Chapter 7
Traffic Shaping

This chapter discusses the various ways you can use your Juniper Networks security device to manage limited bandwidth without compromising quality and availability of the network to all of your users. It contains the following sections:

- “Managing Bandwidth at the Policy Level” on this page
- “Setting Traffic Shaping” on page 194
- “Setting Service Priorities” on page 198
- “Setting Priority Queuing” on page 199
- “Ingress Policing” on page 203
- “Shaping Traffic on Virtual Interfaces” on page 203
- “DSCP Marking and Shaping” on page 214

Traffic shaping is the allocation of the appropriate amount of network bandwidth to every user and application on an interface. The appropriate amount of bandwidth is defined as cost-effective carrying capacity at a guaranteed Quality of Service (QoS). You use a security device to shape traffic by creating policies and by applying appropriate rate controls to each class of traffic going through the device.

Managing Bandwidth at the Policy Level

To classify traffic, you create policies and specify the amount of guaranteed bandwidth and maximum bandwidth, and the priority for each class of traffic. Guaranteed bandwidth and maximum bandwidth are not strictly policy based but, with multiple physical interfaces in the egress zone, are based on both policy and total egress physical interface bandwidth available. The physical bandwidth of every interface is allocated to the guaranteed bandwidth parameter for all policies. If there is any bandwidth left over, it is sharable by any other traffic. In other words, each policy gets its guaranteed bandwidth and shares whatever is left over, on a priority basis (up to the limit of its maximum bandwidth specification), with all other policies.
The traffic-shaping function applies to traffic from all policies. If you turn off traffic shaping for a specific policy, while traffic shaping is still turned on for other policies, the system applies a default traffic-shaping policy to that particular policy, with the following parameters:

- Guaranteed bandwidth 0
- Unlimited maximum bandwidth
- Priority of 7 (the lowest priority setting)

**NOTE:** You can enable a mapping of priority levels to the DiffServ Codepoint Marking system. For more information about DS Codepoint Marking, see “Traffic Shaping” on page 173.

If you do not want the system to assign this default traffic-shaping policy to policies for which you have turned off traffic shaping, you can turn off traffic shaping system wide via the CLI command: `set traffic-shaping mode off`. Use the CLI command: `set traffic-shaping mode on` to turn on shaping on an interface. Or, you can set traffic shaping to automatic in the WebUI: **Configuration > Advanced > Traffic Shaping**. This allows the system to turn on traffic shaping when a policy requires it and to turn off traffic shaping when policies do not require it.

### Setting Traffic Shaping

In this example, you partition 45Mbps of bandwidth on a T3 interface among three departments on the same subnet. The interface ethernet0/1 is bound to the Trust zone, and ethernet0/3 is bound to the Untrust zone.

**Figure 62: Traffic Shaping**
**WebUI**

1. **Bandwidth on Interfaces**
   
   Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:
   
   Traffic Bandwidth: 45000

   ____
   
   **NOTE:** If you do not specify bandwidth settings on an interface, the security device uses the available physical bandwidth.

   Network > Interfaces > Edit (for ethernet0/3): Enter the following, then click OK:
   
   Traffic Bandwidth: 45000

2. **Bandwidth in Policies**

   Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:
   
   Name: Marketing Traffic Shaping
   Source Address:
     Address Book Entry: (select), Marketing
   Destination Address:
     Address Book Entry: (select), Any
   Service: Any
   Action: Permit
   VPN Tunnel: None

   ____
   
   **NOTE:** You can also enable traffic shaping in policies referencing VPN tunnels.

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:
   
   Traffic Shaping: (select)
     Guaranteed Bandwidth: 10000
     Maximum Bandwidth: 15000

   Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:
   
   Name: Sales Traffic Shaping Policy
   Source Address:
     Address Book Entry: (select), Sales
   Destination Address:
     Address Book Entry: (select), Any
   Service: Any
   Action: Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:
   
   Traffic Shaping: (select)
     Guaranteed Bandwidth: 10000
     Maximum Bandwidth: 10000
Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

Name: Support Traffic Shaping Policy
Source Address:
  Address Book Entry: (select), Support
Destination Address:
  Address Book Entry: (select), Any
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

  Traffic Shaping: (select)
  Guaranteed Bandwidth: 5000
  Maximum Bandwidth: 10000

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Allow Incoming Access to Marketing
Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Marketing
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

  Traffic Shaping: (select)
  Guaranteed Bandwidth: 10000
  Maximum Bandwidth: 10000

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Allow Incoming Access to Sales
Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Sales
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

  Traffic Shaping: (select)
  Guaranteed Bandwidth: 5000
  Maximum Bandwidth: 10000
Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Allow Incoming Access to Support
Source Address:
  Address Book Entry: (select), Any
Destination Address:
  Address Book Entry: (select), Support
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

  Traffic Shaping: (select)
  Guaranteed Bandwidth: 5000
  Maximum Bandwidth: 5000

**CLI**

To enable traffic shaping by policy, do the following:

1. **Bandwidth on Interfaces**
   set interface ethernet0/1 bandwidth 45000
   set interface ethernet0/3 bandwidth 45000

   **NOTE:** If you do not specify bandwidth settings on an interface, the security device uses the available physical bandwidth.

