnel .............. 115
  Network topology and assumptions .................................. 115
  General configuration steps ......................................... 117
  Client-side configuration steps ..................................... 117
  Server-side configuration steps ..................................... 118
Example: SSL offloading and reverse proxy web caching for an Internet web server ............................................. 119
  Network topology and assumptions .................................. 119
  Configuration steps ..................................................... 120

**FortiClient WAN optimization** ........................................ 123
Configuring FortiClient WAN optimization ............................ 123
  FortiClient configuration steps ...................................... 124
  FortiGate unit configuration steps ................................... 124

**The FortiGate explicit web proxy** .................................... 125
Configuration overview ................................................... 126
  Proxy auto-config (PAC) configuration .............................. 129
  Authentication realm ................................................... 130
  Global explicit web proxy options .................................. 130
Explicit web proxy authentication ....................................... 130
  IP-Based authentication ............................................. 130
  Per session authentication .......................................... 131
UTM features and the explicit web proxy ................................ 132
  Explicit proxy sessions and protocol options ....................... 133
  Explicit proxy sessions web filtering and FortiGuard web filtering .................................................. 133
  Explicit proxy sessions and antivirus ................................. 134
Example: users on an internal network browsing the Internet through
the explicit proxy with web caching, RADIUS authentication, web filtering and virus scanning .................................................. 134
   General configuration steps .................................................. 135
   Configuring the explicit web proxy - web-based manager .................. 135
   Configuring the explicit web proxy - CLI .................................................. 137
   Testing and troubleshooting the configuration .............................. 138
Explicit web proxy sessions and user limits .................................. 139

FortiGate WCCP ........................................................................ 143
   How WCCP works ..................................................................... 143
   Example: WCCP router and client configuration .......................... 144
      WCCP router configuration ..................................................... 144
   Configuring the forward and return methods and adding authentication . 146
   WCCP Messages ....................................................................... 147
   Troubleshooting WCCP ............................................................... 147
      Real time debugging ............................................................... 147
      Application debugging ......................................................... 147

WAN optimization, web cache and WCCP get and diagnose commands 149
   get test {wa_cs | wa_dbd | wad | wad_diskd | wccpd} <test_level> ................ 149
      Examples ........................................................................... 149
   diagnose wad ......................................................................... 152
      Examples ........................................................................... 152
   diagnose wacs ....................................................................... 154
   diagnose wadbd ...................................................................... 154
   diagnose debug application {wa_cs | wa_dbd | wad | wad_diskd | wccpd}  
      [<debug_level>]. ................................................................. 154

Index ...................................................................................... 155
Introduction

Welcome and thank you for selecting Fortinet products for your network protection.

You can use FortiGate WAN optimization and web caching to improve performance and security of traffic passing between locations on your wide area network (WAN) or from the Internet to your web servers. You can also use the FortiGate unit as an explicit web proxy server. If your FortiGate unit supports web caching, you can also add web caching to the web proxy server.

This document describes how FortiGate WAN optimization, web caching, and web proxy work and also describes how to configure these features.

This chapter contains the following topics:

- Revision history
- Before you begin
- Document conventions
- Entering FortiOS configuration data
- Registering your FortiNet product
- FortiNet products End User License Agreement
- Training
- Documentation
- Customer service and technical support

Revision history

Table 1: Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-420-96996-20101019</td>
<td>Misc. corrections and text improvements. New graphics format implemented.</td>
</tr>
<tr>
<td>01-420-96996-201000504</td>
<td>More info added to “The FortiGate explicit web proxy” on page 125. “WAN optimization, web cache and WCCP get and diagnose commands” on page 149 made into a standalone section.</td>
</tr>
<tr>
<td>01-420-96996-201000413</td>
<td>Updated to FortiOS 4.0 MR2. More info added to “WAN optimization, web cache and WCCP get and diagnose commands” on page 149. Major changes to the following chapters: “WAN optimization and Web cache storage” on page 37 “The FortiGate explicit web proxy” on page 125 “FortiGate WCCP” on page 143 Added testing and troubleshooting sections to some of the configuration examples. For example, “Testing and troubleshooting the configuration” on page 59.</td>
</tr>
</tbody>
</table>
Before you begin

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

- Your FortiGate unit must support WAN optimization, web cache, and web proxy. See “FortiGate models that support WAN optimization” on page 10.
- Your FortiGate unit must include one or more hard disk that must be correctly formatted and partitioned. See “WAN optimization and Web cache storage” on page 37.
- If you enable virtual domains (VDOMs) on the FortiGate unit, WAN optimization, web caching, and web proxy are available separately for each VDOM.
- This guide is based on the assumption that you are a FortiGate administrator. It is not intended for others who may also use the FortiGate unit, such as FortiClient administrators or end users.
- FortiGate WAN optimization is proprietary to Fortinet. FortiGate WAN optimization is compatible only with FortiClient WAN optimization, and will not work with other vendors’ WAN optimization or acceleration features.

At this stage, the following installation and configuration conditions are assumed:

- You have already successfully installed two or more FortiGate units at various locations across your WAN by following the instructions in the appropriate FortiGate unit QuickStart or Installation Guide. You can download FortiGate installation guides from the FortiGate documentation page: http://docs.fortinet.com/fgt.html.
- You have administrative access to the web-based manager and/or CLI.
- The FortiGate units are integrated into your WAN.
- The operation mode has been configured.
- The system time, DNS settings, administrator password, and network interfaces have been configured.
- Firmware, FortiGuard Antivirus and FortiGuard Antispam updates are completed.
- You have added firewall policies to allow your FortiGate units to process traffic.

FortiGate models that support WAN optimization

WAN optimization is available on newer FortiGate models that also support SSL acceleration and byte caching and web caching storage locations such as high-capacity internal hard disks, the FortiGate-ASM-S08 AMC hard disk module, or FortiGate Storage Modules (FSMs). All of these storage locations can provide similar web caching and byte caching performance. If you add more than one storage location (for example, by creating multiple partitions on a storage device, by using more than one FSM, or by using and FSM and AMC hard disk in the same FortiGate unit) you can configure different storage locations for web caching and byte caching.

Table 1: Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-410-96996-20100127</td>
<td>Corrected subnet addresses in examples. In previous versions of this guide examples showed entering the address of a complete subnet as 172.20.120.0. The correct syntax for the web-based manager is 172.20.120.* and the correct syntax for the CLI is 172.20.120.0-172.20.120.255. Added “WAN optimization, web cache and WCCP get and diagnose commands” on page 149.</td>
</tr>
</tbody>
</table>
A storage location is only required for web caching and byte caching. All other WAN optimization features, including SSL acceleration, are supported if a storage location is not available.

You configure WAN optimization storage options from the FortiGate CLI. See "WAN optimization and Web cache storage" on page 37.

How this guide is organized

This FortiOS Handbook chapter describes how to implement WAN optimization, web caching and the web proxy on supported FortiGate units.

The FortiOS Handbook chapter contains the following sections:

**WAN optimization, web cache, and web proxy concepts**: Provides an overview of FortiGate WAN optimization best practices and technologies and some of the concepts and rules for using them. We recommend that you begin with this chapter before attempting to configure your FortiGate unit to use WAN optimization.

**WAN optimization and Web cache storage**: Describes how to configure WAN optimization storage settings to control how data is stored for web caching and byte caching.

**WAN optimization peers and authentication groups**: Describes how to use WAN optimization peers and authentication groups to control access to WAN optimization tunnels.

**Configuring WAN optimization rules**: Provides basic configuration for WAN optimization rules, including adding rules, organizing rules in the rule list and using WAN optimization addresses. This chapter also explains how WAN optimization accepts sessions, as well as how and when you can apply UTM features to WAN optimization traffic.

**WAN optimization configuration examples**: Describes basic active-passive and peer-to-peer WAN optimization configuration examples. This chapter is a good place to start learning how to put an actual WAN optimization network together.

**Web caching**: Describes how WAN optimization web caching works to cache different session types, including HTTPS, and includes web caching configuration examples.

**Advanced configuration example**: Provides a configuration example that combines WAN optimization, web caching, out-of-path WAN optimization, and the use of multiple VDOMs to apply UTM features to sessions being optimized.

**SSL offloading for WAN optimization and web caching**: Describes how to offload SSL processing from web sites to FortiGate units to improve WAN performance for SSL-protected web sites on a WAN.

**FortiClient WAN optimization**: Describes how FortiGate and FortiClient WAN optimization work together and includes an example configuration.

**The FortiGate explicit web proxy**: Describes the FortiGate web proxy and how to add web caching to a proxy configuration. This chapter includes guidance to pass to end-users when they need to configure their web browsers to use the proxy.

**FortiGate WCCP**: Describes FortiGate WCCP and how to configure WCCP and the WCCP client.

**WAN optimization, web cache and WCCP get and diagnose commands**: describes get and diagnose commands available for troubleshooting WAN optimization, web cache, and WCCP.

Document conventions

Fortinet technical documentation uses the conventions described below.
IP addresses

To avoid publication of public IP addresses that belong to Fortinet or any other organization, the IP addresses used in Fortinet technical documentation are fictional and follow the documentation guidelines specific to Fortinet. The addresses used are from the private IP address ranges defined in RFC 1918: Address Allocation for Private Internets, available at http://ietf.org/rfc/rfc1918.txt?number-1918.

Most of the examples in this document use the following IP addressing:

- IP addresses are made up of A.B.C.D
- A - can be one of 192, 172, or 10 - the non-public addresses covered in RFC 1918.
- B - 168, or the branch / device / virtual device number.
  - Branch number can be 0xx, 1xx, 2xx - 0 is Head office, 1 is remote, 2 is other.
  - Device or virtual device - allows multiple FortiGate units in this address space (VDOMs).
  - Devices can be from x01 to x99.
- C - interface - FortiGate units can have up to 40 interfaces, potentially more than one on the same subnet
  - 001 - 099- physical address ports, and non -virtual interfaces
  - 100-255 - VLANs, tunnels, aggregate links, redundant links, vdom-links, etc.
- D - usage based addresses, this part is determined by what device is doing
  - The following gives 16 reserved, 140 users, and 100 servers in the subnet.
  - 001 - 009 - reserved for networking hardware, like routers, gateways, etc.
  - 010 - 099 - DHCP range - users
  - 100 - 109 - FortiGate devices - typically only use 100
  - 110 - 199 - servers in general (see later for details)
  - 200 - 249 - static range - users
  - 250 - 255 - reserved (255 is broadcast, 000 not used)
- The D segment servers can be farther broken down into:
  - 110 - 119 - Email servers
  - 120 - 129 - Web servers
  - 130 - 139 - Syslog servers
  - 140 - 149 - Authentication (RADIUS, LDAP, TACACS+, FSAE, etc)
  - 150 - 159 - VoIP / SIP servers / managers
  - 160 - 169 - FortiAnalyzers
  - 170 - 179 - FortiManagers
  - 180 - 189 - Other Fortinet products (FortiScan, FortiDB, etc.)
  - 190 - 199 - Other non-Fortinet servers (NAS, SQL, DNS, DDNS, etc.)
  - Fortinet products, non-FortiGate, are found from 160 - 189.
The following table shows some examples of how to choose an IP number for a device based on the information given. For internal and dmz, it is assumed in this case there is only one interface being used.

**Table 2: Examples of the IP numbering**

<table>
<thead>
<tr>
<th>Location and device</th>
<th>Internal</th>
<th>Dmz</th>
<th>External</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head Office, one FortiGate</td>
<td>10.011.101.100</td>
<td>10.011.201.100</td>
<td>172.20.120.191</td>
</tr>
<tr>
<td>Head Office, second FortiGate</td>
<td>10.012.101.100</td>
<td>10.012.201.100</td>
<td>172.20.120.192</td>
</tr>
<tr>
<td>Branch Office, one FortiGate</td>
<td>10.021.101.100</td>
<td>10.021.201.100</td>
<td>172.20.120.193</td>
</tr>
<tr>
<td>Office 7, one FortiGate with 9 VDOMs</td>
<td>10.079.101.100</td>
<td>10.079.101.100</td>
<td>172.20.120.194</td>
</tr>
<tr>
<td>Office 3, one FortiGate, web server</td>
<td>n/a</td>
<td>10.031.201.110</td>
<td>n/a</td>
</tr>
<tr>
<td>Bob in accounting on the corporate user network (dhcp) at Head Office, one FortiGate</td>
<td>10.0.11.101.200</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Router outside the FortiGate</td>
<td>n/a</td>
<td>n/a</td>
<td>172.20.120.195</td>
</tr>
</tbody>
</table>
**Example Network configuration**

The network configuration shown in Figure 1 or variations on it is used for many of the examples in this document. In this example, the 172.20.120.0 network is equivalent to the Internet. The network consists of a head office and two branch offices.

**Figure 1: Example network configuration**
Cautions, Notes and Tips

Fortinet technical documentation uses the following guidance and styles for cautions, notes and tips.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Note: Presents useful information, but usually focused on an alternative, optional method, such as a shortcut, to perform a step.

Tip: Highlights useful additional information, often tailored to your workplace activity.
Typographical conventions

Fortinet documentation uses the following typographical conventions:

Table 3: Typographical conventions in Fortinet technical documentation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or</td>
<td>From Minimum log level, select Notification.</td>
</tr>
<tr>
<td>check box label</td>
<td></td>
</tr>
<tr>
<td>CLI input</td>
<td>config system dns</td>
</tr>
<tr>
<td></td>
<td>set primary &lt;address_ipv4&gt;</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td>CLI output</td>
<td>FGT-602803030703 # get system settings</td>
</tr>
<tr>
<td></td>
<td>comments : (null)</td>
</tr>
<tr>
<td></td>
<td>opmode : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are not secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as Central_Office_1.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to VPN &gt; IPSEC &gt; Auto Key (IKE).</td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the FortiOS Handbook.</td>
</tr>
</tbody>
</table>

CLI command syntax conventions

This guide uses the following conventions to describe the syntax to use when entering commands in the Command Line Interface (CLI).

Brackets, braces, and pipes are used to denote valid permutations of the syntax. Constraint notations, such as <address_ipv4>, indicate which data types or string patterns are acceptable value input.

Table 4: Command syntax notation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Square brackets</td>
<td>A non-required word or series of words. For example: [verbose {1</td>
</tr>
</tbody>
</table>
Table 4: Command syntax notation  (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angle brackets</td>
<td>A word constrained by data type. To define acceptable input, the angled brackets contain a descriptive name followed by an underscore (_ _) and suffix that indicates the valid data type. For example: &lt;retries_int&gt; indicates that you should enter a number of retries, such as 5. Data types include:</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_name&gt;: A name referring to another part of the configuration, such as policy_A.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_index&gt;: An index number referring to another part of the configuration, such as 0 for the first static route.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_pattern&gt;: A regular expression or word with wild cards that matches possible variations, such as *@example.com to match all email addresses ending in @example.com.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_fqdn&gt;: A fully qualified domain name (FQDN), such as mail.example.com.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_email&gt;: An email address, such as <a href="mailto:admin@mail.example.com">admin@mail.example.com</a>.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_url&gt;: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as <a href="http://www.fortinet.com/">http://www.fortinet.com/</a>.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_ipv4&gt;: An IPv4 address, such as 192.168.1.99.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_v4mask&gt;: A dotted decimal IPv4 netmask, such as 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_ipv4mask&gt;: A dotted decimal IPv4 address and netmask separated by a space, such as 192.168.1.99 255.255.255.0.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_ipv4/mask&gt;: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as 192.168.1.99/24.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_ipv6&gt;: A colon(:)-delimited hexadecimal IPv6 address, such as 3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_v6mask&gt;: An IPv6 netmask, such as /96.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_ipv6mask&gt;: An IPv6 address and netmask separated by a space.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_str&gt;: A string of characters that is not another data type, such as P@ssw0rd. Strings containing spaces or special characters must be surrounded in quotes or use escape sequences.</td>
</tr>
<tr>
<td></td>
<td>• &lt;xxx_int&gt;: An integer number that is not another data type, such as 15 for the number of minutes.</td>
</tr>
</tbody>
</table>
Table 4: Command syntax notation (Continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curly braces { }</td>
<td>A word or series of words that is constrained to a set of options delimited by either vertical bars or spaces. You must enter at least one of the options, unless the set of options is surrounded by square brackets [ ].</td>
</tr>
<tr>
<td>Options delimited by vertical bars</td>
<td>Mutually exclusive options. For example: {enable</td>
</tr>
<tr>
<td>Options delimited by spaces</td>
<td>Non-mutually exclusive options. For example: {http https ping snmp ssh telnet} indicates that you may enter all or a subset of those options, in any order, in a space-delimited list, such as: ping https ssh</td>
</tr>
<tr>
<td></td>
<td>Note: To change the options, you must re-type the entire list. For example, to add snmp to the previous example, you would type: ping https snmp ssh</td>
</tr>
<tr>
<td></td>
<td>If the option adds to or subtracts from the existing list of options, instead of replacing it, or if the list is comma-delimited, the exception will be noted.</td>
</tr>
</tbody>
</table>

**Entering FortiOS configuration data**

The configuration of a FortiGate unit is stored as a series of configuration settings in the FortiOS configuration database. To change the configuration you can use the web-based manager or CLI to add, delete or change configuration settings. These configuration changes are stored in the configuration database as they are made.

Individual settings in the configuration database can be text strings, numeric values, selections from a list of allowed options, or on/off (enable/disable).

**Entering text strings (names)**

Text strings are used to name entities in the configuration. For example, the name of a firewall address, administrative user, and so on. You can enter any character in a FortiGate configuration text string except, to prevent Cross-Site Scripting (XSS) vulnerabilities, text strings in FortiGate configuration names cannot include the following characters:

" (double quote), & (ampersand), ' (single quote), < (less than) and > (greater than)

You can determine the limit to the number of characters that are allowed in a text string by determining how many characters the web-based manager or CLI allows for a given name field. From the CLI, you can also use the tree command to view the number of characters that are allowed. For example, firewall address names can contain up to 64 characters. When you add a firewall address to the web-based manager you are limited to entering 64 characters in the firewall address name field. From the CLI you can do the following to confirm that the firewall address name field allows 64 characters.

```
config firewall address
  tree
   -- [address] --*name (64)
    | - subnet
    | - type
    | - start-ip
    | - end-ip
```
Note that the tree command output also shows the number of characters allowed for other firewall address name settings. For example, the fully-qualified domain name (fqdn) field can contain up to 256 characters.

**Entering numeric values**

Numeric values are used to configure various sizes, rates, numeric addresses, or other numeric values. For example, a static routing priority of 10, a port number of 8080, or an IP address of 10.10.10.1. Numeric values can be entered as a series of digits without spaces or commas (for example, 10 or 64400), in dotted decimal format (for example the IP address 10.10.10.1) or as in the case of MAC or IPv6 addresses separated by colons (for example, the MAC address 00:09:0F:B7:37:00). Most numeric values are standard base-10 numbers, but some fields (again such as MAC addresses) require hexadecimal numbers.

Most web-based manager numeric value configuration fields limit the number of numeric digits that you can add or contain extra information to make it easier to add the acceptable number of digits and to add numbers in the allowed range. CLI help includes information about allowed numeric value ranges. Both the web-based manager and the CLI prevent you from entering invalid numbers.

**Selecting options from a list**

If a configuration field can only contain one of a number of selected options, the web-based manager and CLI present you a list of acceptable options and you can select one from the list. No other input is allowed. From the CLI you must spell the selection name correctly.

**Enabling or disabling options**

If a configuration field can only be on or off (enabled or disabled) the web-based manager presents a check box or other control that can only be enabled or disabled. From the CLI you can set the option to enable or disable.

**Registering your Fortinet product**

Before you begin configuring and customizing features, take a moment to register your Fortinet product at the Fortinet Technical Support web site, https://support.fortinet.com. Many Fortinet customer services, such as firmware updates, technical support, and FortiGuard Antivirus and other FortiGuard services, require product registration.

For more information, see the Fortinet Knowledge Center article Registration Frequently Asked Questions.

**Fortinet products End User License Agreement**

See the Fortinet products End User License Agreement.
Training

Fortinet Training Services provides courses that orient you quickly to your new equipment, and certifications to verify your knowledge level. Fortinet provides a variety of training programs to serve the needs of our customers and partners world-wide.

To learn about the training services that Fortinet provides, visit the Fortinet Training Services web site at http://campus.training.fortinet.com, or email training@fortinet.com.

Documentation

The Fortinet Technical Documentation web site, http://docs.fortinet.com, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, http://docs.fortinet.com.

Fortinet Knowledge Base

The Fortinet Knowledge Base provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this or any Fortinet technical document to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at https://support.fortinet.com.

You can dramatically improve the time that it takes to resolve your technical support ticket by providing your configuration file, a network diagram, and other specific information. For a list of required information, see the Fortinet Knowledge Base article FortiGate Troubleshooting Guide - Technical Support Requirements.
WAN optimization, web cache, and web proxy concepts

FortiGate WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, web caching, SSL offloading, and secure tunnelling. Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiGate units to reduce the amount of data transmitted across the WAN. Web caching stores web pages on FortiGate units to reduce latency and delays between the WAN and web servers. SSL offloading offloads SSL decryption and encryption from web servers onto FortiGate SSL acceleration hardware. Secure tunnelling secures traffic as it crosses the WAN.

You can apply different combinations of these WAN optimization techniques to a single traffic stream depending on the traffic type. For example, you can apply byte caching and secure tunneling to any TCP traffic. For HTTP traffic, you can also apply protocol optimization and web caching.

Web proxy is a feature related to WAN optimization and web caching. You can configure a FortiGate unit to be a web proxy server. Users on your internal network can browse the Internet through the FortiGate web proxy server. If your FortiGate unit supports web caching, you can add web caching to the web proxy.

This chapter describes:

- WAN optimization topologies
- Explicit Web proxy topology
- WCCP topology
- WAN optimization client/server architecture
- WAN optimization tunnels
- Protocol optimization
- Byte caching
- WAN optimization and HA
- Monitoring WAN optimization

WAN optimization topologies

This section describes some common WAN optimization topologies:

- “Basic WAN optimization topologies” on page 22
- “Out-of-path topology” on page 22
- “Web-cache-only WAN optimization” on page 24
- “WAN optimization with web caching” on page 26
- “WAN optimization and web caching with FortiClient peers” on page 26
Basic WAN optimization topologies

The basic FortiGate WAN optimization topology consists of two FortiGate units operating as WAN optimization peers intercepting and optimizing traffic crossing the WAN between the private networks.

Figure 2: Security device and WAN optimization topology

As shown in Figure 2, the FortiGate units can be deployed as security devices that protect private networks connected to the WAN and also perform WAN optimization. In this configuration, the FortiGate units are configured as typical security devices for the private networks and are also configured for WAN optimization. The WAN optimization configuration intercepts traffic to be optimized as it passes through the FortiGate unit and uses a WAN optimization tunnel with another FortiGate unit to optimize the traffic that crosses the WAN.

As shown in Figure 3, you can also deploy WAN optimization on single-purpose FortiGate units that only perform WAN optimization. In Figure 3, the WAN optimization FortiGate units are located on the WAN outside of the private networks. You can also install the WAN optimization FortiGate units behind the security devices on the private networks.

The WAN optimization configuration is the same for FortiGate units deployed as security devices and for single-purpose WAN optimization FortiGate units. The only differences would result from the different network topologies.

Out-of-path topology

In an out-of-path topology, one or both of the FortiGate units configured for WAN optimization are not directly in the main data path. Instead, the out-of-path FortiGate unit is connected to a device on the data path, and the device is configured to redirect sessions to be optimized to the out-of-path FortiGate unit.
Figure 3: Single-purpose WAN optimization topology

Figure 4: Out-of-path WAN optimization

Figure 4 shows out-of-path FortiGate units configured for WAN optimization and connected directly to FortiGate units in the data path. The FortiGate units in the data path use a method such as policy routing to redirect traffic to be optimized to the out-of-path FortiGate units. The out-of-path FortiGate units establish a WAN optimization tunnel between each other and optimize the redirected traffic.

One of the benefits of out-of-path WAN optimization is that out-of-path FortiGate units only perform WAN optimization and do not have to process other traffic. An in-path FortiGate unit configured for WAN optimization also has to process other non-optimized traffic on the data path.
The out-of-path FortiGate units can operate in NAT/Route or Transparent mode. Other out-of-path topologies are also possible. For example, you can install the out-of-path FortiGate units on the private networks instead of on the WAN. Also, the out-of-path FortiGate units can have one connection to the network instead of two. In a one-arm configuration such as this, firewall policies and routing have to be configured to send the WAN optimization tunnel out the same interface as the one that received the traffic.

**Topology for multiple networks**

As shown in Figure 5, you can create multiple WAN optimization configurations between many private networks. Whenever WAN optimization occurs, it is always between two FortiGate units, but you can configure any FortiGate unit to perform WAN optimization with any of the other FortiGate units that are part of your WAN.

**Figure 5: WAN optimization among multiple networks**

You can also configure WAN optimization between FortiGate units with different roles on the WAN. FortiGate units configured as security devices and for WAN optimization can perform WAN optimization as if they are single-purpose FortiGate units just configured for WAN optimization.

**Web-cache-only WAN optimization**

A WAN optimization web-cache-only topology includes one FortiGate unit that acts as both a proxy server and web cache server. The FortiGate unit intercepts web page requests sent by users, requests web pages from the web servers, caches the web page contents, and returns the web page contents to the users. When the FortiGate unit intercepts subsequent requests for cached web pages, the FortiGate unit contacts the destination web server just to check for changes.
You can also configure a reverse proxy web-cache-only WAN optimization (Figure 7). In this configuration, users on the Internet browse to a web server installed behind a FortiGate unit. The FortiGate unit intercepts the web traffic and caches pages from the web server. Reverse proxy web caching on the FortiGate unit reduces the number of requests that the web server must handle, leaving it free to process new requests that it has not serviced before.
**WAN optimization with web caching**

You can add web caching to a WAN optimization topology when users on a private network communicate with web servers located across the WAN on another private network.

*Figure 8: WAN optimization with web caching topology*

The topology in *Figure 8* is the same as that of *Figure 2 on page 22* with the addition of web caching to the FortiGate unit in front of the private network that includes the web servers. In a similar way, you can add web caching to all of the topologies shown in “WAN optimization topologies” on page 21.

**WAN optimization and web caching with FortiClient peers**

FortiClient WAN optimization works with FortiGate WAN optimization to accelerate remote user access to the private networks behind FortiGate units. The FortiClient application requires a simple WAN optimization configuration to automatically detect if WAN optimization is enabled on the FortiGate unit. Once WAN optimization is enabled, the FortiClient application transparently makes use of the WAN optimization and web caching features available.
Explicit Web proxy topology

You can configure a FortiGate unit to be an explicit web proxy server for Internet web browsing. To use the explicit web proxy, users must add the IP address of the FortiGate interface configured for the explicit proxy to their web browser proxy configuration.

Figure 10: Explicit web proxy topology

If the FortiGate unit supports web caching, you can also add web caching to the explicit web proxy. The FortiGate unit will then caches Internet web pages to improve web browsing performance.
WCCP topology

You can operate a FortiGate unit as a Web Cache Communication Protocol (WCCP) router or cache engine. As a router, the FortiGate unit intercepts web browsing requests from client web browsers and forwards them to a WCCP cache engine. The cache engine returns the required cached content to the client web browser. If the cache server does not have the required content it accesses the content, caches it and returns the content to the client web browser.
FortiGate units can also operate as WCCP cache servers, communicating with WCCP routers, caching web content and providing it to client web browsers as required. WCCP is transparent to client web browsers. The web browsers do not have to be configured to use a web proxy.

**WAN optimization client/server architecture**

Traffic across a WAN typically consists of clients on a client network communicating across a WAN with a remote server network. The clients do this by starting communication sessions from the client network to the server network. To optimize these sessions, you add firewall policies to the client-side FortiGate unit (which is located between the client network and the WAN, see Figure 13) to accept sessions from the client network that are destined for the server network. To apply WAN optimization to these sessions, you must also add WAN optimization rules to the client-side FortiGate unit. The WAN optimization rules intercept sessions accepted by firewall policies and apply WAN optimization to them.

