

Virus Throttling (Connection-Rate Filtering)

Contents

Overview of Connection-Rate Filtering	3-3
Features and Benefits	3-4
General Operation	3-5
Filtering Options	3-5
Sensitivity to Connection Rate Detection	3-5
Application Options	3-6
Operating Rules	3-7
Unblocking a Currently Blocked Host	3-7
General Configuration Guidelines	3-8
For a network that is relatively attack-free:	3-8
For a network that appears to be under significant attack:	3-9
Configuring Connection-Rate Filtering	3-10
Global and Per-Port Configuration	3-10
Enabling Connection-Rate Filtering and Configuring Sensitivity	3-11
Configuring the Per-Port Filtering Mode	3-12
Example of a Basic Connection-Rate Filtering Configuration ..	3-13
Viewing and Managing Connection-Rate Status	3-15
Viewing Connection-Rate Configuration	3-15
Listing Currently-Blocked Hosts	3-17
Unblocking Currently-Blocked Hosts	3-17
Configuring and Applying Connection-Rate ACLs	3-19
Connection-Rate ACL Operation	3-20
Configuring a Connection-Rate ACL Using Source IP Address Criteria	3-21
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

Virus Throttling (Connection-Rate Filtering)

Contents

Example of Using an ACL in a Connection-Rate Configuration	3-27
Connection-Rate ACL Operating Notes	3-29
Connection-Rate Log and Trap Messages	3-31

Overview of Connection-Rate Filtering

Feature	Default	Page Ref
Global Configuration and Sensitivity	Disabled	3-11
Per-Port Configuration	None	3-12
Listing and Unblocking Blocked Hosts	n/a	3-17
Viewing the Current Configuration	n/a	3-15
Configuring Connection-Rate ACLs	None	3-19

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 individual 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 an interface 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 the switch, connection-rate filtering 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.

Features and Benefits

Connection-rate filtering is a countermeasure tool you can use in your incident-management program to help detect and manage worm-type IT security threats received in inbound IP 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 IP 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 IPv4 traffic received inbound with a relatively high rate of IP connection attempts.

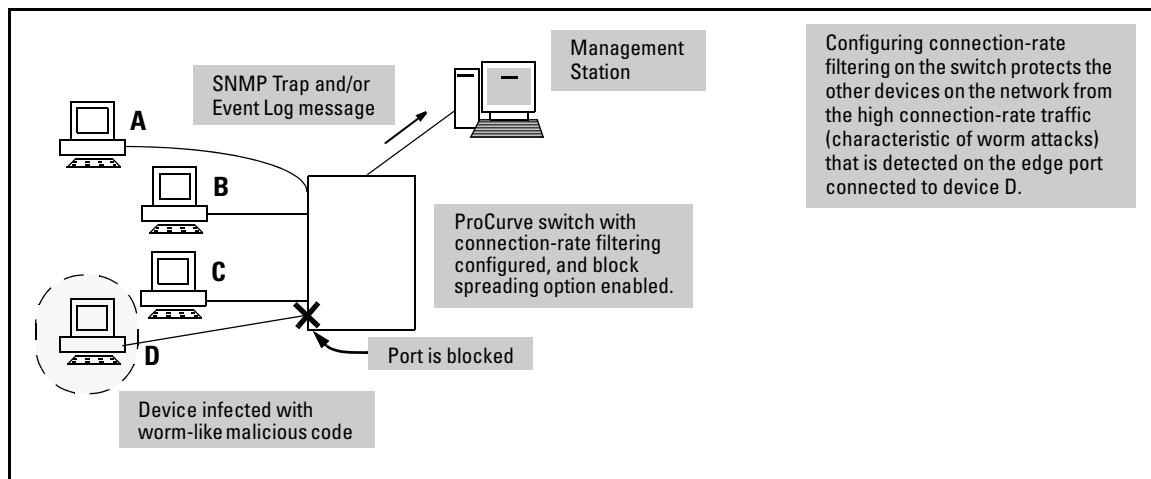


Figure 3-1. Example of Protecting a Network from Agents Using a High IP Connection Rate To Propagate

