Traffic Shaping

FortiOS™ Handbook v2
for FortiOS 4.0 MR2
Contents

Introduction 7
Before you begin ............................................ 7
How this guide is organized ................................. 7
Document conventions ................................. 9
   IP addresses ........................................... 9
Example Network configuration .......................... 10
Cautions, Notes and Tips .................................. 12
Typographical conventions .............................. 12
CLI command syntax conventions ....................... 12
Entering FortiOS configuration data ..................... 14
   Entering text strings (names) ......................... 14
   Entering numeric values ............................. 15
   Selecting options from a list ....................... 15
   Enabling or disabling options ...................... 15
Registering your Fortinet product ....................... 15
Fortinet products End User License Agreement ........ 16
Training ............................................. 16
Documentation ........................................ 16
   Fortinet Tools and Documentation CD .............. 16
   Fortinet Knowledge Base ........................... 16
   Comments on Fortinet technical documentation .... 16
Customer service and technical support ................. 16

The purpose of traffic shaping 19
Quality of Service .................................... 19
Traffic policing ...................................... 20
Bandwidth guarantee, limit, and priority interactions . 21
   FortiGate traffic .................................... 22
   Through traffic ..................................... 22
      Calculation and regulation of packet rates ....... 24
Important considerations ................................ 26

Traffic shaping methods 29
Traffic shaping options .................................. 29
## Contents

- Shared policy shaping .................................................. 29
  - Per policy .............................................................. 30
  - All policies ........................................................... 30
  - Maximum and guaranteed bandwidth .............................. 30
  - Traffic priority ....................................................... 30
  - VLAN, VDOM and virtual interfaces ............................ 31
    - Example .............................................................. 31
  - Per-IP shaping .......................................................... 31
    - Example .............................................................. 31
  - Application control shaping ..................................... 32
    - Example .............................................................. 32
  - Shaping order of operations ..................................... 33
  - Enabling in the firewall policy ................................ 33
    - Reverse direction traffic shaping ............................ 34
    - Application control shaper ................................... 34
  - Type of Service priority ......................................... 34
    - Example .............................................................. 35
  - TOS in FortiOS ......................................................... 35
- Differentiated Services ................................................. 35
  - DSCP examples ........................................................ 37
    - Example .............................................................. 37
    - Example .............................................................. 38
    - Example .............................................................. 38
    - Example .............................................................. 39
  - Tos and DSCP mapping ............................................ 40

### Examples

- QoS using priority from firewall policies ....................... 43
  - Sample configuration ............................................... 44
- QoS using priority from ToS or differentiated services ....... 45
  - Sample configuration ............................................... 46
- Example setup for VoIP .................................................. 46
  - Creating the traffic shapers ....................................... 47
    - VoIP shaper .......................................................... 47
    - FTP shaper ........................................................... 47
    - Regular traffic shaper ........................................... 48
  - Creating firewall policies ......................................... 48

### Troubleshooting

- Interface diagnosis ..................................................... 51
Contents

Shaper diagnose commands .......................................................... 51  
TOS command ................................................................................. 51  
Shared shaper ............................................................................... 52  
Per-IP shaper ................................................................................. 52  
Packet loss with statistics on shapers ........................................... 53  
Packet lost with the debug flow .................................................... 53  
Session list details with dual traffic shaper ................................... 53  
Additional Information .................................................................. 54  

Index .............................................................................................. 55
Introduction

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

The firewall policies are the key component of FortiOS that allows, or disallows, traffic to and from your network. It is through the firewall policies you define who, what and when traffic goes between networks and the Internet.

This guide describes the firewall functionality of FortiOS on all FortiGate units. It includes the purpose of the firewall, how traffic moves through the FortiGate unit, the components involved in the firewall and its policies.

This guide also describes both simple how to steps to configure the basics, and some more involved examples to demonstrate how firewall policies can be employed within FortiOS. Finally, this guide also provides some troubleshooting advice should problems arise when creating firewall policies.

Because of the magnitude of features, this guide will only touch the surface of traffic shaping, Universal Threat Management (UTM) and protection profile information. Other guides are available with more in depth content.

This chapter contains the following topics:

• Before you begin
• Document conventions
• Registering your Fortinet product
• Fortinet products End User License Agreement
• Training
• Documentation
• Customer service and technical support

Before you begin

Before you begin ensure that:

• You have administrative access to the web-based manager and/or CLI.
• The FortiGate unit is integrated into your network.
• 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.

How this guide is organized

FortiGate units can implement Quality of Service (QoS) by applying bandwidth limits and prioritization. Using traffic shaping, you can adjust how your FortiGate unit allocates resources to different traffic types to improve the performance and stability of latency sensitive or bandwidth intensive network applications.
This document discusses Quality of Service (QoS) and traffic shaping, describes FortiGate traffic shaping algorithms, and provides procedures and tips on how to configure traffic shaping on FortiGate units.

This guide contains the following chapters:

- **The purpose of traffic shaping** - describes traffic shaping theories and quality of service.
- **Traffic shaping methods** - describes the different methods of applying traffic shaping within FortiOS, and how to use TOS and Differentiated Services.
- **Examples** - provides some basic examples for the application of shapers.
- **Troubleshooting** - provides diagnose commands to use to troubleshoot traffic shapers to see if they are working correctly.
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 1: 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>
<thead>
<tr>
<th>Convention</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Button, menu, text box, field, or check box label</td>
<td>From <em>Minimum log level</em>, select <em>Notification</em>.</td>
</tr>
<tr>
<td>CLI input</td>
<td><code>config system dns</code></td>
</tr>
<tr>
<td></td>
<td><code>set primary &lt;address_ipv4&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>end</code></td>
</tr>
<tr>
<td>CLI output</td>
<td><code>FGT-602803030703 # get system settings</code></td>
</tr>
<tr>
<td></td>
<td><code>comments</code> : (null)</td>
</tr>
<tr>
<td></td>
<td><code>opmode</code> : nat</td>
</tr>
<tr>
<td>Emphasis</td>
<td>HTTP connections are <strong>not</strong> secure and can be intercepted by a third party.</td>
</tr>
<tr>
<td>File content</td>
<td><code>&lt;HTML&gt;&lt;HEAD&gt;&lt;TITLE&gt;Firewall Authentication&lt;/TITLE&gt;&lt;/HEAD&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>&lt;BODY&gt;&lt;H4&gt;You must authenticate to use this service.&lt;/H4&gt;</code></td>
</tr>
<tr>
<td>Hyperlink</td>
<td>Visit the Fortinet Technical Support web site, <a href="https://support.fortinet.com">https://support.fortinet.com</a>.</td>
</tr>
<tr>
<td>Keyboard entry</td>
<td>Type a name for the remote VPN peer or client, such as <code>Central_Office_1</code>.</td>
</tr>
<tr>
<td>Navigation</td>
<td>Go to <code>VPN &gt; IPSEC &gt; Auto Key (IKE)</code></td>
</tr>
<tr>
<td>Publication</td>
<td>For details, see the <em>FortiOS Handbook</em>.</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 3: Command syntax notation

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Square brackets [ ]** | A non-required word or series of words. For example:  
  
  `[verbose {1 | 2 | 3}]`  
  indicates that you may either omit or type both the `verbose` word and its accompanying option, such as:  
  `verbose 3`  |
| **Angle brackets < >** | 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:  
  `<retries_int>`  
  indicates that you should enter a number of retries, such as 5.  
  Data types include:  
  • `<xxx_name>`: A name referring to another part of the configuration, such as `policyA`.  
  • `<xxx_index>`: An index number referring to another part of the configuration, such as 0 for the first static route.  
  • `<xxx_pattern>`: 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`.  
  • `<xxx_fqdn>`: A fully qualified domain name (FQDN), such as `mail.example.com`.  
  • `<xxx_email>`: An email address, such as `admin@mail.example.com`.  
  • `<xxx_url>`: A uniform resource locator (URL) and its associated protocol and host name prefix, which together form a uniform resource identifier (URI), such as `http://www.fortinet.com/`.  
  • `<xxx_ipv4>`: An IPv4 address, such as `192.168.1.99`.  
  • `<xxx_v4mask>`: A dotted decimal IPv4 netmask, such as `255.255.255.0`.  
  • `<xxx_ipv4mask>`: A dotted decimal IPv4 address and netmask separated by a space, such as `192.168.1.99 255.255.255.0`.  
  • `<xxx_ipv4/mask>`: A dotted decimal IPv4 address and CIDR-notation netmask separated by a slash, such as `192.168.1.99/24`.  
  • `<xxx_ipv6>`: A colon(:)-delimited hexadecimal IPv6 address, such as `3f2e:6a8b:78a3:0d82:1725:6a2f:0370:6234`.  
  • `<xxx_v6mask>`: An IPv6 netmask, such as `/96`.  
  • `<xxx_ipv6mask>`: An IPv6 address and netmask separated by a space.  
  • `<xxx_str>`: 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.  
  • `<xxx_int>`: An integer number that is not another data type, such as 15 for the number of minutes. |
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)
- > (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.