**Figure 13: Client/server architecture**

When a client-side FortiGate unit matches a session with a WAN optimization rule, it uses the information in the rule to attempt to start a WAN optimization tunnel with a server-side FortiGate unit installed in front of the server network. The client-side and server side FortiGate units must be able to identify each other. To do this the client-side FortiGate unit configuration must include the IP address and peer host ID of the server-side FortiGate unit and the configuration of the server-side FortiGate unit must include the IP address and peer host ID of the client-side FortiGate unit. With this information available, when the client-side FortiGate unit attempts to contact the server-side FortiGate unit, the two units share their IP addresses and peer host IDs and confirm that they can create a WAN optimization tunnel between each other.
Firewall policies are not required for WAN optimization on the server-side FortiGate unit. Sessions from the client-side to the server-side FortiGate unit are WAN optimization tunnel requests. As long as the client-side and server-side FortiGate units can identify each other according to peer host ID and IP address the server-side FortiGate unit will accept WAN optimization tunnel requests from the client-side FortiGate unit.

In addition to basic identification by peer host ID and IP address you can configure authentication options to impose authentication using certificates and pre-shared keys. In addition to you can configure FortiGate units involved in WAN optimization to accept connections from any identified peer or restrict connections to specific peers.

**WAN optimization peers**

The client-side and server-side FortiGate units are called WAN optimization peers (see Figure 14) because all of the FortiGate units in a WAN optimization network have the same peer relationship with each other. The client and server roles just relate to how a session is started. Any FortiGate unit configured for WAN optimization can be a client-side and a server-side FortiGate unit at the same time, depending on the direction of the traffic. Client-side FortiGate units initiate WAN optimization sessions and server-side FortiGate units respond to the session requests. Any FortiGate unit can simultaneously be a client-side FortiGate unit for some sessions and a server-side FortiGate unit for others.

**Figure 14: WAN optimization peer and tunnel architecture**

To identify all of the WAN optimization peers that a FortiGate unit can perform WAN optimization with, you add host IDs and IP addresses of all of the peers to the FortiGate unit configuration. The peer IP address is actually the IP address of the peer unit interface that communicates with the FortiGate unit.
Peer-to-peer and active-passive WAN optimization

You can create peer-to-peer and active-passive WAN optimization configurations. Peer-to-peer configurations are less complex because they only require the creation of a WAN optimization rule in the client side FortiGate unit. Active-passive WAN optimization configurations require an active rule on the client side FortiGate unit and a passive rule on the server-side FortiGate unit. For more details about peer to peer and active-passive WAN optimization, see “Configuring WAN optimization rules” on page 45.

WAN optimization and the FortiClient application

PCs running the FortiClient application are client-side peers that initiate WAN optimization tunnels with server-side peer FortiGate units. However, you can have an ever-changing number of FortiClient peers with IP addresses that also change regularly. To avoid maintaining a list of such peers, you can instead configure WAN optimization to accept any peer and use authentication to identify FortiClient peers.

Together, the WAN optimization peers apply the WAN optimization features to optimize the traffic flow over the WAN between the clients and servers. WAN optimization reduces bandwidth requirements, increases throughput, reduces latency, offloads SSL encryption/decryption and improves privacy for traffic on the WAN.

Operating modes and VDOMs

To use WAN optimization, the FortiGate units can operate in either NAT/Route or Transparent mode. The client-side and server-side FortiGate units do not have to be operating in the same mode.

As well, the FortiGate units can be configured for multiple virtual domain (VDOM) operation. You configure WAN optimization for each VDOM and configure one or both of the units to operate with multiple VDOMs enabled.

If a FortiGate unit or VDOM is operating in Transparent mode with WAN optimization enabled, WAN optimization uses the management IP address as the peer IP address of the FortiGate unit instead of the address of an interface.

WAN optimization tunnels

All optimized traffic passes between the FortiGate units or between a FortiClient peer and a FortiGate unit over a WAN optimization tunnel. Traffic in the tunnel can be sent in plain text or encrypted using AES-128bit-CBC SSL.

Both plain text and the encrypted peer-to-peer tunnels use TCP destination port 7810.

Before a tunnel can be started, the peers must be configured to authenticate with each other and to agree on the tunnel configuration. Then, the client-side peer attempts to start a WAN optimization tunnel with the server-side peer. Once the peers authenticate with each other, they bring up the tunnel and WAN optimization communication over the tunnel starts. After a tunnel has been established, multiple WAN optimization sessions can start and stop between peers without restarting the tunnel.
Tunnel sharing

You can use the `tunnel-sharing` WAN optimization rule CLI keyword to configure tunnel sharing for WAN optimization rules with `auto-detect` set to `off`. Tunnel sharing means multiple WAN optimization sessions share the same WAN optimization tunnel. Tunnel sharing can improve WAN performance by reducing the number of WAN optimization tunnels between FortiGate units. Having fewer tunnels means less data to manage. Also, tunnel setup requires more than one exchange of information between the ends of the tunnel. Once the tunnel is set up, each new session that shares the tunnel avoids tunnel setup delays.

Tunnel sharing also uses bandwidth more efficiently by reducing the chances that small packets will be sent down the tunnel. Processing small packets reduces network throughput, so reducing the number of small packets improves performance. A shared tunnel can combine all the data from the sessions being processed by the tunnel and send the data together. For example, suppose a FortiGate unit is processing five WAN optimization sessions and each session has 100 bytes to send. If these sessions use a shared tunnel, WAN optimization combines the packets from all five sessions into one 500-byte packet. If each session uses its own private tunnel, five 100-byte packets will be sent instead. Each packet also requires a TCP ACK reply. The combined packet in the shared tunnel requires one TCP ACK packet. The separate packets in the private tunnels require five.
Tunnel sharing is not always recommended. Aggressive and non-aggressive protocols should not share the same tunnel. An aggressive protocol can be defined as a protocol that is able to get more bandwidth than a non-aggressive protocol. (The aggressive protocols can “starve” the non-aggressive protocols.) HTTP and FTP are considered aggressive protocols. If aggressive and non-aggressive protocols share the same tunnel, the aggressive protocols may take all of the available bandwidth. As a result, the performance of less aggressive protocols could be reduced. To avoid this problem, rules for HTTP and FTP traffic should have their own tunnel. To do this, set tunnel-sharing to private for WAN optimization rules that accept HTTP or FTP traffic.

It is also useful to set tunnel-sharing to express-sharing for applications, such as Telnet, that are very interactive but not aggressive. Express sharing optimizes tunnel sharing for Telnet and other interactive applications where latency or delays would seriously affect the user’s experience with the protocol.

Set tunnel-sharing to sharing for applications that are not aggressive and are not sensitive to latency or delays. WAN optimization rules set to sharing and express-sharing can share the same tunnel.

**Protocol optimization**

Protocol optimization techniques optimize bandwidth use across the WAN. These techniques can improve the efficiency of communication across the WAN optimization tunnel by reducing the amount of traffic required by communication protocols. You can apply protocol optimization to Common Internet File System (CIFS), FTP, HTTP, MAPI, and general TCP sessions.

For example, CIFS provides file access, record locking, read/write privileges, change notification, server name resolution, request batching, and server authentication. CIFS is a fairly “chatty” protocol, requiring many background transactions to successfully transfer a single file. This is usually not a problem across a LAN. However, across a WAN, latency and bandwidth reduction can slow down CIFS performance.

When you set Protocol to CIFS in a WAN optimization rule, the FortiGate units at both ends of the WAN optimization tunnel use a number of techniques to reduce the number of background transactions that occur over the WAN for CIFS traffic.

You can select only one protocol in a WAN optimization rule. For best performance, you should separate the traffic by protocol by creating different WAN optimization rules for each protocol. For example, to optimize HTTP traffic, you should set Port to 80 so that only HTTP traffic is accepted by this WAN optimization rule. For an example configuration that uses multiple rules for different protocols, see “Example: Active-passive WAN optimization” on page 61.

If the WAN optimization accepts a range of different types of traffic, you can set Protocol to TCP to apply general optimization techniques to TCP traffic. However, applying this TCP optimization to a range of different types of traffic is not as effective as applying more protocol-specific optimization to specific types of traffic. TCP protocol optimization uses techniques such as TCP SACK support, TCP window scaling and window size adjustment, and TCP connection pooling to remove TCP bottlenecks.
Byte caching

Byte caching breaks large units of application data (for example, a file being downloaded from a web page) into small chunks of data, labeling each chunk of data with a hash of the chunk and storing those chunks and their hashes in a database. The database is stored on a WAN optimization storage device. Then, instead of sending the actual data over the WAN tunnel, the FortiGate unit sends the hashes. The FortiGate unit at the other end of the tunnel receives the hashes and compares them with the hashes in its local byte caching database. If any hashes match, that data does not have to be transmitted over the WAN optimization tunnel. The data for any hashes that do not match is transferred over the tunnel and added to the byte caching database. Then the unit of application data (the file being downloaded) is reassembled and sent to its destination.

Byte caching is not application specific. Bytes cached from a file in an email can be used to optimize downloading that same file or a similar file from a web page.

The result is less data transmitted over the WAN. Initially, byte caching may reduce performance until a large enough byte caching database is built up.

To enable byte caching, you select **Enable Byte Cache** in a WAN optimization rule. The **Protocol** setting does not affect byte caching. Data is byte cached when it is processed by a WAN optimization rule that includes byte caching.

Byte caching cannot determine whether or not a file is compressed (for example a zip file), and caches compressed and non-compressed versions of the same file separately.

WAN optimization and HA

You can configure WAN optimization on a FortiGate HA cluster. The recommended HA configuration for WAN optimization is active-passive mode. When the cluster is operating, all WAN optimization sessions are processed by the primary unit only. Even if the cluster is operating in active-active mode, HA does not load-balance WAN optimization sessions.

You can also form a WAN optimization tunnel between a cluster and a standalone FortiGate unit or between two clusters.

In a cluster, the primary unit stores only web cache and byte cache databases. These databases are not synchronized to the subordinate units. So, after a failover, the new primary unit must rebuild its web and byte caches.

Rebuilding the byte caches can happen relatively quickly because the new primary unit gets byte cache data from the other FortiGate units that it is participating with in WAN optimization tunnels.

Monitoring WAN optimization

Using WAN optimization monitoring, you can confirm that WAN optimization is accepting traffic and view WAN optimization performance. The monitor presents collected log information in a graphical format to show network traffic summary and bandwidth optimization information.

To view the WAN optimization monitor, go to **WAN Opt. & Cache > Monitor > Monitor**.
**Traffic Summary**

This section provides traffic optimization information. The piechart illustrates the percentage of traffic for supported applications processed during the selected *Period*. The table displays how much traffic has been reduced by WAN optimization by comparing the amount of LAN and WAN traffic for each protocol.

- **Refresh icon**: Refresh the Traffic Summary.
- **Period**: Select a time period to show traffic summary for. You can select:
  - Last 10 Minutes
  - Last 1 Hour
  - Last 1 Day
  - Last 1 Week
  - Last 1 Month
- **Protocol**: The name of the protocol for which sessions are optimized.
- **Reduction Rate**: Displays each application’s optimization rate. For example, a rate of 80% means the amount of data processed by that application has been reduced by 20%.
- **LAN**: The amount of data in MB received from the LAN for each application.
- **WAN**: The amount of data in MB sent across the WAN for each application. The greater the difference between the LAN and WAN data, the greater the amount of data reduced by WAN optimization byte caching, web caching, and protocol optimization.
Bandwidth Optimization: This section shows network bandwidth optimization per time period. A line or column chart compares an application’s pre-optimized (LAN data) size with its optimized size (WAN data).

Refresh icon: Select to refresh the Bandwidth Optimization display.

Period: Select a time frame to show bandwidth optimization. You can select:
- Last 10 Minutes
- Last 1 Hour
- Last 1 Day
- Last 1 Week
- Last 1 Month

Protocol: Select All to display bandwidth optimization for all applications. Select an individual protocol to display bandwidth optimization for that individual protocol.

Chart Type: Select to display bandwidth optimization with a line chart or a column chart.
WAN optimization and Web cache storage

WAN optimization storage is used for storing the byte cache and Web cache databases. In most cases, you can accept the default WAN optimization storage configuration because all of the disk space available on the FortiGate unit is in one partition. By default WAN optimization and logging and archiving are configured to use this partition.

You only have to configure WAN optimization storage if you have more than one possible storage location. This can happen if you have multiple partitions that you can use for storage locations. If you have more than one storage location you can move WAN optimization storage to it. You can also configure WAN optimization to use multiple storage locations.

This chapter contains the following topics:

- Formatting the hard disk
- Configuring WAN optimization and Web cache storage

Formatting the hard disk

In most cases the hard disks on your FortiGate unit should be formatted with one partition that is used for WAN optimization and Logging and Archiving. If for some reason the hard disk is not formatted you can use the following information to format it. In some cases you might also want to use the following commands to erase all data from the hard disk by reformating it.

From the web-based manager go to System > Maintenance > Disk to display information about the hard disk or disks in the FortiGate unit. To format the hard disk, select the format icon. The hard disk format takes a few minutes and the FortiGate unit restarts after formatting is complete.

From this web-based manager page you can also change the WAN optimization and Web Cache Storage size. By default the entire disk can be used for WAN optimization and Web Cache storage. You can also change the WAN optimization storage setting to reduce the amount of storage available for WAN optimization and web caching.

From the CLI you can use the following command to view the current disk format and partition status. See the following example for a FortiGate-51B unit.

```
execute disk list
```

```
Device I1          29.9 GB      ref: 256        SUPER TALENT (IDE)
partition 1      29.9 GB      ref: 257        label: 2B6375792136C707
```

You can use the following command to reformat the hard disk. Use this command if for some reason the disk is not formatted correctly. The command includes the device partition reference number (256) so formats the entire disk and not just the partition.

```
execute disk format 256
```

You can use the following command to reformat the partition. The command includes the partition reference number so formats the partition, removing add data from it. You can use this command to delete all data from the partition and to fix partition errors.

```
execute disk format 257
```
Configuring WAN optimization and Web cache storage

You can use the following command to add multiple WAN optimization storage locations if your FortiGate unit has multiple disk partitions and you want to use more than one for WAN optimization storage:

```plaintext
config system storage
```

Enter `get` to see the name of the default storage location. You cannot edit this storage location, but you can add new ones:

```plaintext
config system storage
   edit new_storage
      set partition <partition_number>
   end
```

Where `<partition_number>` is the number of the partition to create a storage location in. This cannot be the same as the partition added to the default storage location. This command automatically adds a WAN optimization storage location with the name `new_storage`.

Changing the amount of space allocated for WAN optimization and Web cache storage

From the web-based manager you can go to `System > Maintenance > Disk` to edit the WAN optimization & Web Cache storage and change the allocation size to limit the amount of storage available for WAN optimization byte caching and web caching. The size is in Mbytes.

You can use the following command to change the size of any WAN optimization storage location. For example, in the FortiGate-51B the default WAN optimization storage is `Internal`. Use the following command to limit the amount of space allocated for WAN optimization to 20 Gbytes

```plaintext
config wanopt storage
   edit Internal
      set size 20000
   end
```
WAN optimization peers and authentication groups

All communication between WAN optimization peers begins with one WAN optimization peer (or client-side FortiGate unit) sending a WAN optimization tunnel request to another peer (or server-side FortiGate unit). During this process, the WAN optimization peers identify and optionally authenticate each other.

This chapter describes:
- Basic WAN optimization peer requirements
- How FortiGate units process tunnel requests for peer authentication
- Configuring peers
- Configuring authentication groups
- Secure tunneling

Basic WAN optimization peer requirements

WAN optimization requires the following configuration on each peer. For information about configuring local and peer host IDs, see “Configuring peers” on page 41.

- The peer must have a unique host ID.
  Unless authentication groups are used, peers authenticate each other using host ID values. Do not leave the local host ID at its default value.
- The peer must know the host IDs and IP addresses of all of the other peers that it can start WAN optimization tunnels with. This does not apply if you use authentication groups that accept all peers.

All peers must have the same local certificate installed on their FortiGate units if the units authenticate by local certificate. Similarly, if the units authenticate by pre-shared key (password), administrators must know the password. The type of authentication is selected in the authentication group. This applies only if you use authentication groups.

Accepting any peers

Strictly speaking, you do not need to add peers. Instead you can configure authentication groups that accept any peer. However, for this to work, both peers must have the same authentication group (with the same name) and both peers must have the same certificate or pre-shared key.

Accepting any peer is useful if you have many peers or if peer IP addresses change. For example, you could have many travelling FortiClient peers with IP addresses that are always changing as the users travel to different customer sites. This configuration is also useful if you have FortiGate units with dynamic external IP addresses (using DHCP or PPPoE). For most other situations, this method is not recommended as it is less secure than accepting defined peers or a single peer. For more information, see “Configuring authentication groups” on page 42.
How FortiGate units process tunnel requests for peer authentication

When a client-side FortiGate unit attempts to start a WAN optimization tunnel with a peer server-side FortiGate unit, the tunnel request includes the following information:

- the client-side local host ID
- the name of an authentication group, if included in the rule that initiates the tunnel
- if an authentication group is used, the authentication method it specifies: pre-shared key or certificate
- the type of tunnel (secure or not).

For information about configuring the local host ID, peers and authentication groups, see “Configuring peers” on page 41 and “Configuring authentication groups” on page 42.

The authentication group is optional unless the tunnel is a secure tunnel. For more information, see “Secure tunneling” on page 44.

If the tunnel request includes an authentication group, the authentication will be based on the settings of this group as follows:

- The server-side FortiGate unit searches its own configuration for the name of the authentication group in the tunnel request. If no match is found, the authentication fails.
- If a match is found, the server-side FortiGate unit compares the authentication method in the client and server authentication groups. If the methods do not match, the authentication fails.
- If the authentication methods match, the server-side FortiGate unit tests the peer acceptance settings in its copy of the authentication group.
  - If the setting is Accept Any Peer, the authentication is successful.
  - If the setting is Specify Peer, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the peer name in the server-side authentication group. If the names match, authentication is successful. If a match is not found, authentication fails.
  - If the setting is Accept Defined Peers, the server-side FortiGate unit compares the client-side local host ID in the tunnel request with the server-side peer list. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the tunnel request does not include an authentication group, authentication will be based on the client-side local host ID in the tunnel request. The server-side FortiGate unit searches its peer list to match the client-side local host ID in the tunnel request. If a match is found, authentication is successful. If a match is not found, authentication fails.

If the server-side FortiGate unit successfully authenticates the tunnel request, the server-side FortiGate unit sends back a tunnel setup response message. This message includes the server-side local host ID and the authentication group that matches the one in the tunnel request.

The client-side FortiGate unit then performs the same authentication procedure as the server-side FortiGate unit did. If both sides succeed, tunnel setup continues.
Configuring peers

When you configure peers, you first need to add the local host ID that identifies the FortiGate unit for WAN optimization and then add the peer host ID and IP address of each FortiGate unit with which a FortiGate unit can create WAN optimization tunnels.

To configure WAN optimization peers - web-based manager
1. Go to **Wan Opt. & Cache > Peer > Peer**.
2. For **Local Host ID**, enter the local host ID of this FortiGate unit and select **Apply**. If you add this FortiGate unit as a peer to another FortiGate unit, use this ID as its **peer** host ID.

   The local or host ID can contain up to 25 characters and can include spaces.
3. Select **Create New** to add a new peer.
4. For **Peer Host ID**, enter the peer host ID of the peer FortiGate unit. This is the local host ID added to the peer FortiGate unit.
5. For **IP Address**, add the IP address of the peer FortiGate unit. This is the source IP address of tunnel requests sent by the peer, usually the IP address of the FortiGate interface connected to the WAN.
6. Select **OK**.

To configure WAN optimization peers - CLI
In this example, the local host ID is named **HQ_Peer** and has an IP address of 172.20.120.100. Three peers are added, but you can add any number of peers that are on the WAN.
1. Enter the following command to set the local host ID to **HQ_Peer**.

   ```
   config wanopt settings
   set host-id HQ_Peer
   end
   ```

2. Enter the following commands to add three peers.

   ```
   config wanopt peer
   edit Wan_opt_peer_1
   set ip 172.20.120.100
   next
   edit Wan_opt_peer_2
   set ip 172.30.120.100
   next
   edit Wan_opt_peer_3
   set ip 172.40.120.100
   end
   ```
Configuring authentication groups

You need to add authentication groups to support authentication and secure tunneling between WAN optimization peers.

To perform authentication, WAN optimization peers use a certificate or a pre-shared key added to an authentication group so they can identify each other before forming a WAN optimization tunnel. Both peers must have an authentication group with the same name and settings. You add the authentication group to a peer-to-peer or active rule on the client-side FortiGate unit. When the server-side FortiGate unit receives a tunnel start request from the client-side FortiGate unit that includes an authentication group, the server-side FortiGate unit finds an authentication group in its configuration with the same name. If both authentication groups have the same certificate or pre-shared key, the peers can authenticate and set up the tunnel.

Authentication groups are also required for secure tunneling. See "Secure tunneling" on page 44.

To add authentication groups, go to **WAN Opt. & Cache > Peer > Authentication Group**.

**To add an authentication group - web-based manager**

Use the following steps to add any kind of authentication group. It is assumed that if you are using a local certificate to authenticate, it is already added to the FortiGate unit. For more information, see the *FortiGate Certificate Management Guide*.

1. Go to **Wan Opt. & Cache > Peer > Authentication Group**.
2. Select **Create New**.
3. Add a **Name** for the authentication group.
   You will select this name when you add the authentication group to a WAN optimization rule.
4. Select the **Authentication Method**.
   Select **Certificate** if you want to use a certificate to authenticate and encrypt WAN optimization tunnels. You must select a local certificate that has been added to this FortiGate unit. (To add a local certificate, go to **System > Certificates > Local Certificates**.) Other FortiGate units that participate in WAN optimization tunnels with this FortiGate unit must have an authentication group with the same name and certificate.
   Select **Pre-shared key** if you want to use a pre-shared key or password to authenticate and encrypt WAN optimization tunnels. You must add the **Password** (or pre-shared key) used by the authentication group. Other FortiGate units that participate in WAN optimization tunnels with this FortiGate unit must have an authentication group with the same name and password. The password must contain at least 6 printable characters and should be known only by network administrators. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.
5 Configure Peer Acceptance for the authentication group.

Select Accept Any Peer if you do not know the peer host IDs or IP addresses of the peers that will use this authentication group. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP.

Select Accept Defined Peers if you want to authenticate with peers added to the peer list only.

Select Specify Peer and select one of the peers added to the peer list to authenticate with the selected peer only.

For more information, see “Configuring peers” on page 41.

6 Select OK.

7 Add the authentication group to a WAN optimization rule to apply the authentication settings in the authentication group to the rule.

For more information, see “Configuring WAN optimization rules” on page 50.

To add an authentication group that uses a certificate - CLI

Enter the following command to add an authentication group that uses a certificate and can authenticate all peers added to the FortiGate unit configuration.

In this example, the authentication group is named auth_grp_1 and uses a certificate named Example_Cert.

```
config wanopt auth-group
edit auth_grp_1
set auth-method cert
set cert Example_Cert
set peer-accept defined
end
```

To add an authentication group that uses a pre-shared key - CLI

Enter the following command to add an authentication group that uses a pre-shared key and can authenticate only the peer added to the authentication group.

In this example, the authentication group is named auth_peer, the peer that the group can authenticate is named Server_net, and the authentication group uses 123456 as the pre-shared key. In practice you should use a more secure pre-shared key.

```
config wanopt auth-group
edit auth_peer
set auth-method psk
set psk 123456
set peer-accept one
set peer Server_net
end
```

To add an authentication group that accepts WAN optimization connections from any peer - web-based manager

Add an authentication group that accepts any peer for situations where you do not have the Peer Host IDs or IP Addresses of the peers that you want to perform WAN optimization with. This setting is most often used for WAN optimization with the FortiClient application or with FortiGate units that do not have static IP addresses, for example units that use DHCP. An authentication group that accepts any peer is less secure than an authentication group that accepts defined peers or a single peer.
The example below sets the authentication method to \textit{Pre-shared key}. You must add the same password to all FortiGate units using this authentication group.

2. Select \textit{Create New} to add a new authentication group.
3. Configure the authentication group:

\begin{itemize}
  \item \textbf{Name}: Specify any name.
  \item \textbf{Authentication Method}: Pre-shared key
  \item \textbf{Password}: Enter a pre-shared key.
  \item \textbf{Peer Acceptance}: Accept Any Peer
\end{itemize}

\textbf{To add an authentication group that accepts WAN optimization connections from any peer - CLI}

In this example, the authentication group is named \texttt{auth_grp_1}. It uses a certificate named \texttt{WAN_Cert} and accepts any peer.

```
config wanopt auth-group
edit auth_grp_1
  set auth-method cert
  set cert WAN_Cert
  set peer-accept any
end
```

\section*{Secure tunneling}

You can configure WAN optimization rules to use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel. WAN optimization uses FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. Peer-to-peer secure tunnels use the same TCP port as non-secure peer-to-peer tunnels (TCP port 7810).

To use secure tunneling, you must select \textit{Enable Secure Tunnel} in a WAN optimization rule and add an authentication group. The authentication group specifies the certificate or pre-shared key used to set up the secure tunnel. The \textit{Peer Acceptance} setting of the authentication group does not affect secure tunneling.

The FortiGate units at each end of the secure tunnel must have the same authentication group with the same name and the same configuration, including the same pre-shared key or certificate. To use certificates you must install the same certificate on both FortiGate units.

For active-passive WAN optimization you can select \textit{Enable Secure Tunnel} only in the active rule. In peer-to-peer WAN optimization you select \textit{Enable Secure Tunnel} in the WAN optimization rule on both FortiGate units. For information about active-passive and peer-to-peer WAN optimization, see “Configuring WAN optimization rules” on page 45.

For a secure tunneling configuration example, see “Example: Adding secure tunneling to an active-passive WAN optimization configuration” on page 69. Secure tunneling is also used in the configuration example: “Example: SSL offloading for a WAN optimization tunnel” on page 115.
Configuring WAN optimization rules

To configure WAN optimization, you add WAN optimization rules. Similar to firewall policies, when a FortiGate unit receives a connection packet, it analyzes the packet’s source address, destination address, and service (by destination port number), and attempts to locate a matching WAN optimization rule that decides how to optimize the traffic over the WAN. WAN optimization rules also apply features such as byte-caching and protocol optimization to optimized traffic.

You can add one of two types of WAN optimization rules: peer-to-peer and active-passive.

A **peer-to-peer WAN optimization** rule includes a peer host ID. WAN optimization sessions matched by a client-side peer-to-peer rule can only connect to the named server-side peer. When the client-side peer unit initiates a tunnel with the server-side peer, the packets that initiate the tunnel include extra information so that the server-side peer can determine that it is a peer-to-peer tunnel request. This extra information is required because the server-side peer does not require a WAN optimization rule; you just need to add the client peer host ID and IP address to the server-side FortiGate unit peer list. Peer to peer WAN optimization tunnels use port 7810.

For **active-passive WAN optimization**, you add active rules to client-side FortiGate units and passive rules to server-side FortiGate units. A single passive rule can accept tunnel requests from multiple active rules. The configuration of the active rule enables WAN optimization features. The passive rule uses the configuration of the active rules. The one exception is web caching, which is enabled in passive rules.

This chapter describes:

- WAN optimization rules, firewall policies, and UTM protection
- WAN optimization transparent mode
- WAN optimization rule list
- WAN optimization address formats
- Configuring WAN optimization rules

**WAN optimization rules, firewall policies, and UTM protection**

The FortiGate unit applies firewall policies to communication sessions before WAN optimization rules. A WAN optimization rule can be applied to a packet only after the packet is accepted by a firewall policy. WAN optimization processes all sessions accepted by a firewall policy that also match a WAN optimization rule. However, if the firewall policy includes any UTM features, communication sessions accepted by the policy are processed by the UTM engine and not by WAN optimization. Before you add WAN optimization rules, you must add firewall policies to accept the traffic that you want to optimize.

