Virus Throttling (5300xl Switches Only)

Contents

Introduction ................................................................. 3-3
General Operation of Connection-Rate Filtering .................... 3-5
  Filtering Options ...................................................... 3-5
  Sensitivity to Connection Rate Detection ........................ 3-6
  Application Options .................................................. 3-6
Terminology ................................................................. 3-7
Operating Rules ............................................................ 3-8
General Configuration Guidelines ..................................... 3-9
  For a network that is relatively attack-free: ...................... 3-9
  For a network that appears to be under significant attack: ...... 3-10
Basic Connection-Rate Filtering Configuration ..................... 3-11
  Global and Per-Port Configuration ................................ 3-11
    Enabling Connection-Rate Filtering and
    Configuring Sensitivity .......................................... 3-12
    Configuring the Per-Port Filtering Mode ....................... 3-13
    Example of a Basic Connection-Rate Filtering Configuration .. 3-14
Viewing and Managing Connection-Rate Status ...................... 3-16
  Viewing the Connection-Rate Configuration ....................... 3-16
  Listing and Unblocking the Currently-Blocked Hosts .......... 3-18
Configuring and Applying Connection-Rate ACLs ................... 3-20
  Connection-Rate ACL Operation .................................... 3-21
  Configuring a Connection-Rate ACL Using
  Source IP Address Criteria ........................................... 3-22
  Configuring a Connection-Rate ACL Using UDP/TCP Criteria .... 3-23
  Applying Connection-Rate ACLs .................................... 3-26
  Using CIDR Notation To Enter the ACE Mask ..................... 3-26
  Example of Using an ACL in a Connection-Rate Configuration ... 3-27
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection-Rate ACL Operating Notes</td>
<td>3-30</td>
</tr>
<tr>
<td>Connection-Rate Log and Trap Messages</td>
<td>3-31</td>
</tr>
</tbody>
</table>
Introduction

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default</th>
<th>Menu</th>
<th>CLI</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Configuration and Sensitivity</td>
<td>Disabled</td>
<td>—</td>
<td>3-12</td>
<td>—</td>
</tr>
<tr>
<td>Per-Port Configuration</td>
<td>None</td>
<td>—</td>
<td>3-13</td>
<td>—</td>
</tr>
<tr>
<td>Listing and Unblocking Blocked Hosts</td>
<td>n/a</td>
<td>—</td>
<td>3-18</td>
<td>—</td>
</tr>
<tr>
<td>Viewing the Current Configuration</td>
<td>n/a</td>
<td>—</td>
<td>3-16</td>
<td>—</td>
</tr>
<tr>
<td>Configuring Connection-Rate ACLs</td>
<td>None</td>
<td>—</td>
<td>3-20</td>
<td>—</td>
</tr>
</tbody>
</table>

The spread of malicious agents in the form of worms exhibiting worm behavior has severe implications for network performance. Damage can be as minimal as slowing down a network with excessive, unwanted traffic, or as serious as putting attacker-defined code on a system to cause any type of malicious damage that an authorized user could do.

Current methods to stop the propagation of malicious agents rely on use of signature recognition to prevent hosts from being infected. However, the latency between the introduction of a new virus or worm into a network and the implementation and distribution of a signature-based patch can be significant. Within this period, a network can be crippled by the abnormally high rate of traffic generated by infected hosts.

Connection-Rate filtering based on virus throttling technology is recommended for use on the edge of a network. It is primarily concerned with the class of worm-like malicious code that tries to replicate itself by using vulnerabilities on other hosts (that is, weaknesses in network applications behind unsecured ports). Agents of this variety operate by choosing a set of hosts to attack based on an address range (sequential or random) that is exhaustively searched, either by blindly attempting to make connections by rapidly sending datagrams to the address range, or by sending ICMP ping messages to the address range and listening for replies.

Connection-Rate filtering exploits the network behavior of malicious code that tries to create a large number of outbound IP connections on a routed interface in a in a short time. When a host exhibits this behavior, warnings can be sent, and connection requests can be either throttled or dropped to minimize the barrage of subsequent traffic from the host. When enabled on a 5300xl switch with software version E.09.02 or greater, connection-rate filtering based on virus-throttling technology can help reduce the impact of worm-like malicious code and give system administrators more time to isolate and eradicate the threat. Thus, while traditional worm- and virus-
signature updates will still need to be deployed to hosts, the network remains functional and the overall distribution of the malicious code is limited.

Connection-Rate filtering is a countermeasure tool you can use in your incident-management program to help detect an manage worm-type IT security threats received in inbound routed traffic. Major benefits of this tool include:

- Behavior-based operation that does not require identifying details unique to the code exhibiting the worm-like operation.
- Handles unknown worms.
- Needs no signature updates.
- Protects network infrastructure by slowing or stopping routed traffic from hosts exhibiting high connection-rate behavior.
- Allows network and individual switches to continue to operate, even when under attack.
- Provides Event Log and SNMP trap warnings when worm-like behavior is detected
- Gives IT staff more time to react before the threat escalates to a crisis.

**Note**

When configured on a port, connection-rate filtering is triggered by routed IPv4 traffic received inbound with a relatively high rate of IP connection attempts. (Connection-Rate filtering is not triggered by such traffic when both the SA and DA are in the same VLAN—that is, switched traffic). Note that connection-rate filtering applies only to routed traffic. Switched traffic from a blocked or throttled host is not blocked or throttled.
General Operation of Connection-Rate Filtering

Connection-Rate filtering enables notification of worm-like behavior detected in inbound routed traffic and, depending on how you configure the feature, also throttles or blocks such traffic. This feature also provides a method for allowing legitimate, high connection-rate traffic from a given host while still protecting your network from possibly malicious traffic from other hosts.