<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. <strong>Note:</strong> 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. 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>
config firewall address
  tree
  -- [address] --*name (64)
    |- subnet
    |- type
    |- start-ip
    |- end-ip
    |- fqdn (256)
    |- cache-ttl (0,86400)
    |- wildcard
    |- comment (64 xss)
    |- associated-interface (16)
    ++ color (0,32)

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.
The purpose of traffic shaping

Traffic shaping, or traffic management, once included in a firewall policy, controls the bandwidth available and sets the priority of traffic processed by the policy to control the volume of traffic for a specific period (bandwidth throttling) or rate the traffic is sent (rate limiting).

Traffic shaping attempts to normalize traffic peaks and bursts to prioritize certain flows over others. But there is a physical limitation to the amount of data which can be buffered and to the length of time. Once these thresholds have been surpassed, frames and packets will be dropped, and sessions will be affected in other ways. For example, incorrect traffic shaping configurations may actually further degrade certain network flows, since the excessive discarding of packets can create additional overhead at the upper layers that may be attempting to recover from these errors.

A basic traffic shaping approach is to prioritize certain traffic flows over other traffic whose potential discarding is less advantageous. This would mean that you accept sacrificing certain performance and stability on low-priority traffic, to increase or guarantee performance and stability to high-priority traffic.

If, for example, you are applying bandwidth limitations to certain flows, you must accept the fact that these sessions can be limited and therefore negatively impacted.

Note that traffic shaping is effective for normal IP traffic at normal traffic rates. Traffic shaping is not effective during periods when traffic exceeds the capacity of the FortiGate unit. Because packets must be received by the FortiGate unit before they are subject to traffic shaping, if the FortiGate unit cannot process all of the traffic it receives, then dropped packets, delays, and latency are likely to occur.

To ensure that traffic shaping is working at its best, make sure that the interface ethernet statistics show no errors, collisions or buffer overruns.

Accelerated interfaces (NP2, NP4, CE) affect traffic shaping. For more information, see the Hardware Acceleration Guide.

This chapter contains the following sections:

- Quality of Service
- Traffic policing
- Bandwidth guarantee, limit, and priority interactions
- Important considerations

Quality of Service

Quality of service (QoS) is the capability of the network to adjust some quality aspects for selected flows within your overall network traffic, and may include such techniques as priority-based queueing and traffic policing. Because bandwidth is finite and because some types of traffic are slow, jitter or packet loss sensitive, bandwidth intensive, or operation critical, QoS can be a useful tool for optimizing the performance of the various applications on your network.

Before implementing QoS, organizations should first identify the types of traffic that are important to the organization, the types of traffic that use high amounts of bandwidth, and the types of traffic that are sensitive to latency or packet loss.
For example, a company might want to guarantee sufficient bandwidth for revenue producing e-commerce traffic. They need to ensure that transactions can be completed and that clients do not experience service delays and interruptions. At the same time, the company may need to ensure low latency for voice over IP (VoIP) traffic used by sales and customer support, while traffic latency and bursts may be less critical to the success of other network applications such as long term, resumable file transfers. Many organizations discover that QoS is especially important for managing their voice and streaming multi-media traffic. These types of traffic can rapidly consume bandwidth and are sensitive to latency.

Discovering the needs and relative importance of each traffic type on your network will help you to design an appropriate overall approach, including how you will configure each available QoS component technique. Some organizations discover that they only need configure bandwidth limits for some services. Other organizations determine that they need to fully configure interface and firewall policy bandwidth limits for all services, and prioritize queuing of critical services relative to traffic rate.

You can implement QoS on FortiGate units for services including H.323, TCP, UDP, ICMP, and ESP, using the following techniques:

**Traffic policing**
- Drops packets that do not conform to bandwidth limitations.

**Traffic shaping**
- Helps to ensure that the traffic may consume bandwidth at least at the guaranteed rate by assigning a greater priority queue if the guarantee is not being met. Also ensures that the traffic cannot consume bandwidth greater than the maximum at any given instant in time. Flows greater than the maximum rate are subject to traffic policing.

**Queuing**
- Transmits packets in order of their assigned priority queue for that physical interface. All traffic in a higher priority traffic queue must be completely transmitted before traffic in lower priority queues will be transmitted.

When deciding how to configure QoS techniques, it can be helpful to know when FortiGate units employ each technique in the overall traffic processing flow, and the considerations that arise from those mechanisms.

### Traffic policing

As traffic arrives (ingress) and departs (egress) on an interface, the FortiGate unit begins to process the traffic. In later phases of the network processing, such as enforcing maximum bandwidth use on sessions handled by a firewall policy, if the current rate for the destination interface or traffic regulated by that firewall policy is too high, the FortiGate unit may be required to drop the packet. As a result, time spent on prior processing, such as web filtering, decryption or IPS, can be wasted on some packets that are not ultimately forwarded. This also applies to VLAN interfaces as well as physical interfaces.

You can prevent this wasted effort on ingress by configuring the FortiGate unit to preemptively drop excess packets when they are received at the source interface, before most other traffic processing is performed:

```plaintext
config system interface
  edit <interface_name>
    set inbandwidth <rate_int>
  next
end
```

where `<rate_int>` is the bandwidth limit in KB/s. Excess packets will be dropped. If inbandwidth is 0, the rate is not limited.
A similar command is available that can be performed on egress as well using the CLI commands:

```
config system interface
edit <interface_name>
  set outbandwidth <rate_int>
next
end
```

As with ingress, setting the rate to 0 (zero) sets the rate to unlimited.

Rate limiting traffic accepted by the interface enables you to restrict incoming traffic to rates that, while no longer the full capacity of the interface, at the traffic shaping point in the processing are more likely to result in acceptable rates of outgoing traffic per destination interface or all firewall policies. This conserves FortiGate processing resources for those packets that are more likely to be viable completely to the point of egress.

Excessive traffic policing can degrade network performance rather than improve it. For details on factors you may want to consider when configuring traffic policing, see “Important considerations” on page 26.

## Bandwidth guarantee, limit, and priority interactions

After packet acceptance, the FortiGate unit classifies traffic and may apply traffic policing at additional points during processing. It may also apply additional QoS techniques, such as prioritization and traffic shaping. Traffic shaping consists of a mixture of traffic policing to enforce bandwidth limits, and priority queue adjustment to assist packets in achieving the guaranteed rate.

If you have configured prioritization, the FortiGate unit prioritizes egressing packets by distributing them among FIFO (first in, first out) queues associated with each possible priority number. Each physical interface has six priority queues. Virtual interfaces do not have their own queues, and instead use the priority queues of the physical interface to which they are bound.

Each physical interface's six queues are queue 0 to queue 5, where queue 0 is the highest priority queue. However, for the reasons described below, you may observe that your traffic uses only a subset of those six queues. Some traffic may always use a certain queue number. Some queueing may vary by the packet rate or mixture of services. Some queue numbers may be used only by through traffic for which you have configured traffic shaping in the firewall policy that applies to that traffic session. For example:

- Administrative access traffic will always use queue 0.
- Traffic matching firewall policies without traffic shaping may use queue 0, queue 1, or queue 2. Which queue will be used depends on the priority value you have configured for packets with that ToS (type of service) byte value, if you have configured ToS-based priorities.
- Traffic matching firewall policies with traffic shaping may use any queue. Which queue will be used depends on whether the packet rate is currently below the guaranteed bandwidth (queue 0), or above the guaranteed bandwidth (queue 1 to 5, depending on the sum of the firewall policy's Traffic Priority value with the priority that matches the ToS byte). Packets at rates greater than the maximum bandwidth limit are dropped.

Prioritization and traffic shaping behavior varies by your configuration, the service types and traffic volumes, and by whether the traffic is through traffic, or the traffic originates from or terminates at the FortiGate unit itself.
FortiGate traffic

For traffic types originating on or terminating at the FortiGate unit, such as administrative access to the FortiGate through HTTPS or SSH, or IPSec tunnel negotiations, firewall policies do not apply, and therefore FortiGate units do not apply traffic shaping. Such traffic also uses the highest priority queue, queue 0. In other words:

packet priority = 0

Exceptions to this rule include traffic types that, while technically originated by the FortiGate unit, are connections related to a session governed by a firewall policy. For example, if you have enabled scanning by FortiGuard Antivirus, traffic from the sender technically terminates at the FortiGate proxy that scans that traffic type; the FortiGate unit initiates a second connection that transmits scanned content to its destination. Because the second connection’s traffic is technically originating from the FortiGate proxy and therefore the FortiGate unit itself, it uses the highest priority queue, queue 0. However, this connection is logically associated with through traffic, and is therefore subject to possible bandwidth enforcement and guarantees in its governing firewall policy. In this way, it behaves partly like other through traffic.

Through traffic

For traffic passing through the FortiGate unit, which method a FortiGate unit uses to determine the priority queue varies by whether you have enabled Traffic Shaping. Packets may or may not use a priority queue directly or indirectly derived from the type of service (ToS) byte — sometimes used instead with differentiated services — in the packet’s IP header.

