Traffic Shaping
FEATURE OVERVIEW AND CONFIGURATION GUIDE

Traffic Shaping Introduction

This guide describes the traffic shaping feature. Traffic shaping is a network traffic management technique that uses mechanisms to control how software forwarded packets are transmitted on your devices. This includes deciding which packets to transmit, in what order of priority, and at what rate on the output of an interface. Traffic shaping will allow you to optimize or guarantee performance, improve latency, and increase usable bandwidth for some kinds of packets by delaying other kinds.

Products and software version that apply to this guide

This guide applies to AlliedWare Plus™ products that support traffic shaping, running version 5.4.5 or later:

To see whether your product supports traffic shaping, see the following documents:

- The product’s Datasheet
- The AlliedWare Plus Datasheet
- The product’s Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Feature support may change in later software versions. For the latest information, see the above documents.
## Contents

Traffic Shaping Introduction............................................................................................................................. 1  
Products and software version that apply to this guide..................................................................................... 1  
What is Traffic Shaping?................................................................................................................................... 3  
How does Traffic Shaping work?........................................................................................................................ 5  
  Classification..................................................................................................................................................... 5  
  Queuing........................................................................................................................................................... 6  
  Dequeueing.................................................................................................................................................... 7  
  Properties of the default queue....................................................................................................................... 9  
Traffic Shaping Configuration.............................................................................................................................. 10  
  Rule Validity.................................................................................................................................................... 10  
  How to configure traffic shaping................................................................................................................... 11  
  Traffic shaping configuration examples........................................................................................................ 13  
  Show command examples.............................................................................................................................. 16
What is Traffic Shaping?

Traffic in a data network comprises a number of individual data flows. A data flow is a flow of data traffic that shares one or more common aspects, typically a common source/destination and purpose. These factors alone will generally determine the kind of network capability and performance required to transport it. Common aspects are bandwidth, security, reliability, transmission speed and delay.

To adequately cope with traffic requirements as flows move from high bandwidth and relatively secure networks, such as LANs, to low bandwidth and more exposed networks, such as WANs, mechanisms are required to prioritize these flows and assign them appropriately across the network resources available. Traffic shaping provides a method of achieving this.

Further improvements can be achieved if a gateway device between different zones is able to recognize the data flows that are passing through it, and apply policies that allocate resources to flows in a way that will best fit your organization’s data transmission needs.

This process of recognizing flows and appropriately allocating resources to them is known as traffic shaping.

Terms used in this guide:

<table>
<thead>
<tr>
<th>TERM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule</td>
<td>Traffic shaping is specified in the form of traffic shaping rules. Each rule specifies what traffic to match on, and how the matching traffic should be shaped. If you do not specify a rule ID, a number will be automatically generated and it will be greater than the current highest rule ID.</td>
</tr>
<tr>
<td>Filter</td>
<td>Filters match packets that are trying to egress an interface. Traffic shaping uses application rules to match on packets that have been marked and direct them to the correct egress queue.</td>
</tr>
<tr>
<td>Rate</td>
<td>This is equivalent to the Committed Information Rate (CIR). This is the bandwidth that traffic matching a traffic shaping rule is guaranteed to get (as long as the link is not oversubscribed).</td>
</tr>
<tr>
<td>Max</td>
<td>This is the maximum bandwidth that traffic matching a traffic shaping rule can get. If there is spare capacity on the link, traffic can exceed the rate, up to the ceiling value.</td>
</tr>
<tr>
<td>Virtual-bandwidth</td>
<td>Virtual-bandwidth is a way of limiting the egress rate on an interface without changing the line-rate. This might be done if you have a Ethernet connection to a modem, and do not want the modem to be queuing and dropping traffic because it is being sent packets to quickly.</td>
</tr>
<tr>
<td>Zone</td>
<td>A high level abstraction for a logical grouping of networks. This is the highest level of partitioning that traffic shaping policy can be applied to. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and a untrusted zone for the Internet. Other common zones are a Demilitarised Zone (DMZ) for publicly visible web servers and a Virtual Private Network zone for remote access users or tunnels to other networks.</td>
</tr>
<tr>
<td>Network</td>
<td>A high level abstraction for a logical network in a zone. This consists of the IP subnet and an interface over which it is reachable. In a small office, this may be only one subnet. In an enterprise there may be many private networks.</td>
</tr>
</tbody>
</table>
Traffic shaping involves creating rules for selecting particular traffic types and then applying actions specific to these types. Typically you would select traffic by its origin (source address), or where it is going (destination address), and then apply an action such as specifying the minimum bandwidth that this traffic type will be allocated.