Filtering Options

In the default configuration, connection-rate filtering is disabled. When enabled on a port, connection-rate filtering monitors inbound routed traffic for a high rate of connection requests from any given host on the port. If a host appears to exhibit the worm-like behavior of attempting to establish a large number of outbound IP connections (destination addresses, or DAs) in a short period of time, the switch responds in one of the following ways, depending on how connection-rate filtering is configured:

- **Notify only of potential attack:** While the apparent attack continues, the switch generates an Event Log notice identifying the offending host SA and (if a trap receiver is configured on the switch) a similar SNMP trap notice.

- **Notify and reduce spreading:** In this case, the switch temporarily blocks inbound routed traffic from the offending host SA for a “penalty” period and generates an Event Log notice of this action and (if a trap receiver is configured on the switch) a similar SNMP trap notice. When the “penalty” period expires the switch re-evaluates the routed traffic from the host and continues to block this traffic if the apparent attack continues. (During the re-evaluation period, routed traffic from the host is allowed.)

- **Block spreading:** This option blocks routing of the host’s traffic on the switch. When a block occurs, the switch generates an Event Log notice and (if a trap receiver is configured on the switch) a similar SNMP trap notice. Note that system personnel must explicitly re-enable a host that has been previously blocked.
Sensitivity to Connection Rate Detection

The switch includes a global sensitivity setting that enables adjusting the ability of connection-rate filtering to detect relatively high instances of connection-rate attempts from a given source.

Application Options

For the most part, normal network traffic is distinct from the traffic exhibited by malicious agents. However, when a legitimate network host generates multiple connections in a short period of time, connection-rate filtering may generate a “false positive” and treat the host as an infected client. Lowering the sensitivity or changing the filter mode may reduce the number of false positives. Conversely, relaxing filtering and sensitivity provisions lowers the switch’s ability to detect worm-generated traffic in the early stages of an attack, and should be carefully investigated and planned to ensure that a risky vulnerability is not created. As an alternative, you can use connection-rate ACLs (access control lists) or selective enabling to allow legitimate traffic.

Selective Enable. This option involves applying connection-rate filtering only to ports posing a significant risk of attack. For ports that are reasonably secure from attack, then there may be little benefit in configuring them with connection-rate filtering.

Connection-Rate ACLs. The basic connection-rate filtering policy is configured per-port as notify-only, throttle, and block. A connection-rate ACL creates exceptions to these per-port policies by creating special rules for individual hosts, groups of hosts, or entire subnets. Thus, you can adjust a connection-rate filtering policy to create and apply an exception to configured filters on the ports in a VLAN. Note that connection-rate ACLs are useful only if you need to exclude inbound traffic from your connection-rate filtering policy. For example, a server responding to network demand may send a relatively high number of legitimate connection requests. This can generate a false positive by exhibiting the same elevated connection-rate behavior as a worm. Using a connection-rate ACL to apply an exception for this server allows you to exclude the trusted server from connection-rate filtering and thereby keep the server running without interruption.

Note

Use connection-rate ACLs only when you need to exclude a routed traffic source (including traffic with specific UDP or TCP criteria) from a connection-rate filtering policy. Otherwise, the ACL is not necessary.
Terminology

**Bridged Traffic**: See “Switched Traffic”, below.

**DA**: The acronym for *Destination Address*. In an IP packet, this is the destination IP address carried in the header, and identifies the destination intended by the packet’s originator. See also “SA”.

**Routed Traffic**: Traffic moving from an SA in one VLAN to a DA in a different VLAN.

**SA**: The acronym for *Source Address*. In an IP packet, this is the source IP address carried in the header, and identifies the packet’s originator. See also “DA”.

**Switched Traffic**: Traffic moving from an SA in a given VLAN to a DA in the same VLAN. (Sometimes termed “bridged traffic”.)

**Throttle**: For connection-rate filtering applications, this means to temporarily block traffic from a host exhibiting a relatively high incidence of attempts to connect with other devices. Traffic is blocked from the host for a calculated period of time, and then allowed to resume. If the undesired behavior persists, the cycle is repeated.
Operating Rules

- When configuring or changing the configuration of connection-rate filters in the switch, execute the `clear arp` command to reset the routing table.

- Connection-Rate filtering is triggered by inbound IP *routed* traffic exhibiting high rates of IP connections to new hosts. Inbound *switched* traffic with high IP connection rates does not trigger connection-rate filtering. However, after connection-rate filtering has been triggered on a port, all traffic (switched or routed) from the suspect host is subject to the configured connection-rate policy (*notify-only*, *throttle*, or *block*).

- Where the switch is throttling or blocking inbound routed traffic from a host, any outbound routed or switched traffic for that host is still permitted.

- A host blocked by connection-rate filtering remains blocked until explicitly unblocked by one of the following:
  - The `vlan < vid > connection-rate-filter unblock` command (page 3-18)
  - Rebooting the switch
  - Disabling connection-rate filtering using the `no connection-rate-filter` command.
  - Deleting a VLAN removes blocks on any hosts on that VLAN.

Note that changing a port setting from Block to either Throttle or Notify-Only, does not unblock a blocked host on any port previously set to block.
General Configuration Guidelines

As stated earlier, connection-rate filtering is triggered only by routed, inbound traffic generating a relatively high number of new IP connection requests from the same host. Thus, for the switch to apply connection-rate filters, IP routing and multiple VLANs with member ports must first be configured.