General Operation

Connection-rate filtering enables notification of worm-like behavior detected in inbound IP 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 IP 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 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's source IP address and (if a trap receiver is configured on the switch) a similar SNMP trap notice).
- **Throttle**: In this case, the switch temporarily blocks inbound IP traffic from the offending host source IP address 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 traffic from the host and continues to block this traffic if the apparent attack continues. (During the re-evaluation period, IP traffic from the host is allowed.)
- **Block**: This option blocks all IP traffic from the host. 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 a network administrator 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 an IP traffic source (including traffic with specific UDP or TCP criteria) from a connection-rate filtering policy. Otherwise, the ACL is not necessary.

Operating Rules

- Connection-rate filtering does not operate on IPv6 traffic.
- Connection-rate filtering is triggered by inbound IP traffic exhibiting high rates of IP connections to new hosts. After connection-rate filtering has been triggered on a port, all traffic from the suspect host is subject to the configured connection-rate policy (**notify-only**, **throttle**, or **block**).
- When connection-rate filtering is configured on a port, the port cannot be added to, or removed from, a port trunk group. Before this can be done, connection-rate filtering must be disabled on the port.
- Where the switch is throttling or blocking inbound IP traffic from a host, any outbound traffic destined for that host is still permitted.
- Once a throttle has been triggered on a port—temporarily blocking inbound IP traffic—it cannot be undone during operation: the penalty period must expire before traffic will be allowed from the host.

Unblocking a Currently Blocked Host

A host blocked by connection-rate filtering remains blocked until explicitly unblocked by one of the following methods:

- Using the **connection-rate-filter unblock** command (page 3-17).
- 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

Changing a port setting from **block** to **throttle**, **notify-only**, or to **no filter connection-rate**, does not unblock a currently blocked host. Similarly, applying a connection-rate ACL will not unblock a currently blocked host. Refer to the above list for the correct methods to use to unblock a host.

General Configuration Guidelines

As stated earlier, connection-rate filtering is triggered only by inbound IP traffic generating a relatively high number of new IP connection requests from the same host.

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. If SNMP trap receivers are available in your network, use the **snmp-server** command to configure the switch to send SNMP traps.
4. Monitor the Event Log or (if configured) the available SNMP trap receivers to identify hosts exhibiting high connection rates.
5. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
6. 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.)

7. Increase the sensitivity to **Medium** and repeat steps 5 and 6.

Note

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

8. (Optional.) Enable **throttle** or **block** mode on the monitored ports.

Note

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.

9. 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. If SNMP trap receivers are available in your network, use the **snmp-server** command to configure the switch to send SNMP traps.
4. Monitor the Event Log or the available SNMP trap receivers (if configured on the switch) to identify hosts exhibiting high connection rates.
5. Check any hosts that exhibit relatively high connection rate behavior to determine whether malicious code or legitimate use is the cause of the behavior.
6. 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 traffic from reliable hosts.

Configuring Connection-Rate Filtering

Command	Page
Global and Per-Port Configuration	
connection-rate-filter sensitivity < low medium high aggressive >	3-11
filter connection-rate < <i>port-list</i> > < notify-only throttle block >	3-12
show connection-rate-filter < blocked-host >	
Unblocking Hosts	
connection-rate-filter unblock	3-18

Note

As stated previously, connection-rate filtering is triggered by inbound IP traffic exhibiting a relatively high incidence of IP connection attempts from a single source.

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 avoid filtering traffic from specific, trusted source addresses.)

Enabling Connection-Rate Filtering and Configuring Sensitivity

Syntax: connection-rate-filter sensitivity < low | medium | high | aggressive >
no connection-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.*

Options for configuring sensitivity include:

low: *Sets the connection-rate sensitivity to the lowest possible sensitivity, which allows a mean of 54 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 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 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 destinations in less than 1 second, and a corresponding penalty time for Throttle mode (if configured) between 90 and 120 seconds.*

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

Note

The sensitivity settings configured on the switch determines the Throttle mode penalty periods as shown in Table 3-1 on page 3-12.