To apply WAN optimization to traffic that is accepted by a firewall policy containing a UTM features, you can use multiple FortiGate units or multiple VDOMs. You apply the UTM features in the first FortiGate unit or VDOM and then apply WAN optimization in the second FortiGate unit or VDOM. You also add inter-VDOM links between the VDOMs. See the configuration example “Out-of-path WAN optimization with inter-VDOM routing” on page 93.
WAN optimization does not apply source and destination NAT settings included in firewall policies. This means that selecting NAT or adding virtual IPs in a firewall policy does not affect WAN optimized traffic. WAN optimization is also not compatible with firewall load balancing. However, traffic accepted by these policies that is not WAN optimized is processed as expected.

WAN optimization is compatible with identity-based firewall policies. If a session is allowed after authentication and if the identity-based policy that allows the session does not include UTM features, the session can be processed by matching WAN optimization rules.

Firewall traffic shaping is compatible with client/server (active-passive) transparent mode WAN optimization rules. Traffic shaping is ignored for peer-to-peer WAN optimization and for client/server WAN optimization not operating in transparent mode.

**WAN optimization transparent mode**

WAN optimization is transparent to users. This means that with WAN optimization in place, clients connect to servers in the same way as they would without WAN optimization. However, servers receiving packets after WAN optimization “see” different source addresses depending on whether or not transparent mode is selected for WAN optimization. If transparent mode is selected, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be configured to route traffic with client source IP addresses from the server-side FortiGate unit to the server and back to the server-side FortiGate unit.

**Note:** Some protocols, for example CIFS, may not function as expected if transparent mode is not selected. In most cases, for CIFS WAN optimization you should select transparent mode and make sure the server network can route traffic as described to support transparent mode.

If transparent mode is not selected, the source address of the packets received by servers is changed to the address of the server-side FortiGate unit interface that sends the packets to the servers. So servers appear to receive packets from the server FortiGate unit. Routing on the server network is simpler in this case because client addresses are not involved. All traffic appears to come from the server FortiGate unit and not from individual clients.

**Note:** Do not confuse WAN optimization transparent mode with FortiGate transparent mode. WAN optimization transparent mode is configured in individual WAN optimization rules. FortiGate Transparent mode is a system setting that controls how the FortiGate unit (or a VDOM) processes traffic.

**WAN optimization rule list**

The WAN optimization rule list displays WAN optimization rules in their order of matching precedence. WAN optimization rule order affects rule matching. For details about arranging rules in the rule list, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.

For information about WAN optimization rules and firewall policies, see "WAN optimization rules, firewall policies, and UTM protection" on page 45.

Then you add WAN optimization rules that:

- match WAN traffic to be optimized that is accepted by a firewall policy according to source and destination addresses and destination port of the traffic
Configuring WAN optimization rules

- add the WAN optimization techniques to be applied to the traffic.

To view the WAN optimization rule list, go to WAN Opt. & Cache > Rule > Rule.

Figure 17: WAN optimization rule list

<table>
<thead>
<tr>
<th>ID</th>
<th>Source</th>
<th>Destination</th>
<th>Port</th>
<th>Method</th>
<th>Auto-Detect/Protocol</th>
<th>Peer</th>
<th>Mode</th>
<th>SSL</th>
<th>Secure Tunnel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.1.1.1</td>
<td>2.2.2.2</td>
<td>1 65536</td>
<td>Byte Caching</td>
<td>Off</td>
<td>CIFS</td>
<td>Peer_2</td>
<td>Full Optimization</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>1 60</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>1 10</td>
<td>Byte Caching</td>
<td>Active</td>
<td>FTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>21 22</td>
<td>Byte Caching</td>
<td>Active</td>
<td>CIFS</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>1 129</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>445 446</td>
<td>Byte Caching</td>
<td>Active</td>
<td>CIFS</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10.1.100.1</td>
<td>172.16.200.1</td>
<td>443 444</td>
<td>Byte Caching</td>
<td>Active</td>
<td>HTTP</td>
<td>Full Optimization</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Create New
- Add a new WAN optimization rule. New rules are added to the bottom of the list.

Status
- Select to enable a rule or clear to disable a rule. A disabled rule is out of service.

ID
- The rule identifier. Rules are numbered in the order they are added to the rule list.

Source
- The source address or address range that the rule matches. For more information, see "WAN optimization address formats" on page 49.

Destination
- The destination address or address range that the rule matches. For more information, see "WAN optimization address formats" on page 49.

Port
- The destination port number or port number range that the rule matches.

Method
- Indicates whether you have selected byte caching in the WAN optimization rule.

Auto-Detect
- Indicates whether the rule is an active (client) rule, a passive (server) rule or if auto-detect is off. If auto-detect is off, the rule can be peer-to-peer or Web Cache Only.

Protocol
- The protocol optimization WAN optimization technique applied by the rule. For more information, see "Protocol optimization" on page 33.

Peer
- For a peer-to-peer rule, the name of the peer WAN optimizer at the other end of the link.

Mode
- Indicates whether the rule applies Full Optimization or Web Cache Only.

SSL
- Indicates whether the rule is configured for SSL offloading.

Secure Tunnel
- Indicates whether the rule is configured to used a WAN optimization tunnel.

Delete icon
- Delete a rule from the list.

Edit icon
- Edit a rule.

Insert WAN Optimization Rule Before icon
- Add a new rule above the corresponding rule (the New rule screen appears).

Move To icon
- Move the corresponding rule before or after another rule in the list. For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.
How list order affects rule matching

Similar to firewall policies, you add WAN optimization rules to the WAN optimization rule list. The FortiGate unit uses the first-matching technique to select the WAN optimization rule to apply to a communication session.

When WAN optimization rules have been added, each time the FortiGate firewall accepts a communication session, it then searches the WAN optimization rule list for a matching rule. Matching rules are determined by comparing the rule with the session source and destination addresses and destination port. The search begins at the top of the rule list and progresses in order towards the bottom. Each rule in the rule list is compared with the communication session until a match is found. When the FortiGate unit finds the first matching rule, it applies that rule’s specified WAN optimization features to the session and disregards subsequent rules.

If no WAN optimization rule matches, the session is processed according to the firewall policy that originally accepted the session.

As a general rule, you should order the WAN optimization rule list from most specific to most general because of the order in which rules are evaluated for a match, and because only the first matching rule is applied to a session. Subsequent possible matches are not considered or applied. Ordering rules from most specific to most general prevents rules that match a wide range of traffic from superseding and effectively masking rules that match exceptions.

For example, you might have a general WAN optimization rule that applies WAN optimization features but does not apply secure tunneling to most WAN traffic. However, you want to apply secure tunneling to FTP traffic (FTP traffic uses port 21). In this case, you would add a rule that creates a secure tunnel for FTP sessions above the general rule.

![Figure 18: Example: secure tunneling for FTP — correct rule order](image1)

FTP sessions (using port 21) would immediately match the secure tunnel rule. Other kinds of services would not match the FTP rule, so rule evaluation would continue until the search reaches the matching general rule. This rule order has the intended effect. But if you reversed the order of the two rules, positioning the general rule before the FTP rule, all session, including FTP, would immediately match the general rule, and the rule to secure FTP would never be applied. This rule order would not have the intended effect.

![Figure 19: Example: secure tunneling for FTP — incorrect rule order](image2)

Similarly, if specific traffic requires exceptional WAN optimization rule settings, you would position those rules above other potential matches in the rule list. Otherwise, the other matching rules would take precedence, and the required exceptional settings might never be used.
Moving a rule to a different position in the rule list

When more than one rule has been defined, the first matching rule is applied to the traffic session. You can arrange the WAN optimization rule list to influence the order in which rules are evaluated for matches with incoming traffic. For more information, see “How list order affects rule matching” on page 48.

Moving a rule in the rule list does not change its ID, which only indicates the order in which the rule was created.

To move a rule in the WAN optimization rule list - web-based manager

2. In the rule list, note the ID of a rule that is before or after your intended destination.
3. In the row corresponding to the rule that you want to move, select the Move To icon.
4. Select Before or After, and enter the ID of the rule that is before or after your intended destination. This specifies the rule’s new position in the WAN optimization rule list.
5. Select OK.

To move a rule in the WAN optimization rule list - CLI

1. Use the following command to move a WAN optimization rule with ID 34 above the rule in the rule list with ID 10.

   ```
   config wanopt rule
   move 34 before 10
   end
   ```

2. Use the following command to move a WAN optimization rule with ID 5 after the rule in the rule list with ID 1.

   ```
   config wanopt rule
   move 5 after 1
   end
   ```

WAN optimization address formats

A WAN optimization source or destination address can contain one or more network addresses. Network addresses can be represented by an IP address with a netmask or an IP address range.

When representing hosts by an IP address with a netmask, the IP address can represent one or more hosts. For example, a source or destination address can be:

- a single computer, for example, 192.45.46.45
- a subnetwork, for example, 192.168.1.* for a class C subnet
- 0.0.0.0, matches any IP address.

The netmask corresponds to the subnet class of the address being added, and can be represented in either dotted decimal or CIDR format. The FortiGate unit automatically converts CIDR-formatted netmasks to dotted decimal format. Example formats:

- netmask for a single computer: 255.255.255.255, or /32
- netmask for a class A subnet: 255.0.0.0, or /8
- netmask for a class B subnet: 255.255.0.0, or /16
- netmask for a class C subnet: 255.255.255.0, or /24
- netmask including all IP addresses: 0.0.0.0
Valid IP address and netmask formats include:

- x.x.x/x.x.x.x, such as 192.168.1.0/255.255.255.0
- x.x.x/x, such as 192.168.1.0/24

**Note:** An IP address 0.0.0.0 with netmask 255.255.255.255 is not a valid source or destination address.

When representing hosts by an IP range, the range indicates hosts with continuous IP addresses in a subnet, such as 192.168.1.[2-10], or 192.168.1.* to indicate the complete range of hosts on that subnet. You can also indicate the complete range of hosts on a subnet by entering 192.168.1.[0-255] or 192.168.1.0-192.168.1.255. Valid IP range formats include:

- x.x.x.x-x.x.x.x, for example, 192.168.110.100-192.168.110.120
- x.x.x.[x-x], for example, 192.168.110.[100-120]
- x.x.x.*, for a complete subnet, for example: 192.168.110.*
- x.x.x.[0-255] for a complete subnet, such as 192.168.110.[0-255]
- x.x.x.0-x.x.x.255 for a complete subnet, such as 192.168.110.0 - 192.168.110.255

**Note:** You cannot use square brackets [] or asterisks * when adding addresses to the CLI. Instead, you must enter the start and end addresses of the subnet range separated by a dash -. For example, 192.168.20.0-192.168.20.255 for a complete subnet and 192.168.10.10-192.168.10.100 for a range of addresses.

## Configuring WAN optimization rules

This section describes all the details that you can configure for the WAN optimization rules. The options available depend on how you configure a specific rule. The conditions are noted.

### To add a WAN optimization rule - web-based manager

1. Go to **WAN Opt. & Cache > Rule > Rule** and select **Create New**.
2. Configure the WAN optimization rule, using the guidance in the following table, and select **OK**.

| Mode | Select **Full Optimization** to add a rule that can apply all WAN optimization features. Select **Web Cache Only** to add a rule that just applies web caching. If you select **Web Cache Only**, you can configure the source and destination address and port for the rule. You can also select **Transparent Mode** and **Enable SSL**.
| Source | Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. For more information, see "WAN optimization address formats" on page 49.

Only packets whose source address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule. For a passive rule, the server (passive) source address range should be compatible with the source addresses of the matching client (active) rule. To match one passive rule with many active rules, the passive rule source address range should include the source addresses of all of the active rules.
Configuring WAN optimization rules

**Destination**
Enter an IP address, followed by a forward slash (/), then subnet mask, or enter an IP address range separated by a hyphen. For more information, see “WAN optimization address formats” on page 49.

Only a packet whose destination address header contains an IP address matching this IP address or address range will be accepted by and subject to this rule.

**Tip:** For a Web Cache Only rule, if you set Destination to 0.0.0.0, the rule caches web pages on the Internet or any network.

For a passive rule, the server (passive) destination address range should be compatible with the destination addresses of the matching client (active) rule. To match one passive rule with many active rules, the passive rule destination address range should include the destination addresses of all of the active rules.

**Port**
Enter a single port number or port number range. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this rule.

For a passive rule, the server (passive) port range should be compatible with the port range of the matching client (active) rule. To match one passive rule with many active rules, the passive rule port range should include the port ranges of all of the active rules.

**Auto-Detect**
Available only if Mode is set to Full Optimization.
Specify whether the rule is Active (client), Passive (server) or if Auto-Detect is Off. If Auto-Detect is Off, the rule is a peer-to-peer rule.

- For an Active (client) rule, you must select all of the WAN optimization features to be applied by the rule. You can select the protocol to optimize, transparent mode, byte caching, SSL offloading, secure tunneling, and an authentication group.
- A Passive (server) rule uses the settings in the active rule on the client FortiGate unit to apply WAN optimization settings. You can also select web caching for a passive rule.
- If Auto-Detect is Off, the rule must include all required WAN optimization features and you must select a Peer for the rule. Select this option to configure peer-to-peer WAN optimization where this rule can start a WAN optimization tunnel with this peer only.

**Protocol**
Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Active.
Select CIFS, FTP, HTTP, or MAPI to apply protocol optimization for one of these protocols. For information about protocol optimization, see “Protocol optimization” on page 33.
Select TCP if the WAN optimization tunnel accepts sessions that use more than one protocol or that do not use the CIFS, FTP, HTTP, or MAPI protocol.

**Peer**
Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off.
Select the peer host ID of the peer that this peer-to-peer WAN optimization rule will start a WAN optimization tunnel with. You can also select [Create New...] from the list to add a new peer.

**Enable Web Cache**
Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Passive. If Auto-Detect is set to Off, then Protocol must be set to HTTP.
Select to apply WAN optimization web caching to the sessions accepted by this rule. For more information, see “Web caching” on page 75.

**Transparent Mode**
Available only if Mode is set to Full Optimization and Auto-Detect is set to Active or Off, or if Mode is set to Web Cache Only.
Servers receiving packets after WAN optimization “see” different source addresses depending on whether or not you select Transparent Mode.
For more information, see “WAN optimization transparent mode” on page 46.

**Enable Byte Caching**
Available only if Mode is set to Full Optimization, and Auto-Detect is set to Off or Active.
Select to apply WAN optimization byte caching to the sessions accepted by this rule. For more information, see “Byte caching” on page 34.
To add a WAN optimization rule - CLI

Using the guidance in the previous table, enter the following commands. For more information, see the `wanopt` and `rules` listings in the **FortiGate CLI Reference**.

```
config wanopt rule
edit <index_int>
  set auth-group <auth_group_name>
  set auto-detect {active | off | passive}
  set byte-caching {disable | enable}
  set dst-ip <address_ipv4>[-<address-ipv4>]
  set mode {full | webcache-only}
  set peer <peer_name>
  set port <port_int>[-<port-int>]
  set proto {cifs | ftp | http | mapi | tcp}
  set secure-tunnel {disable | enable}
  set src-ip <address_ipv4>[-<address-ipv4>]
  set ssl {disable | enable}
  set status {disable | enable}
  set transparent {disable | enable}
  set tunnel-non-http {disable | enable}
  set tunnel-sharing {express-shared | private | shared}
  set unknown-http-version {best-effort | reject | tunnel}
  set webcache {disable | enable}
end
```

**Processing non-HTTP sessions accepted by an HTTP rule**

From the CLI, use the `tunnel-non-http` keyword of the `config wanopt rule` command to configure how to process non-HTTP sessions when a rule configured to accept and optimize HTTP traffic accepts a non-HTTP session. This can occur if an application sends non-HTTP sessions using an HTTP destination port.
To drop non-HTTP sessions accepted by the rule set tunnel-non-http to disable, or set it to enable to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. In this case, the FortiGate unit applies TCP protocol optimization to non-HTTP sessions.

**Processing unknown HTTP sessions**

Unknown HTTP sessions are HTTP sessions that do not comply with HTTP 0.9, 1.0, or 1.1. From the CLI, use the unknown-http-version keyword of the config wanopt rule command to specify how a rule handles such HTTP sessions.

To assume that all HTTP sessions accepted by the rule comply with HTTP 0.9, 1.0, or 1.1, select best-effort. If a session uses a different HTTP version, WAN optimization may not parse it correctly. As a result, the FortiGate unit may stop forwarding the session and the connection may be lost. To reject HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1, select reject.

To pass HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1, but without applying HTTP protocol optimization, byte-caching, or web caching, you can also select tunnel. TCP protocol optimization is applied to these HTTP sessions.
WAN optimization configuration examples

This chapter provides the following basic examples to illustrate WAN optimization configurations introduced in the previous chapters:

- Example: Basic peer-to-peer WAN optimization configuration
- Example: Active-passive WAN optimization
- Example: Adding secure tunneling to an active-passive WAN optimization configuration

Example: Basic peer-to-peer WAN optimization configuration

Peer-to-peer WAN optimization is the simplest WAN optimization configuration. In a peer to peer configuration the WAN optimization tunnel can be set up only between one client-side FortiGate unit and one server-side FortiGate unit named in the WAN optimization rule added to the client-side FortiGate unit. When the client-side FortiGate unit initiates a tunnel with the server-side FortiGate unit, the packets that initiate the tunnel include extra information so that this server-side FortiGate unit can determine that it is a peer-to-peer tunnel request. This extra information is required because the server-side FortiGate unit does not require a WAN optimization rule; you just need to add the client peer host ID and IP address to the server-side FortiGate unit peer list.

The extra information in the communication session plus the peer list entry allow the server-side FortiGate unit to set up the WAN optimization tunnel with the client-side FortiGate unit by using only the settings on the client-side WAN optimization rule.

**Note:** Traffic shaping is ignored for peer-to-peer WAN optimization.

In a peer-to-peer WAN optimization configuration you create a peer-to-peer WAN optimization rule on the client-side FortiGate unit with Auto-Detect to Off and include the peer host ID of the server-side FortiGate unit. Using this rule, the client-side FortiGate unit can create a WAN optimization tunnel only with the peer that is added to the rule.

You do not have to add a rule to the server-side FortiGate unit. But the server-side FortiGate unit peer list must include the Peer Host ID and IP address of the client FortiGate unit. The server-side FortiGate unit uses the WAN optimization settings in the client-side rule.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Peer_Fgt_1 with a WAN IP address of 172.20.34.12. This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Peer_Fgt_2 with a WAN IP address of 192.168.30.12. This unit is in front of a web server network with IP address 192.168.10.0.
General configuration steps
This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.
2. Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring basic peer-to-peer WAN optimization - web-based manager
Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure the client-side FortiGate unit and firewall policy
1. Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the client-side FortiGate unit:
   
   Local Host ID

   Peer_Fgt_1

2. Select Apply to save your setting.
3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:
   
   Peer Host ID

   Peer_Fgt_2

   IP Address

   192.168.30.12

4. Select OK.
5 Go to Firewall > Policy > Policy and add a firewall policy to the client-side FortiGate unit that accepts traffic to be optimized:

- **Source Interface/Zone**: port1
- **Source Address**: all
- **Destination Interface/Zone**: port2
- **Destination Address**: all
- **Schedule**: always
- **Service**: ANY
- **Action**: ACCEPT


7 Configure the rule:

- **Mode**: Full Optimization
- **Source**: 172.20.120.*
- **Destination**: 192.168.10.*
- **Port**: 1-65535
- **Auto-Detect**: Off
- **Protocol**: MAPI
- **Peer**: Peer_Fgt_2
- **Transparent Mode**: Select
- **Enable Byte Caching**: Select

8 Select OK.

The rule is added to the bottom of the WAN optimization list.

9 If required, move the rule to a different position in the list so that the rule accepts the required MAPI sessions. Depending on your rule list configuration, this may involve moving the rule above more general rules that would also match MAPI traffic.

For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.

**To configure the server-side FortiGate unit**

1 Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the server-side FortiGate unit:

- **Local Host ID**: Peer_Fgt_2

2 Select Apply to save your setting.

3 Select Create New and add a Peer Host ID and the IP Address for the peer side FortiGate unit:

- **Peer Host ID**: Peer_Fgt_1
- **IP Address**: 172.20.34.12

4 Select OK.
Configuring basic peer-to-peer WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit and firewall policy

1. Add the Local Host ID to the client-side FortiGate configuration:

   ```
   config wanopt settings
   set host-id Peer_Fgt_1
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:

   ```
   config wanopt peer
   edit Peer_Fgt_2
   set ip 192.168.30.12
   end
   ```

3. Add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:

   ```
   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```

4. Add the following peer-to-peer rule:

   ```
   config wanopt rule
   edit 2
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set proto mapi
   set peer Peer_Fgt_2
   end
   ```

   Accept default settings for auto-detect (off), transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

5. If required, move the rule to a different position in the list.

   For more information, see "Moving a rule to a different position in the rule list" on page 49.

6. If required, use the move command to change the order of the rules in the list so that the rule accepts the required MAPI sessions. Depending on your rule list configuration, this may involve moving the rule above more general rules that would also match MAPI traffic.

   For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.
To configure the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:

   ```
   config wanopt settings
   set host-id Peer_Fgt_2
   end
   ```

2. Add the client-side Local Host ID to the server-side peer list:

   ```
   config wanopt peer
   edit Peer_Fgt_1
   set ip 192.168.30.12
   end
   ```

Testing and troubleshooting the configuration

To test the configuration attempt to start a web browsing session between the user network and the web server network. For example, from a PC on the user network browse to the IP address of a web server on the web server network, for example http://192.168.10.100. Even though this address is not on the user network you should be able to connect to this web server over the WAN optimization tunnel.

If you can connect, check WAN optimization monitoring (go to WAN Opt. & Cache > Monitor > Monitor). If WAN optimization has been forwarding the traffic the WAN optimization monitor should show the protocol that has been optimized (in this case HTTP) and the reduction rate in WAN bandwidth usage.

If you can't connect you can try the following to diagnose the problem:

- Review your configuration and make sure all details such as address ranges, peer names, and IP addresses are correct.
- Confirm that the firewall policy on the Client-Side FortiGate unit is accepting traffic for the 192.168.10.0 network and that this firewall policy does not include UTM options. You can do this by checking the FortiGate session table from the dashboard. Look for sessions that use the policy ID of this policy.
- Check routing on the FortiGate units and on the user and web server networks to make sure packets can be forwarded as required. The FortiGate units must be able to communicate with each other, routing on the user network must allow packets destined for the web server network to be received by the client side FortiGate unit, and packets from the server side FortiGate unit must be able to reach the web servers etc.

You can use the following `get` and `diagnose` commands to display information about how WAN optimization is operating.

Enter the following command on the client-side FortiGate unit to display WAN optimization tunnel protocol statistics. The `http` tunnel and `tcp` tunnel parts of the command output below shows that WAN optimization has been processing HTTP and TCP packets.

```
get test wad 11
wad tunnel protocol stats:
  http tunnel
    bytes_in=1751767  bytes_out=325468
  ftp tunnel
    bytes_in=0  bytes_out=0
  cifs tunnel
    bytes_in=0  bytes_out=0
  mapi tunnel
    bytes_in=0  bytes_out=0
  tcp tunnel
    bytes_in=3182253  bytes_out=200702
  maintenance tunnel
    bytes_in=11800  bytes_out=15052
```
Enter the following command to display the current WAN optimization peers. You can use this command to make sure all peers are configured correctly. The command output for the client side FortiGate unit shows one peer with IP address 192.168.20.1, peer name Web_servers, and with 10 active tunnels.

```
get test wad 26
peer name=Web_servers ip=192.168.20.1 vd=0 version=1
tunnels(active/connecting/failover)=10/0/0
  sessions=0 n_retries=0 version_valid=true
```

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output for the client-side FortiGate unit shows 10 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to off).

```
diagnose wad tunnel list
```

1. **Tunnel: id=100 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=100 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=348 bytes_out=384

2. **Tunnel: id=99 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=99 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=348 bytes_out=384

3. **Tunnel: id=98 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=98 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=348 bytes_out=384

4. **Tunnel: id=39 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=39 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=1068 bytes_out=1104

5. **Tunnel: id=7 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=7 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=1228 bytes_out=1264

6. **Tunnel: id=8 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=8 ip=192.168.30.12
   - SSL-secured-tunnel=no auth-grp=
   - bytes_in=1228 bytes_out=1264

7. **Tunnel: id=5 type=manual**
   - vd=0 shared=no uses=0 state=3
   - peer name=Web_servers id=5 ip=192.168.30.12
Example: Active-passive WAN optimization

In active-passive WAN optimization you add active WAN optimization rules on the client-side FortiGate unit by setting WAN optimization Auto-Detect to Active. You configure passive WAN optimization rules on the server-side FortiGate unit by setting WAN optimization Auto-Detect to Passive.

You can add multiple active rules for one passive rule to optimize different protocols. Since you do not configure the protocol in the passive rule, one passive rule can be used for each of the active rules. Adding fewer passive rules simplifies the WAN optimization configuration.

Network topology and assumptions

This example configuration includes three active rules on the client-side FortiGate unit and one passive rule in the server-side FortiGate unit. The active rules do the following:

- optimize CIFS traffic from IP addresses 172.20.120.100 to 172.20.120.200
- optimize HTTP traffic from IP addresses 172.20.120.100 to 172.20.120.150
- optimize FTP traffic from IP addresses 172.20.120.151 172.20.120.200.

You can do this by adding three active WAN optimization rules to the client-side FortiGate unit, one for each protocol—with port set to 80 for the HTTP rule, 21 for the FTP rule and 1-65535 for the CIFS rule. Then you arrange the rules in the WAN optimization rule list with the CIFS rule last because the HTTP and FTP rules include single port numbers.
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.
2. Add WAN optimization rules to the FortiGate unit.
3. Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring basic active-passive WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the client-side FortiGate unit:
   
   **Local Host ID**
   
   User_net

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:
   
   **Peer Host ID**
   
   Web_servers
   
   **IP Address**
   
   192.168.20.1
WAN optimization configuration examples

Example: Active-passive WAN optimization

4 Select OK.
5 Go to Firewall > Policy > Policy and select Create New to add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port2</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>ANY</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

To add the active rules to the client-side FortiGate unit

1 Go to WAN Opt. & Cache > Rule > Rule.
2 Select Create New to add the active rule to optimize CIFS traffic from IP addresses 172.20.120.100 to 172.20.120.200:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Full Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>172.20.120.[100-200]</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.10.*</td>
</tr>
<tr>
<td>Port</td>
<td>1 - 65535</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Active</td>
</tr>
<tr>
<td>Protocol</td>
<td>CIFS</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Byte Caching</td>
<td>Select</td>
</tr>
</tbody>
</table>

3 Select OK.
4 Select Create New to add the active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.150:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Full Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>172.20.120.[100-150]</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.10.*</td>
</tr>
<tr>
<td>Port</td>
<td>80</td>
</tr>
<tr>
<td>Auto-Detect</td>
<td>Active</td>
</tr>
<tr>
<td>Protocol</td>
<td>HTTP</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Byte Caching</td>
<td>Select</td>
</tr>
</tbody>
</table>

5 Select OK.
6 Select Create New to add the active rule to optimize FTP traffic from IP addresses 172.20.120.151 172.20.120.200:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Full Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>172.20.120.[151-200]</td>
</tr>
<tr>
<td>Destination</td>
<td>192.168.10.*</td>
</tr>
</tbody>
</table>
Example: Active-passive WAN optimization

WAN Optimization configuration examples

<table>
<thead>
<tr>
<th>Port</th>
<th>21</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Detect</td>
<td>Active</td>
</tr>
<tr>
<td>Protocol</td>
<td>FTP</td>
</tr>
<tr>
<td>Transparent Mode</td>
<td>Select</td>
</tr>
<tr>
<td>Enable Byte Caching</td>
<td>Select</td>
</tr>
</tbody>
</table>

7 Select OK.

8 If required, use the Move To icon to change the order of the rules in the list so that the HTTP and FTP rules are above the CIFS rule in the list. You may need to do this if you have other WAN optimization rules in the list.

