

Copyright Information

Copyright © 2003 - 2007 Internetwork Expert, Inc. All rights reserved.

The following publication, ***CCIE Security Lab Workbook Volume I***, was developed by Internetwork Expert, Inc. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means without the prior written permission of Internetwork Expert, Inc.

Cisco®, Cisco® Systems, CCIE, and Cisco Certified Internetwork Expert, are registered trademarks of Cisco® Systems, Inc. and/or its affiliates in the U.S. and certain countries. All other products and company names are the trademarks, registered trademarks, and service marks of the respective owners. Throughout this manual, Internetwork Expert, Inc. has used its best efforts to distinguish proprietary trademarks from descriptive names by following the capitalization styles used by the manufacturer.

Disclaimer

The following publication, ***CCIE Security Lab Workbook Volume I***, is designed to assist candidates in the preparation for Cisco Systems' CCIE Routing & Switching Lab exam. While every effort has been made to ensure that all material is as complete and accurate as possible, the enclosed material is presented on an "as is" basis. Neither the authors nor Internetnetwork Expert, Inc. assume any liability or responsibility to any person or entity with respect to loss or damages incurred from the information contained in this workbook.

This workbook was developed by Internetnetwork Expert, Inc. and is an original work of the aforementioned authors. Any similarities between material presented in this workbook and actual CCIE™ lab material is completely coincidental.

Table of Contents

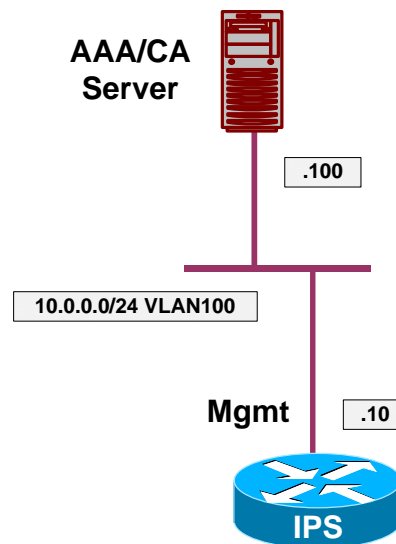
INTRUSION PREVENTION	1
BASIC CONFIGURATION.....	1
IPS Initial Setup	1
Configuring Inline VLAN Pair	4
Promiscuous Mode Monitoring with RSPAN.....	8
Monitoring IPS with IPS Event Viewer	13
EVENT PROCESSING	17
Configuring Event Summarization	17
Creating Custom Signature.....	20
Event Counting	22
Inline Blocking.....	25
Event Action Override.....	27
Event Action Filtering.....	31
IPS Network Access Control (Shunning)	34
Rate Limiting with IPS.....	39

Intrusion Prevention

Basic Configuration

IPS Initial Setup

Objective: Perform basic sensor setup, configuring IP addressing and remote access.



Directions

- Set up the IPS hostname to "IPS".
- Configure IP addressing for management interface as per the diagram, set default gateway to 10.0.0.254.
- Configure management access-list to permit only host 10.0.0.100.
- Enable management via telnet server and set the login banner to "Welcome to IPS".
- Set the system clock.
- Configure SW1 to put AAA/CA server and IPS management interface into the same VLAN 100.

Final Configuration

IPS:

```
IDS# conf t
IDS(config)# service host
IDS(config-hos)# network-settings
IDS(config-hos-net)# host-name IPS
IDS(config-hos-net)# host-ip 10.0.0.10/24,10.0.0.254
IDS(config-hos-net)# telnet-option enabled
IDS(config-hos-net)# login-banner-text Welcome to IPS
IDS(config-hos-net)# access-list 10.0.0.100/32
IDS(config-hos-net)# exit
IDS(config-hos)# exit
Apply Changes?[yes]: yes
IDS(config)# exit
IDS# clock set 17:07 January 5 2007
```

SW1:

```
vlan 100
!
interface range Fa 0/10 , Fa 0/20
 switchport host
 switchport access vlan 100
```

Verification

```
IDS# ping 10.0.0.100
PING 10.0.0.100 (10.0.0.100): 56 data bytes
64 bytes from 10.0.0.100: icmp_seq=0 ttl=128 time=2.1 ms
64 bytes from 10.0.0.100: icmp_seq=1 ttl=128 time=1.8 ms
64 bytes from 10.0.0.100: icmp_seq=2 ttl=128 time=0.7 ms
64 bytes from 10.0.0.100: icmp_seq=3 ttl=128 time=0.5 ms

--- 10.0.0.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.5/1.2/2.1 ms
```

```
IDS# exit
```

```
Welcome to IPS
```

```
IPS login: cisco
```

```
Password:
```

```
Last login: Fri Jan 5 23:49:20 on ttyS0
```

```
***NOTICE***
```