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 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 3-11). (Note: You can use connection-rate ACLs to create exceptions to the configured filtering policy. See “Configuring and Applying Connection-Rate ACLs” on page 3-19.) 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 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 IP connection attempts from a specific host, this option generates the **notify-only** messaging and also blocks all inbound traffic from the offending host for a penalty period. After the penalty period, the switch allows traffic from the offending host to resume, and re-examines the traffic. If the suspect behavior continues, the switch again blocks the 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 IP connection attempts from a specific host, this option generates the **notify-only** messaging and also blocks all inbound traffic from the offending host.*

Table 3-1. Throttle Mode Penalty Periods

Throttle Mode (Sensitivity)	Frequency of IP Connection Requests from the Same Source	Mean Number of New Destination Hosts in the Frequency Period	Penalty Period
Low	< 0.1 second	54	< 30 seconds
Medium	< 1.0 second	37	30 - 60 seconds
High	< 1.0 second	22	60 - 90 seconds
Aggressive	< 1.0 second	15	90 - 120 seconds

Example of a Basic Connection-Rate Filtering Configuration

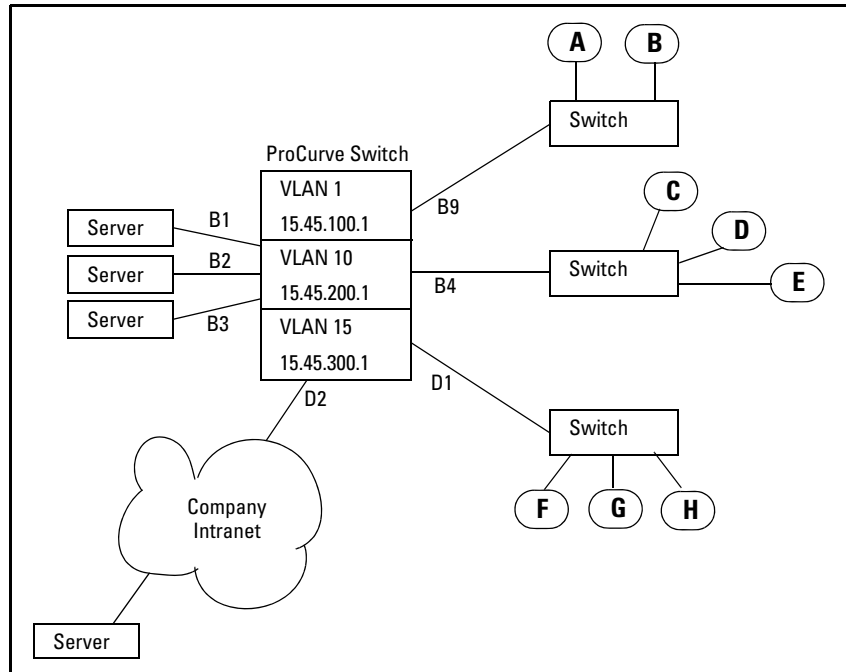


Figure 3-2. Sample Network

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 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.

Virus Throttling (Connection-Rate Filtering)

Configuring Connection-Rate Filtering

```
ProCurve(config)# connection-rate-filter sensitivity low
ProCurve(config)# filter connection-rate b1-b3 throttle
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
Startup configuration:
; J8697A Configuration Editor; Created on release #K.11.XX
hostname "ProCurve"
connection-rate-filter sensitivity low
module 2 type J8702A
module 4 type J8702A
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
```

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

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

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

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

Viewing 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 3-16).