The rule ID is used when trying to match a packet to a particular rule. This means that a packet will be matched by the rule with the lowest ID that it matches all of the parameters for. The priority parameter is used to determine the order that rules are examined for sending a packet out of a queue. The rule ID applies to classifying traffic, while the priority applies to dequeuing traffic.

After creating your rules, you can rearrange their order to match their processing priority and also delete rules that are no longer required.

By appropriately configuring the virtual bandwidth interface rate command, you can simulate a slower link without changing the line rate of the outgoing interface.

You can check your configurations by using the show commands. The show commands enable you to check if traffic shaping is enabled. You can display the rules that you have created, and information about invalid rules for problem solving. You can also display information about packet counters and traffic flow rates and check to see what interfaces that traffic shaping has been applied to.

<table>
<thead>
<tr>
<th>TERM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>A high level abstraction for a single node in a network. This consists of the single IP address that relates that node. This is commonly used if particular devices (e.g. servers) have static IP addresses and need to be specified in firewall or shaping policy.</td>
</tr>
<tr>
<td>Entity</td>
<td>A generic name for any of Zone, Network or Host. An entity is a reference to a single piece of the network (A host, a subnet, or an entire zone).</td>
</tr>
<tr>
<td>Application</td>
<td>A high level abstraction for the types of applications being transported by network traffic. Traffic matching the specified application is identified by the firewall using several different techniques. This can be by matching packets to static network parameters (e.g. FTP always used port 21) or by searching for application signatures in flows of packets (e.g. IRC traffic will have &quot;nick*user&quot; in the packet stream).</td>
</tr>
</tbody>
</table>
How does Traffic Shaping work?

There are three key steps in the traffic shaping process:

1. **Classification**—Recognising which packets belong to which flows or which classes of flow, and applying an internal marker to indicate their classification.

2. **Queuing**—collecting equally-classified packets into egress pipelines, so that different policies can be applied to different pipelines.

3. **Dequeuing**—pulling packets out of the queues, according to some algorithms, and sending them out onto the wire.

**Classification**

Data networks are notable for the immense variety of data communications that they multiplex. Therefore, the process of demultiplexing all the communication strands so that different policies can be applied to different strands is complex. There are such a range of different factors that can be used to differentiate between different flows.

But, the classification rules that are applied to the demultiplexing process must be comprehensible to users, as it is users that write the rules, in the form of configuration commands on the Next Generation Firewall device.

Therefore, AlliedWarePlus defines two concepts that assist with making the classification process comprehensible, and able to be configured in a tractable manner.

The concepts are: **Applications** and **Entities**.

**Applications** are quite a straightforward concept. Simply, these are the end-user application that is generating a data flow. A full list of applications can be displayed using the `show application` or `show application detail` command. Examples of applications are:

- FTP file transfer
- Skype voice call
- Email
- Web Browsing
- Facebook

The Next Generation Firewalls have a sophisticated Deep-packet inspection engine that use a range of rules to determine the application that generated any given packet. The rules can be as simple as "TCP destination port 25 = SMTP email", but in general they involve searching deep into the packet’s data payload to find byte patterns that are characteristic of different applications.
How does Traffic Shaping work?

An entity is an overall term for a network or network element that identifies where a packet has come from or where it is going to.

AlliedWare Plus defines three levels of entity:

- **Host**—the most granular level of entity is an individual network host. A host will be represented by its IP address.
- **Network**—the next level of granularity is a subnet (or collection of subnets) and the network interface via which it is accessed.
- **Zone**—a high level abstraction for a logical grouping of networks. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and an untrusted zone for the Internet. Other common zones are a Demilitarised Zone (DMZ) for publicly visible web servers and a Virtual Private Network zone for remote access users or tunnels to other networks.

AlliedWare Plus designates a data flow to be a series of packets, generated by an identified application, flowing from an identified source entity towards an identified destination entity.

For example, an:

- FTP file transfer from the Trusted Private Zone to the Untrusted Internet Zone
- Email from the Untrusted Internet Zone to a specific email server host in the DMZ zone
- RDP (Remote Desktop) connection from the VPN zone into the Trusted Private Zone

The classification process, therefore, is the process of classifying packets into these types of data flows. The user creates classification rules (we will look at the syntax of these rules further below) to instruct the traffic shaping policy which flows to look for. All packets that do not match any of the designated flows simply fall into the ‘everything else’ category.