For more information, see “How list order affects rule matching” on page 48 and “Moving a rule to a different position in the rule list” on page 49.

To configure the server-side FortiGate unit

1 Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the server-side FortiGate unit:

   Local Host ID     Web_servers

2 Select Apply to save your setting.

3 Select Create New and add a Peer Host ID and the IP Address for the client-side FortiGate unit:

   Peer Host ID     User_net
   IP Address       172.30.120.1

4 Select OK.

5 Go to WAN Opt. & Cache > Rule > Rule and select Create New.

6 Add the passive rule. The source address matches the 172.20.120.100 to 172.20.120.200 IP address range and the 1-65535 port range. You can also enable web caching for the HTTP traffic:

   Mode         Full Optimization
   Source       172.20.120.[100-200]
   Destination  192.168.10.*
   Port         1-65535
   Auto-Detect  Passive
   Enable Web Cache  Select

7 Select OK.

   The rule is added to the bottom of the rule list.

8 If required, move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see “Moving a rule to a different position in the rule list” on page 49.
Configuring basic active-passive WAN optimization - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure peers on the client-side FortiGate unit and add a firewall policy

1. Add the Local Host ID to the client-side FortiGate configuration:

   ```
   config wanopt settings
   set host-id User_net
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:

   ```
   config wanopt peer
   edit Web_servers
   set ip 192.168.20.1
   end
   ```

3. Add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:

   ```
   config firewall policy
   edit 20
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   end
   ```

To add the active rules to the client-side FortiGate unit

1. Add the following active rule to optimize CIFS traffic for IP addresses 172.20.120.100 to 172.20.120.200:

   ```
   config wanopt rule
   edit 2
   set auto-detect active
   set src-ip 172.20.120.100-172.20.120.200
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set proto cifs
   end
   ```

   Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).
2 Add the following active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.150:

```fortigate
config wanopt rule
edit 3
set auto-detect active
set src-ip 172.20.120.100-172.20.120.150
set dst-ip 192.168.10.0-192.168.10.255
set port 80
end
```

Accept default settings for transparent (enable), proto (http), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

3 Add the following active rule to optimize FTP traffic from IP addresses 172.20.120.151 to 172.20.120.200:

```fortigate
config wanopt rule
edit 4
set auto-detect active
set src-ip 172.20.120.151-172.20.120.200
set dst-ip 192.168.10.0-192.168.10.255
set port 21
set proto ftp
end
```

Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

4 If required, use the move command to change the order of the rules in the list so that the HTTP and FTP rules are above the CIFS rule in the list. You may need to do this if you have other WAN optimization rules in the list.

For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.

To configure the server-side FortiGate unit

1 Add the Local Host ID to the server-side FortiGate configuration:

```fortigate
config wanopt settings
set host-id Web_servers
end
```

2 Add the client-side Local Host ID to the server-side peer list:

```fortigate
config wanopt peer
edit User_net
set ip 172.20.120.1
end
```
3 Add the following passive rule to the server-side FortiGate unit:

```fortigate
config wanopt rule
edit 5
   set auto-detect passive
   set src-ip 172.20.120.[100-200]
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set webcache enable
end
```

Accept default settings for `status` (enable) and `mode` (full).

4 If required, use the `move` command to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see "Moving a rule to a different position in the rule list" on page 49.

### Testing and troubleshooting the configuration

To test the configuration attempt to start a web browsing session between the user network and the web server network. For example, from a PC on the user network browse to the IP address of a web server on the web server network, for example `http://192.168.10.100`. Even though this address is not on the user network you should be able to connect to this web server over the WAN optimization tunnel.

If you can connect, check WAN optimization monitoring (go to **WAN Opt. & Cache > Monitor > Monitor**). If WAN optimization has been forwarding the traffic the WAN optimization monitor should show the protocol that has been optimized (in this case HTTP) and the reduction rate in WAN bandwidth usage.

If you can’t connect you can try the following to diagnose the problem:

- Review your configuration and make sure all details such as address ranges, peer names, and IP addresses are correct.
- Confirm that the firewall policy on the Client-Side FortiGate unit is accepting traffic for the 192.168.10.0 network and that this firewall policy does not include UTM options. You can do this by checking the FortiGate session table from the dashboard. Look for sessions that use the policy ID of this policy.
- Check routing on the FortiGate units and on the user and web server networks to make sure packets can be forwarded as required. The FortiGate units must be able to communicate with each other, routing on the user network must allow packets destined for the web server network to be received by the client side FortiGate unit, and packets from the server side FortiGate unit must be able to reach the web servers etc.

You can use the following `get` and `diagnose` commands to display information about how WAN optimization is operating.

Enter the following command to display WAN optimization tunnel protocol statistics. The http tunnel and tcp tunnel parts of the command output below shows that WAN optimization has been processing HTTP and TCP packets.

```fortigate
get test wad 11
wad tunnel protocol stats:
   http tunnel
      bytes_in=1751767 bytes_out=325468
   ftp tunnel
      bytes_in=0 bytes_out=0
   cifs tunnel
      bytes_in=0 bytes_out=0
```
Enter the following command to display the current WAN optimization peers. You can use this command to make sure all peers are configured correctly. The command output for the client side FortiGate unit shows one peer with IP address 192.168.20.1, peer name Web_servers, and with 10 active tunnels.

```bash
get test wad 26
peer name=Web_servers ip=192.168.20.1 vd=0 version=1
tunnels (active/connecting/failover)=10/0/0
  sessions=0 n_retries=0 version_valid=true
```

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output shows 3 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to on).

```bash
diagnose wad tunnel list
```

```
Tunnel: id=139 type=auto
  vd=0 shared=no uses=0 state=1
  peer name= id=0 ip=unknown
  SSL-secured-tunnel=no auth-grp=test
  bytes_in=744 bytes_out=76

Tunnel: id=141 type=auto
  vd=0 shared=no uses=0 state=1
  peer name= id=0 ip=unknown
  SSL-secured-tunnel=no auth-grp=test
  bytes_in=727 bytes_out=76

Tunnel: id=142 type=auto
  vd=0 shared=no uses=0 state=1
  peer name= id=0 ip=unknown
  SSL-secured-tunnel=no auth-grp=test
  bytes_in=727 bytes_out=76

Tunnels total=3 manual=0 auto=3
```
Example: Adding secure tunneling to an active-passive WAN optimization configuration

This example shows how to configure two FortiGate units for active-passive WAN optimization with secure tunneling. The same authentication group is added to both FortiGate units. The authentication group includes a password (or pre-shared key) and has Peer Acceptance set to Accept any Peer. An active rule is added to the client-side FortiGate unit and a passive rule to the server-side FortiGate unit. The active rule uses secure tunneling, optimizes HTTP traffic, and uses Transparent Mode and byte caching.

The authentication group is named Auth_Secure_Tunnel and the password for the pre-shared key is 2345678. The topology for this example is shown in Figure 22. This example includes web-based manager configuration steps followed by equivalent CLI configuration steps. For information about secure tunneling, see “Secure tunneling” on page 44.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called User_net with a WAN IP address of 172.30.120.1. This unit is in front of a network with IP address 172.20.120.0. The server-side FortiGate unit is called Web_servers and has a WAN IP address of 192.168.20.1. This unit is in front of a web server network with IP address 192.168.10.0.

Figure 22: Example active-passive WAN optimization and secure tunneling topology

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers and a firewall policy that accepts traffic to be optimized.
2 Add an authentication group and WAN optimization rule to the client-side FortiGate unit.
3 Configure peers on the server-side FortiGate unit.
4 Add the same authentication group and add a WAN optimization rule to the server-side FortiGate unit.
Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring WAN optimization with secure tunneling - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure peers on the client-side FortiGate unit and add a firewall policy
1 Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the client-side FortiGate unit:
   Local Host ID  User_net
2 Select Apply to save your setting.
3 Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:
   Peer Host ID  Web_servers
   IP Address    192.168.20.1
4 Select OK.
5 Go to Firewall > Policy > Policy and select Create New to add a firewall policy to the client-side FortiGate unit to accept the traffic to be optimized:
   Source Interface/Zone  port1
   Source Address        all
   Destination Interface/Zone  port2
   Destination Address  all
   Schedule              always
   Service                ANY
   Action                 ACCEPT

To add the authentication group and WAN optimization rule to the client-side FortiGate unit
2 Select Create New to add a new authentication group to be used for secure tunneling:
   Name                Auth_Secure_Tunnel
   Authentication Method  Pre-shared key
   Password             2345678
   Peer Acceptance      Accept Any Peer
3 Select OK.
4 Go to *Wan Opt. & Cache > Rule > Rule*.

5 Select *Create New* to add an active rule that enables secure tunneling and includes the authentication group:

- **Mode**: Full Optimization
- **Source**: 172.20.120.[100-200]
- **Destination**: 192.168.10.*
- **Port**: 80
- **Auto-Detect**: Active
- **Protocol**: HTTP
- **Transparent Mode**: Select
- **Enable Byte Caching**: Select
- **Enable Secure Tunnel**: Select
- **Authentication Group**: Auth_Secure_Tunnel

6 Select *OK*.

**To configure peers on the server-side FortiGate unit**

1 Go to *WAN Opt. & Cache > Peer > Peer* and enter a *Local Host ID* for the server-side FortiGate unit:

- **Local Host ID**: Web_servers

2 Select *Apply* to save your setting.

3 Select *Create New* and add a *Peer Host ID* and the *IP Address* for the client-side FortiGate unit:

- **Peer Host ID**: User_net
- **IP Address**: 172.30.120.1

4 Select *OK*.

**To add the authentication group and WAN optimization rule to the server-side FortiGate unit**

1 Go to *Wan Opt. & Cache > Peer > Authentication Group*.

2 Select *Create New* and add a new authentication group to be used for secure tunneling:

- **Name**: Auth_Secure_Tunnel
- **Authentication Method**: Pre-shared key
- **Password**: 2345678
- **Peer Acceptance**: Accept Any Peer

3 Go to *WAN Opt. & Cache > Rule* and select *Create New*.

4 Add the passive rule. The source address matches the 172.20.120.100 to 172.20.120.200 IP address range and the 1-65535 port range. You can also enable web caching for HTTP traffic:

- **Mode**: Full Optimization
- **Source**: 172.20.120.[100-200]
- **Destination**: 192.168.10.*
Example: Adding secure tunneling to an active-passive WAN optimization configuration

WAN Optimization configuration examples

<table>
<thead>
<tr>
<th>Port</th>
<th>1-65535</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Detect</td>
<td>Passive</td>
</tr>
<tr>
<td>Enable Web Cache</td>
<td>Select</td>
</tr>
</tbody>
</table>

5 Select OK.

Configuring WAN optimization with secure tunneling - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure peers on the client-side FortiGate unit and add a firewall policy

1 Add the Local Host ID to the client-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id User_net
   end
   ```

2 Add the server-side Local Host ID to the client-side peer list:
   ```
   config wanopt peer
   edit Web_servers
   set ip 192.168.20.1
   end
   ```

3 Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:
   ```
   config firewall policy
   edit 20
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   set service ANY
   set schedule always
   end
   ```

To add the authentication group and WAN optimization rule to the client-side FortiGate unit

1 Add a new authentication group to be used for secure tunneling:
   ```
   config wanopt auth-group
   edit Auth_Secure_Tunnel
   set auth-method psk
   set psk 2345678
   end
   ```

   Leave peer-accept at its default value.

2 Add the following active rule to optimize HTTP traffic for IP addresses 172.20.120.100 to 172.20.120.200:
   ```
   config wanopt rule
   edit 1
   set auto-detect active
   set src-ip 172.20.120.100-172.20.120.200
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   ```
set proto http
set secure-tunnel enable
set auth-group Auth_Secure_Tunnel
end

Leave the rest of the settings at their default values.

To configure peers on the server-side FortiGate unit

1. Add the Local Host ID to the server-side FortiGate configuration:
   ```
   config wanopt settings
   set host-id Web_servers
   end
   ```

2. Add the client-side Local Host ID to the server-side peer list:
   ```
   config wanopt peer
   edit User_net
   set ip 172.20.120.1
   end
   ```

To add the authentication group and WAN optimization rule to the server-side FortiGate unit

1. Add a new authentication group to be used for secure tunneling:
   ```
   config wanopt auth-group
   edit Auth_Secure_Tunnel
   set auth-method psk
   set psk 2345678
   end
   ```

   Leave peer-accept at its default value.

2. Add the following passive rule to the server-side FortiGate unit:
   ```
   config wanopt rule
   edit 5
   set auto-detect passive
   set src-ip 172.20.120.[100-200]
   set dst-ip 192.168.10.0-192.168.10.255
   set port 1-65535
   set webcache enable
   end
   ```

   Leave status (enable) and mode (full) at their default values.
Web caching

FortiGate WAN optimization web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Web caching supports explicit and transparent proxy caching of HTTP 1.0 and HTTP 1.1 web sites. Web caching also supports caching HTTPS sessions provided that you import the correct certificate. See RFC 2616 for information about web caching for HTTP 1.1.

Web caching involves storing HTML pages, images, servlet responses and other web-based objects for later retrieval. FortiGate units cache these objects within a storage location that is specifically for WAN optimization.

There are three significant advantages to using web caching to improve WAN performance:

• reduced WAN bandwidth consumption because fewer requests and responses go over the WAN
• reduced web server load because there are fewer requests for web servers to handle
• reduced latency because responses for cached requests are available from a local FortiGate unit instead of from across the WAN or Internet.

You can use web caching to cache any web traffic that passes through the FortiGate unit, including web pages from web servers on a LAN, WAN or on the Internet. The FortiGate unit caches web objects for all HTTP traffic processed by WAN optimization rules that include web caching.

You can add WAN optimization rules for that only apply web caching. You can also add web caching to WAN optimization rules for HTTP traffic that also include byte caching, protocol optimization, and other WAN optimization features. If you use WAN optimization rules to apply web caching, end users do not have to configure their web browsers to use the FortiGate unit as a proxy server.

Note: You can also enable web caching for the FortiGate explicit web proxy. For more information, see “To enable web caching for the explicit web proxy - web-based manager” on page 135.

Web caching cannot determine if a file is compressed (for example a zip file) and caches compressed and non-compressed versions of the same file separately. If the HTTP protocol considers the compressed and uncompressed versions of a file the same object, only the compressed or uncompressed file will be cached.

This section contains the following topics:

• Configuring Web Cache Only WAN optimization
• Exempting web sites from web caching
• Example: Web Cache Only WAN optimization
• Configuring active-passive web caching
• Example: Active-passive Web Caching
• Configuring peer-to-peer web caching
• Example: Peer-to-peer web caching
• Changing web cache settings
Configuring Web Cache Only WAN optimization

You can use Web Cache Only WAN optimization to cache web pages from any web server. In a Web Cache Only configuration, only one FortiGate unit is involved. All traffic between a client network and one or more web servers is intercepted by a Web Cache Only WAN optimization rule. This rule causes the FortiGate unit to cache pages from the web servers on the FortiGate unit and makes the cached pages available to users on the client network. Web cache only WAN optimization can be configured for standard and reverse web caching.

In a standard web caching configuration, the FortiGate unit caches pages for users on a client network. The FortiGate unit is installed between the client network and the WAN or Internet, and the web server or servers are located elsewhere on the WAN or Internet. See “Example: Web Cache Only WAN optimization” on page 77 for an example of this configuration.

You can also create a reverse proxy web caching configuration where the FortiGate unit is dedicated to providing web caching for a single web server or server farm. In this second configuration, the FortiGate unit is installed between the server network and the WAN or Internet, and users are located elsewhere on the WAN or Internet. See “Example: SSL offloading and reverse proxy web caching for an Internet web server” on page 119 for an example of this configuration.

WAN optimization rule order affects Web Cache Only rules in the same way as other WAN optimization rules. For more information, see “How list order affects rule matching” on page 48 and “Moving a rule to a different position in the rule list” on page 49.

Exempting web sites from web caching

You may want to exempt some URLs from web caching for a number of reasons. For example, if your users access websites that are not compatible with FortiGate web caching you can add the URLs of these websites to the web caching exempt list. All traffic accepted by WAN optimization and the explicit proxy for these websites will not be cached.

To exempt www.example.com from web caching - web-based manager
2. Add the URL www.example.com to the URL Pattern field and select OK.

To exempt www.example.com from web caching - CLI
1. Enter the following command to add www.example.com to the exempt list.

```sh
cfg/wanopt/webcache
  config cache-exemption enable
  config cache-exemption-list
    edit 1
      set url-pattern www.example.com
      set status enable
    end
  end
end
```

Note: Since only one FortiGate unit is involved in a Web Cache Only configuration, you do not need to change the WAN optimization peer configuration.
2 Enter the following command to enable the web cache exempt list and add two IP address URLs and a web page URL to the list.

```
config wanopt webcache
  set explicit enable
  set cache-exemption enable
  config cache-exemption-list
    edit 1
      set url-pattern "192.168.1.121"
    next
    edit 2
      set url-pattern "google.com/test123/321"
    next
    edit 3
      set url-pattern "1.1.1.1"
    next
  end
end
```

Example: Web Cache Only WAN optimization

This example describes how to configure web caching for users in a client network connecting to a web server network across a WAN.

Network topology and assumptions

This example includes a client network with subnet address 172.20.120.0 connecting to web servers on a network with subnet address 192.168.10.0. Only the communication between the client network and the web server network using Port 80 is to be cached, so the Web Cache Only WAN optimization rule includes the IP addresses of the networks and the Port is set to 80. As well, the firewall policy used in this example includes the addresses of the client and server subnets instead of more general firewall addresses.

Figure 23: Example Web Cache Only topology
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Add firewall addresses and a firewall policy that accepts traffic to be optimized to the FortiGate unit.
2. Add a Web Cache Only WAN optimization rule to the FortiGate unit.

If you perform any additional actions between procedures, your configuration may have different results.

Configuring Web Cache Only WAN optimization - web-based manager

Use the following steps to configure the example WAN optimization configuration from the FortiGate unit web-based manager.

To add the firewall addresses and firewall policy
1. Go to Firewall > Policy > Address and select Create New to add the firewall address for the client network:
   - Address Name: Client_Net
   - Type: Subnet/IP Range
   - Subnet / IP Range: 172.20.120.*
   - Interface: Any

2. Add the firewall address for the web server network:
   - Address Name: Web_Server_Net
   - Type: Subnet/IP Range
   - Subnet / IP Range: 192.168.10.*
   - Interface: Any

3. Go to Firewall > Policy > Policy and select Create New to add a firewall policy that accepts traffic to be web cached:
   - Source Interface/Zone: port1
   - Source Address: Client_Net
   - Destination Interface/Zone: port2
   - Destination Address: Web_Server_Net
   - Schedule: always
   - Service: HTTP
   - Action: ACCEPT

To add a Web Cache Only WAN optimization rule
2. Select Web Cache Only.
3. Configure the Web Cache Only rule:
   - Mode: Web Cache Only
   - Source: 172.20.120.*
**Web caching**

**Example: Web Cache Only WAN optimization**

| Destination | 192.168.10.* |
| Port | 80 |

**Tip:** Usually you would set the port to 80 to cache normal HTTP traffic. But you can change the Port to a different number (for example 8080) or to a port number range so that the FortiGate unit provides web caching for HTTP traffic using other ports.

**Transparent Mode** Select Transparent Mode

**Enable SSL** Do not select Enable SSL.

**Tip:** In this example SSL offloading is disabled. For an example of a reverse proxy Web Cache Only configuration that also includes SSL offloading, see “Example: SSL offloading for a WAN optimization tunnel” on page 115.

4 Select OK.

The rule is added to the bottom of the WAN optimization list.

5 If required, use the Move To icon to move the rule to a different position in the list.

The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 48 and “Moving a rule to a different position in the rule list” on page 49.

**Configuring Web Cache Only WAN optimization - CLI**

Use the following steps to configure the example WAN optimization configuration from the FortiGate unit CLI.

**To add the firewall addresses and firewall policy**

1 Add the firewall address for the client network:

   ```
   config firewall address
   edit Client_Net
   set type iprange
   set start-ip 172.20.120.0
   set end-ip 172.20.120.255
   end
   ```

2 Add the firewall address for the web server network:

   ```
   config firewall address
   edit Web_Server_Net
   set type iprange
   set start-ip 192.168.10.0
   set end-ip 192.168.10.255
   end
   ```

3 Add a firewall policy that accepts traffic to be web cached:

   ```
   config firewall policy
   edit 2
   set srcintf port1
   set dstintf port2
   set srcaddr Client_Net
   set dstaddr Web_Server_Net
   set action accept
   set service HTTP
   set schedule always
   end
   ```
To add a Web Cache Only WAN optimization rule

1. Add the following Web Cache Only rule:

   ```
   config wanopt rule
   edit 2
   set mode webcache-only
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 192.168.10.0-192.168.10.255
   set port 80
   set peer Peer_Fgt_2
   end
   ```

   Accept default settings for transparent (enable), status (enable), ssl (disable), unknown-http-version (tunnel), and tunnel-non-http (disable).

   Tip: In this example, SSL offloading is disabled. For an example of a reverse proxy Web Cache Only configuration that also includes SSL offloading, see “Example: SSL offloading for a WAN optimization tunnel” on page 115.

2. If required, use the `move` command to move the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 48 and “Moving a rule to a different position in the rule list” on page 49.

Testing and troubleshooting the configuration

To test the configuration, attempt to start a web browsing session between the client network and the web server network. For example, from a PC on the client network, browse to the IP address of a web server on the web server network, for example http://192.168.10.100. Even though this address is not on the user network you should be able to connect to this web server over the WAN optimization tunnel.

If you can connect, check WAN optimization monitoring in WAN Opt. & Cache > Monitor > Monitor. If WAN optimization has been forwarding the traffic, the WAN optimization monitor should show the HTTP protocol that has been optimized and the reduction rate in WAN bandwidth usage.

If you cannot connect, try the following to diagnose the problem:

- Review your configuration and make sure all details, such as address ranges, peer names and IP addresses, are correct.
- Confirm that the firewall policy on the Client-Side FortiGate unit is accepting traffic for the 192.168.10.0 network and that this firewall policy does not include UTM options. You can do this by checking the FortiGate session table from the dashboard. Look for sessions that use the policy ID of this policy.
- Check routing on the FortiGate units and on the user and web server networks to make sure packets can be forwarded as required. The FortiGate units must be able to communicate with each other, routing on the user network must allow packets destined for the web server network to be received by the client side FortiGate unit, and packets from the server side FortiGate unit must be able to reach the web servers etc.

You can use the following `get` and `diagnose` commands to display information about how WAN optimization is operating.
Enter the following command on the client-side FortiGate unit to display WAN optimization tunnel protocol statistics. The `http` tunnel and `tcp` tunnel parts of the command output below shows that WAN optimization has been processing HTTP packets. If the http bytes in and bytes out fields are zero, then WAN optimization is not accepting HTTP packets.

```
get test wad 11
wad tunnel protocol stats:
    http tunnel
        bytes_in=1749865 bytes_out=25926
    ftp tunnel
        bytes_in=0 bytes_out=0
    cifs tunnel
        bytes_in=0 bytes_out=0
    mapi tunnel
        bytes_in=0 bytes_out=0
    tcp tunnel
        bytes_in=0 bytes_out=0
    maintenance tunnel
        bytes_in=0 bytes_out=0
```

You can use the following command to display information about the WAN optimization web cache daemon. The command will only display information if the web cache daemon is running and the statistics displayed show the number of open connections and other indications of activity:

```
diagnose wacs stats
Disk 0 /Internal-2B637592136C707/wa_cs
    Current number of open connections: 2
    Number of terminated connections: 7
    Number of requests -- Adds: 206 (0 repetitive keys), Lookups: 860, Conflict incidents: 0
    Percentage of missed lookups: 88.49
    Communication is blocked for 0 client(s)
    Disk usage: 5196 KB (11%)
```

**Configuring active-passive web caching**

You add web caching support to the passive or server side of an active-passive WAN optimization configuration. Web pages are cached on the server-side FortiGate unit so you should also select *Enable Byte Caching* for optimum WAN optimization performance.

For web caching to work, the WAN optimization tunnel must accept HTTP (and optionally HTTPS) traffic. To do this, the active rule on the client side must include the ports used for HTTP (and HTTPS) traffic. Set *Protocol* to *HTTP* to perform protocol optimization of the HTTP traffic. You can also enable SSL offloading and secure tunneling, as well as add an authentication group.
Example: Active-passive Web Caching

This example describes how to configure active-passive web caching for users in a client network connecting to a web server network across a WAN.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Client_Side with a WAN IP address of 172.10.10.1 in front of a user network with IP address 172.20.120.0. The server-side FortiGate unit is called Server_Side and has a WAN IP address of 172.20.20.1. This server-side unit is in front of a web server network with IP address 192.168.10.0. Web caching is enabled on the server-side FortiGate unit.

Figure 24: Example active-passive web cache topology

General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the client-side FortiGate unit by adding peers, a firewall policy that accepts traffic to be optimized, and an active WAN optimization rule.

2. Configure the server-side FortiGate unit by adding peers and a passive WAN optimization rule that includes web caching.

If you perform any additional actions between procedures, your configuration may have different results.

Configuring active-passive web caching - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)
To configure the client-side FortiGate unit

1. Go to **WAN Opt. & Cache > Peer > Peer** and enter a *Local Host ID* for the client FortiGate unit:

   **Local Host ID**  
   **Client Side**

2. Select **Apply** to save your setting.

3. Select **Create New** and add a *Peer Host ID* and the *IP Address* for the server-side FortiGate unit:

   **Peer Host ID**  
   **Server Side**

   **IP Address**  
   172.20.20.1

4. Select **OK**.

5. Go to **Firewall > Policy > Policy** and add a firewall policy that accepts traffic to be web cached:

   **Source Interface/Zone**  
   port1

   **Source Address**  
   all

   **Destination Interface/Zone**  
   port2

   **Destination Address**  
   all

   **Schedule**  
   always

   **Service**  
   ANY

   **Action**  
   ACCEPT

6. Go to **WAN Opt. & Cache > Rule > Rule** and select **Create New**.

7. Configure the rule:

   **Mode**  
   Full Optimization

   **Source**  
   172.20.120.*

   **Destination**  
   192.168.10.*

   **Port**  
   1-65535

   **Auto-Detect**  
   Active

   **Protocol**  
   HTTP

   **Transparent Mode**  
   Select Transparent Mode

   **Enable Byte Caching**  
   Select Enable Byte Caching

8. Select **OK**.

   The rule is added to the bottom of the WAN optimization list.

9. If required, use the **Move To** icon to move the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see “How list order affects rule matching” on page 48 and “Moving a rule to a different position in the rule list” on page 49.
To configure the server-side FortiGate unit

1. Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the server-side FortiGate unit:

   Local Host ID: Server_Side

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the client-side FortiGate unit:

   Peer Host ID: Client_Side
   IP Address: 172.10.10.1


5. Configure the passive web cache rule:

   Mode: Full Optimization
   Source: 172.20.120.*
   Destination: 192.168.10.*
   Port: 1-65535
   Auto-Detect: Passive
   Enable Web Cache: Select

6. Select OK.

   The rule is added to the bottom of the WAN optimization rule list.

7. If required, use the Move To icon to move the rule to a different position in the list.

   For more information, see “Moving a rule to a different position in the rule list” on page 49.

Configuring active-passive web caching - CLI

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

To configure the client-side FortiGate unit

1. Add the Local Host ID to the client-side FortiGate configuration:

   config wanopt settings
   set host-id Client_Side
   end

2. Add the server-side Local Host ID to the client-side peer list:

   config wanopt peer
   edit Server_Side
   set ip 172.20.20.1
   end

3. Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:

   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
set dstaddr all
set action accept
set service ANY
set schedule always
end
end

4 Configure the following active rule:
config wanopt rule
edit 2
set auto-detect active
set src-ip 172.20.120.0-172.20.120.255
set dst-ip 192.168.10.0-192.168.10.255
set port 1-65535
set proto http
end

Accept default settings for transparent (enable), status (enable), mode (full),
byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-
group (null), unknown-http-version (tunnel), and tunnel-non-http
(disable).

5 If required, use the move command to move the rule to a different position in the list.
The order of the rules in the list significantly affects how the rules are applied. For more
information, see “How list order affects rule matching” on page 48 and “Moving a rule
to a different position in the rule list” on page 49.

To configure the server-side FortiGate unit
1 Add the Local Host ID to the server-side FortiGate configuration:
config wanopt settings
    set host-id Server_Side
end

2 Add the client-side Local Host ID to the server-side peer list:
config wanopt peer
    edit Client_Side
    set ip 172.10.10.1
end

3 Add the following passive web cache rule:
config wanopt rule
    edit 5
    set auto-detect passive
    set src-ip 172.20.120.0-172.20.120.255
    set dst-ip 192.168.10.0-192.168.10.255
    set port 1-65535
    set webcache enable
end

Accept default settings for status (enable) and mode (full).

4 If required, use the move command to move the rule to a different position in the list so
that the tunnel request from the client-side FortiGate unit matches with this rule.
For more information, see “Moving a rule to a different position in the rule list” on
page 49.
Configuring peer-to-peer web caching

In a peer-to-peer web caching configuration, you create a peer-to-peer WAN optimization rule on the client-side FortiGate unit and include the peer host ID of the server-side FortiGate unit. In the rule, you set Auto-Detect to Off and select Enable Web Cache. By using this rule, the client-side FortiGate unit can create a WAN optimization tunnel only with the peer that is added to the rule.

In a peer-to-peer configuration, you do not have to add a rule to the server-side FortiGate unit. If the server-side FortiGate unit peer list contains the client FortiGate unit, the server FortiGate unit accepts WAN optimization tunnel connections from the client FortiGate unit and the two units can form a WAN optimization tunnel. The server-side FortiGate unit uses the settings in the rule added to the client-side FortiGate unit.

For web caching to work, the WAN optimization tunnel must allow HTTP (and optionally HTTPS) traffic. To do this, the WAN optimization rule must include the ports used for HTTP (and HTTPS) traffic. Set Protocol to HTTP to perform protocol optimization of the HTTP traffic. You can also enable WAN optimization transparent mode, byte caching, SSL offloading, and secure tunneling, as well as add an authentication group.

Example: Peer-to-peer web caching

This example describes how to configure peer-to-peer web caching for users in a client network connecting to a web server network across a WAN.

Network topology and assumptions

This example configuration includes a client-side FortiGate unit called Client_Side with a WAN IP address of 172.10.10.1 in front of a user network with IP address 172.20.120.0. The server-side FortiGate unit is called Server_Side and has a WAN IP address of 172.20.20.1. This server-side unit is in front of a web server network with IP address 192.168.10.0. Web caching is enabled on the server-side FortiGate unit.

Figure 25: Example peer-to-peer web cache topology
General configuration steps

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1  Configure the client-side FortiGate unit by adding peers, a firewall policy that accepts traffic to be optimized, and a peer-to-peer WAN optimization rule that includes web caching.
2  Configure the server-side FortiGate unit.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

Configuring peer-to-peer web caching - web-based manager

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit web-based manager. (CLI steps follow.)

To configure the client-side FortiGate unit

1  Go to WAN Opt. & Cache > Peer > Peer and enter a Local Host ID for the client FortiGate unit:

   Local Host ID  Client_Side

2  Select Apply to save your setting.

3  Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate unit:

   Peer Host ID  Server_Side
   IP Address    192.168.30.12

4  Select OK.

5  Go to Firewall > Policy > Policy and add a firewall policy that accepts traffic to be web cached:

   Source Interface/Zone  port1
   Source Address        all
   Destination Interface/Zone  port2
   Destination Address    all
   Schedule                always
   Service                 ANY
   Action                  ACCEPT


7  Configure the rule:

   Mode               Full Optimization
   Source             172.20.120.*
   Destination        192.168.10.*
   Port               80
   Auto-Detect        Off
Example: Peer-to-peer web caching

WAN Optimization, Web Cache, Explicit Proxy, and WCCP for FortiOS 4.0 MR2

1. Go to **WAN Opt. & Cache > Peer > Peer** and enter a Local Host ID for the server FortiGate unit:

   **Local Host ID**  Server_Side

2. Select **Apply** to save your setting.

3. Select **Create New** and add a Peer Host ID and the IP Address for the client-side FortiGate unit:

   **Peer Host ID**  Client_Side
   **IP Address**  172.20.34.12

4. Select **OK**.

**Configuring peer-to-peer web caching - CLI**

Use the following steps to configure the example WAN optimization configuration from the client-side and server-side FortiGate unit CLI.

1. Add the Local Host ID to the client-side FortiGate configuration:

   ```
   config wanopt settings
   set host-id Client_Side
   end
   ```

2. Add the server-side Local Host ID to the client-side peer list:

   ```
   config wanopt peer
   edit Server_Side
   set ip 192.168.30.12
   end
   ```

3. Add a firewall policy to the server-side FortiGate unit to accept the traffic to be optimized:

   ```
   config firewall policy
   edit 23
   set srcintf port1
   set dstintf port2
   set srcaddr all
   set dstaddr all
   set action accept
   ```

8. Select **OK**.

   The rule is added to the bottom of the WAN optimization list.

9. If required, use the Move To icon to move the rule to a different position in the list.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.

To configure the server-side FortiGate unit

1. Go to **WAN Opt. & Cache > Peer > Peer** and enter a Local Host ID for the server FortiGate unit:

   **Local Host ID**  Server_Side

2. Select **Apply** to save your setting.

3. Select **Create New** and add a Peer Host ID and the IP Address for the client-side FortiGate unit:

   **Peer Host ID**  Client_Side
   **IP Address**  172.20.34.12

4. Select **OK**.
set service ANY
set schedule always
end
end

4 Configure the following active rule:
config wanopt rule
edit 5
    set auto-detect off
    set src-ip 172.20.120.*
    set dst-ip 192.168.10.*
    set port 80
    set proto http
    set peer Server_Side
    set web cache enable
end

Accept default settings for transparent (enable), status (enable), mode (full),
byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-
group (null), unknown-http-version (tunnel), and tunnel-non-http
(disable).

5 If required, use the move command to the rule to a different position in the list.
The order of the rules in the list significantly affects how the rules are applied. For more
information, see “How list order affects rule matching” on page 48 and “Moving a rule
to a different position in the rule list” on page 49.

To configure the server-side FortiGate unit
1 Add the Local Host ID to the server-side FortiGate configuration:
config wanopt settings
    set host-id Server_Side
end

2 Add the client-side Local Host ID to the server-side peer list:
config wanopt peer
    edit Client_Side
    set ip 172.20.34.12
end

Changing web cache settings

In most cases, the default settings for the WAN optimization web cache are acceptable.
However, you may want to change them to improve performance or optimize the cache for
your configuration. To change these settings, go to WAN Opt. & Cache > Cache >
Settings.

From the FortiGate CLI, you can use the config wanopt webcache command to
change these WAN optimization web cache settings. For more information, see the
FortiGate CLI Reference.

Note: For more information about many of these web cache settings, see RFC 2616.
Always revalidate
Select to always revalidate requested cached objects with content on the server before serving them to the client.

Max cache object size
Set the maximum size of objects (files) that are cached. The default size is 512000 KB. This setting determines the maximum object size to store in the web cache. Objects that are larger than this size are still delivered to the client but are not stored in the FortiGate web cache.

Negative response duration
Set how long in minutes that the FortiGate unit caches error responses from web servers. If error responses are cached, then subsequent requests to the web cache from users will receive the error responses regardless of the actual object status.

The default is 0, meaning error responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes.

Fresh factor
Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100. For cached objects that do not have an expiry time, the web cache periodically checks the server to see if the objects have expired. The higher the Fresh Factor the less often the checks occur.

For example, if you set the Max TTL value and Default TTL to 7200 minutes (5 days) and set the Fresh Factor to 20, the web cache check the cached objects 5 times before they expire, but if you set the Fresh Factor to 100, the web cache will check once.

Max TTL
The maximum amount of time (Time to Live) an object can stay in the web cache without the cache checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days).

Min TTL
The minimum amount of time an object can stay in the web cache before the web cache checks to see if it has expired on the server. The default is 5 minutes.

Default TTL
The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours).

Explicit proxy
Indicates whether the explicit web proxy has been enabled for the FortiGate unit. See “The FortiGate explicit web proxy” on page 125.

Enable cache explicit proxy
Select to use WAN optimization web caching to cache content received by the explicit web proxy.
Ignore

Select the following options to ignore some web caching features.

- **If-modified-since**
  By default, if the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object.

  Enable ignoring if-modified-since to override this behavior.

- **HTTP 1.1 conditionals**
  HTTP 1.1 provides additional controls to the client over the behavior of caches toward stale objects. Depending on various cache-control headers, the FortiGate unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616.

  Enable ignoring HTTP 1.1 Conditionals to override this behavior.

- **Pragma-no-cache**
  Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This means that the FortiGate unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh.

  Because of this behavior, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if you enable ignoring Pragma-no-cache, then the PNC header from the client request is ignored. The FortiGate unit treats the request as if the PNC header is not present.

  Enable ignoring IE reload to cause the FortiGate unit to ignore the PNC interpretation of the Accept / header.

- **IE Reload**
  Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select Refresh. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object.

  Enable ignoring IE reload to cause the FortiGate unit to ignore the PNC interpretation of the Accept / header.

**Cache Expired Objects**

Applies only to type-1 objects. When this option is selected, expired type-1 objects are cached (if all other conditions make the object cacheable).

**Revalidated Pragma-no-cache**

The pragma-no-cache (PNC) header in a client's request can affect how efficiently the FortiGate unit uses bandwidth. If you do not want to completely ignore PNC in client requests (which you can do by selecting to ignore Pragma-no-cache, above), you can nonetheless lower the impact on bandwidth usage by selecting Revalidate Pragma-no-cache.

When you select Revalidate Pragma-no-cache, a client's non-conditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the 304 Not Modified response, which consumes less server-side bandwidth, because the OCS has not been forced to otherwise return full content.

By default, Revalidate Pragma-no-cache is disabled and is not affected by changes in the top-level profile.
Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, you should also configure byte-range support when you configure the `Revalidate pragma-no-cache` option.
Advanced configuration example

This chapter contains an advanced WAN optimization configuration example that combines many of the concepts described in the previous chapters of this document. The configuration example described here includes active-passive rules, web caching, policy routes for out-of-path WAN optimization, and multiple VDOMs with inter-VDOM routing to apply virus scanning (an optionally other UTM feature) to traffic before it is optimized.

Out-of-path WAN optimization with inter-VDOM routing

This example describes how to configure out-of-path WAN optimization to optimize web browsing and FTP file transfers between a client network and a server network.

Network topology and assumptions

The client network connects to the Internet through a FortiGate-300A unit, and the server network connects to the Internet through a cluster of two FortiGate-1000A units.

Adding in-path WAN optimization requires replacing these FortiGate units with models that support WAN optimization or adding new FortiGate units in the data path. In either of these in-path configurations, the optimizing FortiGate units would also be required to support all traffic on the data path plus provide WAN optimization.

The out-of-path topology shown in Figure offloads WAN optimization to out-of-path FortiGate units that only process sessions to be optimized. The topology includes a FortiGate-311B unit installed at the client network and a single FortiGate-620B unit installed at the server network.

Note: The FortiGate-620B unit is installed at the server network because other client networks also use it for WAN optimization. The configuration for those other client networks is not described in this example.

The client-side FortiGate-300A unit uses policy routing to offload WAN optimization of HTTP and FTP sessions by re-directing all HTTP and FTP sessions to the FortiGate-311B unit. The FortiGate-311B and 620B units work together to apply web caching, byte caching, and HTTP and FTP protocol optimization to HTTP and FTP sessions. The WAN optimization tunnel between the 311B and the 620B operates in Transparent mode. The FortiGate-311B unit also web caches all Internet HTTP traffic from the client network.

The client-side FortiGate-311B unit also applies virus scanning (and optionally other UTM features) to the HTTP and FTP traffic. To do this, the FortiGate-311B unit is configured for multiple VDOM operation. A new VDOM named Wanopt is added to the FortiGate-311B. HTTP and FTP sessions are received by the “root” VDOM. Firewall policies in the root VDOM accept HTTP and FTP sessions and apply virus scanning (and optionally other UTM features) to them. To preserve the source addresses of the HTTP and FTP sessions, NAT is not enabled for these policies.

The sessions are then routed through an inter-VDOM link to the Wanopt VDOM. The Wanopt VDOM includes firewall policies that accept the HTTP and FTP sessions and WAN optimization rules that apply WAN optimization and web caching to the sessions.
The server-side FortiGate-620B unit includes a passive WAN optimization rule that accepts WAN optimization tunnel requests from the FortiGate-311B unit. Only one passive rule is required on the FortiGate-620B unit. The FortiGate-620B unit also forwards sessions to the server-side FortiGate-1000A cluster which forwards them to the server network.

WAN optimization is operating in Transparent mode, so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses, the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the firewall policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.

The optimizing FortiGate units operate in NAT/Route mode and are directly connected to the Internet. This configuration requires two Internet connections and two Internet IP addresses for each network. (Reminder: All of the example IP addresses shown in Figure are private IP addresses because all Fortinet documentation examples use only private IP addresses.) If these extra Internet IP addresses are not available, you can install a router between the WAN and the FortiGate units or install the optimizing FortiGate units out of path on the private networks and configure routing on the private networks to route HTTP and FTP sessions to the optimizing FortiGate units.

**Configuration steps**

This example is divided into client-side and the server-side steps, as configured through the web-based manager and the CLI. Use either method, but 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.

This example includes the following sections:
- “Client-side configuration steps - web-based manager” on page 95
- “Server-side configuration steps - web-based manager” on page 102
Client-side configuration steps - web-based manager

This section describes the configuration steps required to redirect HTTP and FTP sessions from the client-side FortiGate-300A unit and to configure the client-side FortiGate-311B unit to optimize HTTP and FTP sessions to the server network and to apply web caching to all other HTTP sessions from the client network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1. Configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit.
2. Configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link.
3. Configure routing for the FortiGate-311B root VDOM.
4. Add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vlink0, and apply virus scanning (and optionally other UTM features).
5. Configure routing for the FortiGate-311B Wanopt VDOM.
6. Add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10.
7. Configure peers for the FortiGate-311B Wanopt VDOM.
8. Add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

To configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit

1. Go to System > Network > Interface, edit port4, and set the port4 IP address to 172.10.10.1/24.
2. Go to Firewall > Policy > Policy and select Create New to add a firewall policy that allows all port5 to port4 HTTP sessions:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>Source Address</th>
<th>Destination Interface/Zone</th>
<th>Destination Address</th>
<th>Schedule</th>
<th>Service</th>
<th>Action</th>
<th>NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>port5</td>
<td>all</td>
<td>port4</td>
<td>all</td>
<td>always</td>
<td>HTTP</td>
<td>ACCEPT</td>
<td>Select</td>
</tr>
</tbody>
</table>

Configure other policy settings that you may require.
3 Select Create New to add a firewall policy that allows all port5 to port4 FTP sessions:

Source Interface/Zone  port5
Source Address          all
Destination Interface/Zone  port4
Destination Address      all
Schedule                 always
Service                  FTP
Action                   ACCEPT
NAT                      Select

Configure other policy settings that you may require.

4 Select OK.

5 If required, use the Move To icon to change the order of the firewall policies.

Follow the normal rules for ordering firewall policies in the policy list. For example, move specific rules above general rules.

6 Go to Router > Static > Policy Route and select Create New to add a policy route to redirect HTTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For HTTP traffic, the protocol is 6 (TCP) and the destination port is 80:

Protocol  6
Incoming interface  port5
Source address / mask  0.0.0.0/0.0.0.0
Destination address / mask  0.0.0.0/0.0.0.0
Destination Ports From 80 to 80
Type of Service bit pattern: 00 (hex)  bit mask: 00 (hex)
Outgoing interface  port4
Gateway Address  172.10.10.2

7 Select OK.

8 Select Create New to add a policy route to redirect FTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For FTP traffic, the protocol is 6 (TCP) and the destination port is 21:

Protocol  6
Incoming interface  port5
Source address / mask  0.0.0.0/0.0.0.0
Destination address / mask  0.0.0.0/0.0.0.0
Destination Ports From 21 to 21
Type of Service bit pattern: 00 (hex)  bit mask: 00 (hex)
Outgoing interface  port4
Gateway Address  172.10.10.2

9 Select OK.
To configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link

1. Go to System > Status > Dashboard.
2. In the System Information widget, select Enable beside Virtual Domain to enable multiple VDOM operation and log back in to the web-based manager.
3. Go to System > VDOM and select Create New to add a new virtual domain named Wanopt.
4. Select OK twice to add the Wanopt VDOM with default resource limits.
5. Go to System > Network, edit the port10 interface, and configure the following settings to add the port10 interface to the Wanopt VDOM:

   ```
   Virtual Domain: Wanopt
   Addressing Mode: Manual
   IP/Netmask: 10.10.10.2/24
   ```

   Configure other settings that you may require.
6. Select OK.
7. Select Create New > VDOM Link and add an inter-VDOM link with the following settings:

   ```
   Name: Vlink
   Interface #0
   Virtual Domain: root
   IP/Netmask: 172.1.1.1/24
   Interface #1
   Virtual Domain: Wanopt
   IP/Netmask: 172.1.1.2/24
   ```

   Select OK.

To configure routing for the FortiGate-311B root VDOM

1. Log in to the root VDOM.
2. Go to Router > Static and select Create New to add a default route. The destination of the default route is the inter-VDOM link interface in the root VDOM. The gateway of the default route is the IP address of the inter-VDOM link interface in the Wanopt VDOM. The result is the default route sends all traffic out the inter-VDOM link and into the Wanopt VDOM:

   ```
   Destination IP/Mask: 0.0.0.0/0.0.0.0
   Device: Vlink0
   Gateway: 172.1.1.2
   Distance: 10
   ```

   Select OK.
4 Select Create New to add a route to send return traffic from the server network destined for the client network out the port1 interface to the port4 interface of the FortiGate-300A which has IP address 172.10.10.1:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>172.20.120.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>port1</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.10.10.1</td>
</tr>
<tr>
<td>Distance</td>
<td>10</td>
</tr>
</tbody>
</table>

5 Select OK.

To add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 destined for Vlink0 and apply virus scanning (and optionally other UTM features)

1 Log in to the root VDOM.

2 Go to Firewall > Policy > Policy and select Create New to add a firewall policy that accepts HTTP sessions received at port1 destined for Vlink0 and applies virus scanning and other UTM features:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Vlink0</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>HTTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Do not select.</td>
</tr>
</tbody>
</table>

Tip: To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.

<table>
<thead>
<tr>
<th>UTM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select UTM, select a protocol options profile and select an antivirus profile. Optionally select other UTM profiles.</td>
</tr>
</tbody>
</table>

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

3 Select OK.
4 Go to Firewall > Policy > Policy and select Create New to add a firewall policy that accepts FTP sessions received at port1 and destined for Vlink0 and applies virus scanning and other UTM features to them:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>all</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>Vlink0</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>FTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Do not select.</td>
</tr>
<tr>
<td><strong>Tip:</strong> To preserve the source addresses of the FTP sessions, NAT should not be enabled for this policy.</td>
<td></td>
</tr>
<tr>
<td>UTM</td>
<td>Select UTM, select a protocol options profile and select an antivirus profile. Optionally select other UTM profiles.</td>
</tr>
</tbody>
</table>

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

5 Select OK.

To configure routing for the FortiGate-311B Wanopt VDOM

1 Log in to the Wanopt VDOM.

2 Go to Router > Static and select Create New to add a default route. The destination of the default route is the port10 interface. The gateway of the default route is the next hop router that the port10 interface connects with:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>0.0.0.0/0.0.0.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>port10</td>
</tr>
<tr>
<td>Gateway</td>
<td>(next hop router IP address)</td>
</tr>
<tr>
<td>Distance</td>
<td>10</td>
</tr>
</tbody>
</table>

3 Select OK.

4 Select Create New to add a route to send return traffic from the server network destined for the client network out the Vlink1 interface to the Vlink0 interface in the root VDOM, which has the IP address 172.1.1.2:

<table>
<thead>
<tr>
<th>Destination IP/Mask</th>
<th>172.20.120.0/24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Vlink1</td>
</tr>
<tr>
<td>Gateway</td>
<td>172.1.1.2</td>
</tr>
<tr>
<td>Distance</td>
<td>10</td>
</tr>
</tbody>
</table>

5 Select OK.
To add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10:

1. Log in to the Wanopt VDOM.
2. Go to Firewall > Policy > Policy and select Create New to add a firewall policy that accepts HTTP sessions received at Vlink1 and destined for port10:

   Source Interface/Zone: Vlink1
   Source Address: all
   Destination Interface/Zone: port10
   Destination Address: all
   Schedule: always
   Service: HTTP
   Action: ACCEPT
   NAT: Select

   **Tip:** NAT is ignored for all HTTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, HTTP sessions for the Internet are intercepted by the Web Cache Only rule, so source NAT is required for replies.

   UTM: Do not select.

   **Tip:** Do not select UTM because you cannot apply UTM and WAN optimization to the same session in the same VDOM. UTM was applied to the session in the root VDOM.

   Configure other settings that you may require.

3. Select OK.
4. Go to Firewall > Policy and select Create New to add a firewall policy that accepts FTP sessions received at Vlink1 and destined for port10:

   Source Interface/Zone: Vlink1
   Source Address: all
   Destination Interface/Zone: port10
   Destination Address: all
   Schedule: always
   Service: FTP
   Action: ACCEPT
   NAT: Select

   **Tip:** NAT is ignored for all FTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, FTP sessions for the Internet are allowed to reach their destination, so source NAT is required for replies.

   UTM: Do not select.

   **Tip:** Do not select UTM because you cannot apply UTM and WAN optimization to the same session in the same VDOM. UTM was applied to the session in the root VDOM.

   Configure other settings that you may require.
To configure peers for the FortiGate-311B Wanopt VDOM

1. Log in to the Wanopt VDOM.
2. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the client-side FortiGate-311B unit:
   - Local Host ID: Client_Fgt
3. Select Apply to save your setting.
4. Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate-620B unit:
   - Peer Host ID: Server_Fgt
   - IP Address: 10.20.20.2
5. Select OK.

To add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM

1. Log in to the Wanopt VDOM.
3. Select Create New to add an active rule to optimize HTTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):
   - Mode: Full Optimization
   - Source: 172.20.120.*
   - Destination: 192.168.10.*
   - Port: 80
   - Auto-Detect: Active
   - Protocol: HTTP
   - Transparent Mode: Select
   - Enable Byte Caching: Select
   - Enable SSL: Do not select.
   - Enable Secure Tunnel: Do not select.
   - Tip: For improved privacy you can select this option and add an authentication group to both optimizing FortiGate units.
   - Authentication Group: Do not select.
4. Select OK.
5. Select Create New to add an active rule to optimize FTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):
   - Mode: Full Optimization
   - Source: 172.20.120.*
   - Destination: 192.168.10.*
   - Port: 21
   - Auto-Detect: Active
Out-of-path WAN optimization with inter-VDOM routing

Advanced configuration example

Server-side configuration steps - web-based manager

This section describes the configuration steps required for the server-side FortiGate-620B unit to perform WAN optimization with the client-side FortiGate-311B unit and to send HTTP and FTP sessions to the server-side FortiGate-1000A cluster. This section also describes how to configure the FortiGate-1000A cluster to forward HTTP and FTP sessions from the client network to the server network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1. Configure routing for the FortiGate-620B unit.
2. Configure peers for the server-side FortiGate-620B unit.
3. Add a passive WAN optimization rule to the server-side FortiGate-620B unit.
4. Configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network.

Also note that if you perform any additional actions between procedures, your configuration may have different results.
To configure routing for the FortiGate-620B unit

1. Go to **Router > Static** and select **Create New** to add a default route. The destination of the default route is the port16 interface. The gateway of the default route is the next hop router that the port16 interface connects with:

   - **Destination IP/Mask**: 0.0.0.0/0.0.0.0
   - **Device**: port16
   - **Gateway**: (next hop router IP address)
   - **Distance**: 10

2. Select **OK**.

3. Select **Create New** to add a route to send traffic for the server network out port1 to the port5 interface of the FortiGate-1000A cluster, which has the IP address 192.20.20.1:

   - **Destination IP/Mask**: 192.168.10.0/24
   - **Device**: port1
   - **Gateway**: 192.20.20.1
   - **Distance**: 10

4. Select **OK**.

To configure peers for the server-side FortiGate-620B unit

1. Go to **WAN Opt. & Cache > Peer** and enter a **Local Host ID** for the server-side FortiGate-620B unit:

   - **Local Host ID**: Server_Fgt

2. Select **Apply** to save your setting.

3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the client-side FortiGate-311B unit:

   - **Peer Host ID**: Client_Fgt
   - **IP Address**: 10.10.10.2

4. Select **OK**.

To add a passive WAN optimization rule to the server-side FortiGate-620B unit

You can add one passive WAN optimization rule to the server-side FortiGate-620B unit for both active rules on the FortiGate-311B unit. This rule can also allow the FortiGate-620B to perform WAN optimization with other client-side devices as long as the required Peer Host IDs are added to the FortiGate-620B configuration and to the client-side configurations.

1. Go to **WAN Opt. & Cache > Rule** and select **Create New** to add a passive rule that accepts any WAN optimization tunnel request:

   - **Mode**: Full Optimization
   - **Source**: 0.0.0.0
   - **Destination**: 192.168.10.*
   - **Port**: 1-65535

   **Tip**: You can also use a narrower port range such as 21-80 or add two rules, one with port set to 80 and one with port set to 21.
Out-of-path WAN optimization with inter-VDOM routing

Advanced configuration example

Auto-Detect: Passive
Enable Web Cache: Select

2 Select OK.

3 If required, use the Move To icon to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule. For more information, see “Moving a rule to a different position in the rule list” on page 49.

To configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network

1 Go to Firewall > Address and select Create New to add an address for the server network:

   Address Name: Server_Net
   Type: Subnet / IP Range
   Subnet / IP Range: 192.168.10.*
   Interface: Any

2 Select OK.

3 Go to Firewall > Address and select Create New to add an address for the client network:

   Address Name: Client_Net
   Type: Subnet / IP Range
   Subnet / IP Range: 172.20.120.*
   Interface: Any

4 Select OK.

5 Go to Firewall > Policy and select Create New to add an firewall policy that accepts HTTP sessions at port5 destined for port1 and the server network:

   Source Interface/Zone: port5
   Source Address: Client_Net
   Destination Interface/Zone: port1
   Destination Address: Server_Net
   Schedule: always
   Service: HTTP
   Action: ACCEPT
   NAT: Do not select.

   Tip: WAN optimization is operating in Transparent mode so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.

6 Select OK.
7 Go to Firewall > Policy and select Create New to add an firewall policy that accepts FTP sessions at port5 destined for port1 and the server network:

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>port5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Client_Net</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>port1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>Server_Net</td>
</tr>
<tr>
<td>Schedule</td>
<td>always</td>
</tr>
<tr>
<td>Service</td>
<td>FTP</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
<tr>
<td>NAT</td>
<td>Do not select</td>
</tr>
</tbody>
</table>

**Tip:** As described above, selecting NAT would cause the loss of client network source IP addresses.

8 Select OK.

**Client-side configuration steps - CLI**

This section describes the configuration steps required to redirect HTTP and FTP sessions from the client-side FortiGate-300A unit and to configure the client-side FortiGate-311B unit to optimize HTTP and FTP sessions to the server network and to apply web caching to all other HTTP sessions from the client network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1 Configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit.

2 Configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link.

3 Configure routing for the FortiGate-311B root VDOM.

4 Add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vink0, and apply virus scanning (and optionally other UTM features).

5 Configure routing for the FortiGate-311B Wanopt VDOM.

6 Add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link and destined for port10.

7 Configure peers for the FortiGate-311B Wanopt VDOM.

8 Add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

To configure the FortiGate-300A unit to redirect all HTTP and FTP sessions to the FortiGate-311B unit

1 Set the FortiGate-300A port4 IP address to 172.10.10.1:
   - config system interface
   - edit port4
     - set ip 172.10.10.1/24
   - end
   - end
2 Add a firewall policy that allows all port5 to port4 HTTP sessions:

```plaintext
config firewall policy
edit 1
set srcintf port5
set dstintf port4
set srcaddr all
set dstaddr all
set action accept
set service HTTP
set schedule always
set nat enable
end
end
```

Configure other policy settings that you may require. For example, you could add virus scanning (and optionally other UTM features).

3 Add a firewall policy that allows all port5 to port4 FTP sessions:

```plaintext
config firewall policy
edit 2
set srcintf port5
set dstintf port4
set srcaddr all
set dstaddr all
set action accept
set service FTP
set schedule always
set nat enable
end
end
```

Configure other policy settings that you may require.

4 If required, use the move command to change the order of the policies in the policy list. Follow the normal rules for ordering firewall policies in the policy list. For example, move specific rules above general rules.

5 Add a policy route to redirect HTTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the HTTP sessions are directed to the FortiGate-311B port1 interface. For HTTP traffic, the protocol is 6 (TCP) and the destination port is 80:

```plaintext
config router policy
edit 1
set protocol 6
set input-device port5
set output-device port4
set src 0.0.0.0/0.0.0.0
set dst 0.0.0.0/0.0.0.0
set start-port 80
set end port 80
set gateway 172.10.10.2
end
end
```

Accept default settings for tos (0x00) and tos-mask (0x00).
6 Add a policy route to redirect FTP traffic received at port5 to exit the FortiGate unit using port4. Set the gateway address of the route to 172.10.10.2 so that the FTP sessions are directed to the FortiGate-311B port1 interface. For FTP traffic, the protocol is 6 (TCP) and the destination port is 21:

```
config router policy
  edit 1
    set protocol 6
    set input-device port5
    set output-device port4
    set src 0.0.0.0/0.0.0.0
    set dst 0.0.0.0/0.0.0.0
    set start-port 21
    set end port 21
    set gateway 172.10.10.2
  end
end
```

Accept default settings for tos (0x00) and tos-mask (0x00).

To configure the FortiGate-311B unit for multiple VDOM operation and add an inter-VDOM link

1 Enable multiple VDOM operation and log back in to the web-based manager:

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

2 Log back in to the CLI.

3 Add a new virtual domain named Wanopt.