For a network that is relatively attack-free:

1. Enable **notify-only** mode on the ports you want to monitor.
2. Set global sensitivity to **low**.
3. Use **clear arp** to clear the arp cache.
4. If SNMP trap receivers are available in your network, use the **snmp-server** command to configure the switch to send SNMP traps.
5. Monitor the Event Log or (if configured) the available SNMP trap receivers to identify hosts exhibiting high connection rates.
6. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
7. Hosts demonstrating high, but legitimate connection rates, such as heavily used servers, may trigger a connection-rate filter. Configure connection rate ACLs to create policy exceptions for trusted hosts. (Exceptions can be configured for these criteria:
   - A single source host or group of source hosts
   - A source subnet
   - Either of the above with TCP or UDP criteria
   (For more on connection rate ACLs, refer to “Application Options” on page 3-6.)
8. Increase the sensitivity to **Medium** and repeat steps 6 and 7.

**Note** On networks that are relatively infection-free, sensitivity levels above **Medium** are not recommended.

9. (Optional.) Enable **throttle** or **block** mode on the monitored ports.
On a given VLAN, to unblock the hosts that have been blocked by the connection-rate feature, use the `vlan < vid > connection-rate filter unblock` command.

10. Maintain a practice of carefully monitoring the Event Log or configured trap receivers for any sign of high connectivity-rate activity that could indicate an attack by malicious code. (Refer to “Connection-Rate Log and Trap Messages” on page 3-31.)

For a network that appears to be under significant attack:

The steps are similar to the general steps for a network that is relatively attack free. The major difference is in policies suggested for managing hosts exhibiting high connection rates. This allows better network performance for unaffected hosts and helps to identify hosts that may require updates or patches to eliminate malicious code.

1. Configure connection-rate filtering to `throttle` on all ports.
2. Set global sensitivity to `medium`.
3. Use `clear arp` to clear the arp cache.
4. If SNMP trap receivers are available in your network, use the `snmp-server` command to configure the switch to send SNMP traps.
5. Monitor the Event Log or the available SNMP trap receivers (if configured on the switch) to identify hosts exhibiting high connection rates.
6. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
7. On hosts you identify as needing attention to remove malicious behavior:
   - To immediately halt an attack from a specific host, group of hosts, or a subnet, use the per-port block mode on the appropriate port(s).
   - After gaining control of the situation, you can use connection-rate ACLs to more selectively manage traffic to allow receipt of normal routed traffic from reliable hosts.
Basic Connection-Rate Filtering Configuration

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global and Per-Port Configuration</td>
<td></td>
</tr>
<tr>
<td>connection-rate-filter sensitivity &lt; low</td>
<td>medium</td>
</tr>
<tr>
<td>filter connection-rate &lt; port-list &gt; &lt; notify-only</td>
<td>throttle</td>
</tr>
<tr>
<td>show connection-rate-filter &lt; blocked-host &gt;</td>
<td></td>
</tr>
<tr>
<td>Unblocking Hosts Per-VLAN</td>
<td></td>
</tr>
<tr>
<td>vlan &lt; vid &gt; connection-rate-filter unblock</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

As mentioned earlier, connection-rate filtering is triggered by inbound, routed traffic exhibiting a relatively high incidence of IP connection attempts from a single source. If connection-rate filtering throttles or blocks traffic from a source, all routed traffic from that source is throttled or blocked. Traffic switched within the VLAN is not affected.

Using this feature requires that IP routing and multiple VLANs are enabled.

Global and Per-Port Configuration

Use the commands in this section to enable connection-rate filtering on the switch and to apply the filtering on a per-port basis. (You can use the ACL commands in the next section to adjust a filter policy on a per-vlan basis to allow traffic from specific, trusted SAs to be routed without being subjected to the filtering.)

**Note**

Immediately after you enable or disable connection-rate filtering, the CLI prompts you to reboot the switch. ProCurve strongly recommends that you perform the reboot to help ensure optimal switch performance.
Enabling Connection-Rate Filtering and Configuring Sensitivity

**Syntax:**  
connection-rate-filter sensitivity < low | medium | high | aggressive >  
noreconnection-rate-filter

*This command:*

- Enables connection-rate filtering.
- Sets the global sensitivity level at which the switch interprets a given host's attempts to connect to a series of different devices as a possible attack by a malicious agent residing in the host.

*The no form of the command disables connection-rate filtering on the switch.*

*Note:* For optimum performance, reboot the switch after you enable or disable connection-rate filtering.

**low:** Sets the connection-rate sensitivity to the lowest possible sensitivity, which allows a mean of 54 routed destinations in less than 0.1 seconds, and a corresponding penalty time for Throttle mode (if configured) of less than 30 seconds.

**medium:** Sets the connection-rate sensitivity to allow a mean of 37 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 30 and 60 seconds.

**high:** Sets the connection-rate sensitivity to allow a mean of 22 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 60 and 90 seconds.

**aggressive:** Sets the connection-rate sensitivity to the highest possible level, which allows a mean of 15 routed destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 90 and 120 seconds.
Configuring the Per-Port Filtering Mode

**Syntax:** filter connection-rate < port-list > < notify-only | throttle | block >
no filter connection-rate < port-list >

Configures the per-port policy for responding to detection of a relatively high number of inbound, routed IP connection attempts from a given source. The level at which the switch detects such traffic depends on the sensitivity setting configured by the `connection-rate-filter sensitivity` command (page 3-12). (Note: You can use connection-rate ACLs to create exceptions to the configured filtering policy. See “Configuring and Applying Connection-Rate ACLs” on page 3-20.) The `no` form of the command disables connection-rate filtering on the ports in `#< port-list>`.  