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at: <http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to

```
export@cisco.com.  
  
***LICENSE NOTICE***  
There is no license key installed on the system.  
The system will continue to operate with the currently installed  
signature set. A valid license must be obtained in order to apply  
signature updates. Please go to http://www.cisco.com/go/license  
to obtain a new license or install a license.  
IPS#  
  
IPS# conf t  
IPS(config)# serv host  
IPS(config-hos)# network-settings  
IPS(config-hos-net)# show setting  
network-settings  
-----  
host-ip: 10.0.0.10/24,10.0.0.254 default: 10.1.9.201/24,10.1.9.1  
host-name: IPS default: sensor  
telnet-option: enabled default: disabled  
access-list (min: 0, max: 512, current: 1)  
-----  
network-address: 10.0.0.100/32  
-----  
ftp-timeout: 300 seconds <defaulted>  
login-banner-text: Welcome to IPS default:  
-----
```

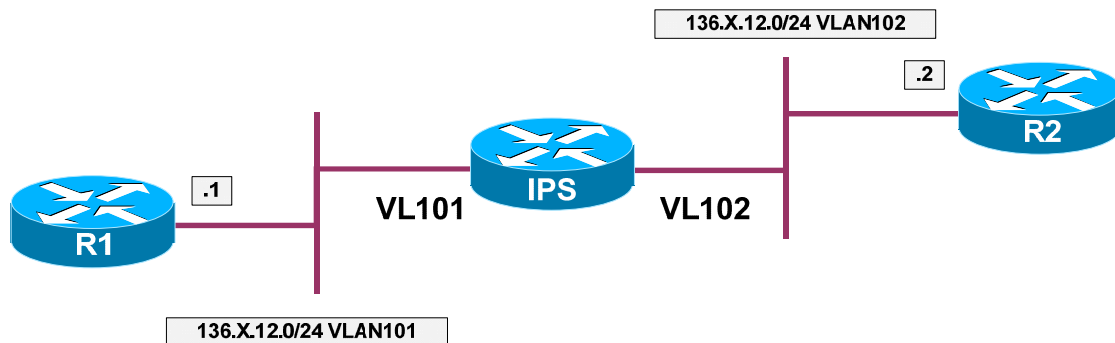


Further Reading

[IPS Initial Tasks](#)

Configuring Inline VLAN Pair

Objective: Configure IPS appliance inline mode with a VLAN pair.



Directions

- Create VLANs 101,102 on SW1 and SW2. Configure the switchports for R1 and R2 into respective VLANs.
- Configure trunk links between SW1 and SW2.
- Configure IP addressing on R1 and R2 as per the diagram.
- Configure the switchport for the IPS sensing interface as 802.1q trunk.
- Configure physical interface Fa 0/0 on IPS. Create subinterface 1 with “inline-vlan-pair” type. Map VLANs 101 and 102 as VLAN pair for this subinterface.
- Assign the subinterface to the analysis engine.

Final Configuration

IPS:

Create Inline VLAN Pair

```
IDS# conf t
IDS(config)# service interface
IDS(config-int)# physical-interfaces fastEthernet0/0
IDS(config-int-phy)# subinterface-type inline-vlan-pair
IDS(config-int-phy-inl)# subinterface 1
IDS(config-int-phy-inl-sub)# vlan1 101
IDS(config-int-phy-inl-sub)# vlan2 102
IDS(config-int-phy-inl-sub)# exit
IDS(config-int-phy-inl)# exit
IDS(config-int-phy)# admin-state enabled
IDS(config-int-phy)# exit
IDS(config-int)# exit
Apply Changes:[yes]: yes
```

Assign the subinterface to the Analysis Engine:

```
IDS(config)# service analysis-engine
IDS(config-ana)# virtual-sensor vs0
```

```
IDS(config-ana-vir)# physical-interface fastEthernet0/0 subinterface-number 1
IDS(config-ana-vir)# exit
IDS(config-ana)# exit
Apply Changes:[yes]: yes
IDS(config)#
```

SW1 & SW2:

```
!
! Create VLANs and configure trunks
!
vlan 101,102
!
interface range Fa 0/21 - 23
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

SW1:

```
!
! Configure access-ports for R1/R2:
!
interface Fa 0/1
 switchport host
 switchport access vlan 101
!
interface Fa 0/2
 switchport host
 switchport access vlan 102
```

SW2:

```
!
! Configure the link to the IPS sensing interface as Trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 101,102
 switchport mode trunk
```

R1:

```
interface Ethernet 0/0
 no shutdown
 ip address 136.1.12.1 255.255.255.0
```

R2:

```
interface Ethernet 0/0
 no shutdown
 ip address 136.1.12.2 255.255.255.0
```

Verification