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
Port                | Filter Mode
-----|-----
B13                 | NOTIFY-ONLY
B14                 | THROTTLE
B15                 | BLOCK
B16                 | BLOCK
```

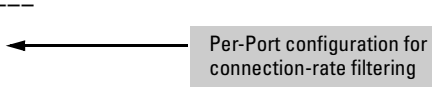


Figure 3-4. Example of Displaying the Connection-Rate Status, Sensitivity, and Per-Port Configuration

Virus Throttling (Connection-Rate Filtering)

Configuring Connection-Rate Filtering

To view the complete connection-rate configuration, including any ACLs (page 3-19), use **show config** (for the startup-config file) or **show running** (for the running-config file). For example:

```
ProCurve (config)# show config
Startup configuration:
; J8697A Configuration Editor; Created on
hostname "ProCurve"
connection-rate-filter sensitivity medium
ip access-list connection-rate-filter "Sample"
  filter ip 13.28.234.180 0.0.15.255
  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
snmp-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 13.28.234.181 255.255.240.0
  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
```

Entry showing that connection-rate-filtering is enabled and set to "medium" sensitivity.

Example of a connection-rate filtering ACL appearing in the configuration.

Example of a connection-rate filtering ACL appearing in a VLAN configuration.

Example of per-port connection-rate filtering policies appearing in the configuration.

Figure 3-5. Example of Connection-Rate Filtering Configuration in the Startup-Config File

Listing 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.

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

VLAN ID	Source IP Address	Filter Mode
10	13.28.234.175	THROTTLE
10	13.28.234.179	THROTTLE
15	13.28.234.180	BLOCK

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

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

VLAN ID	Source IP Address
15	13.28.234.180

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

Unblocking Currently-Blocked Hosts

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. (The source IP address 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
```

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: connection-rate-filter unblock < all | host | ip-addr >

all: *Unblocks all hosts currently blocked due to action by connection-rate filtering on ports where block mode has been configured.*

host < ip-addr >: *Unblocks the single host currently blocked due to action by connection-rate filtering on ports where block mode has been configured.*

ip-addr < mask > : *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: There is also an option to unblock any host belonging to a specific VLAN using the **vlan <vid> connection-rate-filter unblock** command.*

Note

For a complete list of options for unblocking hosts, see page 3-7.

Configuring and Applying Connection-Rate ACLs

Command	Page
ip access-list connection-rate-filter < crf-list-name >	3-21, 3-23
< filter ignore > ip < any host < ip-addr > ip-addr < mask >>	3-21
< filter ignore > < udp tcp > < source > < options >	3-23
vlan < vid > ip access-group < crf-list-name > connection-rate-filter	

A host sending legitimate 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 to 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 source IP address 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.

Note

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 Chapter 10, “IPv4 Access Control Lists (ACLs)”.

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.