If Traffic Shaping is not enabled in the firewall policy, the FortiGate unit neither limits nor guarantees bandwidth, and traffic for that session uses the priority queue determined directly by matching the ToS byte in its header with your configured values:

```
config system global
   set tos-based-priority {high | low | medium}
end
```

or, if you have configured a priority specifically for that TOS byte value:

```
config system tos-based-priority
   edit <id_int>
      set tos [0-15]
      set priority {high | low | medium}
   next
end
```

where tos is the value of the ToS byte in the packet’s IP header, and high has a priority value of 0 and low is 2. Priority values configured in the second location will override the global ToS-based priority. In other words:

packet priority = ToS-based priority

For example, you might specify that packets with a ToS byte value of 2 should use queue 0, the highest priority queue:

```
config system tos-based-priority
   edit 15
      set tos 2
      set priority high
   next
end
```
If Traffic Shaping is enabled in the firewall policy using shared traffic shapers, the FortiGate unit may instead or also subject packets to traffic policing, or priority queue increase in an effort to meet bandwidth guarantees configured in the shaper:

```bash
config firewall shaper traffic-shaper
edit <shaper_name>
...
set priority {high | medium | low}
set maximum-bandwidth <rate>
set guaranteed-bandwidth <rate>
end
```

where high has a priority value of 1 and low is 3, and <rate_int> is the bandwidth limit in KB/s.

**Figure 2: Traffic queueing as packet rate increases**

- If the current packet rate is less than Guaranteed Bandwidth, packets use priority queue 0. In other words:
  
  packet priority = 0

- If the current packet rate is greater than Guaranteed Bandwidth but less than Maximum Bandwidth, the FortiGate unit assigns a priority queue by adding the numerical value of the firewall policy-based priority, where the value of High is 1, and Low is 3, with the numerical value of the ToS-based priority, where high has a priority value of 0 and low is 2. Because the two values are added, depending on the your configured ToS-based priorities, packets in this category could use queues from queue 1 to queue 5. In other words:

  packet priority = ToS-based priority + firewall policy-based priority

For example, if you have enabled Traffic Shaping in the firewall policy, and the firewall policy's Traffic Priority is Low (value 3), and the priority normally applied to packets with that ToS byte is medium (value 1), then packets have a total packet priority of 4, and use priority queue 4.

- If the current packet rate exceeds Maximum Bandwidth, excess packets are dropped.
Calculation and regulation of packet rates

Packet rates specified for Maximum Bandwidth or Guaranteed Bandwidth are:

\[
\text{rate} = \frac{\text{amount}}{\text{time}}
\]

where rate is expressed in kilobytes per second (KB/s).

Burst size at any given instant cannot exceed the amount configured in Maximum Bandwidth. Packets in excess are dropped. Packets deduct from the amount of bandwidth available to subsequent packets and available bandwidth regenerates at a fixed rate. As a result, bandwidth available to a given packet may be less than the configured rate, down to a minimum of 0 KB/s.

Rate calculation and behavior can alternatively be described using the token bucket metaphor, where:

- a traffic flow has an associated bucket, which represents burst size bounds, and is the size of your configured bandwidth limit
- the bucket receives tokens, which represent available bandwidth, at the fixed configured rate
- as time passes, tokens are added to the bucket, up to the capacity of the bucket; excess tokens are discarded
- when a packet arrives, the packet must deduct bandwidth tokens from the bucket equal to its packet size in order to egress
- packets cannot egress if there are insufficient tokens to pay for its egress; these nonconforming packets are dropped

Bursts are not redistributed over a longer interval, so bursts are propagated rather than smoothed, although their peak size is limited.

Maximum burst size is the capacity of the bucket (the configured bandwidth limit); actual size varies by the current number of tokens in the bucket, which may be less than bucket capacity, due to deductions from previous packets and the fixed rate at which tokens accumulate. A depleted bucket refills at the rate of your configured bandwidth limit. Bursts cannot borrow tokens from other time intervals. This behavior is illustrated in Figure 3 on page 25.
By limiting traffic peaks and token regeneration in this way, the available bandwidth at a given moment may be less than bucket capacity, but your limit on the total amount per time interval is ensured. That is, total bandwidth use during each interval of 1 second is at most the integral of your configured rate.

You may observe that external clients, such as FTP or BitTorrent clients, initially report rates between Maximum Bandwidth and twice that of Maximum Bandwidth, depending on the size of their initial burst. This is notably so when a connection is initiated following a period of no network activity. The apparent discrepancy in rates is caused by a difference of perspective when delimiting time intervals. A burst from the client may initially consume all tokens in the bucket, and before the end of 1 second, as the bucket regenerates, be allowed to consume almost another bucket’s worth of bandwidth. From the perspective of the client, this constitutes one time interval. From the perspective of the FortiGate unit, however, the bucket cannot accumulate tokens while full; therefore, the time interval for token regeneration begins after the initial burst, and does not contain the burst. These different points of reference result in an initial discrepancy equal to the size of the burst — the client’s rate contains it, but the FortiGate unit’s rate does not. If the connection is sustained to its limit and time progresses over an increasing number of intervals, however, this discrepancy decreases in importance relative to the bandwidth total, and the client’s reported rate will eventually approach that of the FortiGate unit’s configured rate limit.

For example, your Maximum Bandwidth might be 50 KB/s and there has been no network activity for one or more seconds. The bucket is full. A burst from an FTP client immediately consumes 50 KB. Because the bucket completely regenerates over 1 second, by the time almost another 1 second has elapsed from the initial burst, traffic can consume another 49.999 KB, for a total of 99.999 KB between the two points in time. From the vantage point of an external FTP client regulated by this bandwidth limit, it therefore initially appears that the bandwidth limit is 99.999 KB/s, almost twice the configured limit of 50 KB/s. However, bucket capacity only regenerates at your configured rate of 50 KB/s, and so the
connection can only consume a maximum of 50 KB during each second thereafter. The result is that as bandwidth consumption is averaged over an increasing number of time intervals, each of which are limited to 50 KB/s, the effects of the first interval’s doubled bandwidth size diminishes proportionately, and the client’s reported rate eventually approach your configured rate limit. This effect is illustrated in Table 4 on page 26.

Table 4: Effects of a 50 KB/s limit on client reported rates

<table>
<thead>
<tr>
<th>Total size transferred (KB)</th>
<th>Time (s)</th>
<th>Rate reported by client (KB/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>99.999 (50 + 49.999)</td>
<td>1</td>
<td>99.999</td>
</tr>
<tr>
<td>149.999</td>
<td>2</td>
<td>74.999</td>
</tr>
<tr>
<td>199.999</td>
<td>3</td>
<td>66.666</td>
</tr>
<tr>
<td>249.999</td>
<td>4</td>
<td>62.499</td>
</tr>
<tr>
<td>299.999</td>
<td>5</td>
<td>59.998</td>
</tr>
<tr>
<td>349.999</td>
<td>6</td>
<td>58.333</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Guaranteed Bandwidth can also be described using a token bucket metaphor. However, because this feature attempts to achieve or exceed a rate rather than limit it, the FortiGate unit does not discard non-conforming packets, as it does for Maximum Bandwidth; instead, when the flow does not achieve the rate, the FortiGate unit increases the packets’ priority queue, in an effort to increase the rate.

Guaranteed and maximum bandwidth rates apply to the bidirectional total for all sessions controlled by the firewall policy. For example, an FTP connection may entail two separate connections for the data and control portion of the session; some packets may be reply traffic rather than initiating traffic. All packets for both connections are counted when calculating the packet rate for comparison with the guaranteed and maximum bandwidth rate.

Important considerations

In essence, by implementing QoS, you trade some performance and/or stability from traffic X by discarding packets or introducing latency in order to improve performance and stability of traffic Y. The best traffic shaping configuration for your network will appropriately balance the needs of each traffic flow by considering not only the needs of your particular organization, but also the resiliency and other characteristics of each particular service. For example, you may find that web browsing traffic is both more resistant to interruptions or latency and less business critical than UDP or VoIP traffic, and so you might implement less restrictive QoS measures on UDP or VoIP traffic than on HTTP traffic.

An appropriate QoS configuration will also take into account the physical limits of your network devices, and the interactions of the aforementioned QoS mechanisms, described in “Bandwidth guarantee, limit, and priority interactions” on page 21.

You may choose to configure QoS differently based upon the hardware limits of your network and FortiGate unit. Traffic shaping may be less beneficial in extremely high-volume situations where traffic exceeds a network interface’s or your FortiGate model’s overall physical capacity. A FortiGate unit must have sufficient resources, such as memory and processing power, to process all traffic it receives, and to process it at the required rate; if it does not have this capacity, then dropped packets and increased latency
are likely to occur. For example, if the total amount of memory available for queueing on a physical interface is frequently exceeded by your network’s typical packet rates, frames and packets must be dropped. In such a situation, you might choose to implement QoS using a higher model FortiGate unit, or to configure an incoming bandwidth limit on each interface.