```
R2#ping 136.1.12.1 repeat 100
```

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 136.1.12.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 4/4/20 ms
```

```
IDS# show events alert past 00:01:00
```

```
evIdsAlert: eventId=1167967799445317083 severity=medium vendor=Cisco
```



```
originator:
  hostId: IDS
  appName: sensorApp
  appInstanceId: 331
time: 2007/01/05 03:25:23 2007/01/05 03:25:23 UTC
signature: description=ICMP Flood id=2152 version=S1
  subsigId: 0
interfaceGroup:
vlan: 102
participants:
  attacker:
    addr: locality=OUT 136.1.12.2
  target:
    addr: locality=OUT 136.1.12.1
riskRatingValue: 75
interface: fe0_0
protocol: icmp
```

IDS# **show interfaces fastEthernet0/0**

MAC statistics from interface FastEthernet0/0

Statistics From Subinterface 1

Statistics From Vlan 101

```
Total Packets Received On This Vlan = 509
Total Bytes Received On This Vlan = 42108
Total Packets Transmitted On This Vlan = 105
Total Bytes Transmitted On This Vlan = 12070
```

Statistics From Vlan 102

```
Total Packets Received On This Vlan = 105
Total Bytes Received On This Vlan = 12070
Total Packets Transmitted On This Vlan = 509
Total Bytes Transmitted On This Vlan = 42108
```

Interface function = Sensing interface

Description =

Media Type = TX

Missed Packet Percentage = 0

Inline Mode = Subinterfaced

Pair Status = N/A

Link Status = Up

Link Speed = Auto_100

Link Duplex = Auto_Full

Total Packets Received = 1131

Total Bytes Received = 96372

Total Multicast Packets Received = 0

Total Broadcast Packets Received = 0

Total Jumbo Packets Received = 0

Total Undersize Packets Received = 0

Total Receive Errors = 0

Total Receive FIFO Overruns = 0

Total Packets Transmitted = 614

Total Bytes Transmitted = 54178

Total Multicast Packets Transmitted = 0

Total Broadcast Packets Transmitted = 0

Total Jumbo Packets Transmitted = 0

Total Undersize Packets Transmitted = 0

Total Transmit Errors = 0

Total Transmit FIFO Overruns = 0

Dropped Packets From Vlans Not Mapped To Subinterfaces = 517

Dropped Bytes From Vlans Not Mapped To Subinterfaces = 42194

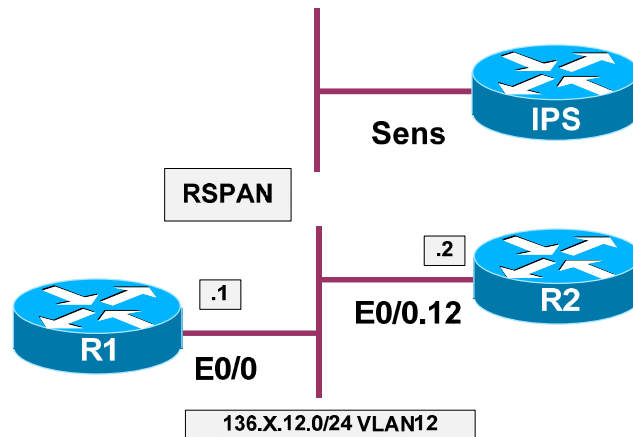


Further Reading

[Inline VLAN Pair Mode](#)

Promiscuous Mode Monitoring with RSPAN

Objective: Configure the IPS to monitor traffic in promiscuous mode.



Directions

- Assign the switchports of R1 on SW1 to the respective VLAN 12. Configure the trunk links between SW1 and SW2.
- Configure dot1q trunk between SW1 and R2, and create subinterface for VLAN 12 at R2
- Configure IP addressing on R1 and R2 per the diagram.
- Configure RSPAN source session on SW1 to monitor traffic on VLAN 12. Traffic should be sent over remote VLAN 500.
- Configure RSPAN remote monitoring session on SW2. Copy traffic arriving on VLAN 500 to port Fa 0/10. (IPS sensing interface).
- Enable physical interface Fa 0/0 on IPS, and assign it to the Analysis Engine.