2. **Bandwidth in Policies**
   set policy name “Marketing Traffic Shaping” from trust to untrust marketing any any permit traffic gbw 10000 priority 0 mbw 15000
   set policy name “Sales Traffic Shaping Policy” from trust to untrust sales any any permit traffic gbw 10000 priority 0 mbw 10000
   set policy name “Support Traffic Shaping Policy” from trust to untrust support any any permit traffic gbw 5000 priority 0 mbw 10000
   set policy name “Allow Incoming Access to Marketing” from untrust to trust any marketing any permit traffic gbw 10000 priority 0 mbw 10000
   set policy name “Allow Incoming Access to Sales” from untrust to trust any sales any permit traffic gbw 5000 priority 0 mbw 10000
   set policy name “Allow Incoming Access to Support” from untrust to trust any support any permit traffic gbw 5000 priority 0 mbw 5000

   save
Setting Service Priorities

The traffic-shaping feature on Juniper Networks security devices allows you to perform priority queuing on the bandwidth that is not allocated to guaranteed bandwidth, or unused guaranteed bandwidth. Priority queuing is a feature that allows all your users and applications to have access to available bandwidth as they need it, while ensuring that important traffic can get through, if necessary at the expense of less important traffic. Queuing allows the security device to buffer traffic in up to eight different priority queues. These eight queues are:

- High priority
- 2nd priority
- 3rd priority
- 4th priority
- 5th priority
- 6th priority
- 7th priority
- Low priority (default)

The priority setting for a policy means that the bandwidth not already guaranteed to other policies is queued on the basis of high priority first and low priority last. Policies with the same priority setting compete for bandwidth in a round robin fashion. The security device processes all of the traffic from all of the policies with high priority before processing any traffic from policies with the next lower priority setting, and so on, until all traffic requests have been processed. If traffic requests exceed available bandwidth, the lowest priority traffic is dropped.

**CAUTION:** Be careful not to allocate more bandwidth than the interface can support. The policy configuration process does not prevent you from creating unsupported policy configurations. You can lose data if the guaranteed bandwidth on contending policies surpasses the traffic bandwidth set on the interface.

If you do not allocate any guaranteed bandwidth, then you can use priority queuing to manage all of traffic on your network. That is, all high priority traffic is sent before any 2nd priority traffic is sent, and so on. The security device processes low priority traffic only after all other traffic has been processed.
Setting Priority Queuing

In this example, you configure the guaranteed and maximum bandwidth (in Mbps) for three departments—Support, Sales, and Marketing—as shown in Table 30.

<table>
<thead>
<tr>
<th></th>
<th>Outbound Guaranteed</th>
<th>Inbound Guaranteed</th>
<th>Combined Guaranteed</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support</td>
<td>5</td>
<td>5</td>
<td>10</td>
<td>High</td>
</tr>
<tr>
<td>Sales</td>
<td>2.5</td>
<td>3.5</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>Marketing</td>
<td>2.5</td>
<td>1.5</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>10</td>
<td>20</td>
<td></td>
</tr>
</tbody>
</table>

If all three departments send and receive traffic concurrently through the firewall, the security device must allocate 20 Mbps of bandwidth to fulfill the guaranteed policy requirements. The interface ethernet0/1 is bound to the Trust zone, and ethernet0/3 is bound to the Untrust zone.

Figure 63: Priority Queuing

WebUI

1. **Bandwidth on Interfaces**
   Interfaces > Edit (for ethernet0/1): Enter the following, then click **OK**:
   Traffic Bandwidth: 40000

   Interfaces > Edit (for ethernet0/3): Enter the following, then click **OK**:
   Traffic Bandwidth: 40000
2. **Bandwidth in Policies**

   Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

   - **Name:** Sup-out
   - **Source Address:**
     - Address Book Entry: (select), Support
   - **Destination Address:**
     - Address Book Entry: (select), Any
   - **Service:** Any
   - **Action:** Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   - **Traffic Shaping:** (select)
   - **Guaranteed Bandwidth:** 5000
   - **Maximum Bandwidth:** 40000
   - **Traffic Priority:** High priority
   - **DiffServ Codepoint Marking:** (select)

---

**NOTE:** Differentiated Services (DS) is a system for tagging (or “marking”) traffic at a position within a hierarchy of priority. DS Codepoint Marking maps the ScreenOS priority level of the policy to the first three bits of codepoint in the DS field in the IP packet header. For more information about DS Codepoint Marking, see “Traffic Shaping” on page 173.