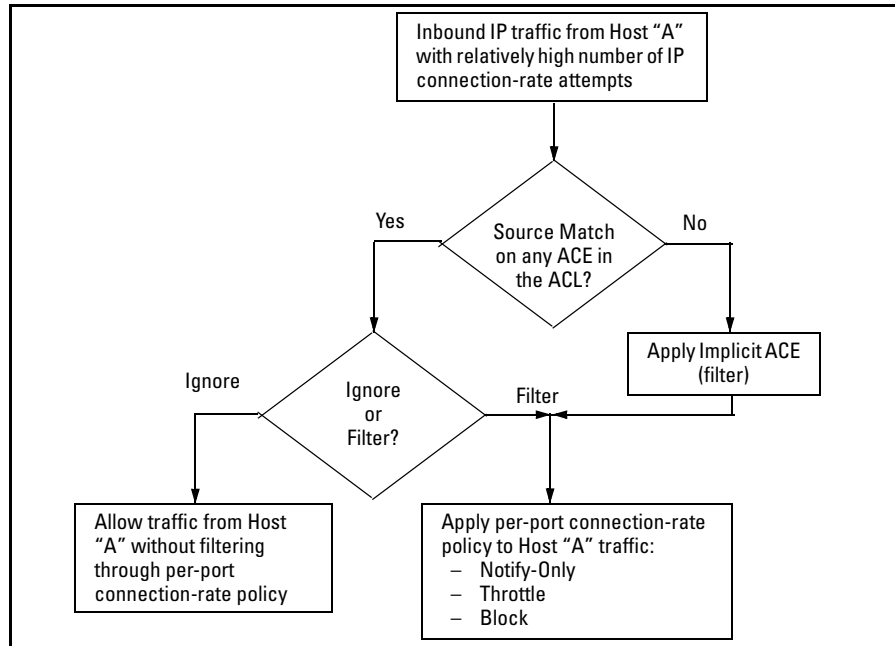


Figure 3-8. Connection-Rate ACL Applied to Traffic Received Through a Given Port

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 of the traffic that the ACE affects.

< filter | ignore >

The **filter** option assigns policy filtering to traffic with source IP address (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, refer to page 3-21.)

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 ACEs action (filter or ignore) to IP traffic having any SA.*

host < ip-addr >: *Applies the ACEs 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 >.

< tcp-data > or < 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-old: 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
```

Ignore (allow) tcp traffic from the host at 15.75.10.11 with both source and destination tcp ports of 1812.

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

Filter (drop) udp traffic from the subnet at 15.75.10.0 with a source udp port number not equal to 162 and a destination udp port number of 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

IP Address Used In an ACL with CIDR Notation	Resulting ACL Mask	Meaning
10.38.240.125/15	0.1.255.255	The leftmost 15 bits must match; the remaining bits are wildcards.
10.38.240.125/20	0.0.15.255	The leftmost 20 bits must match; the remaining bits are wildcards.
10.38.240.125/21	0.0.7.255	The leftmost 21 bits must match; the remaining bits are wildcards.
10.38.240.125/24	0.0.0.255	The leftmost 24 bits must match; the remaining bits are wildcards.
10.38.240.125/32	0.0.0.0	All bits must match.

For more on ACE masks, refer to “How an ACE Uses a Mask To Screen Packets for Matches” on page 10-38.

Example of Using an ACL in a Connection-Rate Configuration

This example adds connection-rate ACLs to the basic example on page 3-13.

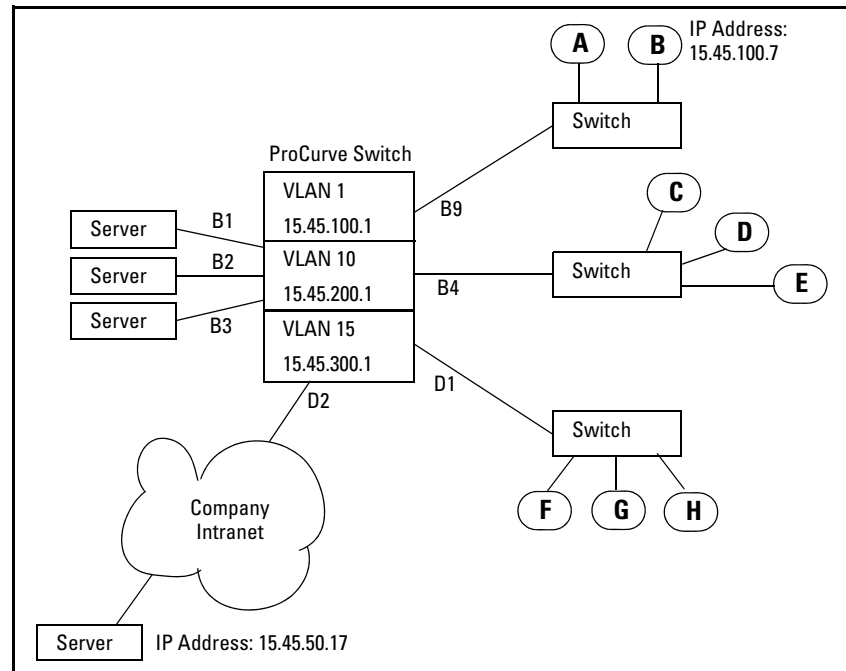


Figure 3-10. Sample Network

In the basic example on page 3-13, 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

Virus Throttling (Connection-Rate Filtering)

Configuring and Applying Connection-Rate ACLs

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 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 source IP address (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.

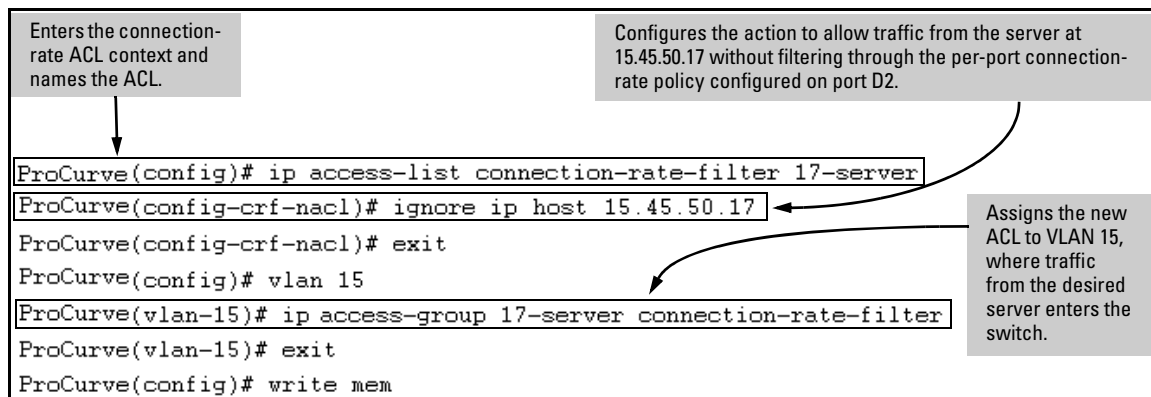


Figure 3-11. Creating and Assigning a Connection Rate ACL