**Queuing**

As each traffic classification rule is defined, the software creates a corresponding FIFO (first-in-first-out) queue to hold the packets that match the rule.

By separating the different classifications of packets out into different queues is a convenient way for the software to then apply the processes of bandwidth allocation, prioritization, throttling, and so on to each identified flow or set of flows separately.
How does Traffic Shaping work?

Each queue has a default capacity of 1000 packets. When a queue is full, any other packets that are classified into that queue are simply discarded.

Queues are associated with egress interfaces, as the purpose of the queues is to corral the packets in preparation for transmitting them out through an egress interface.

The interface to which any given rule's queue is associated is determined from the to entity in the rule, i.e., it is the interface that connects to that to entity. If there are multiple interfaces that connect to a given to entity (as can be the case when the to entity is a whole zone), then a separate queue is created on each of those interfaces.

There are some restrictions on the types of interfaces to which queues can be associated:

- Queues should not be associated with Tunnel interfaces. However, traffic being transmitted through a tunnel can still be shaped on the underlying physical interface via which the tunnel exits the Next Generation Firewall device, by matching on the tunnel encapsulated traffic.

- Queues are not associated with individual Ethernet sub-interfaces. Rather, they are associated with the parent interface. Therefore, to shape traffic using an Ethernet sub-interface, apply the rule (using the to entity) to the sub-interface. This allows the classification to work on the sub-interface. However, the queue will be managed on the parent interface.

- It is unlikely that you will want to shape traffic using a VLAN as the outgoing interface, as the LAN side of the router tends to be bandwidth rich compared to the WAN. If you do, you should keep in mind that the link between the CPU and the switch ports on the router is 1Gb/s. Therefore, if you have multiple VLANs, it is easily possible to oversubscribe this link.

Traffic using a bridge interface cannot be shaped. This is because the device does not check Layer 3 parameters of traffic being bridged, so traffic shaping rules cannot be matched.

Default queue

Every interface has a default queue associated with it, in addition to any queues that are created due to classification rules. The purpose of the default queue is to hold the 'everything else' traffic that does not match any of the classification rules.

Dequeuing

It is in the dequeuing process that the shaping really occurs.

With the packets classified, and stored in their respective egress queues, the software can then apply the shaping rules to service the queues (take packets from the queues and put them onto the wire) in the manner that best suits the organization’s needs. Traffic shaping uses Hierarchical Token Bucket (HTB) queues to shape the traffic as it is dequeued.

For more information on HTB, see: Hierarchical Token Bucket.
Before discussing the dequeuing process itself, there are a number of traffic management mechanisms that need to be introduced.

- **Rate**: The reserved bandwidth that is set aside for a given queue. This is the amount of bandwidth that the queue is guaranteed to have access to (provided the total sum of reserved bandwidths configured for queues on a given interface does not exceed the capacity of the interface).

- **Max**: The maximum bandwidth that a given queue can use. If there is spare capacity on the link, then the queue can exceed its configured rate (reserved bandwidth), but only up to the ceiling value.

- **Priority**: This determines the order in which queues are serviced. Queues with a lower priority will be dequeued first, provided they have not exceeded their allocated bandwidth. So, if a high-priority queue (one with a low priority value) has packets sitting in it, and it is not currently exceeding its allocated bandwidth limit, then it will be serviced before lower-priority queues that might have packets sitting in them. The purpose of this is to provide low latency to flows that need low latency (like voice conversations) by minimising the amount of time that the flow’s packets spend sitting around in egress queues.

- **Virtual bandwidth**: There are circumstances in which, for traffic shaping purposes, it is useful to treat an interface as though its bandwidth were less than its actual bandwidth.

The most common such circumstance is the case where a device is connected by Ethernet to a modem or low-end router, which in turn is connected to a lower-bandwidth WAN link. If the data rate being sent out the Ethernet interface toward the modem/router exceeds the capacity of the WAN link, then the modem/router will drop packets. If that low-end device has little traffic management capability, then the packets will just be dropped in an uncontrolled manner.
How does Traffic Shaping work?

However, if the egress bandwidth of the intelligent device’s Ethernet interface is artificially limited to the bandwidth of the downstream WAN link, then the packet dropping will be performed, in a controlled manner, in the intelligent device.