- **notify-only:** If the switch detects a relatively high number of routed IP connection attempts from a specific host, `notify-only` generates an Event Log message. Sends a similar message to any SNMP trap receivers configured on the switch.  
- **throttle:** If the switch detects a relatively high number of routed IP connection attempts from a specific host, this option generates the `notify-only` messaging and also blocks all routed traffic inbound from the offending host for a penalty period. After the penalty period, the switch allows routed traffic from the offending host to resume, and re-examines the traffic. If the suspect behavior continues, the switch again blocks the routed traffic from the offending host and repeats the cycle. For the penalty periods, refer to table 3-1, below.  
- **block:** If the switch detects a relatively high number of routed IP connection attempts from a specific host, this option generates the `notify-only` messaging and also blocks all routed and switched traffic inbound from the offending host.

<table>
<thead>
<tr>
<th>Throttle Mode</th>
<th>Frequency of IP Connection Requests from the Same Source</th>
<th>Mean Number of New Destination Hosts in the Frequency Period</th>
<th>Penalty Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>&lt; 0.1 second</td>
<td>54</td>
<td>&lt; 30 seconds</td>
</tr>
<tr>
<td>Medium</td>
<td>&lt; 1.0 second</td>
<td>37</td>
<td>30 - 60 seconds</td>
</tr>
<tr>
<td>High</td>
<td>&lt; 1.0 second</td>
<td>22</td>
<td>60 - 90 seconds</td>
</tr>
<tr>
<td>Aggressive</td>
<td>&lt; 1.0 second</td>
<td>15</td>
<td>90 - 120 seconds</td>
</tr>
</tbody>
</table>
Example of a Basic Connection-Rate Filtering Configuration

**Figure 3-2. Sample Network**

**Basic Configuration.** Suppose that in the sample network, the administrator wanted to enable connection-rate filtering and configure the following response to high connection-rate traffic on the 5300xl switch:

- Ports B1 - B3: Throttle traffic from the transmitting host(s).
- Port B4: Respond with Notify-Only to identify the transmitting host(s).
- Ports B9, D1, and D2: Block traffic from the transmitting host(s).

Figure 3-3 illustrates the configuration steps and resulting startup-config file.
ProCurve(config)# connection-rate-filter sensitivity low

Enables connection-rate filtering and sets the sensitivity to "low".

The switch should be rebooted for optimal performance after enabling or disabling connection rate filtering.

ProCurve(config)# filter connection-rate b1-b3 throttle

Configures the desired responses to inbound, high connectivity-rate traffic on the various ports.

ProCurve(config)# filter connection-rate b4 notify-only

ProCurve(config)# filter connection-rate b9,d1-d2 block

ProCurve(config)# write mem

ProCurve(config)# show config

Start up configuration:

; J4850A Configuration Editor: Created on release #E.09.01

hostname "ProCurve"

Connection-rate-filter sensitivity low

Indicates that connectivity-rate filtering is enabled at the "low" sensitivity setting.

module 2 type J8161A
module 4 type J8161A
ip routing
snmp-server community "public" Unrestricted
snmp-server host 15.45.200.75 "public"

vlan 1

name "DEFAULT_VLAN"
untagged B5-B24
ip address dhcp-bootp
no untagged B1-B4.D1-D24
ip proxy-arp
exit

vlan 10

name "VLAN10"
untagged B1-B4
no ip address
ip proxy-arp
exit

vlan 15

name "VLAN15"
untagged D1-D24
no ip address
ip proxy-arp
exit

filter connection-rate B4 notify-only
filter connection-rate B1-B3 throttle
filter connection-rate b9,d1-d2 block

Shows the per-port configuration for the currently enabled connectivity-rate filtering.

Figure 3-3. Example of a Basic Connection-Rate Configuration
Viewing and Managing Connection-Rate Status

The commands in this section describe how to:

- View the current connection-rate configuration
- List the currently blocked hosts
- Unblock currently blocked hosts (on a per-VLAN basis).

Viewing the Connection-Rate Configuration

Use the following command to view the basic connection-rate configuration. If you need to view connection-rate ACLs and/or any other switch configuration details, use show config or show running (page 3-17).

**Syntax:** `show connection-rate-filter`

Displays the current global connection-rate status (enabled/disabled) and sensitivity setting, and the current per-port configuration. This command does not display the current (optional) connection-rate ACL configuration, if any.

```
ProCurve(config)# show connection-rate-filter

Connection Rate Filter Configuration

Global Status:   Enabled
Sensitivity:     Medium

<table>
<thead>
<tr>
<th>Port</th>
<th>Filter Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>B13</td>
<td>NOTIFY-ONLY</td>
</tr>
<tr>
<td>B14</td>
<td>THROTTLE</td>
</tr>
<tr>
<td>B15</td>
<td>BLOCK</td>
</tr>
<tr>
<td>B16</td>
<td>BLOCK</td>
</tr>
</tbody>
</table>
```