```
config vdom
  edit Wanopt
end
```

4 Add the port10 interface to the Wanopt VDOM:

```
config global
  config system interface
    edit port10
      set vdom Wanopt
      set IP 10.10.10.2/24
    end
  end
```

5 Add an inter-VDOM named Vlink and configure the Vlink0 and Vlink1 interfaces:

```
config global
  config system vdom-link
    edit Vlink
    config system interface
      edit Vlink0
        set vdom root
        set ip 172.1.1.1/24
      next
      edit Vlink1
        set vdom Wanopt
        set ip 172.1.1.2/24
    end
end
```
To configure routing for the FortiGate-311B root VDOM

1. Log in to the root VDOM from the CLI.

2. Add a default route. The destination of the default route is the inter-VDOM link interface in the root VDOM. The gateway of the default route is the IP address of the inter-VDOM link interface in the Wanopt VDOM. The result is the default route sends all traffic out the inter-VDOM link and into the Wanopt VDOM:

   ```
   config router static
   edit 1
   set dst 0.0.0.0/0.0.0.0
   set device Vlink0
   set gateway 172.1.1.2
   set distance 10
   end
   ```

3. Add a route to send return traffic from the server network destined for the client network out the port1 interface to the port4 interface of the FortiGate-300A which has IP address 172.10.10.1:

   ```
   config router static
   edit 2
   set dst 172.20.120.0/24
   set device port1
   set gateway 172.10.10.1
   set distance 10
   end
   ```

To add firewall policies to the FortiGate-311B root VDOM to accept HTTP and FTP sessions received at port1 and destined for Vlink0 and apply virus scanning and optionally other UTM features)

1. Log in to the root VDOM from the CLI.

2. Add a firewall policy that accepts HTTP sessions received at port1 and applies virus scanning to them:

   ```
   config firewall policy
   edit 20
   set srcintf port1
   set dstintf Vlink0
   set srcaddr all
   set dstaddr all
   set action accept
   set service HTTP
   set schedule always
   set utm-status enable
   set profile-protocol-options default
   set av-profile scan
   end
   ```

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

Tip: To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.
3 Add a firewall policy that accepts FTP sessions received at port1 and applies virus scanning to them:

```plaintext
cfg firewall policy
edit 20
   set srcintf port1
   set dstintf Vlink0
   set srcaddr all
   set dstaddr all
   set action accept
   set service FTP
   set schedule always
   set utm-status enable
   set profile-protocol-options default
   set av-profile scan
end
```

**Tip:** To preserve the source addresses of the HTTP sessions, NAT should not be enabled for this policy.

Configure other policy settings that you may require. You can also use more specific firewall addresses or add one firewall policy that accepts both FTP and HTTP traffic.

**To configure routing for the FortiGate-311B Wanopt VDOM**

1 Log in to the Wanopt VDOM from the CLI.

2 Add a default route. The destination of the default route is the port10 interface. The gateway of the default route is the next hop router that the port10 interface connects with:

```plaintext
cfg router static
edit 1
   set dst 0.0.0.0/0.0.0.0
   set device port10
   set gateway (next hop router IP address)
   set distance 10
end
```

3 Add a route to send return traffic from the server network destined for the client network out the Vlink1 interface to the Vlink0 interface in the root VDOM, which has the IP address 172.1.1.2:

```plaintext
cfg router static
edit 2
   set dst 172.20.120.0/24
   set device Vlink1
   set gateway 172.1.1.2
   set distance 10
end
```

**To add firewall policies to the FortiGate-311B Wanopt VDOM to accept HTTP and FTP sessions received at the Vlink1 interface of the inter-VDOM link destined for port10**

1 Log in to the Wanopt VDOM from the CLI.

2 Add a firewall policy that accepts HTTP sessions received at Vlink1 and destined for port10:
config firewall policy
edit 20
   set srcintf Vlink1
   set dstintf port10
   set srcaddr all
   set dstaddr all
   set action accept
   set service HTTP
   set schedule always
   set nat enable
end

Tip: NAT is ignored for all HTTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, HTTP sessions for the Internet are intercepted by the Web Cache Only rule, so source NAT is required for replies.

Tip: Do not enable UTM because you cannot apply UTM features and WAN optimization to the same session in the same VDOM. Virus scanning was applied to the session in the root VDOM.

Configure other settings that you may require.

3 Go to Firewall > Policy and select Create New to add a firewall policy that accepts FTP sessions received at Vlink1 and destined for port10:

config firewall policy
edit 20
   set srcintf Vlink1
   set dstintf port10
   set srcaddr all
   set dstaddr all
   set action accept
   set service FTP
   set schedule always
   set nat enable
end

Tip: NAT is ignored for all HTTP sessions for the server network because these sessions are intercepted by a full optimization WAN optimization rule. However, HTTP sessions for the Internet are intercepted by the Web Cache Only rule, so source NAT is required for replies.

Tip: Do not enable UTM because you cannot apply UTM features and WAN optimization to the same session in the same VDOM. Virus scanning was applied to the session in the root VDOM.

Configure other settings that you may require.

To configure peers for the FortiGate-311B Wanopt VDOM

1 Log in to the Wanopt VDOM from the CLI.
2 Add the Local Host ID for the client-side FortiGate-311B unit:
   config wanopt settings
      set host-id Client_Fgt
   end
3 Add a Peer Host ID and the IP Address for the server-side FortiGate-620B unit.

```bash
config wanopt peer
  edit Server_Fgt
    set ip 10.20.20.2
  end
```

To add WAN optimization rules for HTTP and FTP to the FortiGate-311B Wanopt VDOM

1 Log in to the Wanopt VDOM from the CLI.

2 Add an active rule to optimize HTTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

```bash
config wanopt rule
  edit 4
    set auto-detect active
    set src-ip 172.20.120.0-172.20.120.255
    set dst-ip 192.168.10.0-192.168.10.255
    set port 80
    set proto http
  end
```

Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

Tip: For improved privacy you can enable secure-tunnel and add an authentication group to both optimizing FortiGate units.

3 Add an active rule to optimize FTP traffic from IP addresses on the Client network (172.20.120.0) with a destination address on the server network (192.168.10.0):

```bash
config wanopt rule
  edit 5
    set auto-detect active
    set src-ip 172.20.120.0-172.20.120.255
    set dst-ip 192.168.10.0-192.168.10.255
    set port 21
    set proto ftp
  end
```

Accept default settings for transparent (enable), status (enable), mode (full), byte-caching (enable), ssl (disable), secure-tunnel (disable), auth-group (null), unknown-http-version (tunnel), and tunnel-non-http (disable).

Tip: For improved privacy you can enable secure-tunnel and add an authentication group to both optimizing FortiGate units.
4 Add a rule to web cache HTTP traffic from IP addresses on the Client network (172.20.120.0) with any destination address:
   config wanopt rule
   edit 6
   set mode webcache-only
   set src-ip 172.20.120.0-172.20.120.255
   set dst-ip 0.0.0.0
   set port 80
   set proto http
   end

   Accept default settings for transparent (enable), status (enable), ssl (disable), unknown-http-version (tunnel), and tunnel-non-http (disable).

5 If required, use the move command to move the Web Cache Only rule below the full optimization HTTP and FTP rules in the list. The Web Cache Only rule should be below the full optimization rules because it will match all HTTP traffic and you need HTTP sessions with destination address 192.168.10.0 to match the full optimization HTTP rule.

   For more information, see “Moving a rule to a different position in the rule list” on page 49.

**Server-side configuration steps - CLI**

This section describes the configuration steps required for the server-side FortiGate-620B unit to perform WAN optimization with the client-side FortiGate-311B unit and to send HTTP and FTP sessions to the server-side FortiGate-1000A cluster. This section also describes how to configure the FortiGate-1000A cluster to forward HTTP and FTP sessions from the client network to the server network.

The section breaks down the client-side configuration into smaller procedures. For best results, follow the procedures in the order given:

1 Configure routing for the FortiGate-620B unit.

2 Configure peers for the server-side FortiGate-620B unit.

3 Add a passive WAN optimization rule to the server-side FortiGate-620B unit.

4 Configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port 80 and forward them out port1 to the server network.

Also note that if you perform any additional actions between procedures, your configuration may have different results.

**To configure routing for the FortiGate-620B unit**

1 Add a default route. The destination of the default route is the port16 interface. The gateway of the default route is the next hop router that the port16 interface connects with:

   config router static
   edit 1
   set dst 0.0.0.0/0.0.0.0
   set device port16
   set gateway (next hop router IP address)
   set distance 10
   end
2 Add a route to send traffic for the server network out port1 to the port5 interface of the FortiGate-1000A cluster, which has the IP address 192.20.20.1:

```bash
config router static
edit 2
set dst 192.168.10.0/24
set device port1
set gateway 192.20.20.1
set distance 10
end
```

To configure peers for the server-side FortiGate-620B unit

1 Add the Local Host ID for the server-side FortiGate-620B unit:

```bash
config wanopt settings
set host-id Server_Fgt
end
```

2 Add a Peer Host ID and the IP Address for the client-side FortiGate-311B unit:

```bash
config wanopt peer
edit Client_Fgt
set ip 10.10.10.2
end
```

To add a passive WAN optimization rule to the server-side FortiGate-620B unit

You can add one passive WAN optimization rule to the server-side FortiGate-620B unit for both active rules on the FortiGate-311B unit. This rule can also allow the FortiGate-620B to perform WAN optimization with other client-side devices as long as the required Peer Host IDs are added to the FortiGate-620B configuration and to the client-side configurations.

1 Go to WAN Opt. & Cache > Rule and select Create New to add a passive rule that accepts any WAN optimization tunnel request:

```bash
config wanopt rule
edit 5
set auto-detect passive
set src-ip 0.0.0.0
set dst-ip 192.168.10.0-192.168.10.255
set port 1-65535
set webcache enable
end
```

Accept default settings for status (enable) and mode (full).

Tip: You can also use a narrower port range such as 21-80 or add two rules, one with port set to 80 and one with port set to 21.

2 If required, use the move command to move the rule to a different position in the list so that the tunnel request from the client-side FortiGate unit matches with this rule.

For more information, see “Moving a rule to a different position in the rule list” on page 49.
To configure the FortiGate-1000A cluster to accept HTTP and FTP connections at port5 and forward them out port1 to the server network

1 Add a firewall address for the server network:
   config firewall address
   edit Server_Net
   set type iprange
   set start-ip 192.168.10.0
   set end-ip 192.168.10.255
   end

2 Add a firewall address for the client network:
   config firewall address
   edit Client_Net
   set type iprange
   set start-ip 172.20.120.0
   set end-ip 172.20.120.255
   end

3 Go to Firewall > Policy and select Create New to add an firewall policy that accepts HTTP sessions at port5 destined for port1 and the server network:
   config firewall policy
   edit 10
   set srcintf port5
   set dstintf port1
   set srcaddr Client_Net
   set dstaddr Server_Net
   set action accept
   set service HTTP
   set schedule always
   end
   end

   Tip: WAN optimization is operating in Transparent mode so the packets from the client network include their client network source IP addresses. To preserve these source IP addresses, the firewall policies on the FortiGate-1000A cluster that accept the sessions from the FortiGate-620B unit should not apply NAT. If the policies were to apply NAT, the client network addresses would be replaced with the port1 IP address of the FortiGate-1000A cluster and the client network source IP addresses would be lost.

4 Go to Firewall > Policy and select Create New to add an firewall policy that accepts FTP sessions at port5 destined for port1 and the server network:
   config firewall policy
   edit 11
   set srcintf port5
   set dstintf port1
   set srcaddr Client_Net
   set dstaddr Server_Net
   set action accept
   set service FTP
   set schedule always
   end
   end

   Tip: As described above, selecting NAT would cause the loss of the client network source IP addresses.
SSL offloading for WAN optimization and web caching

WAN optimization SSL offloading uses the FortiGate unit to encrypt and decrypt SSL sessions. WAN optimization supports SSL offloading for HTTP and HTTPS sessions to and from web servers. The FortiGate unit intercepts HTTPS traffic from clients and decrypts it before sending it as HTTP clear text to the web server. The HTTP clear text response from the web server is encrypted by the FortiGate unit and returned to the client as an HTTPS session. The result should be a performance improvement because SSL encryption and decryption is offloaded from the server to the FortiGate unit's FortiASIC SSL encryption/decryption engine. You can also combine SSL offloading with other WAN optimization techniques such as HTTP protocol optimization, byte caching, and web caching to further enhance web server performance.

You enable SSL offloading by selecting Enable SSL in a WAN optimization rule. You must also add SSL servers to support SSL offloading by using the CLI command `config wanopt ssl-server`.

You must add one WAN optimization SSL server configuration to a FortiGate unit for each HTTP server for which you are configuring SSL offloading. This SSL server configuration must also include the HTTP server CA. You load this certificate into the FortiGate unit as a local certificate and then add it to the SSL server configuration using the `ssl-cert` keyword. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

You can configure one WAN optimization rule to offload SSL encryption/decryption for multiple HTTP servers. To do this, you configure the WAN optimization rule source and destination addresses, so that the rule accepts packets destined for all of the HTTP servers for which you want offloading. Then you add one SSL server configuration for each of the HTTP servers.

A number of SSL offloading configurations are possible. This chapter demonstrates two:

- Example: SSL offloading for a WAN optimization tunnel
- Example: SSL offloading and reverse proxy web caching for an Internet web server

Example: SSL offloading for a WAN optimization tunnel

This example shows how to configure basic SSL offloading for a WAN optimization tunnel. This basic SSL offloading configuration can be applied to many network configurations.

Network topology and assumptions

In this example, clients on a client network use https://192.168.10.20 to browse to a web server. A WAN optimization rule with Auto-Detect set to Off on the client-side FortiGate unit accepts sessions from the clients with source addresses on the 172.20.120.0 network and with a destination address of 192.168.10.0 and a destination port of 443. In this rule, Enable Secure Tunnel is selected so that the tunnel is encrypted. To support the encrypted tunnel, the configuration also includes an authentication group with a pre-shared key. Both FortiGate units must have the same authentication group with the same pre-shared key.
The server-side FortiGate unit includes an SSL server configuration with `ip` set to 192.168.10.20 and `port` to 443. The unit also includes the web server CA.

**Figure 27: SSL offloading WAN optimization configuration**

When the client-side FortiGate unit accepts an HTTPS connection for 192.168.10.20, the SSL server configuration provides the information that the client-side unit needs to decrypt the traffic and send it in clear text across a WAN optimization tunnel to the server-side unit. The server-side unit then forwards the clear text packets to the web server.

The web server CA is not downloaded from the server side to the client-side FortiGate unit. Instead, the client-side FortiGate unit proxies the SSL parameters from the client side to the server side, which returns an SSL key and other required information to the client-side unit so that it can decrypt and encrypt HTTPS traffic.

**Note:** In this peer-to-peer configuration you do not need to add a WAN optimization rule to the server-side FortiGate unit as long as this server-side unit includes the peer host ID of the client-side FortiGate unit in its peer list. However, you can set `Auto-Detect` to `Active` on the client-side FortiGate unit and then add a passive rule to the server-side unit.

In this example, you do not require the secure tunnel and the authentication group configurations, but they are included to show how to protect the privacy of the WAN optimization tunnel. Alternatively, you could configure a route-based IPSec VPN between the FortiGate units and use IPSec to protect the privacy of the WAN optimization tunnel.

In this example, it is assumed that you have a local CA named `Web_Server_Cert_1.crt` stored in a file that you will import when you configure the server-side FortiGate unit.
General configuration steps

This example is divided into client-side and server-side steps, as configured through the web-based manager, and with CLI instructions provided for CLI-only steps. 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. You also need access to the CLI to perform CLI-only steps.

Client-side configuration steps

To configure the client-side FortiGate unit

1. Go to WAN Opt. & Cache > Peer and enter a Local Host ID for the server-side FortiGate unit:
   - Local Host ID: User_net

2. Select Apply to save your setting.

3. Select Create New and add a Peer Host ID and the IP Address for the peer side FortiGate unit:
   - Peer Host ID: Web_servers
   - IP Address: 192.168.10.1

4. Select OK.

5. Go to WAN Opt. & Cache > Peer > Authentication Group and select Create New to add an authentication group named SSL_auth_grp to the client-side FortiGate unit.
   The authentication group includes a pre-shared key and the peer added in step 3. An authentication group with the same name and the same pre-shared key must also be added to the server-side FortiGate unit. This authentication group is required for the secure tunnel:
   - Name: SSL_auth_grp
   - Authentication Method: Pre-shared key
   - Password: <pre-shared_key>
   - Peer Acceptance: Specify Peer: Web_servers

6. Select OK.

7. Go to WAN Opt. & Cache > Rule and select Create New to add the WAN optimization rule:
   - Mode: Full Optimization
   - Source: 172.20.120.*
   - Destination: 192.168.10.*
   - Port: 443
   - Auto-Detect: Off
   - Protocol: HTTP
   - Peer: Web_servers
   - Transparent Mode: Select
   - Enable Byte Caching: Select
   - Enable SSL: Select
Example: SSL offloading for a WAN optimization tunnel

SSL offloading for WAN optimization and web caching

Server-side configuration steps

To configure the server-side FortiGate unit

1. Go to **WAN Opt. & Cache > Peer** and enter a **Local Host ID** for the server-side FortiGate unit:
   - Local Host ID: Web_servers

2. Select **Apply** to save your setting.

3. Select **Create New** and add a **Peer Host ID** and the **IP Address** for the peer side FortiGate unit:
   - Peer Host ID: User_net
   - IP Address: 172.20.120.1

4. Select **OK**.

5. Go to **WAN Opt. & Cache > Peer > Authentication Group** and select **Create New** to add an authentication group named SSL_auth_grp to the server-side FortiGate unit.

   The authentication group includes a pre-shared key and the peer added to the server-side FortiGate unit in step 3:
   - Name: SSL_auth_grp
   - Authentication Method: Pre-shared key
   - Password: <pre-shared_key>
   - Peer Acceptance: Specify Peer: User_net

6. Select **OK**.

7. Go to **System > Certificates > Local Certificates** and select **Import** to import the web server’s CA.

   For **Type**, select **Local Certificate**. Select the **Browse** button to locate the file, Web_Server_Cert_1.crt.

   The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

8. From the CLI, enter the following command to add the SSL server to the server-side FortiGate unit:

   ```
   config wanopt ssl-server
   edit example_server
   set ip 192.168.10.20
   set port 443
   set ssl-cert Web_Server_Cert_1
   end
   ```

   Configure other **ssl-server** settings that you may require for your configuration.
Example: SSL offloading and reverse proxy web caching for an Internet web server

This example shows how to configure SSL offloading for a reverse proxy Web Cache Only WAN optimization configuration.

Network topology and assumptions

In this configuration, clients on the Internet use HTTPS to browse to a web server. The FortiGate unit intercepts the HTTPS traffic, and a Web Cache Only WAN optimization rule with SSL offloading enabled decrypts the traffic before sending it to the web server. The FortiGate unit also caches pages from the web server. Replies from the web server are encrypted by the FortiGate unit before returning to the web browsing clients.

The Web Cache Only rule enables transparent mode because the FortiGate unit is performing NAT between the Internet and the HTTP server and the web server network is not configured to route Internet traffic between the FortiGate unit and the web server.

In this configuration, the FortiGate unit is operating in reverse proxy mode. Reverse proxy caches can be placed directly in front of a particular server. Web caching on the FortiGate unit reduces the number of requests that the web server must handle, therefore leaving it free to process new requests that it has not serviced before.

Using a reverse proxy configuration:

- avoids the capital expense of additional web servers by increasing the capacity of existing servers
- serves more requests for static content from web servers
- serves more requests for dynamic content from web servers
- reduces operating expenses including the cost of bandwidth required to serve content
- accelerates the response time of web servers and of page download times to end users.

When planning a reverse proxy implementation, the web server's content should be written so that it is "cache aware" to take full advantage of the reverse proxy cache.

In reverse proxy mode, the FortiGate unit functions more like a web server for the clients it services. Unlike internal clients, external clients are not reconfigured to access the proxy server. Instead, the site URL routes the client to the FortiGate unit as if it were a web server. Replicated content is delivered from the proxy cache to the external client without exposing the web server or the private network residing safely behind the firewall.

In this example, the site URL translates to IP address 192.168.10.1, which is the port2 IP address of the FortiGate unit. The port2 interface is connected to the Internet.

This example also includes two Web Cache Only rules, one that accepts the HTTP traffic for web caching and one that accepts the HTTPS traffic for SSL offloading and web caching. You could instead add only one rule for both the HTTP and HTTPS traffic.

For this example, it is also assumed that all HTTP traffic uses port 80 and all HTTPS traffic uses port 443.

The FortiGate unit includes the web server CA and an SSL server configuration for IP address 172.10.20.30 and port to 443. The name of the file containing the CA is Rev_Proxy_Cert_1.crt.
Configuration steps

To configure the FortiGate unit as a reverse proxy web cache server

1. Go to Firewall > Virtual IP and select Create New to add a virtual IP that translates the destination IP address from 192.168.10.1 to 172.10.20.30:

   - Name: Reverse_proxy_VIP
   - External Interface: port2
   - Type: Read only description of currently mode, usually Static NAT.
   - External IP Address/Range: 192.168.10.1
   - Mapped IP Address/Range: 172.10.20.30
   - Port Forwarding: Do not select.

2. Select OK to save your settings.

3. Go to Firewall > Policy and select Create New to add a port2 to port1 firewall policy that accepts HTTP and HTTPS traffic from the Internet:

   - Do not select UTM features. Set the destination address to the virtual IP. You do not have to enable NAT.
   - Source Interface/Zone: port2
   - Source Address: all
   - Destination Interface/Zone: port1
   - Destination Address: Reverse_proxy_VIP
   - Service: HTTP and HTTPS
     - Note: Select Multiple to display a screen for entering more than one service.
   - Action: ACCEPT

4. Select OK to save your settings.
5 Go to WAN Opt. & Cache > Rule and select Create New to add a Web Cache Only WAN optimization rule.

6 Configure the rule to accept the HTTP traffic accepted by the firewall policy:

- **Mode**: Web Cache Only
- **Source**: 0.0.0.0
- **Destination**: 192.168.10.1
  
  **Note**: You need to set Destination to the IP address that is translated by the virtual IP (192.168.10.1) and not to the server IP (172.10.20.30).
- **Port**: 80
- **Transparent Mode**: Select
- **Enable SSL**: Do not select

7 Select OK.
   The rule is added to the bottom of the WAN optimization list.

8 If required, move the rule to a different position in the list.
   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.

To configure the FortiGate unit for SSL offloading of HTTPS traffic

The firewall policy added in the first procedure accepts HTTPS traffic so you do not have to add another one.

1 Go to WAN Opt. & Cache > Rule and select Create New to add a Web Cache Only WAN optimization rule.

2 Configure the rule to accept the HTTPS traffic accepted by the firewall policy:

- **Mode**: Web Cache Only
- **Source**: 0.0.0.0
- **Destination**: 192.168.10.1
  
  **Note**: You need to set Destination to the IP address that is translated by the virtual IP (192.168.10.1) and not to the server IP (172.10.20.30).
- **Port**: 443
- **Transparent Mode**: Select
- **Enable SSL**: Select

3 Select OK.
   The rule is added to the bottom of the WAN optimization list.

4 If required, move the rule to a different position in the list.
   The HTTPS rule can be above or below the HTTP rule.
   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.
To add an SSL server to offload SSL encryption and decryption for the web server.

1. Go to System > Certificates > Local Certificates and select Import to import the web server’s CA. For Type, select Local Certificate. Select the Browse button to locate the file Rev_Proxy_Cert_1.crt.

   The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

2. From the CLI, enter the following command to add the SSL server.

   ```
   config wanopt ssl-server
   edit rev_proxy_server
   set ip 172.10.20.30
   set port 443
   set ssl-cert Rev_Proxy_Cert_1
   end
   ```

3. Configure other ssl-server settings that you may require for your configuration.

   The order of the rules in the list significantly affects how the rules are applied. For more information, see "How list order affects rule matching" on page 48 and "Moving a rule to a different position in the rule list" on page 49.
FortiClient WAN optimization

FortiClient WAN optimization works together with WAN optimization on a FortiGate unit to accelerate network traffic between a PC running version 4.0 or greater of the FortiClient application and a network behind a FortiGate unit. When a user of a PC with FortiClient WAN optimization enabled attempts to connect to network resources behind a server-side FortiGate unit, the FortiClient application automatically detects if WAN optimization is enabled on the FortiGate unit. If WAN optimization is detected and the FortiClient application can successfully negotiate a WAN optimization tunnel with the FortiGate unit, a WAN optimization tunnel starts.

FortiClient WAN optimization includes protocol optimization settings selected in the FortiClient application and byte caching (byte caching is enabled by default in the FortiClient application and cannot be disabled). Web caching is applied if selected in the passive rule on the FortiGate unit that accepts FortiClient WAN optimization tunnel requests.

This chapter describes how to configure the FortiClient application for WAN optimization and how to configure a FortiGate unit to accept WAN optimization tunnel requests from the FortiClient application.

Figure 29: FortiClient WAN optimization topology

Configuring FortiClient WAN optimization

Configuring WAN optimization with the FortiClient application consists of enabling WAN optimization for the FortiClient application and configuring the FortiGate unit to accept WAN optimization tunnel requests from the FortiClient application.
FortiClient configuration steps

To configure WAN Optimization for the FortiClient application
1. From the FortiClient user interface, go to Status > WAN Optimization.
2. Select Enable WAN Optimization.
3. Enable the protocols to be optimized: HTTP (web browsing), CIFS (Windows file sharing), MAPI (Microsoft Exchange) and FTP (file transfers).
4. Set Maximum Disk Cache to 512, 1024, or 2048 MB.
   The default is 512 MB. If the PC hard disk can accommodate a larger cache, better optimization performance is possible.
5. Select Apply.

FortiGate unit configuration steps

To configure FortiClient WAN Optimization on the FortiGate unit
Because PCs running the FortiClient application can have IP addresses that change often, it is usually not practical to add PCs running the FortiClient application to the WAN optimization peer list. Instead, a FortiGate unit that accepts WAN optimization tunnel requests from the FortiClient application should be configured to accept any peer (see “Accepting any peers” on page 39) by adding an authentication group named auth-fc with Peer acceptance set to Accept Any Peer.

On the FortiGate unit, you also need to add a passive rule that includes source and destination addresses that will accept connections from the IP addresses of PCs running the FortiClient application. If these PCs can be anywhere on the Internet, the source address for this rule is 0.0.0.0. You can also use a more restrictive address range if the PCs running the FortiClient application have a restricted range of addresses.
You do not need to add firewall policies to the FortiGate unit because it is on the server side of the WAN optimization tunnel.
2. Configure the authentication group:
   - Name: auth-fc
   - Authentication Method: Certificate
   - Certificate: Fortinet_Firmware
   - Peer Acceptance: Accept Any Peer
3. Select OK.
5. Configure a rule to accept FortiClient WAN optimization sessions:
   - Mode: Full Optimization
   - Source: 0.0.0.0
   - Destination: 0.0.0.0
   - Port: 1-65535
   - Auto-Detect: Passive
6. Select OK.
The FortiGate explicit web proxy

You can use the FortiGate explicit web proxy to enable explicit HTTP, and HTTPS proxying on one or more FortiGate interfaces. The explicit web proxy also supports proxying FTP sessions from a web browser and proxy auto-config (PAC) to provide automatic proxy configurations for explicit web proxy users. From the CLI you can also configure the explicit web proxy to support SOCKS sessions from a web browser.

**Note:** Web proxies are configured for each VDOM when multiple VDOMs are enabled.

In most cases you would configure the explicit web proxy for users on a network by enabling the explicit web proxy on the FortiGate interface connected to that network. Users on the network would configure their web browsers to use a proxy server for HTTP and HTTPS, FTP, or SOCKS and set the proxy server IP address to the IP address of the FortiGate interface connected to their network. Users could also enter the PAC URL into their web browser PAC configuration to automate their web proxy configuration using a PAC file stored on the FortiGate unit.

**Caution:** Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

If the FortiGate unit is operating in Transparent mode, users would configure their browsers to use a proxy server with the FortiGate unit management IP address. The web proxy receives web browser sessions to be proxied at FortiGate interfaces with the explicit web proxy enabled. The web proxy uses FortiGate routing to route sessions through the FortiGate unit to a destination interface. Before a session leaves the exiting interface, the explicit web proxy changes the source addresses of the session packets to the IP address of the exiting interface. When the FortiGate unit is operating in Transparent mode the explicit web proxy changes the source addresses to the management IP address. For more information about explicit web proxy sessions, see “Explicit web proxy sessions and user limits” on page 139.

Figure 30: Example explicit web proxy topology
To allow all explicit web proxy traffic to pass through the FortiGate unit you can set the explicit web proxy default firewall proxy action to accept. However, in most cases you would want to use firewall policies to control explicit web proxy traffic and apply firewall features such as access control/authentication, UTM, and traffic logging. You can do this by keeping the default explicit web proxy firewall policy action to deny and then adding web-proxy firewall policies.

Web-proxy firewall policies can selectively allow or deny traffic, apply authentication using identity-based policies, enable traffic logging, and use UTM options to apply virus scanning, web filtering, and DLP to explicit web proxy traffic. There are some limitations to the UTM features that can be applied to explicit web proxy sessions. See “UTM features and the explicit web proxy” on page 132.

You cannot configure IPsec, SSL VPN, or Traffic shaping for explicit web proxy traffic. Firewall policies for the web proxy can only include firewall addresses not assigned to a FortiGate unit interface or with interface set to any.

Authentication of explicit web proxy sessions uses HTTP authentication and can be based on the user’s source IP address or on cookies from the user’s web browser. For more information, see “Explicit web proxy authentication” on page 130.

To use the explicit proxy, users must add the IP address of a FortiGate interface on which the explicit proxy is enabled and the explicit proxy port number (default 8080) to the proxy configuration settings of their web browsers.

On FortiGate units that support WAN optimization, you can also enable web caching for explicit web proxy sessions.

This section describes:

- Configuration overview
- Explicit web proxy authentication
- UTM features and the explicit web proxy
- Example: users on an internal network browsing the Internet through the explicit proxy with web caching, RADIUS authentication, web filtering and virus scanning
- Explicit web proxy sessions and user limits

Configuration overview

You can use the following general steps to configure the explicit web proxy.

To enable the explicit web proxy - web-based manager

1. Go to System > Network > Interface and enable the explicit web proxy for one or more FortiGate interfaces.

   **Caution:** Enabling the explicit web proxy on an interface connected to the Internet is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address.

2. Go to System > Network > Web Proxy. Select Enable Explicit Web Proxy to turn on the explicit web proxy for HTTP and HTTPS traffic.

   You can also select FTP to enable the web proxy for FTP sessions in a web browser (not an FTP client) and PAC to enable automatic proxy configuration.
3 Select OK.

The default explicit web proxy configuration has Default Firewall Policy Action set to Deny and requires you to add a firewall policy to allow access to the explicit proxy. This configuration is recommended because you can use firewall policies to control access to the explicit web proxy and also apply firewall features such as logging, UTM, and authentication (by adding identity-based policies).

4 Go to Firewall > Policy > Policy and select Create New and set the Source Interface/Zone to web-proxy.

You can add multiple web-proxy firewall policies.

5 Configure the firewall policy as required to accept the traffic that you want to be processed by the explicit web proxy.

The source address of the policy should match client source IP addresses. The firewall address selected as the source address cannot be assigned to a FortiGate interface. The Interface field of the firewall address must be blank or it must be set to Any.

The destination address of the policy should match the IP addresses of web sites that clients are connecting to. Usually the destination address would be all if proxying Internet web browsing.

Traffic sent to the explicit web proxy that is not accepted by a web-proxy firewall policy is dropped. If Default Firewall Policy Action is set to Allow then all web-proxy sessions are allowed.

For example the following firewall policy allows users on an internal network to access the Internet through the wan1 interface of a FortiGate unit.

<table>
<thead>
<tr>
<th>Source Interface/Zone</th>
<th>web-proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Address</td>
<td>Internal_subnet</td>
</tr>
<tr>
<td>Destination Interface/Zone</td>
<td>wan1</td>
</tr>
<tr>
<td>Destination Address</td>
<td>all</td>
</tr>
<tr>
<td>Action</td>
<td>ACCEPT</td>
</tr>
</tbody>
</table>

6 You can select other firewall policy options as required.

For example, you can apply UTM protection to web proxy sessions and log allowed web proxy traffic.

7 You can also select Enable Identity Based Policy to apply authentication to explicit web proxy sessions.

8 You can add multiple identity based policies to apply different authentication for different user groups and also apply different UTM and logging settings for different user groups.
To enable the explicit web proxy - CLI

1. Enter the following command to enable the explicit web proxy for the internal interface.

   ```
   config system interface
   edit internal
   set explicit-web-proxy enable
   end
   ```

2. Enter the following command to turn on the explicit web proxy for HTTP and HTTPS traffic.

   ```
   config web-proxy explicit
   set status enable
   end
   ```

   You can also enter the following command to enable the web proxy for FTP sessions in a web browser.

   ```
   config web-proxy explicit
   set ftp-over-http enable
   end
   ```

   The default explicit web proxy configuration has `sec-default-action` set to `deny` and requires you to add a firewall policy to allow access to the explicit proxy.

3. Use the following command to add a firewall address that matches the source address of users who connect to the explicit proxy.

   ```
   config firewall address
   edit Internal_subnet
   set type iprange
   set start-ip 10.31.101.1
   set end-ip 10.31.101.255
   end
   ```

   The source address for a web-proxy firewall policy cannot be assigned to a FortiGate unit interface.

4. Use the following command to add a firewall policy that allows all users on the 10.31.101.0 subnet to use the explicit web proxy for connections through the wan1 interface to the Internet.

   ```
   config firewall policy
   edit 2
   set srcintf web-proxy
   set dstintf wan1
   set scraddr Internal_subnet
   set dstaddr all
   set action accept
   set identity-based enable
   set schedule always
   config identity-based-policy
   edit 1
   set groups Internal_users
   set utm-status enable
   set profile-protocol-options default
   set av-profile Scan
   set logtraffic enable
   set schedule always
   set service ANY
   end
   ```
The firewall address selected as the source address cannot be assigned to a FortiGate unit interface. Either the field must be blank or it must be set to Any.

5 Use the following command to change global web proxy settings, for example to set the maximum request length for the explicit web proxy to 10:

```
config web-proxy global
    set max-request-length 10
end
```

Proxy auto-config (PAC) configuration

A proxy auto-config (PAC) file defines how web browsers can choose a proxy server for receiving HTTP content. PAC files include the FindProxyForURL(url, host) JavaScript function that returns a string with one or more access method specifications. These specifications cause the web browser to use a particular proxy server or to connect directly.

To configure PAC for explicit web proxy users, you can use the port that PAC traffic from client web browsers use to connect to the explicit proxy. Explicit proxy users must configure their web browser’s PAC proxy settings to use the PAC port.

**PAC File Content**

You can edit the default PAC file from the web-based manager or use the following command to upload a custom PAC file:

```
config web-proxy explicit
    set pac-file-server-status enable
    set pac-file data <pac_file_str>
end
```

Where `<pac_file_str>` is the contents of the PAC file. Enter the contents of the PAC file. Enclose the PAC file text in quotes. You can copy the contents of a PAC text file and paste the contents into the CLI using this option. Enter the command followed by two sets of quotes then place the cursor between the quotes and paste the file content.

The maximum PAC file size is 8192 bytes. You can use any PAC file syntax that is supported by your users’s browsers. The FortiGate unit does not parse the PAC file.

To use PAC, users must add an automatic proxy configuration URL (or PAC URL) to their web browser proxy configuration. The default PAC file URL is:

```
http://<interface_ip>:<PAC_port_int>/<pac_file_str>
```

For example, if the interface with the explicit web proxy has IP address 172.20.120.122, the PAC port is the same as the default HTTP explicit proxy port (8080) and the PAC file name is `proxy.pac` the PAC file URL would be:

```
http://172.20.120.122:8080/proxy.pac
```

From the CLI you can use the following command to display the PAC file url:

```
get web-proxy explicit
```

**Unknown HTTP version**

You can select the action to take when the proxy server must handle an unknown HTTP version request or message. Set unknown HTTP version to Reject or Best Effort. Best Effort attempts to handle the HTTP traffic as best as it can. Reject treats known HTTP traffic as malformed and drops it. The Reject option is more secure.
Authentication realm

You can enter an authentication realm to identify the explicit web proxy. The realm can be any text string of up to 63 characters. If the realm includes spaces enclose it in quotes. When a user authenticates with the explicit proxy the HTTP authentication dialog includes the realm so you can use the realm to identify the explicitly web proxy for your users.

Global explicit web proxy options

Proxy FQDN
Enter the fully qualified domain name (FQDN) for the proxy server. This is the domain name to enter into browsers to access the proxy server.

Max HTTP request length
Enter the maximum length of an HTTP request. Larger requests will be rejected.

Max HTTP message length
Enter the maximum length of an HTTP message. Larger messages will be rejected.

Add headers to Forwarded Requests
The web proxy server will forward HTTP requests to the internal network. You can include the following headers in those requests:

Client IP Header
Enable to include the Client IP Header from the original HTTP request.

Via Header
Enable to include the Via Header from the original HTTP request.

X-forwarded-for Header
Enable to include the X-Forwarded-For (XFF) HTTP header. The XFF HTTP header identifies the originating IP address of a web client or browser that is connecting through an HTTP proxy, and the remote addresses it passed through to this point.

Front-end HTTPS Header
Enable to include the Front-end HTTP Header from the original HTTPS request.

Explicit web proxy authentication

You can add identity-based policies to apply authentication to explicit web proxy sessions. You can use authentication to control access to the explicit proxy. You can also use identity-based policies to identify users and apply different UTM features to different users.

Authentication of web proxy sessions uses HTTP basic and digest authentication as described in RFC 2617 (HTTP Authentication: Basic and Digest Access Authentication) and prompts the user for credentials from the browser allowing individual users to be identified by their web browser instead of IP address. HTTP authentication allows the FortiGate unit to identify multiple users accessing services from a shared IP address. You can also select IP-based authentication to authenticate users according to their source IP address.

IP-Based authentication

IP-based authentication applies authentication by source IP address. Once a user authenticates, all sessions to the explicit web proxy from that IP address are assumed to be from that user and are accepted until the authentication timeout ends or the session times out.

This method of authentication is similar to standard (non-web proxy) firewall authentication and may not produce the desired results if multiple users share IP addresses (such as in a network that uses virtualization solutions or includes a NAT device between the users and the explicit web proxy).
To configure IP-based authentication, add a firewall policy for the explicit web proxy, set the source interface/zone to web-proxy, select Enable Identify Based Policy, and make sure IP Based is selected before adding identity-based policies. You can also set the authentication method to basic, digest, NTLM or FSAE.

Use the following CLI command to add IP-based authentication to a firewall policy. IP-based authentication is selected by setting `ip-based` to `enable`.

```
config firewall policy
edit 3
  set srcintf web-proxy
  set dstintf port1
  set scraddr User_network
  set dstaddr all
  set action accept
  set identity-based enable
  set ip-based enable
  config identity-based-policy
    edit 1
      set groups Internal_users
      set service ANY
      set schedule always
  end
end
```

**Per session authentication**

If you don’t select *IP Based* the FortiGate unit applies HTTP authentication per session. This authentication is browser-based (see Figure 31 on page 132). When a client enters a user name and password in their browser to authenticate with the explicit web proxy, this information is stored by the browser. Each new session started by the same web browser also has to be authenticated but the browser does this automatically. If the user starts another browser on the same PC or closes and then re-opens their browser they have to authenticate again.

Since the authentication is browser-based, multiple clients with the same IP address can authenticate with the proxy using their own credentials. HTTP authentication provides authentication for multiple user sessions from the same source IP address. This can happen if there is a NAT device between the users and the FortiGate unit. HTTP authentication also supports authentication for other configurations that share one IP address among multiple users. These includes Citrix products and Windows Terminal Server and other similar virtualization solutions.

To configure per session authentication, add a firewall policy for the explicit proxy, set the source interface/zone to web-proxy, select Enable Identify Based Policy, and make sure IP Based is not selected before adding identity-based policies. You can also set the authentication method to basic, digest, NTLM or FSAE.

Use the following CLI command to add per session authentication to a firewall policy. Per session authentication is selected by setting `ip-based` to `disable`.

```
config firewall policy
edit 5
  set srcintf web-proxy
  set dstintf port1
  set scraddr User_network
  set dstaddr all
  set action accept
  set identity-based enable
```
set ip-based disable
config identity-based-policy
edit 1
   set groups Internal_users
   set service ANY
   set schedule always
end
end

Figure 31: Per session HTTP authentication

UTM features and the explicit web proxy

You can apply protocol options, antivirus, web filtering, FortiGuard Web Filtering and data leak prevention (DLP) including DLP archiving to explicit web proxy sessions. UTM features are applied by selecting them in a web proxy firewall policy or an identity based policy in a web proxy firewall policy. You cannot apply intrusion protection (IPS), email filtering, application control, or VoIP UTM features to explicit web proxy sessions.

To apply intrusion protection to explicit web proxy traffic you can add DoS policies to the FortiGate interfaces that receive and send explicit proxy traffic. However, you cannot apply application control to explicit web proxy traffic, so you cannot filter explicit web proxy traffic by application and explicit proxy traffic does not contribute to application control monitoring or reporting.
Explicit proxy sessions and protocol options

Since the traffic accepted by the explicit web proxy is known to be either HTTP, HTTPS, or FTP over HTTP and since the ports are already known by the proxy, the explicit proxy does not use the HTTP or HTTPS port protocol options settings.

When adding UTM features to a web proxy firewall policy, you must select a protocol options profile. In most cases you can select the default protocol options profile. You could also create a custom protocol options profile.

The explicit web proxy supports the following protocol options:

- Enable chunked bypass
- HTTP oversized file action and threshold

The explicit web proxy does not support the following protocol options:

- Client comforting
- Server comforting
- Monitor content information from dashboard. URLs visited by explicit users are not added to dashboard usage and log and archive statistics widgets.

Explicit proxy sessions web filtering and FortiGuard web filtering

For explicit proxy sessions, the FortiGate unit applies web filtering to an HTTP request when it receives the headers of the request. If web filtering allows the HTTP request, it is forwarded to the web server. If web filtering blocks the HTTP request is, the request is dropped and a blocking HTTP response is generated by the FortiGate unit and returned to the client web browser.

The explicit web proxy completely supports the following web filter options and their configuration settings. For example, all web filter content filtering and URL filtering actions and types are supported:

- Web content filtering
- Web URL filtering
- Advanced filtering
- FortiGuard Web Filtering to allow, block, and log web pages according to FortiGuard categories and classifications
- FortiGuard local categories
- FortiGuard web filtering reports
- Block invalid URLs
- HTTP POST Action
- Provide details for HTTP 4xx and 5xx errors
- Allow websites when a rating error occurs
- Strict blocking
- Rate URLs by domain and IP address
- Block HTTP redirects by rating

The explicit web proxy does not support:

- Safe search
- FortiGuard Web Filtering overrides
- FortiGuard Web Filtering quotas
- Web resume download block
**Example: users on an internal network browsing the Internet through the explicit proxy with web caching, RADIUS authentication, web filtering and virus scanning**

This example describes how to configure the explicit proxy for the example network shown in Figure 32. In this example, users on the internal network connect to the explicit proxy through the Internal interface of the FortiGate-51B unit. The explicit web proxy is configured to use port 8888 so users must configure their web browser proxy settings to use port 8888 and IP address 10.31.101.100.

**Figure 32: Example explicit web proxy network topology**

- Daily log of remaining quota

Also the web page displayed when FortiGuard Web Filtering blocks a web page through the explicit proxy may be different than the page displayed through a normal firewall session.

**Explicit proxy sessions and antivirus**

For explicit proxy sessions, the FortiGate unit applies antivirus scanning to HTTP POST requests and HTTP responses. The FortiGate unit starts virus scanning a file in an HTML session when it receives a file in the body of an HTML request. The explicit proxy can receive HTTP responses from either the originating web server or the FortiGate web cache module.

Flow-based virus scanning is not available for explicit web proxy sessions. Even if the FortiGate unit is configured to use flow-based antivirus, explicit web proxy sessions use the regular virus database.
In this example, explicit web proxy users must authenticate with a RADIUS server before getting access to the proxy. To apply authentication, the firewall policy that accepts explicit web proxy traffic includes an identity based policy that applies per session authenticating to explicit proxy users and includes a user group with the RADIUS server in it. The identity based policy also applies UTM web filtering and virus scanning.

**General configuration steps**

This section breaks down the configuration for this example into smaller procedures. For best results, follow the procedures in the order given:

1. Enable the explicit proxy on one or more interfaces.
2. Enable the explicit proxy for HTTP and HTTPS and change the HTTP and HTTPS ports to 8888.
3. Enable web caching for the explicit proxy.
4. Add a RADIUS server and user group for the explicit proxy.
5. Add web filtering and antivirus profiles for the explicit proxy.
6. Add a firewall policy for the explicit proxy.

**Configuring the explicit web proxy - web-based manager**

Use the following steps to configure the explicit web proxy from FortiGate web-based manager.

**To enable the explicit web proxy on the Internal interface - web-based manager**

1. Go to **System > Network > Interface**.
2. Edit the internal interface.
3. Select **Enable Explicit Web Proxy**.
4. Select **OK**.

**To enable and configure the explicit web proxy - web-based manager**

1. Go to **System > Network > Web Proxy** and change the following settings:
   - **Enable Explicit Web Proxy**: Select HTTP/HTTPS.
   - **Listen on Interfaces**: Should show internal to indicate that the explicit web proxy is enabled on the internal interface.
   - **HTTP Port**: 8888
   - **HTTPS Port**: 8888
   - **Realm**: You are authenticating with the explicit web proxy.
   - **Default Firewall Policy Action**: Deny
2. Select **Apply**.

**To enable web caching for the explicit web proxy - web-based manager**

1. Go to **WAN Opt. & Cache > Cache > Settings**.
2. Select **Enable Cache Explicit Proxy**.
3. Select **Apply**.
To add a RADIUS server and user group for the explicit proxy - web-based manager

1. Go to User > Remote > Radius.
2. Select Create New to add a new RADIUS server:
   - Name: RADIUS_1
   - Primary Server Name/IP: 10.31.101.200
   - Primary Server Secret: RADIUS_server_secret
   - Name: Explicit_proxy_user_group
   - Type: Firewall
   - Members: RADIUS_1
4. Select OK.

To add web filtering and antivirus profiles for the explicit proxy - web-based manager

1. Go to UTM > Web Filter > Profile and select Create New.
2. Configure a web filter profile name Explicit_proxy_wf_profile with the required options.
   For example, you could configure FortiGuard web filtering.
3. Go to UTM > AntiVirus > Profile and select Create New.
4. Configure an antivirus profile named Scan with the required options.
   For example, you should select virus scanning for HTTP.

To add a firewall policy for the explicit proxy - web-based manager

1. Go to Firewall > Address > Address and select Create New.
2. Add a firewall address for the internal network:
   - Address Name: Internal_subnet
   - Type: Subnet / IP Range
   - Subnet / IP Range: 10.31.101.[1-255]
3. Go to Firewall > Policy > Policy and select Create New.
4. Configure the explicit web proxy firewall policy.
   - Source Interface/Zone: web-proxy
   - Source Address: Internal_subnet
   - Destination Interface/Zone: wan1
   - Destination Address: all
   - Action: ACCEPT
5. Select Enable Identity Based Policy, make sure IP Based is not selected and Auth Method is set to Basic.
6. Select Add and configure the following settings for the identity based policy:
   - User Group: Explicit_policy
   - UTM: Select
   - Protocol Options: default
Configuring the explicit web proxy - CLI

Use the following steps to configure the example explicit web proxy configuration from the CLI.

To enable the explicit web proxy on the Internal interface - CLI
1 Enter the following command to enable the explicit web proxy on the internal interface.
   ```
   config system interface
   edit internal
   set explicit-web-proxy enable
   end
   ```

To enable and configure the explicit web proxy - CLI
1 Enter the following command to enable the explicit proxy and set the TCP port that proxy accepts HTTP and HTTPS connections on to 8888.
   ```
   config web-proxy explicit
   set status enable
   set http-incoming-port 8888
   set https-incoming-port 8888
   set realm "You are authenticating with the explicit web proxy"
   set sec-default-action deny
   end
   ```

To enable web caching for the explicit web proxy - CLI
1 Enter the following command to enable web caching for the explicit web proxy.
   ```
   config wanopt webcache
   set explicit enable
   end
   ```

To add a RADIUS server and user group for the explicit proxy - CLI
1 Enter the following command to add a RADIUS server:
   ```
   config user radius
   edit RADIUS_1
   set server 10.31.101.200
   set secret RADIUS_server_secret
   end
   ```
2 Enter the following command to add a user group for the RADIUS server.
   ```
   config user group
   edit Explicit_proxy_user_group
   set group-type firewall
   set member RADIUS_1
   end
   ```

To add web filtering and antivirus profiles for the explicit proxy - CLI
1 Enter the following command to add a web filter profile that enables HTTP URL filtering for the explicit web proxy.
config webfilter profile
  edit Explicit_wf_pro
  config http
    set options urlfilter
  end
  config web
    set urlfilter-table 1
  end
end

2 Enter the following command to add an antivirus profile:
config antivirus profile
  edit Explicit_av_pro
  config http
    set options scan
  end
end

To add a firewall policy for the explicit proxy - CLI
1 Enter the following command to add a firewall address for the internal subnet:
config firewall address
  edit Internal_subnet
  set type iprange
  set start-ip 10.31.101.1
  set end-ip 10.31.101.255
end

2 Enter the following command to add the explicit web proxy firewall policy:
config firewall policy
  edit 0
  set srcintf web-proxy
  set dstintf wan1
  set srcaddr Internal_subnet
  set dstaddr all
  set action accept
  set schedule always
  set identity-based enable
  set ipbased disable
  set auth-method basic
  config identity-based-policy
    edit 1
    set groups Explicit_Proxy_user_group
    set schedule always
    set utm-status enable
    set av-profile Explicit_av_pro
    set webfilter-profile Explicit_wf_pro
    set profile-protocol-options default
    set groups Explicit_proxy_user_group
  end
end

Testing and troubleshooting the configuration
You can use the following steps to verify that the explicit web proxy configuration is working as expected:
To test the explicit web proxy configuration

1. Configure a web browser on the internal subnet to use a proxy at IP address 10.31.101.100 and port 8888.
2. Browse to an Internet web page.
   The web browser should pop up an authentication window that includes the phrase that you added to the Realm option.
3. Enter the username and password for an account on the RADIUS server.
   If the account is valid you should be allowed to browse web pages on the Internet.
4. Close the browser and clear its cache and cookies.
5. Restart the browser and connect to the Internet.
   You could also start a second web browser on the same PC. Or you could start a new instance of the same browser as long as the browser asks for a user name and password again.
   You should have to authenticate again because identity-based policies are set to session-based authentication.
6. If this basic functionality does not work, check your FortiGate and web browser configuration settings.
7. Browse to a URL on the URL filter list and confirm that the web page is blocked.
   The antivirus configuration should block the file.
   Sessions for web-proxy firewall policies do not appear on the Top Sessions dashboard widget and the count column for firewall policies does not display a count for explicit web proxy firewall policies.
9. You can use the following command to display explicit web proxy sessions
   `get test wad 60`
   IP based users:

   Session based users:
   `user:0x9c20778, username:User1, vf_id:0, ref_cnt:9`

   Total allocated user:1
   Total user count:3, shared user quota:50, shared user count:3
   This command output shows one explicit web proxy user with user name User1 authenticated using session-based authentication.

Explicit web proxy sessions and user limits

Web browsers and web servers open and close multiple sessions with the explicit proxy. Some sessions open and close very quickly. HTTP 1.1 keepalive sessions are persistent and can remain open for long periods of time. Sessions can remain on the explicit web proxy session list after a user has stopped using the proxy (and has, for example, closed their browser). If an explicit web proxy session is idle for more than 3600 seconds it is torn down by the explicit web proxy. See RFC 2616 for information about HTTP keepalive/persistent HTTP sessions.
The FortiGate unit adds two sessions to its session table for every explicit web proxy session started by a web browser. An entry is added to the session table for the session from the web browser to the explicit web proxy. All of these sessions have the same destination port as the explicit web proxy port (usually 8080). An entry is also added to the session table for the session between the exiting FortiGate interface and the web server destination of the session. All of these sessions have a FortiGate interface IP address and the source address of the session and usually have a destination port of 80.

Web Proxy sessions that appear in the Top sessions dashboard widget do not include the Policy ID of the web-proxy firewall policy that accepted them. However, the web-proxy sessions appear in the Top Sessions dashboard widget with a destination port that matches the explicit web proxy port number (usually 8080). The proxied sessions from the FortiGate unit have their source address set to the IP address of the FortiGate unit interface that the sessions use to connect to their destinations (for example, for connections to the Internet the source address would be the IP address of the FortiGate interface connected to the Internet).

FortiOS limits the number of explicit web proxy users. The number of users varies by FortiGate model from as low as 10 to up to 18000 for high end models such as the FortiGate-3950B. You can use the following command to display the limit on the number of explicit web proxy users for a FortiGate unit:

```
get test wad 62
```

```
Total user count:3, shared user quota:50, shared user count:3
   vd=root max=0 guarantee=0 used=3
```

This command output shows that the explicit web proxy user limit (the shared user quota) for this FortiGate unit is 50 users.

You can not change this limit. If your FortiGate unit is configured for multiple VDOMs this limit must be shared by all VDOMs. You can also use VDOM resource limiting to limit the number of explicit web proxy users for the FortiGate unit and for each VDOM. To limit the number of explicit web proxy users for the FortiGate unit from the web-based manager enable multiple VDOMs and go to System > VDOM > Global Resources or use the following command:

```
config global
   config system resource-limits
      set webproxy 50
   end
end
```

To limit the number of explicit web proxy users for a VDOM, from the web-based manager enable multiple VDOMs and go to System > VDOM > VDOM and edit a VDOM or use the following command to change the number of explicit web proxy users for VDOM_1:

```
config global
   config system vdom-property
      edit VDOM_1
         set webproxy 25
      end
   end
```

The VDOM resource limit pages on the web-based manager also display the current number of explicit web proxy users. You can also use the `get test wad 60` CLI command to view the number of explicit web proxy users. For example:

```
get test wad 60
IP based users:
   user:0x9ab8350 username:User1, vf_id:0, ip_addr:10.31.101.10, ref_cnt:9
```
Session based users:
  user:0x9ac3c40, username:User2, vf_id:0, ref_cnt:3
  user:0x9ab94f0, username:User3, vf_id:0, ref_cnt:1

Total allocated user:3
Total user count:3, shared user quota:50, shared user count:3

Users may be displayed with this command even if they are no longer actively using the proxy. All idle sessions time out after 3600 seconds.

The command output shows three explicit web proxy users. The user named User1 has authenticated with a firewall policy that includes IP-based authentication and the user’s source IP address is 10.31.101.10. The users named User2 and User3 have authenticated with a firewall policy that includes session-based authentication.

You can use the following command to flush all current explicit web proxy users. This means delete information about all users and force them re-authenticate.