---

Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

   - **Name:** Sal-out
   - **Source Address:**
     - Address Book Entry: (select), Sales
   - **Destination Address:**
     - Address Book Entry: (select), Any
   - **Service:** Any
   - **Action:** Permit

   > Advanced: Enter the following, then click **Return** to set the advanced options and return to the basic configuration page:

   - **Traffic Shaping:** (select)
   - **Guaranteed Bandwidth:** 2500
   - **Maximum Bandwidth:** 40000
   - **Traffic Priority:** 2nd priority
   - **DiffServ Codepoint Marking:** Enable
Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

Name: Mar-out
Source Address:
    Address Book Entry: (select), Marketing
Destination Address:
    Address Book Entry: (select), Any
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

Traffic Shaping: (select)
Guaranteed Bandwidth: 2500
Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (select)

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Sup-in
Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), Support
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

Traffic Shaping: (select)
Guaranteed Bandwidth: 5000
Maximum Bandwidth: 40000
Traffic Priority: High priority
DiffServ Codepoint Marking: (select)

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Sal-in
Source Address:
    Address Book Entry: (select), Any
Destination Address:
    Address Book Entry: (select), Sales
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

Traffic Shaping: (select)
Guaranteed Bandwidth: 3500
Maximum Bandwidth: 40000
Setting Priority Queuing

Traffic Priority: 2nd priority
DiffServ Codepoint Marking: (select)

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

Name: Mar-in
Source Address:
   Address Book Entry: (select), Any
Destination Address:
   Address Book Entry: (select), Marketing
Service: Any
Action: Permit

> Advanced: Enter the following, then click Return to set the advanced options and return to the basic configuration page:

Traffic Shaping: (select)
   Guaranteed Bandwidth: 1500
   Maximum Bandwidth: 40000
Traffic Priority: 3rd priority
DiffServ Codepoint Marking: (select)

CLI

1. Bandwidth on Interfaces
   set interface ethernet0/1 bandwidth 40000
   set interface ethernet0/3 bandwidth 40000

2. Bandwidth in Policies
   set policy name sup-out from trust to untrust support any any permit traffic gbw 5000 priority 0 mbw 40000 enable
   set policy name sal-out from trust to untrust sales any any permit traffic gbw 2500 priority 2 mbw 40000 dscp enable
   set policy name mar-out from trust to untrust marketing any any permit traffic gbw 1500 priority 3 mbw 40000 dscp enable

   set policy name sup-in from untrust to trust any support any permit traffic gbw 5000 priority 0 mbw 40000 dscp enable
   set policy name sal-in from untrust to trust sales any permit traffic gbw 3500 priority 2 mbw 40000 dscp enable
   set policy name mar-in from untrust to trust any marketing any permit traffic gbw 1500 priority 3 mbw 40000 dscp enable
   save

NOTE: Some devices require that you explicitly enable DSCP marking by setting a system-wide environmental variable. Refer to your hardware manual to find out if your device requires that you explicitly enable DSCP marking before using it in policies. If your device requires it, use the following command to enable DSCP marking system wide: set envar ipsec-dscp-mark = yes. This variable cannot be set using the WebUI. Use the unset envar ipsec-dscp-mark to disable DSCP marking system wide.
Ingress Policing

Ingress policing is traffic control at the ingress side of the security device. By constraining the flow of traffic at the point of ingress, traffic exceeding your bandwidth setting is dropped with minimal processing, conserving system resources. You can configure ingress policing at the interface level and in security policies.

You configure ingress policing on an interface by setting a maximum bandwidth (the mbw keyword). The following command, for example, limits bandwidth on ethernet0/1, the ingress interface, to 22 Mbps:

```
set interface ethernet0/1 bandwidth ingress mbw 22000
```

Incoming traffic on ethernet0/1 exceeding this bandwidth is dropped. If you set traffic shaping at the interface, you must also set traffic-shaping mode to on (`set traffic-shaping mode on`).

To apply ingress policing to a specific application, however, requires a policy. The following command creates a policy called `my_ftp` that limits FTP bandwidth on the ingress side of the security device to 10 Mbps:

```
set policy my_ftp from untrust to trust any any ftp permit traffic pbw 10000
```

Incoming FTP traffic exceeding the configured policing bandwidth (the pbw keyword) is dropped. You can also set mbw in the policy, but at the policy level mbw applies only to the egress side of traffic flow—traffic exceeding your configured rate is still processed, and is dropped only at the egress side (see Figure 65, “Traffic-Shaping Packet Flow” on page 206). You can configure mbw or pbw in a policy, but not both.