Incorrect traffic shaping configurations can actually further degrade certain network flows, because excessive discarding of packets or increased latency beyond points that can be gracefully handled by that protocol can create additional overhead at upper layers of the network, which may be attempting to recover from these errors. For example, a configuration might be too restrictive on the bandwidth accepted by an interface, and may therefore drop too many packets, resulting in the inability to complete or maintain a SIP call.

To optimize traffic shaping performance, first ensure that the network interface’s Ethernet statistics are clean of errors, collisions, or buffer overruns. To check the interface, enter the following diagnose command to see the traffic statistics:

```
diagnose hardware deviceinfo nic <port_name>
```

If these are not clean, adjust FortiGate unit and settings of routers or other network devices that are connected to the FortiGate unit. For additional information, see “Troubleshooting” on page 51.

Once Ethernet statistics are clean, you may want to use only some of the available FortiGate QoS techniques, or configure them differently, based upon the nature of FortiGate QoS mechanisms described in “Bandwidth guarantee, limit, and priority interactions” on page 21. Configuration considerations include:

- For maximum bandwidth limits, ensure that bandwidth limits at the source interface and/or the firewall policy are not too low, which can cause the FortiGate unit to discard an excessive number of packets.

- For prioritization, consider the ratios of how packets are distributed between available queues, and which queue is used by which types of services. If you assign most packets to the same priority queue, it negates the effects of configuring prioritization. If you assign many high bandwidth services to high priority queues, lower priority queues may be starved for bandwidth and experience increased or indefinite latency. For example, you may want to prioritize a latency-sensitive service such as SIP over a bandwidth-intensive service such as FTP. Consider also that bandwidth guarantees can affect the queue distribution, assigning packets to queue 0 instead of their typical queue in high-volume situations.

- You may or may not want to guarantee bandwidth, because it causes the FortiGate unit to assign packets to queue 0 if the guaranteed packet rate is not currently being met. Comparing queueing behavior for lower- and higher-bandwidth situations, this would mean that effects of prioritization only become visible as traffic volumes rise and exceed their guarantees. Because of this, you might want only some services to use bandwidth guarantees, to avoid the possibility that in high-volume situations all traffic uses the same queue, thereby negating the effects of configuring prioritization.
Important considerations

Traffic Shaping for FortiOS 4.0 MR2

For prioritization, configure prioritization for all through traffic. You may want to configure prioritization by either ToS-based priority or firewall policy priority, but not both. This simplifies analysis and troubleshooting.

Traffic subject to both firewall policy and ToS-based priorities will use a combined priority from both of those parts of the configuration, while traffic subject to only one of the prioritization methods will use only that priority. If you configure both methods, or if you configure either method for only a subset of your traffic, packets for which a combined priority applies will frequently receive a lower priority queue than packets for which you have only configured one priority method, or for which you have not configured prioritization.

For example, if both ToS-based priority and firewall policy priority both dictate that a packet should receive a “medium” priority, in the absence of bandwidth guarantees, a packet will use queue 3, while if only ToS-based priority had been configured, the packet would have used queue 1, and if only firewall policy-based priority had been configured, the packet would have used queue 2. If no prioritization had been configured at all, the packet would have used queue 0.

For example alternative QoS implementations that illustrate these considerations, see “Examples” on page 43.
Traffic shaping methods

In FortiOS, there are three types of traffic shaping configuration. Each has a specific function, and all can be used together in varying configurations. Policy shaping enables you to define the maximum bandwidth and guaranteed bandwidth set for a firewall policy, while per-IP shaping enables you to define traffic control on a more granular level. Application traffic shaping goes further, enabling traffic controls on specific applications or application groupings.

This chapter describes the types of traffic shapers and how to configure them in the web-based manager and the CLI.

This chapter includes topics on

- Shared policy shaping
- Per-IP shaping
- Application control shaping
- Shaping order of operations
- Enabling in the firewall policy
- Type of Service priority
- Differentiated Services
- Tos and DSCP mapping

Traffic shaping options

When configuring traffic shaping for your network, there are three different methods to control the flow of network traffic to ensure that the desired traffic gets through while also limiting the bandwidth that users use for other less important or bandwidth consuming traffic. The three shaping options are:

- shared policy shaping - bandwidth management by firewall policies
- per-IP shaping - bandwidth management by user IP addresses
- application control shaping - bandwidth management by application

Shared policy shaping and per IP shaping are enabled within the firewall policy, while the application control shaping is configured in UTM > Application Control and enabled in the firewall policy by selecting UTM and selecting the application control profile from the drop-down list.

For more information on setting up the shapers in a firewall policy, and how the FortiGate unit triages the different shapers, see “Shaping order of operations” on page 33.

Shared policy shaping

Traffic shaping by firewall policy enables you to control the maximum and/or guaranteed throughput for a selected firewall policy or group of policies. When configuring a shaper, you can select to apply the bandwidth shaping per policy or for all policies. Depending on your selection, the FortiGate unit will apply the shaping rules differently.
Per policy

When selecting a shaper to be per policy, the FortiGate unit will apply the shaping rules defined to each firewall policy individually.

For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four firewall policies monitoring traffic through the FortiGate unit. Three of these have the shaper enabled. Each firewall policy has the same maximum bandwidth of 1000 Kb/s.

Per policy 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.

All policies

When selecting a shaper to be for all policies - For All Policies Using This Shaper - the FortiGate unit applies the shaping rules to all policies using the same shaper. For example, the shaper is set to be per policy with a maximum bandwidth of 1000 Kb/s. There are four firewall policies monitoring traffic through the FortiGate unit. All four have the shaper enabled. Each firewall policy must share the defined 1000 Kb/s, and is set on a first come, first served basis. For example, if policy 1 uses 800 Kb/s, the remaining three must share 200 Kb/s. As policy 1 uses less bandwidth, it is opened up to the other policies to use as required. Once used, any other policies will encounter latency until free bandwidth opens from a policy currently in use.

Maximum and guaranteed bandwidth

The maximum bandwidth instructs the firewall policy what the largest amount of traffic allowed using the policy. Depending on the service or the users included for the firewall policy, this number can provide a larger or smaller throughput depending on the priority you set for the shaper.

The guaranteed bandwidth ensures there is a consistent reserved bandwidth available for a given service or user. When setting the guaranteed bandwidth, ensure that the value is significantly less than the bandwidth capacity of the interface, otherwise no other traffic will pass through the interface or very little an potentially causing unwanted latency.

**Note:** Setting both Guaranteed Bandwidth and Maximum Bandwidth to 0 (zero), effectively blocks traffic.

Traffic priority

Select a Traffic Priority of high, medium or low, so the FortiGate unit manages the relative priorities of different types of traffic. For example, a policy for connecting to a secure web server needed to support e-commerce traffic should be assigned a high traffic priority. Less important services should be assigned a low priority. The firewall provides bandwidth to low-priority connections only when bandwidth is not needed for high-priority connections.

Be sure to enable traffic shaping on all firewall policies. If you do not apply any traffic shaping rule to a policy, the policy is set to high priority by default.

Distribute firewall policies over all three priority queues.
VLAN, VDOM and virtual interfaces

Policy-based traffic shaping does not use queues directly. It shapes the traffic and if the packet is allowed by the firewall policy, then a priority is assigned. That priority controls what queue the packet will be put in upon egress. VLANs, VDOMs, aggregate ports and other virtual devices do not have queues and as such, traffic is sent directly to the underlying physical device where it is queued and affected by the physical ports.

This is also the case with IPsec connections.

Example

The following steps creates a Per Policy traffic shaper called “Throughput” with a maximum traffic amount of 120,000 KB/s, and a guaranteed traffic of 50,000 KB/s with a high traffic priority.

To create the shared shaper - web-based manager

1. Go to Firewall > Traffic Shaper > Shared and select Create New.
2. Enter the Name Throughput.
3. Select Per Policy.
4. Select the Maximum Bandwidth check box and enter the value 120000.
5. Select the Guaranteed Bandwidth check box and enter the value 50000.
6. Set the Traffic Priority to High.
7. Select OK.

To create the shared shaper - CLI

```
config firewall shaper traffic-shaper
edit Throughput
   set per-policy enable
   set maximum-bandwidth 120000
   set guaranteed-bandwidth 50000
   set priority high
end
```

Per-IP shaping

Traffic shaping by IP enables you to apply traffic shaping to all source IP addresses in the firewall policy. As well as controlling the maximum bandwidth users of a selected policy, you can also define the maximum number of concurrent sessions.

Per-IP traffic shaping enables you limit the behavior of every member of a policy to avoid one user from using all the available bandwidth - it now is shared within a group equally. Using a per-IP shaper avoids having to create multiple policies for every user you want to apply a shaper.

Note: Per-IP traffic shaping is not supported over NP2 interfaces.

Example

The following steps creates a Per-IP traffic shaper called “Accounting” with a maximum traffic amount of 120,000 KB/s, and the number of concurrent sessions of 200.
Application control shaping

Traffic shaping is also possible for specific applications. Through the UTM > Application Control feature, you can configure a specific application’s maximum bandwidth. When configuring the application control features, if the application is set to pass, you can set the traffic shaping options. The shapers available are those set up in the Firewall > Traffic Shaping menu.