```
ProCurve(config)# show config
Startup configuration:

; J8697A Configuration Editor; Created on release #K.11.XX

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 J8702A
module 4 type J8702A
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
```

The new switch configuration includes the ACL configured in figure 3-11.

Shows the assignment of the above connection-rate ACL to VLAN 15.

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

Connection-Rate ACL Operating Notes

- **ACE Types:** 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.
- **Implicit ACE**: 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.
- **Monitoring Shared Resources**: Active instances of throttling or blocking a client that is generating a high rate of connection requests uses internal routing switch resources that are shared with several other features. The routing switch provides ample resources for all features. However, if the internal resources become fully subscribed, new instances of throttling or blocking cannot be initiated until the necessary resources are released from other uses. (Event Log messages and SNMP traps are not affected.) For information on determining current resource availability and usage, refer to the appendix titled "Monitoring Resources" in the *Management and Configuration Guide* for your switch.

Connection-Rate Log and Trap Messages

These messages appear in the switch's Event Log identifying the source IP address of a connection-rate filtering event. If SNMP trap receivers are configured on the switch, it also sends the messages to the designated receiver(s).

Message	Meaning
Address not found in list of blocked hosts.	Appears in the CLI when the connection-rate-filter unblock command has been executed to unblock hosts that are not currently blocked.
W <mm/dd/yy hh:mm:ss> 00694 FFI: Src IP address <xxx.xxx.xxx.xxx> high connection rate, port <port number>	A warning that results when a port configured for notify-only detects a relatively high number of connection-rate attempts from a host.
W <mm/dd/yy hh:mm:ss> 00695 FFI: Src IP address <xxx.xxx.xxx.xxx> throttled, port <port number>	A warning and indication of the switch's response when a port configured for throttle detects a relatively high number of connection-rate attempts from a host.
W <mm/dd/yy hh:mm:ss> 00696 FFI: Src IP address <xxx.xxx.xxx.xxx> blocked, port <port number>	A warning and indication of the switch's response when a port configured for block detects a relatively high number of connection-rate attempts from a host.

Virus Throttling (Connection-Rate Filtering)
Connection-Rate Log and Trap Messages