Figure 3-4. Example of Displaying the Connection-Rate Status, Sensitivity, and Per-Port Configuration
To view the complete connection-rate configuration, including any ACLs (page 3-20), use `show config` (for the startup-config file) or `show running` (for the running-config file). For example:

```
ProCurve(config)# show config
Startup configuration:
: J4850A Configuration Editor; Created on hostname "ProCurve"
Connection-rate-filter sensitivity medium
ip access-list connection-rate-filter "Sample"
    filter ip 13.28.234.180 0.0.0.0 255.255.255.255
    ignore ip 0.0.0.0 255.255.255.255
    exit
module 2 type J8161A
module 4 type J8161A
ip routing
logging 13.28.234.180
snap-server community "public" Unrestricted
vlan 1
    name "DEFAULT_VLAN"
    untagged B1-B12,B19-B24,D1-D24
    no ip address
    no untagged B13-B18
    ip proxy-arp
    exit
vlan 15
    name "VLAN_15"
    untagged B13-B18
    ip address 13.28.234.181 255.255.255.255
    ip proxy-arp
    ip connection-rate-filter-access-group "Sample"
    exit
filter connection-rate B13 notify-only
filter connection-rate B14 throttle
filter connection-rate B15-B16 block
```

Figure 3-5. Example of Connection-Rate Filtering Configuration in the Startup-Config File
Listing and Unblocking the Currently-Blocked Hosts

**Syntax:**
```
show connection-rate-filter < all-hosts | blocked-hosts | throttled-hosts >
```

**all-hosts:** Lists, by VLAN membership, all hosts currently detected in a throttling or blocking state, along with a state indicator.

**throttled-hosts:** Lists, by VLAN membership, the hosts currently in a throttling state due to connection-rate action.

**blocked-hosts:** Lists, by VLAN membership, the hosts currently blocked by connection-rate action.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Source IP Address</th>
<th>Filter Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>13.28.234.175</td>
<td>THROTTLE</td>
</tr>
<tr>
<td>10</td>
<td>13.28.234.179</td>
<td>THROTTLE</td>
</tr>
<tr>
<td>10</td>
<td>13.28.234.180</td>
<td>BLOCK</td>
</tr>
</tbody>
</table>

**Figure 3-6. Example of Listing the Hosts Currently in Any Connection-Rate State**

```
ProCurve Switch 5304XL(config)# show connection-rate-filter all
```

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Source IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>15.28.234.180</td>
</tr>
</tbody>
</table>

**Figure 3-7. Example of Listing the Hosts Currently Blocked by Connection-Rate Filtering**

If a host becomes blocked by triggering connection-rate filtering on a port configured to block high connection rates, the host remains blocked on all ports on the switch, even if you change the per-port filtering configuration or disable connection-rate filtering. (The SA block imposed by connection-rate filtering does not age-out.) This is to help prevent a malicious host from automatically regaining access to the network. When a host becomes blocked the switch generates the following Event Log message and also sends a similar message to any configured SNMP trap receivers.

```
Src IP xxx.xxx.xxx.xxx blocked
```
Virus Throttling (5300xl Switches Only)
Basic Connection-Rate Filtering Configuration

**Note**
ProCurve recommends that, before you unblock a host that has been blocked by connection-rate filtering, you inspect the host with current antivirus tools and remove any malicious agents that pose a threat to your network.

If a trusted host frequently triggers connection-rate blocking with legitimate, high connection-rate traffic, then you may want to consider either changing the sensitivity level on the associated port or configuring a connection-rate ACL to create a filtering exception for the host.

**Syntax:** `vlan < vid > connection-rate-filter unblock < all | host | ip-addr >`

- **all:** *In the specified VLAN, unblocks all hosts currently blocked due to action by connection-rate filtering on ports where block mode has been configured.*
- **host < ip-addr >:** *In the specified VLAN, unblocks the single host currently blocked due to action by connection-rate filtering on ports where block mode has been configured.*
- **ip-addr < mask >:** *In the specified VLAN, unblocks traffic from any host in the specified subnet currently blocked due to action by connection-rate filtering on ports where block mode has been configured.*

**Note**
Rebooting the switch unblocks all hosts affected by a connection-rate filter block.
Configuring and Applying Connection-Rate ACLs

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip access-list connection-rate-filter &lt; crf-list-name &gt;</td>
<td>3-22, 3-23</td>
</tr>
<tr>
<td>&lt; filter</td>
<td>ignore &gt; ip &lt; any</td>
</tr>
<tr>
<td>&lt; filter</td>
<td>ignore &gt; &lt; udp</td>
</tr>
<tr>
<td>vlan &lt; vid &gt; ip access-group &lt; crf-list-name &gt; connection-rate-filter</td>
<td></td>
</tr>
</tbody>
</table>

A host sending legitimate, routed traffic can trigger connection-rate filtering in some circumstances. If you can verify that such a host is indeed sending valid traffic and is not a threat to your network, you may want to configure a connection-rate ACL (access control list) that allows this traffic to bypass the configured connection-rate filtering.

A connection-rate Access Control List (ACL) is an optional tool that consists of one or more explicitly configured Access Control Entries (ACEs) used to specify whether to enforce the configured connection-rate policy on traffic from a particular source.

Use of connection-rate ACLs provides the option to apply exceptions to the configured connection-rate filtering policy. This enables you to allow legitimate traffic from a trusted source, and apply connection-rate filtering only to inbound traffic from untrusted sources. For example, where a connection-rate policy has been configured, you can apply a connection-rate ACL that causes the switch bypass connection-rate policy filtering on traffic from:

- A trusted server exhibiting a relatively high IP connection rate due to heavy demand
- A trusted traffic source on the same port as other, untrusted traffic sources.