Example

This example sets the traffic shaping definition for Facebook to a medium priority, a default traffic shaper.

To add traffic shaping for Facebook - web-based manager

1. Go to UTM > Application Control List.
2. Select Create New to create a new application group, and enter the name Web.
3. Select OK.
4. Select Create New.
5. Select Web from the Category drop-down list.
6. Select Facebook from the Application drop-down list.
7. Select Pass for the Action.
8. Select Traffic Shaping and select medium-priority from the drop-down list.
9. Select OK.
To add traffic shaping for Facebook - CLI

```bash
config application list
  edit web
    config entries
      edit 1
        set category 12
        set application 15832
        set action pass
        set shaper medium-priority
      end
    end
end
```

Shaping order of operations

The FortiGate unit offers three different traffic shaping options, all of which can be enabled at the same time within the same firewall policy. Generally speaking, the hierarchy for shapers in FortiOS is:

- Application Control shaper
- Firewall policy shaper
- Per-IP shaper

With this hierarchy, if an application control list has a traffic shaper defined, it will have precedence always over any other firewall policy shaper. For example, with the example above creating an application control for Facebook, the shaper defined for Facebook will supersede any firewall policy enabled traffic shapers. While the Facebook application may reach its maximum bandwidth, the user can still have the bandwidth room available from the shared shaper and, if enabled, the per-IP shaper.

Equally, any firewall policy shared shaper will have precedence over any per-IP shaper. However, traffic that exceeds any of these shapers will be dropped. For example, the policy shaper will take effect first, however, if the per-IP shaper limit is reached first, then traffic for that user will be dropped even if the shared shaper limit for the policy has not been exceeded.

Enabling in the firewall policy

All traffic shapers are enabled within a firewall policy, including the Application Control shapers. As such, the shapers are in effect after any DoS sensor policies, and before any routing or packet scanning occurs.

To enable traffic shaping - web-based manager

1. Go to Firewall > Policy.
2. Select Create New or select an existing policy and select Edit.
4. Select the shaping option and select the shaper from the drop-down list.
5. Select OK.
To enable traffic shaping - CLI

```
config firewall policy
  edit <policy_number>
  ...
  set traffic-shaper <shaper_name>
end
```

Reverse direction traffic shaping

The shaper you select for the policy (shared shaper) will affect the traffic in the direction defined in the policy. For example, if the source port is port 1 and the destination is port 3, the shaping affects the flow in this direction only. By selecting Reverse Direction Traffic Shaping, you can define the traffic shaper for the policy in the opposite direction. In this example, from port 3 to port 1.

Application control shaper

Application control shapers are in effect within the application control profile. Within the firewall policy options, select UTM then Application Control and select the application from the list.

Type of Service priority

Type of service (TOS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, as described in RFC 791, using criteria of delay, priority, reliability, and minimum cost. Each quality helps gateways determine the best way to route datagrams. A router maintains a TOS value for each route in its routing table. The lowest priority TOS is 0, the highest is 7 when bits 3, 4, and 5 are all set to 1. There are 4 other bits that are seldom used or reserved that are not included here. Together these bits are the tos variable of the tos-based-priority command. The router tries to match the TOS of the datagram to the TOS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero TOS route. Using increased quality may increase the cost of delivery because better performance may consume limited network resources.

| bits 0, 1, 2 | Precedence | Some networks treat high precedence traffic as more important traffic. Precedence should only be used within a network, and can be used differently in each network. Typically you do not care about these bits. |
| bit 3 | Delay | When set to 1, this bit indicates low delay is a priority. This is useful for such services as VoIP where delays degrade the quality of the sound. |
| bit 4 | Throughput | When set to 1, this bit indicates high throughput is a priority. This is useful for services that require lots of bandwidth such as video conferencing. |
| bit 5 | Reliability | When set to 1, this bit indicates high reliability is a priority. This is useful when a service must always be available such as with DNS servers. |
| bit 6 | Cost | When set to 1, this bit indicates low cost is a priority. Generally there is a higher delivery cost associated with enabling bits 3, 4, or 5, and bit 6 indicates to use the lowest cost route. |
| bit 7 | Reserved for future use | Not used at this time. |

The TOS value is set in the CLI using the commands:
config system tos-based-priority
  edit <name>
    set tos <ip_tos_value>
    set priority [high | medium | low]
  end

Where `tos` is Enter the value of the type of service byte in the IP datagram header with a value between 0 and 15, and `priority` is the priority of this type of service. `priority`. These priority levels conform to the firewall traffic shaping priorities. For a list of ToS values and their DSCP equivalents see “Tos and DSCP mapping” on page 40.

Example

config system tos-based-priority
  edit 1
    set tos 1
    set priority low
  next
  edit 4
    set tos 4
    set priority medium
  next
  edit 6
    set tos 6
    set priority high
  next
end

TOS in FortiOS

Traffic shaping and TOS follow the following sequence:

1  The CLI command tos-based-priority acts as a tos-to-priority mapping. FortiOS maps the TOS to a priority when it receives a packet.

2  Traffic shaping settings adjust the packet’s priority according the traffic.

3  Deliver the packet based on its priority.

Differentiated Services

Differentiated Services describes a set of end-to-end Quality of Service (QoS) capabilities. End-to-end QoS is the ability of a network to deliver service required by specific network traffic from one end of the network to another. By configuring differentiated services, you configure your network to deliver particular levels of service for different packets based on the QoS specified by each packet.

Differentiated Services (also called DiffServ) is defined by RFC 2474 and 2475 as enhancements to IP networking to enable scalable service discrimination in the IP network without the need for per-flow state and signaling at every hop. Routers that can understand differentiated services sort IP traffic into classes by inspecting the DS field in IPv4 header or the Traffic Class field in the IPv6 header.
You can use the FortiGate Differentiated Services feature to change the DSCP (Differentiated Services Code Point) value for all packets accepted by a policy. The network can use these DSCP values to classify, mark, shape, and police traffic, and to perform intelligent queuing. DSCP features are applied to traffic by configuring the routers on your network to apply different service levels to packets depending on the DSCP value of the packet.

If the differentiated services feature is not enabled, the FortiGate unit treats traffic as if the DSCP value is set to the default (00), and will not change IP packets' DSCP field. DSCP values are also not applied to traffic if the traffic originates from a FortiGate unit itself.

The FortiGate unit applies the DSCP value to the differentiated services (formerly TOS) field in the first word of the IP header. The typical first word of an IP header, with the default DSCP value, is 4500:

- 4 for IPv4
- 5 for a length of five words
- 00 for the default DSCP value

You can change the packet's DSCP field for traffic initiating a session (forward) or for reply traffic (reverse) and enable each direction separately and configure it in the firewall policy.

**Note:** Changes to DSCP values in a firewall policy effect new sessions. If traffic must use the new DSCP values immediately, clear all existing sessions.

DSCP is enabled using the CLI command:

```bash
config firewall policy
  edit <policy_number>
    ...
    set diffserv-forward enable
    set diffservcode-forward <binary_integer>
    set diffserv-reverse enable
    set diffservcode-rev <binary_integer>
  end
```

For more information on the different DSCP commands, see the examples below and the CLI Reference.

**Note:** If you only set `diffserv-forward` and `diffserv-reverse` without setting the corresponding `diffservcode` values, the FortiGate unit will reset the bits to zero.

For a list of DSCP values and their ToS equivalents see "Tos and DSCP mapping" on page 40.
DSCP examples

For all the following DSCP examples, the FortiGate and client PC configuration is the following diagram.

![Diagram](image)

Example

In this example, an ICMP ping is executed between User 1 and FortiGate B, through a FortiGate unit. DSCP is disabled on FortiGate B, and FortiGate A contains the following configuration:

```
config firewall policy
edit 2
set srcintf port6
set dstintf port3
set src addr all
set dstaddr all
set action accept
set schedule always
set service ANY
set diffserv-forward enable
set diffservcode-forward 101110
end
```

As a result, FortiGate A changes the DSCP field for outgoing traffic, but not to its reply traffic. The binary DSCP values used map to the following hexadecimal TOS field values, which are observable by a sniffer (also known as a packet tracer):

- DSCP 000000 is TOS field 0x00
- DSCP 101110 is TOS field 0xb8, the recommended DSCP value for expedited forwarding (EF)

If you performed an ICMP ping between User 1 and User 2, the following output illustrates the IP headers for the request and the reply by sniffers on each of FortiGate unit's network interfaces. The right-most two digits of each IP header are the TOS field, which contains the DSCP value.