```
get test wad 61
```

**Note:** Users that authenticate with explicit web-proxy firewall policies do not appear in the User > Monitor > Firewall list and selecting De-authenticate All Users has no effect on explicit web proxy users.

How the number of concurrent explicit proxy users is determined depends on their authentication method:

- For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LDAP, FSAE, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user.

- For IP Based authentication, or no authentication, or if no web-proxy firewall policy has been added, 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.

The explicit web proxy does not limit the number of active sessions for each user. As a result the actual explicit web proxy session count is usually much higher than the number of explicit web proxy users. If an excessive number of explicit web proxy sessions is compromising system performance you can limit the amount of users if the FortiGate unit is operating with multiple VDOMs.
FortiGate WCCP

The Web Cache Communication Protocol (WCCP) is a content-routing technology that integrates cache engines into network infrastructure. FortiGate units support WCCPv1 and WCCPv2. This chapter describes how to configure FortiGate unit to operate as a WCCP router or WCCP client. As a WCCP router a FortiGate unit redirects HTTP traffic to WCCP cache engines (web caches). As a WCCP client you can add firewall policies to a FortiGate unit to filter WCCP sessions.

A FortiGate unit in NAT/Route or transparent mode can operate as a WCCP router. To operate as a WCCP client a FortiGate unit must be in NAT/Route mode. WCCP communication between routers and clients uses UDP port 2048. This communication can be a GRE tunnel or just use layer 2 forwarding.

**Note:** A WCCP router can also be called a WCCP server. A WCCP cache engine can also be called a WCCP client.

**How WCCP works**

The following sequence assumes you have configured a FortiGate unit to be a WCCP router and another FortiGate unit to be a WCCP client. In many networks a FortiGate unit will be filling one of the router or client roles and the other role would be filled by another device. For example, a third-party device could be the WCCP router and the FortiGate unit would be the WCCP client.

1. A client web browser sends a request for web content.
2. The FortiGate unit is configured as a WCCP router intercepts the request and forwards it to the FortiGate unit configured as a WCCP client.
   The communication between the router and the client is over a GRE tunnel using port 2048.
3. The FortiGate unit configured as a WCCP client intercepts the WCCP session and applies a firewall policy to the session. This firewall policy can apply FortiGate features such as UTM to the WCCP session.
4. The FortiGate unit configuration as a WCCP client forwards the request to its destination.
5. Replies to the session are returned to the FortiGate unit configured as a WCCP client.
6. The client caches the reply to a configured cache server and returns it to the WCCP router.
   This communication is also over the GRE tunnel.
7. The WCCP router returns the request to the client web browser.
   Subsequent requests for the same content may be served from the cache servers connected to the WCCP client instead of from the Internet.
   The client web browser is not aware that all this is taking place and does not have to be configured to use a web proxy.
The WCCP configuration requires HTTP traffic from client web browsers to be directed through the FortiGate unit operating as the WCCP router. You must enable WCCP on the FortiGate interface that receives the HTTP traffic.

Example: WCCP router and client configuration

This example describes how to configure the FortiGate units in Figure 33. One to operate as a WCCP router and the other to operate as a WCCP client. All WCCP settings are configured from the CLI.

WCCP router configuration

Use the following steps to configure the FortiGate unit as a WCCP router.

To configure a FortiGate unit as a WCCP router

1. Enable WCCP on the wan1 interface because this interface will handle WCCP traffic.
   ```
   config system interface
   edit wan1
   set wccp enable
   end
   ```

2. Add a WCCP service group that controls the communication between the router and the client:
   ```
   config system wccp
   edit 1
   set router-id 172.20.120.10
   ```
set server list 172.20.120.20
set authentication enable
set password Passw8rd
end

3 Add a firewall policy that accepts traffic from the LAN heading for the Internet and enables WCCP. The result is traffic accepted by this firewall policy is processed by the WCCP router.

config firewall policy
edit 1
set srcintf port2
set dstintf port1
set srcaddr all
set dstaddr all
set action accept
set schedule always
set service HTTP
set wccp enable
set nat enable
end

WCCP client configuration

Use the following steps to configure a FortiGate unit as a WCCP client.

To configure a FortiGate unit as a WCCP client

1 Enable WCCP on the port1 and port3 interfaces. The port1 interface accepts WCCP packets from the WCCP router and the port3 interface communicates with the cache servers using WCCP.

config system interface
edit port1
set wccp enable
next
edit port3
set wccp enable
end

2 Configure the FortiGate unit to operate as a WCCP client.

config system settings
set wccp-cache-engine enable
end

You cannot enter this command if you have already added a WCCP service group to the FortiGate configuration.

When you enter this command an interface named w.<vdom_name> is added to the FortiGate configuration (for example w.root). All traffic redirected from a WCCP router is considered to be received at this interface of the FortiGate unit operating as a WCCP client. A default route to this interface with lowest priority is added.

3 Add a WCCP service group that controls the communication between the router and the client.

config system wccp
edit 3
set router-list 172.20.120.10
set assignment-weight 100
set authentication enable
Configuring the forward and return methods and adding authentication

The WCCP forwarding method determines how intercepted traffic is transmitted from the WCCP router to the WCCP cache engine. There are two different forwarding methods:

- **GRE forwarding** (the default) encapsulates the intercepted packet in an IP GRE header with a source IP address of the WCCP router and a destination IP address of the target WCCP cache engine. The result is a tunnel that allows the WCCP router to be multiple hops away from the WCCP cache server.

- **L2 forwarding** rewrites the destination MAC address of the intercepted packet to match the MAC address of the target WCCP cache engine. L2 forwarding requires that the WCCP router is Layer 2 adjacent to the WCCP client.

You can use the following command on a FortiGate unit configured as a WCCP router to change the forward and return methods to L2:

```bash
config system wccp
edit 1
set forward-method L2
set return-method L2
end
```

You can also set the forward and return methods to any in order to match the cache server configuration.

By default the WCCP communication between the router and cache servers is unencrypted. If you are concerned about attackers sniffing the information in the WCCP stream you can use the following command to enable hash-based authentication of the WCCP traffic. You must enable authentication on the router and the cache engines and all must have the same password.

```bash
config system wccp
edit 1
set authentication enable
```
When the WCCP service is active on a web cache server it periodically sends a WCCP HERE I AM broadcast or unicast message to the FortiGate unit operating as a WCCP router. This message contains the following information:

- Web cache identity (the IP address of the web cache server).
- Service info (the service group to join).

If the information received in the previous message matches what is expected, the FortiGate unit replies with a WCCP I SEE YOU message that contains the following details:

- Router identity (the FortiGate unit’s IP address.
- Sent to IP (the web cache IP addresses to which the packets are addressed)

When both ends receive these two messages the connection is established, the service group is formed and the designated web cache is elected.

Troubleshooting WCCP

Two types of debug commands are available for debugging or troubleshooting a WCCP connection between a FortiGate unit operating as a WCCP router and its WCCP cache engines.

Real time debugging

The following commands can capture live WCCP messages:

```
diag debug en
 diag debug application wccpd <debug level>
```

Application debugging

The following commands display information about WCCP operations:

```
get test wccpd <integer>
diag test application wccpd <integer>
```

Where `<integer>` is a value between 1 and 5:

1. Display WCCP stats
2. Display WCCP config
3. Display WCCP cache servers
4. Display WCCP services
5. Display WCCP assignment

Enter the following command to view debugging output:

```
diag test application wccpd 3
```

Sample output from a successful WCCP connection:

```
service-0 in vdom-root: num=1, usable=1
cache server ID:
  len=44, addr=172.16.78.8, weight=4135, status=0
  rcv_id=6547, usable=1, fm=1, nq=0, dev=3(k3),
```

```
set password <password>
end
```
to=192.168.11.55
ch_no=0, num_router=1:
192.168.11.55

Sample output from the same command from an unsuccessful WCCP connection (because of a service group password mismatch):

```
service-0 in vdom-root: num=0, usable=0
diag debug application wccpd -1
Sample output:
wccp_on_recv()-98: vdom-root recv: num=160, dev=3(3), 172.16.78.8->192.168.11.55
wccp2_receive_pkt()-1124: len=160, type=10, ver=0200, length=152
wccp2_receive_pkt()-1150: found component:t=0, len=20
wccp2_receive_pkt()-1150: found component:t=1, len=24
wccp2_receive_pkt()-1150: found component:t=3, len=44
wccp2_receive_pkt()-1150: found component:t=5, len=20
wccp2_receive_pkt()-1150: found component:t=8, len=24
wccp2_check_security_info()-326: MD5 check failed
```
WAN optimization, web cache and WCCP get and diagnose commands

The following get and diagnose commands are available for troubleshooting WAN optimization, web cache, and WCCP.

- `get test {wa_cs | wa_dbd | wad | wad_diskd | wccpd} <test_level>`
- `diagnose wad`
- `diagnose wads`
- `diagnose wadbd`
- `diagnose debug application {wa_cs | wa_dbd | wad | wad_diskd | wccpd} [debug_level]`

**get test {wa_cs | wa_dbd | wad | wad_diskd | wccpd} <test_level>**

Display usage information about WAN optimization and web-cache-related applications. Use `<test_level>` to display different information.

- `get test wa_cs <test_level>`
- `get test wa_dbd <test_level>`
- `get test wad <test_level>`
- `get test wad_diskd <test_level>`
- `get test wccpd <test_level>`

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wad</td>
<td>Display information about the WAN optimization application.</td>
</tr>
<tr>
<td>wa_cs</td>
<td>Display information about the WAN optimization web cache server.</td>
</tr>
<tr>
<td>wa_dbd</td>
<td>Display information about the WAN optimization storage server application.</td>
</tr>
<tr>
<td>wad_diskd</td>
<td>Display information about the WAN optimization disk access daemon application.</td>
</tr>
<tr>
<td>wccp</td>
<td>Display information about the WCCP application.</td>
</tr>
</tbody>
</table>

**Examples**

Enter the following command to display WAN optimization tunnel protocol statistics. The http tunnel and tcp tunnel parts of the command output below shows that WAN optimization has been processing HTTP and TCP packets.

```plaintext
get test wad 11
wad tunnel protocol stats:
  http tunnel
    bytes_in=1751767 bytes_out=325468
  ftp tunnel
    bytes_in=0 bytes_out=0
  cifs tunnel
    bytes_in=0 bytes_out=0
  mapi tunnel
    bytes_in=0 bytes_out=0
```
Enter the following command to display the current WAN optimization peers. You can use this command to make sure all peers are configured correctly. The command output shows one peer with IP address 172.20.120.141, peer name Web_servers, with 10 active tunnels.

```
get test wad 26
peer name=Web_servers ip=172.20.120.141 vd=0 version=1
  tunnels (active/connecting/failover)=10/0/0
  sessions=0 n_retries=0 version_valid=true
```

Enter the following command to restart the WAN optimization web cache server.

```
get test wa_cs 99
```

Enter the following command to display all test options:

```
get test wad
```

**WAD Test Usage**

1: display total memory usage  
3: display proxy status  
4: display all stats and connections  
8: display all fix-sized advanced memory stats  
9: display all variable advanced memory stats  
10: toggle cifs read-ahead  
11: display tunnel protocol stats  
12: flush tunnel protocol stats  
13: display http protocol stats  
14: flush http protocol stats  
15: display cifs protocol stats  
16: flush cifs protocol stats  
17: display ftp protocol stats  
18: flush ftp protocol stats  
19: display mapi protocol stats  
20: flush mapi protocol stats  
21: display tcp protocol stats  
22: flush tcp protocol stats  
23: display all protocols stats  
24: flush all protocols stats  
25: display all listeners  
26: display all peers  
27: display DNS stats  
30: display Byte Cache DB state  
31: flush Byte Cache DB stats  
32: display Web Cache DB state  
33: flush Web Cache DB stats  
35: display tunnel compressor state  
36: flush tunnel compressor stats  
38: display rules  
40: display cache state  
41: flush cache stats  
42: display all fix-sized advanced memory stats in details  
43: display all variable advanced memory stats in details
WAN optimization, web cache and WCCP get and diagnose commands

45: display memory cache state
46: flush memory cache stats
47: display SSL stats
48: flush SSL stats
49: display SSL mem stats
50: display Web Cache stats
51: flush Web Cache stats
52: flush idle Web cache objects
53: display firewall policies
54: display WAD tunnel stats.
55: display WAD fsae state.
56yxxx: set xxx concurrent Web Cache session for object storage y.
57yxxxx: set xxxx(32K, 64K,...) unconfirmed write/read size per Web Cache object for object storage y.
58yxxxx: set xxxxx maximum output buffer size for object storage y.
59yxxx: set lookup lowmark(only if more to define busy status) to be xx for object storage y.
60: display current web proxy users
61: flush current web proxy users
62: display current web proxy user summary
63: display cache exemption patterns
66: toggle dumping URL when daemon crashes.
70yxxx: set xxx maximum output buffer size for byte storage y.
71yxxxx: set number of buffered add requests to be xxx for byte storage y.
72yxxxxx: set number of buffered query requests to be xxxx for byte storage y.
73yxxxxxx: set number of concurrent query requests to be xxxxx for byte storage y.
800..899: mem_check/cmem commands (800 for help & usage)
80000..89999: mem_check/cmem commands with 1 arg (800 for help & usage)
8000000..8999999: mem_check/cmem commands with 2 args (800 for help & usage)
90: set to test disk failure
91: unset to test disk failure
92: trigger a disk failure event
98: gracefully stopping wad proxy
99: restart proxy
diagnose wad

Display diagnostic information about the WAN optimization daemon (wad).

diagnose wad console-log {disable | enable}
diagnose wad filter {clear | dport | dst | list | negate | protocol | sport | src | vd}
diagnose wad history
diagnose wad session
diagnose wad stats {cache | cifs | clear | crypto | ftp | http | list | mapi | mem | summary | tcp | tunnel}
diagnose wad tunnel

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-log</td>
<td>Enable or disable displaying WAN optimization log messages on the CLI console.</td>
</tr>
<tr>
<td>filter</td>
<td>Set a filter for listing WAN optimization daemon sessions or tunnels. clear reset or clear the current log filter settings. dport enter the destination port range to filter by. dst enter the destination address range to filter by. list display the current log filter settings</td>
</tr>
<tr>
<td>history</td>
<td>Display statistics for one or more WAN optimization protocols for a specified period of time (the last 10 minutes, hour, day or 30 days).</td>
</tr>
<tr>
<td>session</td>
<td>Display diagnostics for WAN optimization sessions or clear active sessions.</td>
</tr>
<tr>
<td>stats</td>
<td>Display statistics for various parts of WAN optimization such as cache statistics, CIFS statistics, MAPI statistics, HTTP statistics, tunnel statistics etc. You can also clear WAN optimization statistics and display a summary.</td>
</tr>
<tr>
<td>tunnel</td>
<td>Display diagnostic information for one or all active WAN optimization tunnels. Clear all active tunnels. Clear all active tunnels.</td>
</tr>
</tbody>
</table>

Examples

Enter the following command to list all of the running WAN optimization tunnels and display information about each one. The command output shows 10 tunnels all created by peer-to-peer WAN optimization rules (auto-detect set to off).

```
diagnose wad tunnel list
```

```
Tunnel: id=100 type=manual
  vd=0 shared=no uses=0 state=3
  peer name=Web_servers id=100 ip=172.20.120.141
  SSL-secured-tunnel=no auth-grp=
  bytes_in=348 bytes_out=384

Tunnel: id=99 type=manual
  vd=0 shared=no uses=0 state=3
  peer name=Web_servers id=99 ip=172.20.120.141
  SSL-secured-tunnel=no auth-grp=
  bytes_in=348 bytes_out=384

Tunnel: id=98 type=manual
  vd=0 shared=no uses=0 state=3
  peer name=Web_servers id=98 ip=172.20.120.141
  SSL-secured-tunnel=no auth-grp=
  bytes_in=348 bytes_out=384
```
Tunnel: id=39 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=39 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1068 bytes_out=1104

Tunnel: id=7 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=7 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnel: id=8 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=8 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnel: id=5 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=5 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnel: id=4 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=4 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnel: id=1 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=1 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnel: id=2 type=manual
device=0 shared=no uses=0 state=3
peer name=Web_servers id=2 ip=172.20.120.141
SSL-secured-tunnel=no auth-grp=
bytes_in=1228 bytes_out=1264

Tunnels total=10 manual=10 auto=0
**diagnose wacs**

Display diagnostic information for the web cache database daemon (wacs).

- `diagnose wacs clear`
- `diagnose wacs recents`
- `diagnose wacs restart`
- `diagnose wacs stats`

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear</td>
<td>Remove all entries from the web cache database.</td>
</tr>
<tr>
<td>recents</td>
<td>Display recent web cache database activity.</td>
</tr>
<tr>
<td>restart</td>
<td>Restart the web cache daemon and reset statistics.</td>
</tr>
<tr>
<td>stats</td>
<td>Display web cache statistics.</td>
</tr>
</tbody>
</table>

**diagnose wadbd**

Display diagnostic information for the WAN optimization database daemon (wadbd).

- `diagnose wadbd {check | clear | recents | restart | stats}`

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>check</td>
<td>Check WAN optimization database integrity.</td>
</tr>
<tr>
<td>clear</td>
<td>Remove all entries from the WAN optimization database.</td>
</tr>
<tr>
<td>recents</td>
<td>Display recent WAN optimization database activity.</td>
</tr>
<tr>
<td>restart</td>
<td>Restart the WAN optimization daemon and reset statistics.</td>
</tr>
<tr>
<td>stats</td>
<td>Display WAN optimization statistics.</td>
</tr>
</tbody>
</table>

**diagnose debug application {wa_cs | wa_dbd | wad | wad_diskd | wccpd} [<debug_level>]**

View or set the debug level for displaying WAN optimization and web cache-related daemon debug messages. Include a `<debug_level>` to change the debug level. Leave the `<debug_level>` out to display the current debug level. Default debug level is 0.

- `diagnose debug application wa_cs [<debug_level>]`
- `diagnose debug application wa_dbd [<debug_level>]`
- `diagnose debug application wad [<debug_level>]`
- `diagnose debug application wccpd [<debug_level>]`

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>wa_cs</td>
<td>Set the debug level for the web cache server.</td>
</tr>
<tr>
<td>wa_dbd</td>
<td>Set the debug level for the WAN optimization database server.</td>
</tr>
<tr>
<td>wad</td>
<td>Set the debug level for the WAN optimization daemon.</td>
</tr>
<tr>
<td>wccpd</td>
<td>Set the debug level for the WCCP daemon.</td>
</tr>
</tbody>
</table>
Index

A
accept action
firewall policy, 35, 36
accept any peer, 39
active-passive
WAN optimization rules, 45
always revalidate, 90
antivirus
explicit web proxy, 132
application control
explicit web proxy, 132
authentication, 46
authentication method, 42
Citrix, 131
explicit web proxy, 130, 131
HTTP, 131
NAT device, 131
peer, 40
proxy, 131
WAN optimization peer authentication, 39
Windows Terminal Server, 131
authentication group
authentication method, 42
certificate, 42
password, 42
pre-shared key, 42

B
bandwidth
maximum, 47
byte cache, 21

C
cache
exempting from web caching, 76
cache engine
WCCP, 143
cache expired objects, 91
certificate
authentication group, 42
certification, 20
CIDR, 49
Citrix
authentication, 131
CLI syntax conventions, 16
client
WCCP, 143
comments, documentation, 20
configuring
WAN optimization peer, 41
conventions, 11

D
default
password, 10
default TTL
web cache, 90
DLP
explicit web proxy, 132
document conventions
CLI syntax, 16
documentation, 20
commenting on, 20
conventions, 11
Fortinet, 20

E
E Reload, 91
enable cache explicit proxy, 90
exempt
web cache, 76
expired objects
cache, 91
explicit mode
WAN optimization, 46, 51
explicit proxy
enable cache, 90
explicit web proxy, 125
antivirus, 132
application control, 132
authentication, 130, 131
DLP, 132
FortiGuard overrides, 133
FortiGuard quotas, 133
FortiGuard Web Filtering, 133
FortiGuard web filtering, 132
FTP, 125
HTTPS, 125
intrusion protection, 132
IPS, 132
PAC, 125
protocol options, 132
proxy auto-config, 125
SOCKS, 125
UTM, 127, 132
web filtering, 132

F
FAQ, 20
firewall
policy matching, 48

Cross-Site Scripting
protection from, 18
customer service, 20

customer service, 20

http://docs.fortinet.com/ • Feedback
firewall load balancing, 46
firewall policy, 30, 45
  accept action, 35, 36
  changing the position in the policy list, 49
deleting, 49
identity-based, 46
insert policy before, 47
matching, 48
maximum bandwidth, 47
moving, 49
traffic priority, 47
FortiClient peer, 31
FortiGate documentation
  commenting on, 20
FortiGuard
  Antispam, 10
  Antivirus, 10, 19
  services, 19
FortiGuard overrides
  explicit web proxy, 133
FortiGuard quotas
  explicit web proxy, 133
FortiGuard Web Filtering
  explicit web proxy, 133
FortiGuard web filtering
  explicit web proxy, 132
Fortinet
  Knowledge Center, 20
  Technical Documentation, 20
  Technical Documentation, conventions, 11
  Technical Support, 20
  Technical Support, registering with, 19
  Training Services, 20
Fortinet customer service, 20
Fortinet documentation, 20
Fortinet Knowledge Center, 20
fresh factor
  web cache, 90
FTP
  explicit web proxy, 125
G
glossary, 20
H
host ID
  peer, 30
how-to, 20
HTTP, 91
  authentication, 131
  unknown HTTP sessions, 53
HTTP 1.1 conditionals, 91
HTTP rule
  non-HTTP sessions, 52
HTTPS
  explicit web proxy, 125
I
identity-based firewall policies, 46
if-modified-since, 91
ignore
  web cache setting, 91
insert policy before
  firewall policy, 47
installation, 10
introduction
  Fortinet documentation, 20
intrusion protection
  explicit web proxy, 132
IP address
  peer, 30
  private network, 12
IPS
  explicit web proxy, 132
K
Knowledge Center, 20
L
load balancing, 46
M
matching
  firewall policy, 48
max cache object size
  web cache, 90
max TTL
  web cache, 90
maximum bandwidth, 47
firewall policy, 47
traffic shaping, 47
min TTL
  web cache, 90
mode
  operation, 10
monitoring
  WAN optimization, 34
moving a firewall policy, 49
N
NAT, 46
NAT device
  authentication, 131
NAT/Route mode, 31
negative response duration
  web cache, 90
non-HTTP sessions
  HTTP rule, 52
O
operation mode, 10
out of path
  topology, 22
overrides
  explicit web proxy, 133
P
PAC
explicit web proxy, 125
password
administrator, 10
authentication group, 42
peer
accept any peer, 39
host ID, 30
IP address, 30
WAN optimization, 39
peer authentication, 40
WAN optimization, 39
peer-to-peer
WAN optimization rules, 45
policy
accept action, 35, 36
changing the position in the policy list, 49
deleting, 49
firewall, 30
insert policy before, 47
matching, 48
maximum bandwidth, 47
move, 49
traffic priority, 47
pragma-no-cache, 91
pre-shared key
authentication group, 42
product registration, 19
protocol optimization, 21
protocol options
explicit web proxy, 132
proxy
antivirus, 132
DLP, 132
explicit web proxy authentication, 131
FortiGuard web filtering, 132
protocol options, 132
web filtering, 132
proxy auto-config
explicit web proxy, 125
Q
quota
explicit web proxy, 133
R
registering
with Fortinet Technical Support, 19
revalidated pragma-no-cache, 91
reverse proxy
web cache, 25, 119
RFC
1918, 12
router
WCCP, 143
routing
configuring, 125
rule, 45
active-passive, 45
non-HTTP sessions, 52
peer-to-peer, 45
unknown HTTP sessions, 53
WAN optimization, 45
S
secure tunnelling, 21
server
WCCP, 143
sharing
WAN optimization tunnels, 32
SOCKS
explicit web proxy, 125
SSL offloading, 21
T
TCP port
WAN optimization tunnels, 31
technical
documentation, 20
documentation conventions, 11
notes, 20
support, 20
technical support, 20
topology
out of path, 22
Traffic Priority, 47
traffic priority
firewall policy, 47
traffic shaping, 47
traffic shaping, 46
maximum bandwidth, 47
traffic priority, 47
Training Services, 20
Transparent mode, 31
tunnel
sharing WAN optimization tunnels, 32
TCP port, 31
WAN optimization, 31
tunnel request, 40
tunnel-non-http, 52
U
unknown HTTP sessions, 53
UTM, 45
explicit web proxy, 127, 132
web proxy, 127
V
VDOMs, 31
virtual domains, 31
virtual IP
WAN optimization, 46
virus
explicit web proxy, 132
vulnerability
Cross-Site Scripting, 18
XSS, 18

W
WAN optimization
and virtual IPs, 46
explicit mode, 51
FortiGate models supported, 10
monitoring, 34
peer authentication, 39
peers, 39
transparent mode, 51
WAN optimization peer
configuring, 41
WCCP, 143
cache engine, 143
client, 143
router, 143
server, 143
topology, 28
web cache, 21, 90
active-passive WAN optimization, 81
adding to passive WAN optimization rule, 81
always revalidate, 90
client/server WAN optimization, 81
default TTL, 90
exempt, 76
fresh factor, 90
max cache object size, 90
maximum TTL, 90
minimum TTL, 90
negative response duration, 90
non-standard ports, 79
peer to peer WAN optimization, 86
reverse proxy, 25, 119
Web Cache Communication Protocol
See WCCP, 143
web filtering
explicit web proxy, 132
explicit web proxy and FortiGuard web filtering, 133
web proxy, 125
antivirus, 132
authentication, 130, 131
DLP, 132
FortiGuard Web Filtering, 133
FortiGuard web filtering, 132
protocol options, 132
UTM, 127
web filtering, 132
Windows Terminal Server
authentication, 131
X
X-Forwarded-For (XFF), 130
XSS vulnerability
protection from, 18