Final Configuration

```

SW1 & SW2:
!
! Configure VLANs and trunk links
!
vlan 12
vlan 500
  remote
!
! Configure the trunk links between SW1 & SW2
!
interface Fa 0/23
  switchport trunk encapsulation dot1q
  switchport mode trunk

SW1:
!
! Assign switchports to the access VLAN
!
    
```

```

interface Fa 0/1
  switchport host
  switchport access vlan 12
!
interface Fa 0/2
  switchport trunk encapsulation dot1q
  switchport mode trunk
!
!  Configure RSPAN source session
!
monitor session 1 source vlan 12 rx
monitor session 1 destination remote vlan 500 reflector Fa 0/19

```

```

SW2:
!
!  Configure RSPAN destination session
!
monitor session 1 source remote vlan 500
monitor session 1 destination interface fa 0/10

```

```

R1:
interface Ethernet 0/0
  no shutdown
  ip address 136.1.12.1 255.255.255.0

```

```

R2:
interface Ethernet 0/0
  no shutdown
!
interface Ethernet 0/0.12
  encapsulation dot1q 12
  ip address 136.1.12.2 255.255.255.0

```

```

IPS:
!
!  Make sure Fa 0/0 is enabled and assign it to the virtual sensor
!
IPS# conf t
IPS(config)# service interface
IPS(config-int)# physical-interfaces fastEthernet0/0
IPS(config-int-phy)# admin-state enabled
IPS(config-int-phy)# exit
IPS(config-int)# exit
IPS(config)# service analysis-engine
IPS(config-ana)# virtual-sensor vs0
IPS(config-ana-vir)# physical-interface fastEthernet0/0
IPS(config-ana-vir)# exit
IPS(config-ana)# exit
Apply Changes:[yes]: yes

```

Verification

```
SW1#show vlan id 500
```

VLAN Name	Status	Ports
500 VLAN0500	active	Fa0/21, Fa0/22, Fa0/23

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----

```

500 enet 100500 1500 - - - - - 0 0

Remote SPAN VLAN
-----
Enabled

Primary Secondary Type          Ports
-----
SW1#show monitor session 1
Session 1
-----
Type           : Remote Source Session
Source VLANs   :
  RX Only      : 12
Dest RSPAN VLAN : 500

SW2#show vlan id 500

VLAN Name                Status    Ports
-----
500 VLAN0500              active    Fa0/13, Fa0/21, Fa0/22, Fa0/23

VLAN Type  SAID          MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
-----
500 enet  100500      1500 -     -     -     -   -         0      0

Remote SPAN VLAN
-----
Enabled

Primary Secondary Type          Ports
-----

SW2#show monitor session 1
Session 1
-----
Type           : Remote Destination Session
Source RSPAN VLAN : 500
Destination Ports : Fa0/10
  Encapsulation  : Native
  Ingress        : Disabled

R1#ping 136.1.12.2 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 99 percent (99/100), round-trip min/avg/max = 1/2/4 ms

IPS# show events alert past 00:01:00

evIdsAlert: eventId=1167967799445317308 severity=medium vendor=Cisco
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 331
time: 2007/01/06 13:12:24 2007/01/06 13:12:24 UTC
signature: description=ICMP Flood id=2152 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0