The criteria for an exception can include the SA of traffic from a specific host, group of hosts, or a subnet, and can also include source and destination TCP/UDP criteria. This allows you to apply a notify-only, throttling, or blocking policy while allowing exceptions for legitimate traffic from specific sources. You can also allow exceptions for traffic with specific TCP or UDP criteria.

For more information on when to apply connection-rate ACLs, refer to “Application Options” on page 3-6.
Connection-Rate ACLs are a special case of the switch’s ACL feature. If you need information on other applications of ACLs or more detailed information on how ACLs operate, refer to the chapter titled “Access Control Lists (ACLs) for the Series 5300xl Switches” in the Advanced Traffic Management Guide for your 5300xl switch.

**Connection-Rate ACL Operation**

A connection-rate ACL applies to inbound traffic on all ports configured for connection-rate filtering in the assigned VLAN, and creates an exception to the connection-rate filter policy configured on each port. A connection-rate ACL has no effect on ports in the VLAN that are not configured for connection-rate filtering.

A connection-rate ACL accepts inbound, legitimate traffic from trusted sources without filtering the traffic for the configured connection-rate policy. You can configure an ACL to assign policy filtering (filter) for traffic from some sources and no policy filtering (ignore) for traffic from other sources. However, the implicit filter invoked as the last entry in any connection-rate ACL ensures that any traffic not specifically excluded from policy filtering (by the ignore command) will be filtered by the configured policy for the port on which that traffic entered the switch.

![Flowchart](image_url)

Figure 3-8. Connection-Rate ACL Applied to Traffic Received Through a Given Port
Configuring a Connection-Rate ACL Using Source IP Address Criteria

(To configure a connection-rate ACL using UDP/TCP criteria, go to page 3-23.)

**Syntax:** `ip access-list connection-rate-filter < crf-list-name>`

Creates a connection-rate-filter ACL and puts the CLI into the access control entry (ACE) context:

```
ProCurve(config-crf-nacl)#
```

If the ACL already exists, this command simply puts the CLI into the ACE context.

**Syntax:** `< filter | ignore > ip < any | host < ip-addr > | ip-addr < mask-length >>`

Used in the ACE context (above) to specify the action of the connection-rate ACE and the source IP address (SA) of the traffic that the ACE affects.

```
< filter | ignore >
```

The `filter` option assigns policy filtering to traffic with an SA matching the source address in the ACE. The `ignore` option specifies bypassing policy filtering for traffic with an SA that matches the source address in the ACE.

```
ip < any | host < ip-addr > | ip-addr < mask-length >
```

Specifies the SA criteria for traffic addressed by the ACE.

- `any`: Applies the ACEs action (`filter` or `ignore`) to traffic having any SA.
- `host < ip-addr>`: Applies the ACEs action (`filter` or `ignore`) to traffic having the specified host SA.
- `ip-addr < mask-length>`: Applies the ACEs action (`filter` or `ignore`) to traffic having an SA within the range defined by either:

```
< src-ip-addr/cidr-mask-bits>
or
< src-ip-addr < mask >
```

Use this criterion for traffic received from either a subnet or a group of IP addresses. The mask can be in either dotted-decimal format or CIDR format with the number of significant bits. Refer to “Using CIDR Notation To Enter the ACE Mask” on page 3-26.
Configuring a Connection-Rate ACL Using UDP/TCP Criteria

(To configure a connection-rate ACL using source IP address criteria, turn to page 3-22.)

**Syntax:**  
`ip access-list connection-rate-filter < crf-list-name>`

*Creates a connection-rate-filter ACL and puts the CLI into the access control entry (ACE) context:*

```
ProCurve(config-crf-nacl) #
```

*If the ACL already exists, this command simply puts the CLI into the ACE context.*

**Syntax:**

```
< filter | ignore > < udp | tcp > < any >
< filter | ignore > < udp | tcp > < host < ip-addr > > [ udp/tcp-options ]
< filter | ignore > < udp | tcp > < ip-addr < mask-length > > [ udp/tcp-options ]
```

*Used in the ACE context (above) to specify the action of the connection-rate ACE (filter or ignore), and the UDP/TCP criteria and SA of the IP traffic that the ACE affects.*

```
< filter | ignore >
```

*filter: This option assigns a policy of filtering (dropping) IP traffic having an SA that matches the source address criteria in the ACE.*

*ignore: This option specifies a policy of allowing IP traffic having an SA that matches the source address criteria in the ACE.*

```
< udp | tcp > < any | host < ip-addr > | ip-addr < mask-length > >
```

*Applies the filter or ignore action to either TCP packets or UDP packets having the specified SA.*

*any: Applies the ACE’s action (filter or ignore) to IP traffic having any SA.*

*host < ip-addr>: Applies the ACE’s action (filter or ignore) to IP traffic having the specified host SA.*
ip-addr < mask-length>: Applies the ACEs action (filter or ignore) to IP traffic having an SA within the range defined by either:

< src-ip-addr/cidr-mask-bits>
or
<src-ip-addr < mask>>

Use this criterion for traffic received from either a subnet or a group of IP addresses. The mask can be in either dotted-decimal format or CIDR format with the number of significant bits. Refer to “Using CIDR Notation To Enter the ACE Mask” on page 3-26.