Configuration and enforcement of ingress policing on virtual interfaces is the same as on physical interfaces, with the one exception that you can also configure guaranteed bandwidth (the gbw keyword) on virtual interfaces (see Policy-Level Traffic Shaping on page 205). On physical interfaces, guaranteed bandwidth is the same as maximum bandwidth.

**NOTE:** Ingress policing on tunnel interfaces is enforced after the encrypted packets are decrypted by the VPN engine.

Shaping Traffic on Virtual Interfaces

In the context of traffic shaping, the term virtual interfaces refers only to subinterfaces and tunnel interfaces—not to other types of virtual interfaces, such as virtual security interfaces (VSI), or aggregate or redundant interfaces. You cannot configure shaping parameters in policies created in a vsys. Similarly, bandwidth cannot be shaped on interfaces owned (inherited) by a user-created vsys. See Volume 10: Virtual Systems for more information.

Traffic shaping (as distinct from ingress policing) concerns traffic management at the egress side of the security device. As with physical interfaces, you shape traffic on virtual interfaces by setting bandwidth values at the interface level, and in policies.
**Interface-Level Traffic Shaping**

Traffic shaping at the interface level is control of the minimum and maximum rate of traffic flow on a specific interface. You control minimum bandwidth by specifying a guaranteed bandwidth (\( \text{gbw} \)). This means that no matter what else happens on the device, this minimum rate is guaranteed to the appropriate traffic. The maximum bandwidth (\( \text{mbw} \)) you set establishes the rate traffic can never exceed. By default, maximum bandwidth on a physical interface is the carrying capacity of the interface; therefore, you cannot set guaranteed bandwidth on the physical interface.

In the context of traffic shaping, the term virtual interfaces refers to subinterfaces bound to physical interfaces and, by extension, tunnel interfaces bound to those subinterfaces—creating a hierarchy of interfaces. A subinterface bound to a physical interface is said to be the child of the physical interface, its parent. Accordingly, a tunnel interface bound to a subinterface is the child of that subinterface, the physical interface being its grandparent. Figure 64 on page 204 illustrates these dependencies.

**Figure 64: Interface Hierarchy**

When working with virtual interfaces, bear in mind the following rules of interface hierarchy:

- Guaranteed bandwidth allocated to subinterfaces cannot be greater than the carrying capacity of the physical interface they are bound to. In Figure 64, for example, the combined \( \text{gbw} \) of ethernet0/1.1 and ethernet0/1.2 is 7000 Kbps, 3000 Kbps below the \( \text{mbw} \) of ethernet0/1. Note, however, that the combined maximum bandwidth of these two subinterfaces exceeds the carrying capacity of the physical interface they are bound to by 2000 Kbps. This is acceptable because the \( \text{mbw} \) keyword is used only to limit traffic to a maximum rate. If traffic falls below a maximum setting on a subinterface, that bandwidth is available to any other subinterface bound to the same physical interface.

- Guaranteed bandwidth allocated to tunnel interfaces cannot be greater than the guaranteed bandwidth of the subinterface they are bound to.

- If guaranteed bandwidth is not configured for the immediate parent, bandwidth is taken from the grandparent interface.

- Total guaranteed bandwidth of children cannot exceed parent guaranteed bandwidth.
Child maximum bandwidth cannot exceed parent maximum bandwidth.

As already stated, you cannot configure guaranteed bandwidth on physical interfaces because guaranteed bandwidth is the same as maximum bandwidth, which is the link speed of the interface. On virtual interfaces, however, you can configure egress `gbw` and `mbw`. You can also configure ingress `mbw`, which is ingress policing at the interface level. The following command guarantees a minimum out-going bit rate of 1000 Kbps on ethernet0/4.1, and a maximum rate, both incoming and outgoing, of 2000 Kbps:

```
set interface ethernet0/4.1 bandwidth egress gbw 1000 mbw 2000 ingress mbw 2000
```

You set bandwidth in the WebUI on the Network > Interfaces > Edit page.

After setting bandwidth, you use the `get traffic-shaping interface` command to see the actual bandwidth flowing through the security device. For example, you might have traffic entering on ethernet0/1 and exiting on ethernet0/3. If you set ingress bandwidth on ethernet0/1, the command `get traffic-shaping interface ethernet0/3` will show actual throughput on the device.

If you set traffic shaping at the interface, you must also set traffic-shaping mode to on (`set traffic-shaping mode on`).