```

```

participants:
  attacker:
    addr: locality=OUT 136.1.12.1
  target:
    addr: locality=OUT 136.1.12.2
riskRatingValue: 75
interface: fe0_0
protocol: icmp

evIdsAlert: eventId=1167967799445317309 severity=medium vendor=Cisco
originator:
  hostId: IPS
  appName: sensorApp
  appInstanceId: 331
time: 2007/01/06 13:12:24 2007/01/06 13:12:24 UTC
signature: description=ICMP Flood id=2152 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: locality=OUT 136.1.12.1
  target:
    addr: locality=OUT 136.1.12.2
riskRatingValue: 75
interface: fe0_0
protocol: icmp

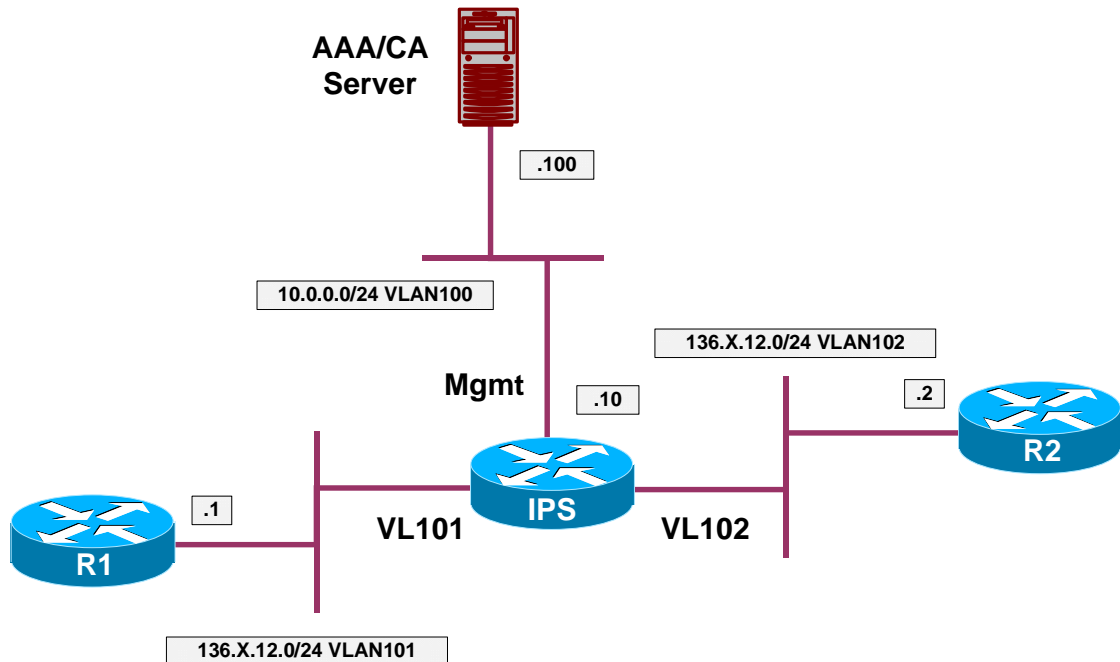
IPS# show interfaces
Interface Statistics
  Total Packets Received = 54529
  Total Bytes Received = 4362856
  Missed Packet Percentage = 0
  Current Bypass Mode = Auto_off
MAC statistics from interface FastEthernet0/0
  Interface function = Sensing interface
  Description =
  Media Type = TX
  Missed Packet Percentage = 0
  Inline Mode = Unpaired
  Pair Status = N/A
  Link Status = Up
  Link Speed = Auto_100
  Link Duplex = Auto_Full
  Total Packets Received = 54529
  Total Bytes Received = 4362856
  Total Multicast Packets Received = 0
  Total Broadcast Packets Received = 0
  Total Jumbo Packets Received = 0
  Total Undersize Packets Received = 0
  Total Receive Errors = 0
  Total Receive FIFO Overruns = 0
  Total Packets Transmitted = 41768
  Total Bytes Transmitted = 3143926
  Total Multicast Packets Transmitted = 0
  Total Broadcast Packets Transmitted = 0
  Total Jumbo Packets Transmitted = 0
  Total Undersize Packets Transmitted = 0
  Total Transmit Errors = 0
  Total Transmit FIFO Overruns = 0
<output omitted>

```

```
IPS# show statistics analysis-engine
Analysis Engine Statistics
  Number of seconds since service started = 140395
  Measure of the level of current resource utilization = 0
  Measure of the level of maximum resource utilization = 0
  The rate of TCP connections tracked per second = 0
  The rate of packets per second = 0
  The rate of bytes per second = 22
Receiver Statistics
  Total number of packets processed since reset = 42305
  Total number of IP packets processed since reset = 3410
Transmitter Statistics
  Total number of packets transmitted = 42548
  Total number of packets denied = 10686
  Total number of packets reset = 0
Fragment Reassembly Unit Statistics
  Number of fragments currently in FRU = 0
  Number of datagrams currently in FRU = 0
TCP Stream Reassembly Unit Statistics
  TCP streams currently in the embryonic state = 0
  TCP streams currently in the established state = 0
  TCP streams currently in the closing state = 0
  TCP streams currently in the system = 0
  TCP Packets currently queued for reassembly = 0
The Signature Database Statistics.
  Total nodes active = 6
  TCP nodes keyed on both IP addresses and both ports = 0
  UDP nodes keyed on both IP addresses and both ports = 1
  IP nodes keyed on both IP addresses = 1
Statistics for Signature Events
  Number of SigEvents since reset = 10
Statistics for Actions executed on a SigEvent
  Number of Alerts written to the IdsEventStore = 10
```

Monitoring IPS with IPS Event Viewer

Objective: Configure IPS Event Viewer to monitor the IPS appliance.



Directions

- Configure the devices as per the “Intrusion Prevention/Basic Configuration” scenario “[IPS Initial Setup](#)”.
- Configure the devices as per the “Intrusion Prevention/Basic Configuration” scenario “[Configuring Inline VLAN Pair](#)”.
- Add new device to IPS Event Viewer. Use IP address 10.0.0.10 and use HTTPs as communication protocol.