The artificial lowering of an interface’s bandwidth is referred to as applying a virtual bandwidth.

Properties of the default queue

It might be natural to expect that the default queue is treated in a ‘you will get looked at when everybody else is empty’ manner. But, in fact, that is not the case. By default the default queue has a priority of 4. So, the default queue can sit somewhere in the middle of the mix with all the other queues.

From the bandwidth limit point of view, the default queue is allocated a rate that is determined by what is left over from all the other queues’ configured rates.

The formula for calculating the rate for the default queue is:

1. Take the interface’s egress bandwidth.
2. Subtract 5% (just to give some margin of error, so that the sum of all the rates does not quite fill the whole egress bandwidth).
3. Add up all the rate values configured on all the other queues on the same interface.
4. Subtract that sum off the other queues’ rates.
5. The default queue’s rate is whatever is left.

This means:
- Default queue’s rate = interface bandwidth – 5% - (sum of all the other queues’ rates)

If the interface has been configured with a virtual bandwidth, then the calculation is different:
- Default queue’s rate = virtual bandwidth - (sum of all the other queues’ rates)

**Note:** The extra 5% is not subtracted in this case, as the virtual bandwidth is already providing a buffer that prevents the whole interface from being oversubscribed.
Traffic Shaping Configuration

Traffic shaping is configured by defining a set of traffic shaping rules. Each rule defines:

- The rule ID
- The application to match
- The entity that the traffic is coming from
- The entity that the traffic is travelling to
- A reserved rate for the traffic
- A maximum rate for the traffic
- A priority for the queue

Packets are classified against each rule in order, using the rule ID. Once a packet has been successfully matched against a rule, it is not checked against any other rules. Therefore packets matching multiple rules will be shaped according to the rule with the lowest ID. Each rule creates a queue on the outgoing interface which is associated with the to entity. If there is more than one interface specified in that entity, traffic shaping will create a queue on each interface. The Rule ID parameter does not influence dequeuing. The order that rules are dequeued is only influenced by the rules priority.

Rule validity

Shaping rules must be valid. Rules that are not valid will not be applied to egress interfaces, and will not have any impact on traffic flow.

To be valid, a rule has to meet certain criteria:

- If the maximum rate for the rule is not specified, it defaults to the reserved rate of the rule
- If the priority of the rule is not specified, it defaults to 4
- The application the rule references must exist, or it must be the special case any
- The application the rule references must have a protocol, or a mark provided by deep packet inspection (DPI)
- The source entity the rule references must exist
- The source entity the rule references must have either an IPv4 or and IPv6 address
- If the source entity the rule references has an interface, the interface must exist
- The destination entity the rule references must exist
- The destination entity the rule references must have either an IPv4 or IPv6 address
- The destination entity the rule references must have an interface configured for each subnet
- The destination entity the rule references must only reference valid interfaces

The source entity and the destination entity must both reference the same address family i.e. they both have to have IPv4 addresses, or both have IPv6 address
# How to configure traffic shaping

Enable traffic shaping from global configuration mode. From traffic shaping mode you can then create your rules for particular traffic types and then apply specific actions to the traffic types.

After you have created your rules you can rearrange the order that they run, and if required you can remove rules that are no longer needed.

Now that you have created and edited your rules, you can configure the virtual bandwidth if required. The virtual bandwidth can be removed if required using the `no` variant of this command.

Run the `show` commands to check your traffic shaping configurations and edit as required.

## Step 1. Create your traffic shaping rule

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>awplus# configure terminal</code></td>
<td>Enter Configuration mode.</td>
</tr>
<tr>
<td><code>awplus(config)# traffic-shaping</code></td>
<td>Enter traffic shaping mode.</td>
</tr>
<tr>
<td><code>awplus(config-ts)# rule [&lt;ID&gt;] match &lt;application_name&gt; from &lt;source_entity&gt; to &lt;destination_entity&gt; rate &lt;1-100000000&gt; [max &lt;1-100000000&gt;] [priority &lt;0-7&gt;]</code></td>
<td>Enter your traffic shaping rule specifying the rule ID, application name, source entity, destination entity, rate, maximum rate and queue priority. If you do not specify a rule ID, a number will be automatically generated and it will be greater than the current highest rule ID.</td>
</tr>
</tbody>
</table>