![Example Output](image)
Example

In this example, an ICMP ping is executed between User 1 and FortiGate B, through FortiGate A. DSCP is disabled on FortiGate B, and FortiGate A contains the following configuration:

```bash
config firewall policy
edit 2
    set srcintf port6
    set dstintf port3
    set src addr all
    set dstaddr all
    set action accept
    set schedule always
    set service ANY"
    set diffserv-forward enable
    set diffserv-rev enable
    set diffservcode-forward 101110
    set diffservcode-rev 101111
end
```

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic. The binary DSCP values in map to the following hexadecimal TOS field values, which are observable by a sniffer (also known as a packet tracer):

- DSCP 000000 is TOS field 0x00
- DSCP 101110 is TOS field 0xb8, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field 0xbc

If you performed an ICMP ping between User 1 and User 2, the output below illustrates the IP headers observed for the request and the reply by sniffer on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the TOS field, which contains the DSCP value.

Example

In this example, an ICMP ping is executed between User 1 and FortiGate B, through FortiGate A. DSCP is enabled for both traffic directions on FortiGate A, and enabled only for reply traffic on FortiGate B. FortiGate A contains the following configuration:

```bash
config firewall policy
edit 2
    set srcintf port6
    set dstintf port3
    set src addr all
    set dstaddr all
    set action accept
    set schedule always
    set service ANY
    set diffserv-forward enable
    set diffserv-rev enable
    set diffservcode-forward 101110
end
```
Traffic shaping methods

set diffservcode-rev 101111
end

FortiGate B contains the following configuration:

config firewall policy
edit 2
set srcintf wan2
set dstintf internal
set src addr all
set dstaddr all
set action accept
set schedule always
set service ANY
set diffserv-rev enable
set diffservcode-rev 101101
end

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic, and FortiGate B changes the DSCP field only for reply traffic. The binary DSCP values in this configuration map to the following hexadecimal TOS field values:

- DSCP 000000 is TOS field 0x00
- DSCP 101101 is TOS field 0xb4
- DSCP 101110 is TOS field 0xb8, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field 0xbc

If you performed an ICMP ping between User 1 and User 2, the output below illustrates the IP headers observed for the request and the reply by sniffers on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the TOS field, which contains the DSCP value.

```
User 1                      User 2
+---+----------------+---+----------------+
| 45 | 4500           | 45 | 4500           |
| 45 | 4500           | 45 | 4500           |
| 45 | 4500           | 45 | 4500           |
| 45 | 4500           | 45 | 4500           |
| 45 | 45bc           | 45 | 45bc           |
| 45 | 45bc           | 45 | 45bc           |
| 45 | 45b4           | 45 | 45b4           |
| 45 | 45b4           | 45 | 45b4           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 45b8           | 45 | 45b8           |
| 45 | 4500           | 45 | 4500           |
```

Example

In this example, HTTPS and DNS traffic is sent from User 1 to FortiGate B, through FortiGate A. DSCP is enabled for both traffic directions on FortiGate A, and enabled only for reply traffic on FortiGate B. FortiGate A contains the following configuration:

config firewall policy
edit 2
set srcintf port6
set dstintf port3
set src addr all
set dstaddr all
set action accept
set schedule always
set service ANY
set diffserv-forward enable
set diffserv-rev enable
set diffservcode-forward 101110
set diffservcode-rev 101111
end
FortiGate B contains the following configuration:

```
config firewall policy
edit 2
  set srcintf wan2
  set dstintf internal
  set src addr all
  set dstaddr all
  set schedule always
  set service ANY
  set diffserv-rev enable
  set diffservcode-rev 101101
end
```

As a result, FortiGate A changes the DSCP field for both outgoing traffic and its reply traffic, but FortiGate B changes the DSCP field only for reply traffic which passes through its internal interface. Since the example traffic does not pass through the internal interface, FortiGate B does not mark the packets. The binary DSCP values in this configuration map to the following hexadecimal TOS field values:

- DSCP 000000 is TOS field \texttt{0x00}
- DSCP 101101 is TOS field \texttt{0xb4}, which is configured on FortiGate B but not observed by the sniffer because the example traffic originates from the FortiGate unit itself, and therefore does not match that firewall policy.
- DSCP 101110 is TOS field \texttt{0xb8}, the recommended DSCP value for expedited forwarding (EF)
- DSCP 101111 is TOS field \texttt{0xbc}

If you sent HTTPS or DNS traffic from User 1 to FortiGate B, the following would illustrate the IP headers observed for the request and the reply by sniffers on each of FortiGate A's and FortiGate B's network interfaces. The right-most two digits of each IP header are the TOS field, which contains the DSCP value.

![Diagram](image)

**Tos and DSCP mapping**

The table below lists the mapping of DSCP and ToS hexadecimal values for each service for QoS.

<table>
<thead>
<tr>
<th>Service Class</th>
<th>DSCP Bits</th>
<th>DSCP Value</th>
<th>ToS Value</th>
<th>ToS Hexidecimal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Control</td>
<td>111000</td>
<td>56-63</td>
<td>224</td>
<td>0xE0</td>
</tr>
<tr>
<td>Internetwork Control</td>
<td>110000</td>
<td>48-55</td>
<td>192</td>
<td>0xC0</td>
</tr>
<tr>
<td>Critical - Voice Data (RTP)</td>
<td>101110</td>
<td>46</td>
<td>184</td>
<td>0xB8</td>
</tr>
<tr>
<td></td>
<td>101000</td>
<td>40</td>
<td>160</td>
<td>0xA0</td>
</tr>
</tbody>
</table>
### Table 6: ToS to DSCP mappings

<table>
<thead>
<tr>
<th>Flash Override</th>
<th>ToS</th>
<th>DSCP (in decimal)</th>
<th>Hex</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video Data</td>
<td>100010</td>
<td>34</td>
<td>136</td>
</tr>
<tr>
<td></td>
<td>100100</td>
<td>36</td>
<td>144</td>
</tr>
<tr>
<td></td>
<td>100110</td>
<td>38</td>
<td>152</td>
</tr>
<tr>
<td></td>
<td>100000</td>
<td>32</td>
<td>128</td>
</tr>
<tr>
<td>Flash Voice Control</td>
<td>011010</td>
<td>26</td>
<td>104</td>
</tr>
<tr>
<td></td>
<td>011100</td>
<td>28</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td>011110</td>
<td>30</td>
<td>120</td>
</tr>
<tr>
<td></td>
<td>011000</td>
<td>24</td>
<td>96</td>
</tr>
<tr>
<td>Immediate Deterministic (SNA)</td>
<td>010010</td>
<td>18</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>010100</td>
<td>20</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>010110</td>
<td>22</td>
<td>88</td>
</tr>
<tr>
<td></td>
<td>010000</td>
<td>16</td>
<td>64</td>
</tr>
<tr>
<td>Priority Controlled Load</td>
<td>001010</td>
<td>10</td>
<td>40</td>
</tr>
<tr>
<td></td>
<td>001100</td>
<td>12</td>
<td>48</td>
</tr>
<tr>
<td></td>
<td>001110</td>
<td>14</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>001000</td>
<td>8</td>
<td>32</td>
</tr>
<tr>
<td>Routine - Best Effort</td>
<td>000000</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Routine - Penalty Box</td>
<td>000010</td>
<td>2</td>
<td>8</td>
</tr>
</tbody>
</table>
Examples

While it is possible to configure QoS using a combination of firewall policies and in ToS-based priorities, and to distribute traffic over all six of the possible queues for each physical interface, the results of those configurations can be more difficult to analyze due to their complexity. In those cases, prioritization behavior can vary by several factors, including traffic volume, ToS (type of service) or differentiated services markings, and correlation of session to a firewall policy.

The following simple examples illustrate QoS configurations using either prioritization by firewall policy, or prioritization by ToS byte, but not both. The examples also assume you are not configuring traffic shaping for interfaces that receive hardware acceleration from network processing units (NPU).

QoS using priority from firewall policies

Configurations implementing QoS using the priority values defined in firewall policies are capable of applying bandwidth limits and guarantees.

In addition to configuring traffic shaping, you may also choose to limit bandwidth accepted by each interface. This can be useful in scenarios where bandwidth being received on source interfaces frequently exceeds the maximum bandwidth limit defined in the firewall policy. In this case, rather than wasting processing power on packets that will only be dropped later in the processing to enforce those limits, you may choose to preemptively police the traffic.

Note that if you implement QoS using firewall policies rather than ToS byte, the FortiGate unit applies QoS to all packets controlled by the policy. Control is less granular than prioritization by ToS byte, but has the benefits of correlating quality of service to a firewall policy, enabling you to distribute traffic over up to four of the possible 6 priority queues (queue 0 to queue 3), not requiring other devices in your network to set or respect the ToS byte, and of enabling you to configure bandwidth limits and guarantees.

In this example, we limit the bandwidth accepted by each source interface, limit the bandwidth used by sessions controlled by the firewall policy, and then configure prioritized queueing on the destination interface based upon the priority in the firewall policy, subject to alternative assignment to queue 0 when necessary to achieve the guaranteed packet rate.