[ udp/tcp-options ]
destination-port < tcp-data > [source-port < tcp-data >]
source-port < tcp-data > [destination-port < tcp-data >]

destination-port < udp-data > [source-port < udp-data >]
source-port < udp-data > [destination-port < udp-data >]
tcp-data: < operator > < tcp-port-#>
udp-data: < operator > < udp-port-#>

operator: < eq | gt | lt | neq | range >

eq < port-nbr-or-name>: “Equal To”; to have a match with the ACE entry, the TCP or UDP source-port number in a packet must be equal to the specified port number.
gt: < port-nbr-or-name>: “Greater Than”; to have a match with the ACE entry, the TCP or UDP source-port number in a packet must be greater than the specified port number.
lt < port-nbr-or-name>: “Less Than”; to have a match with the ACE entry, the TCP or UDP source-port number in a packet must be less than the specified port number.
neq < port-nbr-or-name>: “Not Equal”; to have a match with the ACE entry, the TCP or UDP source-port number in a packet must not be equal to the specified port number.
range < start-port-nbr/name > < end-port-nbr/name >: To have a match with the ACE entry, the TCP or UDP source-port number in a packet must be in the range < start-port-nbr/name > < end-port-nbr/name >.
Virus Throttling (5300xi Switches Only)
Configuring and Applying Connection-Rate ACLs

\(<\text{tcp-data}>\) or \(<\text{udp-data}>\)

**TCP or UDP Port Number or (Well-Known) Port Name:** Use the TCP or UDP port number required for the desired match. The switch also accepts certain well-known TCP or UDP port names as alternates to their corresponding port numbers:

- **TCP/UDP-PORT:** Specify port by number.
- **bootpc:** Bootstrap Protocol, client (68)
- **bootps:** Bootstrap Protocol, server (67)
- **dns:** Domain Name Service (53)
- **ntp:** Network Time Protocol (123)
- **radius:** Remote Authentication Dial-In User Service (1812)
- **radius-ol:** Remote Authentication Dial-In User Service 1645
- **rip:** Routing Information Protocol (520)
- **snmp:** Simple Network Management Protocol (161)
- **snmp-trap:** Simple Network Management Protocol (162)
- **tftp:** Trivial File Transfer Protocol (69)

```
ProCurve(config)# ignore tcp host 15.75.10.11 destination-port eq 1812
source-port eq 1812

ProCurve(config)# filter udp 15.75.10.0/24 source-port neq 162
destination-port eq 162
```

**Figure 3-9. Examples of Connection-Rate ACEs Using UDP/TCP Criteria**
Applying Connection-Rate ACLs

To apply a connection-rate ACL, use the access group command described below. Note that this command differs from the access group command for non-connection-rate ACLs.

**Syntax:**

```
[no] vlan < vid > ip access-group < crf-list-name > connection-rate-filter
```

This command applies a connection-rate access control list (ACL) to inbound traffic on ports in the specified VLAN that are configured for connection-rate filtering. (A connection-rate ACL does not apply to ports in the VLAN that are not configured for connection-rate filtering.) The no form of the command removes the connection-rate ACL assignment from the VLAN.

**Note:** The switch allows only one connection-rate ACL assignment per VLAN. If a connection-rate ACL is already assigned to a VLAN and you assign another connection-rate ACL to that VLAN, the second ACL overwrites the first one. (A connection-rate ACL can be in addition to any standard or extended ACLs already assigned to the VLAN.)

Using CIDR Notation To Enter the ACE Mask

You can use CIDR (Classless Inter-Domain Routing) notation to enter ACE masks. The switch interprets the bits specified with CIDR notation as the IP address bits in an ACE and the corresponding IP address bits in a packet. The switch then converts the mask to inverse notation for ACE use.

**Table 3-2. Examples of CIDR Notation for Masks**

<table>
<thead>
<tr>
<th>IP Address Used In an ACL with CIDR Notation</th>
<th>Resulting ACL Mask</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>18.38.240.125/15</td>
<td>0.1.255.255</td>
<td>The leftmost 15 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/20</td>
<td>0.0.15.255</td>
<td>The leftmost 20 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/21</td>
<td>0.0.7.255</td>
<td>The leftmost 21 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/24</td>
<td>0.0.0.255</td>
<td>The leftmost 24 bits must match; the remaining bits are wildcards.</td>
</tr>
<tr>
<td>18.38.240.125/32</td>
<td>0.0.0.0</td>
<td>All bits must match.</td>
</tr>
</tbody>
</table>
For more on ACE masks, refer to “How an ACE Uses a Mask To Screen Packets for Matches” in the chapter titled “Access Control Lists (ACLs for the Series 5300xl Switches” in the Advanced Traffic Management Guide for your switch.

Example of Using an ACL in a Connection-Rate Configuration

This example adds connection-rate ACLs to the basic example on page 3-14.

![Sample Network Diagram](image)

**Figure 3-10. Sample Network**

In the basic example on page 3-14, the administrator configured connection-rate blocking on port D2. However:

- The administrator has elevated the connection-rate sensitivity to **high**.
- The server at IP address 15.45.50.17 frequently transmits a relatively high rate of legitimate connection requests, which now triggers connection-rate blocking of the server's IP address on port D2. This causes periodic, unnecessary blocking of access to the server.
The administrator needs to maintain blocking protection from the “Company Intranet” while allowing access to the server at 15.45.50.17. Because the server is carefully maintained as a trusted device, the administrator’s solution is to configure a connection-rate ACL that causes the switch to ignore (circumvent) connection-rate filtering for inbound traffic from the server, while maintaining the filtering for all other inbound routed traffic on port D2.

The configuration steps include:

1. Create the connection-rate ACL with a single entry:
   - Use the IP address of the desired server.
   - Include a CIDR notation of “32” for the ACL mask. (Which means the mask will allow only traffic whose SA exactly matches the specified IP address.)
   - The ACL will automatically include the implicit filter ACE as the last entry, which means that any traffic that is not from the desired server will be subject to filtering by the connection-rate policy configured on port D2.