Final Configuration

IEV:

File > New > Device

Device Properties

New Sensor Information

Sensor IP Address: 10.0.0.10

Sensor Name: IPS

User Name: cisco

Password: *****

Web Server Port: 443

Choose the communication protocol

Use encrypted connection (https)

Use non-encrypted connection (http)

Event Start Time (UTC)

Latest Alerts

Start Date (YYYY:MM:DD): [] : [] : []

Start Time (HH:MM:SS): [] : [] : []

Exclude alerts of the following severity level(s)

Informational

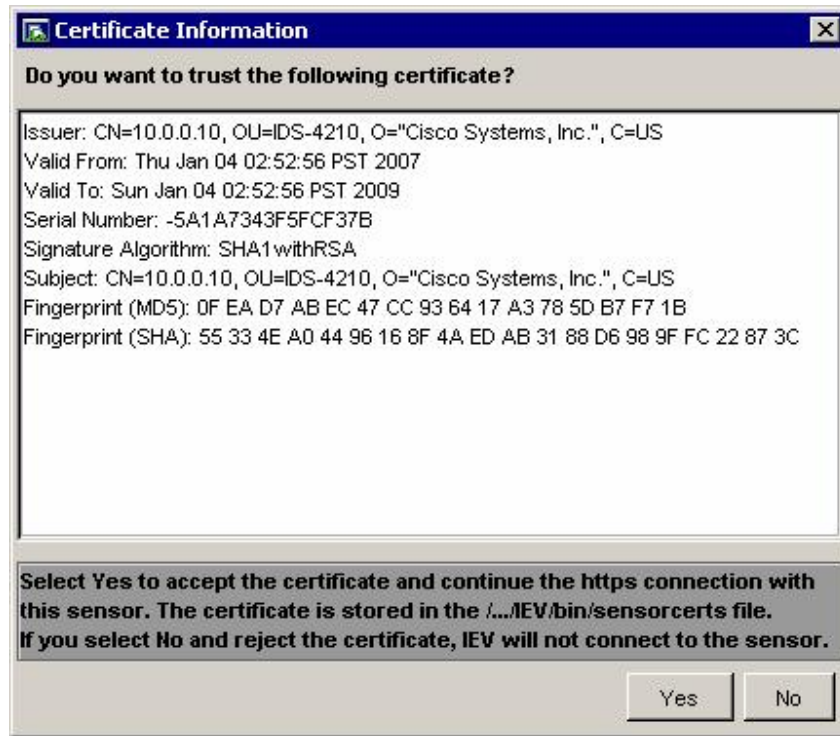
Low

Medium

High

OK Cancel

Accept the Certificate:



Verification

IEV:

Tools > RealTime Dashboard > Launch Dashboard

```
R2#ping 136.1.12.1 repeat 100
```

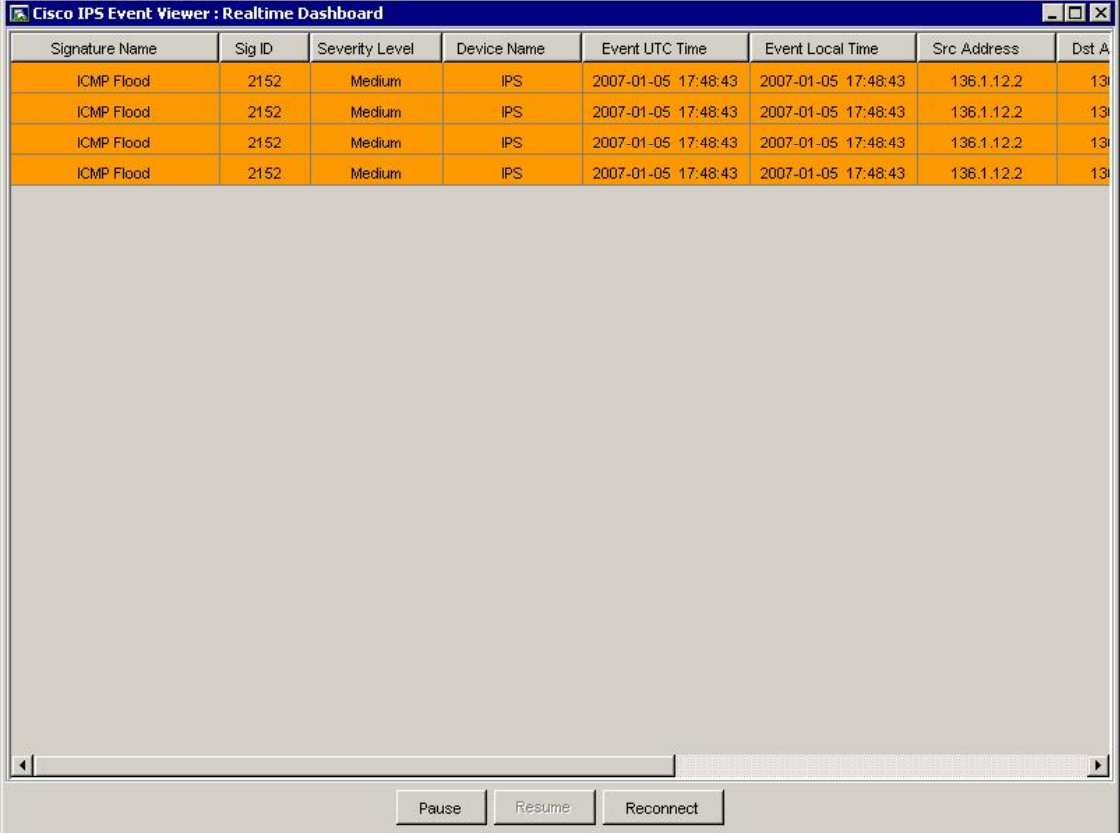
Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to 136.1.12.1, timeout is 2 seconds:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!  
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Success rate is 100 percent (100/100), round-trip min/avg/max = 4/4/8 ms