### Policy-Level Traffic Shaping

You shape traffic at the policy level to allocate bandwidth for particular types of traffic. The following command guarantees a minimum 1Mbps bandwidth to FTP traffic, and drops any traffic exceeding 2 Mbps:

```
set policy from trust to untrust any any ftp permit traffic gbw 1000 pbw 2000
```

Note that this command uses the policing bandwidth (`pbw`) keyword. You can use `pbw` or `mbw` in a policy, but not both. The advantage to using `pbw` is that traffic is dropped at the ingress side of the security device, reducing throughput processing and conserving system resources. (See “Ingress Policing” on page 203.)

In the WebUI, after creating a policy, click the Advanced button to configure traffic-shaping parameters.

Although you must set traffic-shaping mode to on to shape traffic on interfaces, it is not necessary to turn on traffic shaping when shaping traffic in policies. This is because traffic-shaping mode is set to auto by default. When a session becomes active and policy lookup discovers traffic shaping, ScreenOS turns on traffic shaping for that session.
Packet Flow

Figure 65 illustrates the part of the packet flow through the security device that is affected by traffic shaping and policing. (See “Packet-Flow Sequence” on page 10 for a complete picture of packet flow.) Packets exceeding pbw (or mbw configured at the interface) are dropped at step 9; shaping and DSCP marking occur at step 10, and packets exceeding mbw (configured in a policy) are dropped at step 11.

Figure 65: Traffic-Shaping Packet Flow

Example: Route-Based VPN with Ingress Policing

This example illustrates how to enforce ingress policing at the interface level for encrypted traffic. Ingress policing is configured on both the subinterface (ethernet0/2.1, maximum bandwidth: 1200 Kbps) and the tunnel interface (tunnel.1, maximum bandwidth: 1000 Kbps). You set the policing rate on the subinterface higher than on the tunnel interface bound to it to allow for the overhead of encryption (assuming, in this example, that all traffic received on the subinterface is meant for the tunnel interface). Policing on the subinterface is applied to the encrypted packets, while policing on the tunnel interface is applied to the decrypted inner packets. All encrypted traffic over 1200 Kbps on ethernet0/2.1 is dropped. And all decrypted (clear text) traffic over 1000 Kbps on the tunnel.1 interface is dropped.

Figure 66: Route-Based VPN
**WebUI (Configuration for Device1)**

1. **Interfaces**
   - Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:
     - IP Address/Netmask: 10.1.1.1/24
     - Zone: Trust
   - Network > Interfaces > Sub-IF > New: Enter the following, then click Apply:
     - Interface Name: (Select) ethernet0/2 and enter: 1
     - Zone: Untrust
     - IP Address/Netmask: 2.2.2.1/24
     - VLAN Tag: 128
   - Network > Interfaces > New Tunnel IF: Enter the following, then click Apply:
     - Tunnel Interface Name: 1
     - Zone: Untrust
     - Unnumbered (select) ethernet0/2.1
     - Interface: ethernet0/2.1

2. **Route**
   - Network > Routing > Destination > trust-vr New: Enter the following, then click OK:
     - Network Address/Netmask: 10.2.0.0/24
     - Interface (select): Tunnel.1

3. **IKE**
   - VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click OK:
     - Gateway Name: device1_ike
     - Security Level: Standard
     - Remote Gateway Type:
       - Static IP Address: (select), IP Address/Hostname: 2.2.2.2
     - Preshared Key
       - Preshared Key: secret
       - Outgoing Interface: ethernet0/2.1
   - VPNs > AutoKey IKE New: Enter the following, then click OK:
     - VPN Name: device1_vpn
     - Gateway Name: device1_ike
     - Advanced: Enter the following advanced settings, then click Return to return to the basic AutoKey IKE configuration page:
       - Bind to: (Select) Tunnel Interface, (Select) tunnel.1
CLI (Configuration for the Device1)

1. Interfaces
   set interface ethernet0/1 zone trust
   set interface ethernet0/1 ip 10.1.1.1/24
   set interface ethernet0/2.1 tag 128 zone untrust
   set interface tunnel.1 zone trust
   set interface ethernet0/2.1 ip 2.2.2.1/24
   set interface tunnel.1 ip unnumbered interface ethernet0/2.1
   set route 10.2.0.0/24 int tunnel.1

2. IKE
   set ike gateway device1_iike address 2.2.2.2 outgoing-interface ethernet0/2.1
   preshare sec-level standard
   set vpn device1_vpn gateway 208a_iike sec-level standard
   set vpn device1_vpn bind interface tunnel.1
   save

WebUI (Configuration for Device2)

1. Interfaces
   Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:
   - IP Address/Netmask: 10.2.0.2/24
   - Zone: Trust
   