To limit bandwidth accepted by an interface

In the CLI, enter the following commands:

config system interface
edit <name_str>
   set inbandwidth <rate_int>
next
end

where <rate_int> is the bandwidth limit in KB/s. Excess packets will be dropped.
To configure bandwidth guarantees, limits, and priorities

1. Go to Firewall > Traffic Shaper > Shared, and select Create New.
2. Enter a name for the shaper.
3. Enter the Guaranteed Bandwidth, if any.
   Bandwidth guarantees affect prioritization. While packet rates are less than this rate, they use priority queue 0. If this is not the effect you intend, consider entering a small guaranteed rate, or enter 0 to effectively disable bandwidth guarantees.
4. Enter Maximum Bandwidth.
   Packets greater than this rate will be discarded.
5. Select the Traffic Priority.
   High has a priority value of 1, while Low is 3. While the current packet rate is below Guaranteed Bandwidth, the FortiGate unit will disregard this setting, and instead use priority queue 0.
6. Select OK.

Sample configuration

This sample configuration limits ingressing bandwidth to 500 KB/s. It also applies separate traffic shapers to FTP and HTTP traffic. In addition to the interface bandwidth limit, HTTP traffic is subject to a firewall policy bandwidth limit of 200 KB/s.

All egressing FTP traffic greater than 10 KB/s is subject to a low priority queue (queue 3), while all egressing HTTP traffic greater than 100 KB/s is subject to a medium priority queue (queue 2). That is, unless FTP traffic rates are lower than their guaranteed rate, and web traffic rates are greater than their guaranteed rate, FTP traffic is lower priority than web traffic.

Traffic less than these guaranteed bandwidth rates use the highest priority queue (queue 0).

Set the inbandwidth limits. This setting is only available in the CLI:
```
config system interface
edit wan1
   set inbandwidth 500
next
end
```

Create the traffic shapers or FTP and HTTP.

To configure the shapers - web-based manager

1. Go to Firewall > Traffic Shaper > Shared, and select Create New.
2. Enter FTP for the name of the shaper.
3. Enter the Guaranteed Bandwidth, of 10 KBps.
4. Enter Maximum Bandwidth of 500 KBps.
5. Select the Traffic Priority of Low.
6. Select OK.
7. Select Create New.
8. Enter HTTP for the name of the shaper.
9. Enter the Guaranteed Bandwidth, of 100 KBps.
10. Enter Maximum Bandwidth of 200 KBps.
11 Select the Traffic Priority of Medium.
12 Select OK.

**To configure the shapers - CLI**

```cli
config firewall shaper traffic-shaper
edit FTP
    set maximum-bandwidth 500
    set guaranteed-bandwidth 10
    set per-policy enable
    set priority low
end
next
edit HTTP
    set maximum-bandwidth 200
    set guaranteed-bandwidth 100
    set per-policy enable
    set priority medium
end
```

**QoS using priority from ToS or differentiated services**

Configurations implementing QoS using the priority values defined in either global or specific ToS byte values are not capable of applying bandwidth limits and guarantees, but are capable of prioritizing traffic at per-packet levels, rather than uniformly to all services matched by the firewall policy.

In addition to configuring traffic prioritization, you may also choose to limit bandwidth being received by each interface. This can sometimes be useful in scenarios where you want to limit traffic levels, but do not want to configure traffic shaping within a firewall policy. This has the benefit of policing traffic at a point before the FortiGate unit performs most processing.

Note that if you implement QoS using ToS octet rather than firewall policies, the FortiGate unit applies QoS on a packet by packet basis, and priorities may be different for packets and services controlled by the same firewall policy. This is more granular control than prioritization by firewall policies, but has the drawbacks that quality of service is may not be uniform for multiple services controlled by the same firewall policy, packets will only use up to three of the six possible queues (queue 0 to queue 2), and bandwidth cannot be guaranteed. Other devices in your network must also be able to set or preserve ToS bytes.

In this example, we limit the bandwidth accepted by each source interface, and then configure prioritized queueing on the destination interface based upon the value of the ToS byte located in the IP header of each accepted packet.

To limit bandwidth accepted by an interface, in the CLI, enter the following commands:

```cli
config system interface
edit <name_str>
    set inbandwidth <rate_int>
next
end
```

where `<rate_int>` is the bandwidth limit in KB/s. Excess packets will be dropped.

To configure priorities, in the CLI, configure the global priority value using the following commands:

```cli
config system global
```
set tos-based-priority {high | low | medium}
end

where high has a priority value of 0 and low is 2.

If you want to prioritize some ToS byte values differently than the global ToS-based priority, configure the priority for packets with that ToS byte value using the following commands:

cfg system tos-based-priority
cfg <id_int>
set tos [0-15]
set priority {high | low | medium}
next
def

where and tos is the value of the ToS byte in the packet’s IP header, and high has a priority value of 0 and low is 2. Priority values configured in this location will override the global ToS-based priority.

Sample configuration

This sample configuration limits ingressing bandwidth to 500 KB/s. It also queues egressing traffic based upon the ToS byte in the IP header of ingressing packets.

Unless specified for the packet’s ToS byte value, packets use the low priority queue (queue 2). For ToS byte values 4 and 15, the priorities are specified as medium (value 1) and high (value 0), respectively.

cfg system interface
cfg wan1
set inbandwidth 500
next
def
cfg system global
set tos-based-priority low
def
cfg system tos-based-priority
cfg 4
set tos 4
set priority medium
next
cfg 15
set tos 15
set priority high
next
def

Example setup for VoIP

In this example, there are three traffic shaping requirements for a network:

• Voice over IP (VoIP) requires a guaranteed, high-priority for bandwidth for telephone communications.

• FTP bursts must be contained so as not to consume any available bandwidth. As such this traffic needs to be throttled to a smaller amount.

• A consistent bandwidth requirement is needed for all other email and web-based traffic.
To enable this requirement, you need to create three separate shapers and three firewall policies for each traffic type.

**Note:** For this example, the actual values are not actual values, they are used for the simplicity of the example.

### Creating the traffic shapers

First create the traffic shapers that define the maximum and guaranteed bandwidth. The shared shapers will be used, some with per-policy and some all policies as shown in the table, to better control traffic.

#### VoIP shaper

The VoIP functionary is a key component to the business as a communication tool and as such requires a guaranteed bandwidth.

**To create a VoIP shaper - web-based manager**

1. Go to **Firewall > Traffic Shaping > Shared**.
2. Enter the **Name** voip.
3. Select **Per Policy**.
4. Enter the **Maximum Bandwidth** of 1000 Kb/s
5. Enter the **Guaranteed Bandwidth** of 800 Kb/s.
7. Select OK.

**To create a VoIP shaper - CLI**

```bash
config firewall shaper traffic-shaper
e   edit voip
    set maximum-bandwidth 1000
    set guaranteed-bandwidth 800
    set per-policy enable
    set priority high
end
```

This ensures that whatever number of policies use this shaper, the defined bandwidth will always be the same. At the same time, the bandwidth is continually guaranteed at 800 Kb/s but if available can be as much as 1000 Kb/s. Setting the priority to high ensures that the FortiGate unit always considers VoIP traffic as the most important.

#### FTP shaper

The FTP shaper sets the maximum bandwidth to use to avoid sudden spikes by sudden uploading or downloading of large files, and interfering with other more important traffic.

**To create a FTP shaper - web-based manager**

1. Go to **Firewall > Traffic Shaping > Shared**.
2. Enter the **Name** ftp.
3. Select **For all Policies Using This Shaper**.
4. Enter the **Maximum Bandwidth** of 200 Kb/s
5  Enter the Guaranteed Bandwidth of 200 Kb/s.
6  Select a Traffic Priority of Low.
7  Select OK.

To create a FTP shaper - CLI

```bash
config firewall shaper traffic-shaper
edit ftp
  set maximum-bandwidth 200
  set guaranteed-bandwidth 200
  set priority low
end
```

For this shaper, the maximum and guaranteed bandwidth are set low and to the same value. In this case, the bandwidth is restricted to a specific amount. By also setting the traffic priority low ensures more important traffic will be able to pass before FTP traffic.

Regular traffic shaper

The regular shaper sets the maximum bandwidth and guaranteed bandwidth for everyday business traffic such as web and email traffic.

To create a regular shaper - web-based manager

1  Go to Firewall > Traffic Shaping > Shared.
2  Enter the Name daily_traffic.
3  Select Per Policy.
4  Enter the Maximum Bandwidth of 600 Kb/s
5  Enter the Guaranteed Bandwidth of 600 Kb/s.
6  Select a Traffic Priority of Medium.
7  Select OK.

To create a regular shaper - CLI

```bash
config firewall shaper traffic-shaper
edit daily_traffic
  set maximum-bandwidth 600
  set guaranteed-bandwidth 600
  set per-policy enable
  set priority medium
end
```

For this shaper, the maximum and guaranteed bandwidth are set to a moderate value of 600 Kb/s. It is also set for per policy, which ensures each firewall policy for day-to-day business traffic has the same distribution of bandwidth.

Creating firewall policies

To employ the shaper, create firewall policies that use the shapers within the policies. Create a separate policy for each service and enable traffic shaping. For example, a policy for FTP traffic, a policy for SIP and so on.