IEV:



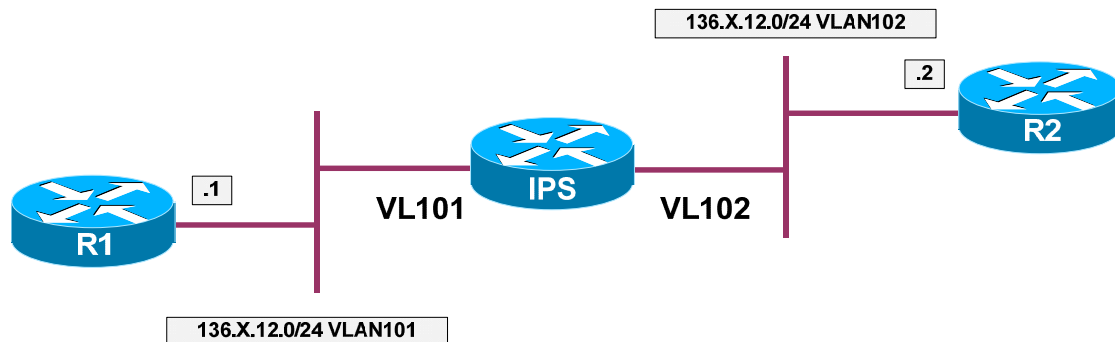
The screenshot displays the Cisco IPS Event Viewer Realtime Dashboard. It features a table with the following columns: Signature Name, Sig ID, Severity Level, Device Name, Event UTC Time, Event Local Time, Src Address, and Dst Address. The table contains four rows of data, all representing ICMP Flood events. Below the table is a large grey area, likely a log viewer, and a control bar with buttons for Pause, Resume, and Reconnect.

Signature Name	Sig ID	Severity Level	Device Name	Event UTC Time	Event Local Time	Src Address	Dst Address
ICMP Flood	2152	Medium	IPS	2007-01-05 17:48:43	2007-01-05 17:48:43	136.1.12.2	136.1.12.2
ICMP Flood	2152	Medium	IPS	2007-01-05 17:48:43	2007-01-05 17:48:43	136.1.12.2	136.1.12.2
ICMP Flood	2152	Medium	IPS	2007-01-05 17:48:43	2007-01-05 17:48:43	136.1.12.2	136.1.12.2
ICMP Flood	2152	Medium	IPS	2007-01-05 17:48:43	2007-01-05 17:48:43	136.1.12.2	136.1.12.2

Event Processing

Configuring Event Summarization

Objective: Configure IPS to summarize alerts produced by a signature



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario “[Configuring Inline VLAN pair](#)”
- Enable “ICMP Echo” signature (sig ID 2004) in the IPS
- Configure alert frequency to summarize alerts based on 15 seconds interval
- Do not perform global summarization, leave attacker/victim details in the reports

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 2004 0
Rack1IPS(config-sig-sig)# status
Rack1IPS(config-sig-sig-sta)# enabled true
Rack1IPS(config-sig-sig-sta)# exit
Rack1IPS(config-sig-sig)# alert-frequency
Rack1IPS(config-sig-sig-ale)# summary-mode summarize
Rack1IPS(config-sig-sig-ale-sum)# summary-interval 15
    
```

Verification

```

Rack1IPS(config-sig-sig)# alert-frequency
Rack1IPS(config-sig-sig-ale)# show settings
  alert-frequency
  -----
    
```

```

summary-mode
-----
  summarize
  -----
    summary-interval: 15 default: 30
    summary-key: AxBx <defaulted>
    specify-global-summary-threshold
    -----
      yes
      -----
        global-summary-threshold: 200 <defaulted>
        -----
          -----
            -----
              -----
                -----

```

Rack1R1#ping 136.1.12.2 size 1200 repeat 100

Type escape sequence to abort.
 Sending 100, 1200-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:
 !!!
 !!!
 Success rate is 100 percent (100/100), round-trip min/avg/max = 8/10/24 ms

Rack1IPS# show events alert past 00:01:00