2. Assigning the ACL to the VLAN through which traffic from the server enters the switch.

```plaintext
ProCurve(config)# ip access-list connection-rate-filter 17-server
ProCurve(config-crf-nacl)# ignore ip host 15.45.50.17
ProCurve(config-crf-nacl)# exit
ProCurve(config)# vlan 15
ProCurve(vlan-15)# ip access-group 17-server connection-rate-filter
ProCurve(vlan-15)# exit
ProCurve(config)# write mem
```

Figure 3-11. Creating and Assigning a Connection Rate ACL
ProCurve(config)# show config
Startup configuration:

; J4850A Configuration Editor; Created on release #E.09.01

hostname "ProCurve"
connection-rate-filter sensitivity high
ip access-list connection-rate-filter "17-server" ignore ip 15.45.50.17 0.0.0.0
exit
module 2 type J8161A
module 4 type J8161A
ip routing
snmp-server community "public" Unrestricted
snmp-server host 15.45.200.75 "public"
vlan 1
  name "DEFAULT_VLAN"
  untagged B5-B24
  ip address dhcp-bootp
  no untagged B1-B4 D1-D24
  ip proxy-arp
  exit
vlan 10
  name "VLAN10"
  untagged B1-B4
  no ip address
  ip proxy-arp
  exit
vlan 15
  name "VLAN15"
  untagged D1-D24
  no ip address
  ip proxy-arp
  ip access-group "17-server" connection-rate-filter
  exit
filter connection-rate B4 notify-only
filter connection-rate B1-B3 throttle
filter connection-rate B9 D1-D2 block

Figure 3-12. Example of Switch Configuration Display with a Connection-Rate ACL
Connection-Rate ACL Operating Notes

- A connection-rate ACL allows you to configure two types of ACEs (Access Control Entries):
  - **ignore < source-criteria >**: This ACE type directs the switch to permit all inbound traffic meeting the configured < source-criteria > without filtering the traffic through the connection-rate policy configured on the port through which the traffic entered the switch. For example, **ignore host 15.45.120.70** tells the switch to permit traffic from the host at 15.45.120.70 without filtering this host’s traffic through the connection-rate policy configured for the port on which the traffic entered the switch.
  - **filter < source-criteria >**: This ACE type does the opposite of an ignore entry. That is, all inbound traffic meeting the configured < source-criteria > must be filtered through the connection-rate policy configured for the port on which the traffic entered the switch. This option is most useful in applications where it is easier to use **filter** to specify suspicious traffic sources for screening than to use **ignore** to specify exceptions for trusted traffic sources that don’t need screening. For example, if the host at 15.45.127.43 requires connection-rate screening, but all other hosts in the VLAN do not, you would configure and apply a connection-rate ACL with **filter ip host 15.45.127.43** as the first ACE and **ignore ip any** as the second ACE. In this case, the traffic from host 15.45.127.43 would be screened, but traffic from all other hosts on the VLAN would be permitted without connection-rate screening.

- A connection-rate ACL includes a third, implicit **filter ip any** ACE which is automatically the last ACE in the ACL. This implicit ACE does not appear in displays of the ACL configuration, but is always present in any connection-rate ACL you configure. For example, assume that a port is configured with a connection-rate policy and is in a VLAN configured with a connection-rate ACL. If there is no match between an incoming packet and the ACE criteria in the ACL, then the implicit **filter ip any** sends the packet for screening by the connection-rate policy configured on that port. To preempt the implicit **filter ip any** in a given connection-rate ACL, you can configure **ignore IP any** as the last explicit ACE in the connection-rate ACL. The switch will then ignore (permit) traffic that is not explicitly addressed by other ACEs configured sequentially earlier in the ACL without filtering the traffic through the existing connection-rate policy.
Connection-Rate Log and Trap Messages

These messages appear in the switch’s Event Log. If SNMP trap receivers are configured on the switch, it also sends the messages to the designated receiver(s).

<table>
<thead>
<tr>
<th>Message</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address not found in list of blocked hosts.</td>
<td>Appears in the CLI when the <code>vlan &lt; vid &gt; connection-rate-filter unblock</code> command has been executed to unblock hosts that are not currently blocked.</td>
</tr>
<tr>
<td>W &lt; <code>mm/dd/yy hh:mm:ss</code> &gt; virusfilt: Source IP address <code>&lt;xxx.xxx.xxx.xxx&gt;</code> is exhibiting virus-like behavior</td>
<td>A warning that results when a port configured for <code>notify-only</code> detects a relatively high number of connection-rate attempts from a host.</td>
</tr>
<tr>
<td>W &lt; <code>mm/dd/yy hh:mm:ss</code> &gt; virusfilt: Source IP address <code>&lt;xxx.xxx.xxx.xxx&gt;</code> has been throttled</td>
<td>A warning and indication of the switch’s response when a port configured for <code>throttle</code> detects a relatively high number of connection-rate attempts from a host.</td>
</tr>
<tr>
<td>W &lt; <code>mm/dd/yy hh:mm:ss</code> &gt; virusfilt: Src IP <code>&lt;xxx.xxx.xxx.xxx&gt;</code> blocked</td>
<td>A warning and indication of the switch’s response when a port configured for <code>block</code> detects a relatively high number of connection-rate attempts from a host.</td>
</tr>
</tbody>
</table>
— This page is intentionally unused. —