## Step 2. Change the order of your rules if required

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>awplus(config-ts)# move rule &lt;10-65535&gt; to 10-65535&gt;</code></td>
<td>Enter this move command to rearrange the order of your rules. Specify your rule IDs to change the order of processing.</td>
</tr>
</tbody>
</table>

## Step 3. Remove a rule

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`awplus(config-ts)# no rule {&lt;ID&gt;</td>
<td>all}`</td>
</tr>
</tbody>
</table>

## Step 4. Configure virtual bandwidth

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>awplus(config-ts)# virtual-bandwidth interface &lt;interface-name&gt; rate &lt;1-100000000&gt;</code></td>
<td>Enter the interface name and the rate.</td>
</tr>
<tr>
<td><code>awplus(config-ts)# no virtual-bandwidth interface &lt;interface-name&gt;</code></td>
<td>Use the <code>no</code> variant of the virtual-bandwidth command to remove the virtual bandwidth configuration.</td>
</tr>
</tbody>
</table>
### Step 5: Run show commands to check your configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show traffic-shaping</code></td>
<td>Enter the show traffic-shaping command to check if traffic shaping is enabled or disabled.</td>
</tr>
<tr>
<td><code>show traffic-shaping rule</code></td>
<td>Enter the show traffic-shaping rule command to display your rules.</td>
</tr>
<tr>
<td><code>show traffic-shaping rule config-check</code></td>
<td>Enter this command to display information about invalid rules.</td>
</tr>
<tr>
<td><code>show traffic-shaping rule counters</code></td>
<td>Enter this command to show your packet counters and traffic flow rate.</td>
</tr>
</tbody>
</table>
## Traffic shaping configuration examples

### Example 1:
This example shows how to create a rule to reserve a minimum bandwidth of 100 Kbps for SSH traffic between WAN and private networks with a priority of 2. First the zones LAN and WAN are created, with a single subnet in each. Then the shaping rule is added in traffic-shaping mode.

```
awplus# configure terminal

awplus(config)# zone lan

awplus(config-zone)# network all

awplus(config-network)# ip subnet 172.168.10.0/24

awplus(config)# zone wan

awplus(config-zone)# network remote-office-10

awplus(config-network)# ip subnet 172.168.20.0/24 eth1

awplus(config-network)# traffic-shaping

awplus(config-ts)# rule 3 match ssh from lan to wan
rate 100 max 1000 priority 2

awplus# configure terminal

awplus(config)# zone internet

awplus(config-zone)# network all

awplus(config-network)# 0.0.0.0/0 interface eth1

awplus(config-network)# traffic-shaping

awplus(config-ts)# rule 5 match ftp from lan to internet rate 1 max 10000 priority 7
```

### Example 2:
This example shows how to create a rule to stop ftp traffic from blocking other outbound traffic, while still letting it use the full 10Mb link.

```
awplus# configure terminal

awplus(config)# zone internet

awplus(config-zone)# network all

awplus(config-network)# 0.0.0.0/0 interface eth1

awplus(config-network)# traffic-shaping

awplus(config-ts)# rule 5 match ftp from lan to internet rate 1 max 10000 priority 7
```
Example 3: This example shows how to create a rule to reserve 3MB for CustomerA trying to reach the Internet from the predefined zones as in the example above.

```bash
awplus(config-network)# configure terminal
awplus(config-network)# traffic-shaping
awplus(config-ts)# rule 7 match any from customerA to internet rate 3000
```

Example 4: This example shows how to create a rule to shape all traffic flowing from the predefined common zone to the predefined WAN zone to have a data rate of 5Mbps with a maximum rate of 10Mbps.

```bash
awplus(config-network)# configure terminal
awplus(config-network)# traffic-shaping
awplus(config-ts)# rule 9 match any from lan to wan rate 5000 max 10000
```

Example 5: This example shows creating a rule to shape ftp traffic, so that it does not starve other traffic classes on a 10Mb link.

```bash
awplus(config-network)# configure terminal
awplus(config-network)# traffic-shaping
awplus(config-ts)# rule 30 match ftp from common to wan rate 1 max 10000 priority 7
```

Example 6: This example shows how to rearrange the processing order of existing rules. Rule 3 will be processed after rule 5.

```bash
awplus(config-ts)# move rule 3 to 5
```

Example 7: This example shows how to delete rule 25 only.

```bash
awplus(config-ts)# no rule 25
```
Example 8: This example shows how to delete all existing rules.

```
awplus(config-ts)#
no rule all
```
Enter the `all` parameter to delete all rules.