For the following steps the VoIP traffic shaper is enabled as well as the reverse direction option. This ensures that return traffic for a VoIP call has the same guaranteed bandwidth as the outgoing call.
To enable traffic shaping in the firewall policy - web-based manager

1. Go to **Firewall > Policy** and select **Create New**.

2. Enter the following and select:
   - **Source interface/Zone**: Internal
   - **Source address**: All
   - **Destination interface/Zone**: WAN1
   - **Destination address**: All
   - **Schedule**: always
   - **Service**: SIP
   - **Action**: ALLOW

3. Select **Traffic Shaping**.

4. From the drop-down list, select the voip shaper created in the previous steps.

5. Select **Reverse Direction Traffic Shaping**.

6. Select **OK**.

To enable traffic shaping in the firewall policy - CLI

```
config firewall policy
edit 6
   set srcintf internal
   set scraddr all
   set dstintf wan1
   set dstaddr all
   set action accept
   set schedule always
   set service sip
   set traffic-shaper voip
   set reverse-traffic-shaper voip
end
```
Troubleshooting

This chapter outlines some troubleshooting tips and steps to diagnose the shapers and whether they are working correctly. These diagnose commands include:

- diagnose system tos-based-priority
- diagnose firewall shaper traffic-shaper
- diagnose firewall per-ip-shaper
- diagnose debug flow

This chapter includes the topics:

- Interface diagnosis
- Shaper diagnose commands
- Packet loss with statistics on shapers
- Packet lost with the debug flow
- Session list details with dual traffic shaper
- Additional Information

Interface diagnosis

To optimize traffic shaping performance, first ensure that the network interface’s Ethernet statistics are clean of errors, collisions, or buffer overruns. To check the interface, enter the following diagnose command to see the traffic statistics:

```
   diagnose hardware deviceinfo nic <port_name>
```

Shaper diagnose commands

There are specific diagnose commands you can use to verify the configuration and flow of traffic, including packet loss due to the employed shaper.

All of these diagnose troubleshooting commands are supported in both IPv4 and IPv6.

TOS command

Use the following command to list command to view information of the TOS lists and traffic.

```
   diagnose system tos-based-priority
```

This example displays the priority value currently correlated with each possible TOS byte value. Priority values are displayed in order of their corresponding TOS byte values, which can range between 0 and 15, from lowest TOS byte value to highest.

For example, if you have not configured TOS-based priorities, the following appears...

```
   0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
```

...reflecting that all packets are currently using the same default priority, high (value 0).
If you have configured a TOS-based priority of low (value 2) for packets with a ToS byte value of 3, the following appears...

```
0 0 0 2 0 0 0 0 0 0 0 0 0 0 0 0
```

...reflecting that most packets are using the default priority value, except those with a ToS byte value of 3.

**Shared shaper**

To view information for the shared traffic shaper for firewall policies enter the command

```
diagnose firewall shaper traffic-shaper list
```

The resultant output displays the information on all available shapers. The more shapers available the longer the list. For example:

```
name Throughput
maximum-bandwidth 1200000 KB/sec
guaranteed-bandwidth 50000 KB/sec
current-bandwidth 0 B/sec
priority 1
packets dropped 0
```

Additional commands include:

```
diagnose firewall shaper traffic-shaper state - provides the total number of traffic shapers on the FortiGate unit.
diagnose firewall shaper traffic-shaper stats - provides summary statistics on the shapers. Sample output looks like the following:

shapers 9 ipv4 0 ipv6 0 drops 0
```

**Per-IP shaper**

To view information for the per-IP shaper for firewall policies enter the command

```
diagnose firewall shaper per-ip-shaper list
```

The resultant output displays the information on all available per-IP shapers. The more shapers available the longer the list. For example:

```
name accounting_group
maximum-bandwidth 200000 KB/sec
maximum-concurrent-session 55
packet dropped 0
```

Additional commands include:

```
diagnose firewall shaper per-ip-shaper state - provides the total number of per-ip shapers on the FortiGate unit.
diagnose firewall shaper per-ip-shaper stats - provides summary statistics on the shapers. Sample output looks like the following:

memory allocated 3 packet dropped: 0
```

You can also clear the per-ip statistical data to begin a fresh diagnoses using:

```
diagnose firewall shaper per-ip-shaper clear
```
Packet loss with statistics on shapers

For each shaper there are counters that allow to verify if packets have been discarded. To view this information, in the CLI, enter the command diagnose firewall shaper.

The results will look similar to the following output:

```
diagnose firewall shaper traffic-shaper list

  name limit_GB_25_MB_50_LQ
  maximum-bandwidth 50 KB/sec
  guaranteed-bandwidth 25 KB/sec
  current-bandwidth 51 KB/sec
  priority 3
  dropped 1291985
```

The diagnose command output is different if the shapers are configured either per-policy or shared between policies. For per-IP the output would be:

```
diagnose firewall shaper per-ip-shaper list

  name accounting_group
  maximum-bandwidth 200000 KB/sec
  maximum-concurrent-session 55
  packet dropped 3264220
```

Packet lost with the debug flow

When using the debug flow diagnostic command, there is a specific message information that a packet has exceed the shaper limits and therefore discarded:

```
diagnose debug flow show console enable
diagnose debug flow filter addr 10.143.0.5
diagnose debug flow trace start 1000

id=20085 trace_id=11 msg="vd-root received a packet(proto=17, 10.141.0.11:3735->10.143.0.5:5001) from port5."
id=20085 trace_id=11 msg="Find an existing session, id-0000eabc, original direction"
id=20085 trace_id=11 msg="exceeded shaper limit, drop"
```

Session list details with dual traffic shaper

When a Firewall Policy has a different traffic shaper for each direction, it is reflected in the session list output from the CLI:

```
diagnose system session list

session info: proto=6 proto_state=02 expire=115 timeout=3600
flags=00000000 sock
flag=00000000 sockport=0 av_idx=0 use=4
origin-shaper=Limit_25Mbps prio=1 guarantee 25600/sec max 204800/sec traffic 48/sec
reply-shaper=Limit_100Mbps prio=1 guarantee 102400/sec max 204800/sec traffic 0/sec
ha_id=0 hakey=44020
policy_dir=0 tunnel=/
state=may_dirty rem os rs
```
Additional Information

- Packets discarded by the shaper impact flow-control mechanisms like TCP. For more accurate testing results prefer UDP protocol.
- Traffic shaping accuracy is optimum for firewall policies without a protection profile where no FortiGate content inspection is processed.
- Do not oversubscribe an outbound throughput. For example, sum[guaranteed BW] < outbound. For accuracy in bandwidth calculation, it is required to set the “outbandwidth” parameter on the interfaces. For more information see “Bandwidth guarantee, limit, and priority interactions” on page 21.
- The FortiGate unit is not prioritizing traffic based on the DSCP marking configured in the firewall policy. However, TOS based prioritizing can be made at ingress. For more information see “Differentiated Services” on page 35.
Index

A
all policies, 30
application control, 32

B
bandwidth, 24
guaranteed, 21, 30
maximum, 30
zero, 30
block traffic, 30

certification, 16
CLI
syntax conventions, 12
comments, documentation, 16
conventions, 9
Cross-Site Scripting (XSS), 14
customer service, 16

differentiated services, 35
mapping, 40
document conventions
CLI syntax, 12
documentation, 16
commenting on, 16
conventions, 9

F
FAQ, 16
firewall policy, 33
flow, reverse shaping, 34
FortiGate documentation
commenting on, 16
FortiGuard
Antivirus, 15
services, 15
Fortinet
Knowledge Base, 16
Technical Documentation, 16
Technical Documentation, conventions, 9
Technical Support, 16
Technical Support, registering with, 15
Technical Support, web site, 15
Training Services, 16
Fortinet customer service, 16

glossary, 16
guaranteed bandwidth, 24, 30

H
how-to, 16

I
IP address
private network, 9
IP header
differentiated services, 36
ToS, 34
IPsec, 31

K
Knowledge Base, 16

L
limited bandwidth, 21

M
maximum bandwidth, 24, 30

N
NP2 interface, 31

O
order of operations for shapers, 33

P
packet rates, 24
per policy shaper, 30
per-IP, 31
NP2 interface, 31
priority traffic, 30
product registration, 15

Q
quality of service, 19
queuing, 20

R
registering
with Fortinet Technical Support, 15
RFC
1918, 9
RFC 2474, 35
RFC 2475, 35
RFC 791, 34

S
shaper
   all policies, 30
   application control, 32
   firewall policy, 33
   per policy, 30
   per-IP, 31
   processing order, 33
   shared, 29
   shared shaper, 29

T
technical
   documentation, 16
   documentation conventions, 9
   notes, 16
   support, 16
   technical support, 16

ToS, 34
   byte value, 22
   mapping, 40
traffic
   policing, 20
   priority, 30
   reverse shaping, 34
   shaping, 20
Training Services, 16
   type of service, 34

V
   VDOM, 31
   virtual interfaces, 31
   VLAN, 31

X
   XSS, 14

Z
   zero bandwidth, 30