   Network > Interfaces > Sub-IF > New: Enter the following, then click Apply:
   - Interface Name: (Select) ethernet0/2 and enter: 1
   - Zone: Untrust
   - IP Address/Netmask: 2.2.2.2/24
   - VLAN Tag: 128

   Network > Interfaces > Tunnel IF > New: Enter the following, then click Apply:
   - Tunnel Interface Name: 1
   - Unnumbered: (select) ethernet0/2.1
   - Interface: ethernet0/2.1

2. Bandwidth on Interfaces
   Network > Interfaces > Edit (for ethernet0/2.1): Enter the following, then click OK:
   - Traffic Bandwidth, Ingress: 1200

   Network > Interfaces > Edit (for tunnel.1): Enter the following, then click OK:
   - Traffic Bandwidth, Ingress: 1000

3. Route
   Network > Routing > Destination > trust-vr New: Enter the following, then click OK:
   - Network Address/Netmask: 10.1.1.0/24
   - Interface (select): Tunnel.1
4. **IKE**

VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click OK:

- Gateway Name: device2_ike
- Security Level: Standard
- Remote Gateway Type:
  - Static IP Address: (select), IP Address/Hostname: 2.2.2.2

**Preshared Key**

- Preshared Key: secret
- Outgoing Interface: ethernet0/2.1

VPNs > AutoKey IKE New: Enter the following, then click OK:

- VPN Name: device2_vpn
- Gateway Name: device2_ike

> Advanced: Enter the following advanced settings, then click **Return** to return to the basic AutoKey IKE configuration page:

- Bind to: (Select) Tunnel Interface, (Select) tunnel.1

5. **Policies**

Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

- Service: Any
- Action: Permit

Policy > Policies > (From: Untrust, To: Trust) New: Enter the following, then click OK:

- Service: Any
- Action: Permit

**CLI (Configuration for the Device2)**

1. **Interfaces**

- set interface ethernet0/1 zone trust
- set interface ethernet0/1 ip 10.2.0.2/24
- set interface ethernet0/2.1 tag 128 zone untrust
- set interface ethernet0/2.1 ip 2.2.2.2/24
- set interface tunnel.1 zone untrust
- set interface tunnel.1 ip unnumbered interface ethernet0/2.1
- set route 10.1.1.0/24

2. **Bandwidth on interfaces**

- set interface ethernet0/2.1 bandwidth ingress mbw 1200
- set interface tunnel.1 bandwidth ingress mbw 1000

3. **IKE**

- set ike gateway device2_ike address 2.2.2.1 preshare secret sec-level standard
- set vpn device2_vpn gateway 208b_ike sec-level standard
- set vpn device2_vpn bind interface tunnel.1
4. Policy
   set policy from trust to untrust any any any permit
   set policy from untrust to trust any any any permit
   save

**Example: Policy-Based VPN with Ingress Policing**

This example illustrates how to enforce ingress policing at both the interface level and in policies. On the ethernet0/1 interface on Device1, you set the ingress maximum bandwidth at 20000 Kbps. With this setting, all traffic over 20000 Kbps from clients connected to Device1 on the ethernet0/1 interface, is dropped. Ingress policing at the interface applies to all the traffic that arrives on that interface. For finer granularity, you can apply ingress policing at the policy level. In this example, you create policies to restrict all ingress FTP protocol traffic on Device1 by creating policies between the trust and untrust zones, and set the policing bandwidth to 5000 Kbps. All FTP traffic over 5000 Kbps from the trust zone to the untrust zone is dropped.

**Figure 67: Policy-Based VPN**

1. Interfaces
   Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:
   - IP Address/Netmask: 10.1.1.1/24
   - Zone: Trust
   - Interface mode: (select) NAT

   Network > Interfaces > Edit (for ethernet0/2): Enter the following, then click OK:
   - IP Address/Netmask: 2.1.1.1/24
   - Zone: Untrust
   - Interface mode: (select) Route
2. **IKE VPN**

   VPNs > AutoKey Advanced > Gateway > New: Enter the following, then click OK:

   - Gateway Name: device2_ike
   - Security Level: Standard
   - Remote Gateway Type: 
     - Static IP Address: (select), IP Address/Hostname: 2.2.2.2
   
   Preshared Key
   - Preshared Key: secret
   - Outgoing Interface: ethernet0/2
   
   > Advanced: Enter the following advanced settings, then click OK to return to basic Gateway configuration page:
   
   - Phase 1 Proposal: pre-g2-3des-sha

   VPNs > AutoKey IKE New: Enter the following, then click OK:

   - VPN Name: device2_vpn
   - Gateway Name: device2_ike

3. **Interface-Based Policing**

   Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:

   - Traffic Bandwidth, Ingress: 20000

4. **Routing**

   Network > Routing > Destination > New: Enter the following, then click OK:

   - Network IP Address/Netmask: 10.2.1.0/24
   - Interface: (select), ethernet0/2
   - Gateway IP Address: 2.2.2.2

5. **Policies**

   Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click OK:

   - Name: 1
   - Service: FTP
   - Action: Tunnel
   - Tunnel VPN: (select), device2_vpn
   - Modify matching bidirectional VPN policy: (select)
   
   > Advanced: Enter the following advanced settings, then click Return to return to the basic Policies configuration page:
   
   - Traffic Shaping (select) Policing Bandwidth: 5000

**CLI (Configuration for Device1)**

1. **Interfaces**

   set interface ethernet0/1 zone trust
   set interface ethernet0/2 zone untrust
   set interface ethernet0/1 ip 10.1.1.1/24
set interface ethernet0/1 nat
set interface ethernet0/2 ip 2.1.1.1/24
set interface ethernet0/1 route

2. IKE VPN
set ike gateway device2_ike address 2.2.2.2 main outgoing interface ethernet0/2
  preshare secret proposal pre-g2-3des-sha
set vpn device2_vpn gateway device2_ike no-replay tunnel idletime 0 sec-level
  standard

3. Routing
set route 10.2.1.0/24 interface ethernet0/2 gateway 2.2.2.2

4. Policies
set policy from trust to untrust any any ftp tunnel vpn device2_vpn pair-policy 2
  traffic pbw 5000
set policy from untrust to trust any any ftp tunnel vpn netscreeen2_vpn pair-policy 1
  traffic pbw 5000

5. Interface-Based Policing
set interface ethernet0/1 bandwidth ingress mbw 20000
save

WebUI (Configuration for Device2)

1. Interfaces
   Network > Interfaces > Edit (for ethernet0/1): Enter the following, then click OK:
     IP Address/Netmask: 1.1.1.1/24
     Zone: Trust
     Interface mode: (select) Route
   Network > Interfaces > Edit (for ethernet0/2): Enter the following, then click OK:
     IP Address/Netmask: 10.2.2.1/24
     Zone: Untrust
     Interface mode: (select) NAT

2. IKE VPN
   VPNS > AutoKey Advanced > Gateway > New: Enter the following, then click OK:
     Gateway Name: device1_ike
     Security Level: Standard
     Remote Gateway Type:
       Static IP Address: (select), IP Address/Hostname: 2.1.1.1
3. **Preshared Key**
   - Preshared Key: secret
   - Outgoing Interface: ethernet0/2

   > Advanced: Enter the following advanced settings, then click **OK** to return to basic Gateway configuration page:

   Phase 1 Proposal: pre-g2-3des-sha

**VPNs** > **AutoKey IKE** New: Enter the following, then click **OK**:

- VPN Name: device1_vpn
- Gateway Name: device1_ike

4. **Routing**
   - Network > Routing > Destination > New: Enter the following, then click **OK**:

   - Network IP Address/Netmask: 10.1.1.0/24
   - Interface: (select), ethernet0/2
   - Gateway IP Address: 1.1.1.1

5. **Policies**
   - Policy > Policies > (From: Trust, To: Untrust) New: Enter the following, then click **OK**:

   - Name: 1
   - Service: FTP
   - Action: Tunnel
   - Tunnel VPN: (select), device1_vpn
   - Modify matching bidirectional VPN policy: (select)

**CLI (Configuration for Device2)**

1. **Interfaces**
   - set interface ethernet0/1 1.1.1.2/24
   - set interface ethernet0/1 route
   - set interface ethernet0/2 ip 10.2.2.1/24
   - set interface ethernet0/2 nat

2. **IKE VPN**
   - set ike gateway device1_ike address 2.1.1.1 main outgoing interface ethernet0/2
   - preshare secret proposal pre-g2-3des-sha
   - set vpn device1_vpn gateway device1_ike no-replay tunnel idletime 0 sec-level
     standard

3. **Routing**
   - set route 10.1.1.0/24 interface ethernet0/1 gateway 1.1.1.1

4. **Policies**
   - set policy id 1 from trust to untrust any any ftp tunnel vpn device1_vpn pair-policy 2
   - set policy id 2 from untrust to trust any any ftp tunnel vpn device1_vpn pair-policy 1
   - save
Traffic Shaping Using a Loopback Interface

Traffic shaping is not supported on loopback interfaces, because no traffic is actually transmitted on a loopback interface. However, a loopback interface is often used as an anchor point (for example in the case of a VPN, to derive the source IP address), while the data is transmitted on an actual egress interface. When using a loopback interface in a VPN, therefore, you configure traffic shaping on the outgoing interface. ScreenOS then associates the session with the real outgoing interface, which it deduces from the routing table, dynamically updating the association as the routing table changes.