Example 9: This example shows how to configure the virtual bandwidth in eth1 to 10Mb.

```
awplus(config-ts)#
virtual-bandwidth interface eth1 rate 10000
```
Enter the interface name and rate.

Example 10: This example shows how to remove the virtual bandwidth configuration.

```
awplus(config-ts)#
no virtual-bandwidth interface eth1
```
Enter the `no` variant of the virtual bandwidth command and the interface name.

After completing and editing your traffic shaping rules, exit out of traffic shaping mode and global configuration mode so you can run the `show` commands to check your configuration.

```
alplus(config-ts)#
exit
```
Enter exit to come out of traffic-shaping mode.

```
awplus(config)#
exit
```
Enter exit to exit out of Global Configuration mode.
**Show command examples**

Use the `show traffic-shaping` command to check if traffic shaping is enabled or disabled.

**Figure 1: Example output from the show traffic-shaping command**

```
awplus# show traffic-shaping
Traffic shaping is disabled
4 rules configured (3 valid rules)
Virtual-bandwidth configured on 1 interfaces
```

This example shows the output of the `show traffic-shaping rule` command displaying all of the configured rules. This output is showing rule 40 as invalid with a message instructing you to run the `show traffic-shaping rule config-check` command to find out why the rule is invalid.

**Figure 2: Example output from the show traffic-shaping rule command**

```
[* = Rule is not valid - see "show traffic-shaping rule config-check"]

<table>
<thead>
<tr>
<th>ID</th>
<th>App</th>
<th>From</th>
<th>To</th>
<th>Rate</th>
<th>Maximum</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>any</td>
<td>common</td>
<td>wan</td>
<td>5000</td>
<td>5000</td>
<td>4</td>
</tr>
<tr>
<td>15</td>
<td>any</td>
<td>health</td>
<td>wan</td>
<td>3000</td>
<td>5000</td>
<td>2</td>
</tr>
<tr>
<td>20</td>
<td>any</td>
<td>health</td>
<td>common</td>
<td>2000</td>
<td>2000</td>
<td>7</td>
</tr>
<tr>
<td>30</td>
<td>any</td>
<td>common</td>
<td>common</td>
<td>10000</td>
<td>10000</td>
<td>4</td>
</tr>
<tr>
<td>*40</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>10000</td>
<td>10000</td>
<td>4</td>
</tr>
<tr>
<td>50</td>
<td>any</td>
<td>wan</td>
<td>common</td>
<td>1000</td>
<td>5000</td>
<td>1</td>
</tr>
</tbody>
</table>
```

This example shows the output of the `show traffic-shaping rule config-check` command and displays information about invalid rules. Rule 40 is invalid for the reasons displayed.

**Figure 3: Example output from the show traffic-shaping rule config-check command**

```
awplus# show traffic-shaping rule config-check
Rule 40:
  "From" entity does not exist
  "To" entity does not exist
```
This example shows the output of the **show traffic-shaping rule counters** command and displays your packet counters and traffic flow rate.

**Figure 4: Example output from the show traffic-shaping rule counters command**

```
awplus# show traffic-shaping rule counters
Interface eth1:
Default Queue:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
Rule 10:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
Rule 15:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
Rule 20:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
Rule 30:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
Rule 50:
  0 packets sent, 0 bytes sent, 0 packets dripped
  Rate: 0 pps, 0 kbps
```

This example shows the **show traffic-shaping interface** command and the output to check that the shaping configuration has been applied to an interface.

**Figure 5: Example output from the show traffic-shaping interface command**

```
awplus# show traffic-shaping interface
Interface eth1:
  Interface bandwidth: 1000000kbps
  Shaped bandwidth: 950000kbps
  Reserved bandwidth: 21000kbps
  Default queue bandwidth: 929000kbps
```

This example shows the final traffic shaping configuration.

**Figure 6: Example output from the show running-config traffic-shaping command**

```
awplus#show running-config traffic-shaping
traffic-shaping
  virtual-bandwidth interface eth1 rate 10000
  rule 3 match ssh from wan to private rate 100 max 1000 priority 2
  rule 5 match ftp from lan to internet rate 1 max 10000 priority 7
  rule 7 match any from customerA to internet rate 3000
  rule 9 match any from lan to wan rate 5000 max 10000
  rule 30 match ftp from common to wan rate 1 max 10000 priority 7
```