DSCP Marking and Shaping

As stated earlier in this chapter, Differentiated Services (DS) is a system for tagging (or “marking”) traffic at a position within a hierarchy of priority. Differentiated Services Codepoint (DSCP) marking maps the ScreenOS priority level of the policy to the first three bits of codepoint in the DS field in the IP packet header. (See Setting Service Priorities on page 198 for more information).

You can shape traffic in a policy that uses DSCP marking, or you can use DSCP marking independent of traffic shaping. Traffic shaping governs how traffic is processed on the security device and can be configured at the interface level or in policies. DSCP marking, which you set at the policy level, governs how traffic is processed by downstream routers.

NOTE: Some devices require that you explicitly enable DSCP marking by setting a system-wide environmental variable. Refer to your hardware manual to find out if your device requires that you explicitly enable DSCP marking before using it in policies. If your device requires it, use the following command to enable DSCP marking system wide: set envar ipsec-dscp-mark = yes. This variable cannot be set using the WebUI. Use the unset envar ipsec-dscp-mark to disable DSCP marking system wide.

If you specify DSCP marking in a policy but do not set a value, ScreenOS maps the policy priority to an equivalent IP precedence priority in the DSCP system. It does this by overwriting the first 3 bits in the ToS byte with the IP precedence priority. For example, if you create a policy that gives all traffic a priority of, for example, 2 (0 is the highest priority), and you enable DSCP marking, ScreenOS queues traffic for that policy with level 2 priority at the egress interface and marks it with an equivalent IP precedence priority. The following command creates a policy that gives priority 2 to all traffic, and enables DSCP marking:

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable
```

But if you give DSCP a `dscp-byte value` of, for example, 46 (the highest priority), the security device still queues traffic at the egress interface at priority 2 but overwrites the first 6 bits of the ToS byte with the DSCP value.

```
set policy from trust to untrust any any any permit traffic priority 2 dscp enable value 46
```
DSCP marking is supported on all platforms and can be configured with traffic shaping or independently. Table 31 shows how DSCP marking works for clear packets in policies, Figure 66 shows how DSCP marking works for clear packets in policy-based VPNs, Table 33 shows how DSCP marking works for clear packets in route-based VPNs.

**Table 31: DSCP Marking for Clear-Text Traffic**

<table>
<thead>
<tr>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear packet with no marking on the policy.</td>
<td>No marking.</td>
</tr>
<tr>
<td>Clear packet with marking on the policy.</td>
<td>The packet is marked based on the policy.</td>
</tr>
<tr>
<td>Premarked packet with no marking on the policy.</td>
<td>Retain marking in the packet.</td>
</tr>
<tr>
<td>Premarked packet with marking on the policy.</td>
<td>Overwrite marking in the packet based on the</td>
</tr>
<tr>
<td></td>
<td>policy.</td>
</tr>
</tbody>
</table>

**Table 32: DSCP Marking for Policy-Based VPNs**

<table>
<thead>
<tr>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear packet into policy-based VPN with no marking on the policy.</td>
<td>No marking.</td>
</tr>
<tr>
<td>Clear packet into policy-based VPN with marking on the policy.</td>
<td>The inner packet and ESP header are both marked, based on the policy.</td>
</tr>
<tr>
<td>Premarked packet into policy-based VPN with no marking on the policy.</td>
<td>Copy the inner packet marking to the ESP header, retain marking in the inner packet.</td>
</tr>
<tr>
<td>Premarked packet into policy-based VPN with marking on the policy.</td>
<td>Overwrite the marking in the inner packet based on the policy, and copy the inner packet marking to the ESP header.</td>
</tr>
</tbody>
</table>

**Table 33: DSCP Marking for Route-Based VPNs**

<table>
<thead>
<tr>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear packet into route-based VPN with no marking on the policy.</td>
<td>No marking.</td>
</tr>
<tr>
<td>Clear packet into route-based VPN with marking on the policy.</td>
<td>The inner packet and ESP header are both marked, based on the policy.</td>
</tr>
<tr>
<td>Premarked packet into route-based VPN with no marking on the policy.</td>
<td>Copy the inner packet marking to the ESP header, retain marking in the inner packet.</td>
</tr>
<tr>
<td>Premarked packet into route-based VPN with marking on the policy.</td>
<td>Overwrite the marking in the inner packet based on the policy, and copy the inner packet marking to the ESP header.</td>
</tr>
</tbody>
</table>