```

evIdsAlert: eventId=1168711179445317212 severity=informational vendor=Cisco
  originator:
    hostId: Rack1IPS
    appName: sensorApp
    appInstanceId: 331
    time: 1993/04/16 05:26:39 1993/04/16 05:26:39 UTC
    signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
  interfaceGroup:
    vlan: 101
  participants:
    attacker:
      addr: locality=OUT 136.1.12.1
    target:
      addr: locality=OUT 136.1.12.2
  riskRatingValue: 25
  interface: fe0_0
  protocol: icmp

```

<output omitted>

```

evIdsAlert: eventId=1168711179445317229 severity=informational vendor=Cisco
  originator:
    hostId: Rack1IPS
    appName: sensorApp
    appInstanceId: 331
    time: 1993/04/16 05:26:54 1993/04/16 05:26:54 UTC
    signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
  interfaceGroup:
    vlan: 101
  participants:
    attacker:
      addr: locality=OUT 136.1.12.1
    target:
      addr: locality=OUT 136.1.12.2

```

```
summary: final=true initialAlert=1168711179445317212 summaryType=Regular 100
alertDetails: Regular Summary: 100 events this interval ;
riskRatingValue: 25
interface: fe0_0
protocol: icmp
```

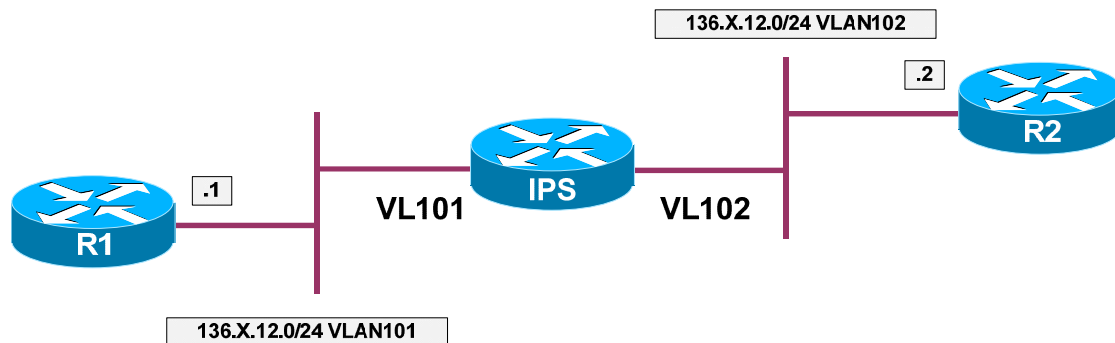


Further Reading

[Alert Frequency](#)

Creating Custom Signature

Objective: Create custom signature in the IPS to catch pre-defined string in telnet session



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario [“Configuring Inline VLAN pair”](#)
- Create new signature number 60005, based on TCP.STRING engine
- Configure new signature to watch connections on TCP port 23
- Configure new signature to match on string “% Bad passwords”
- This signature should fire an alarm on every occurrence of the string

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# engine string-tcp
Rack1IPS(config-sig-sig-str)# service-ports 23
Rack1IPS(config-sig-sig-str)# direction from-service
Rack1IPS(config-sig-sig-str)# regex-string % Bad passwords
Rack1IPS(config-sig-sig-str)# exit
Rack1IPS(config-sig-sig)# alert-frequency
Rack1IPS(config-sig-sig-ale)# summary-mode fire-all
Rack1IPS(config-sig-sig-ale-fir)# exit
Rack1IPS(config-sig-sig-ale)# exit
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes:[yes]: yes
    
```

Verification

```

R2:
line vty 0 4
 login
    
```

```

password cisco

Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open

User Access Verification


Password: a
Password: a
Password: a
% Bad passwords

[Connection to 136.1.12.2 closed by foreign host]

Rack1IPS# show events alert past 00:01:00

evIdsAlert: eventId=1168711179445317231 severity=medium vendor=Cisco
  originator:
    hostId: Rack1IPS
    appName: sensorApp
    appInstanceId: 331
    time: 1993/04/16 05:54:51 1993/04/16 05:54:51 UTC
    signature: description=My Sig id=60005 version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup:
    vlan: 102
  participants:
    attacker:
      addr: locality=OUT 136.1.12.2
      port: 23
    target:
      addr: locality=OUT 136.1.12.1
      port: 11002
  context:
    fromTarget:
000000  FF FB 01 FF FB 03 FF FD  18 FF FD 1F 0D 0A 0D 0A  .....
000010  55 73 65 72 20 41 63 63  65 73 73 20 56 65 72 69  User Access Veri
000020  66 69 63 61 74 69 6F 6E  0D 0A 0D 0A 50 61 73 73  fication....Pass
000030  77 6F 72 64 3A 20 FF FE  20 FF FD 21 FF FA 21 00  word: .. ..!...!
000040  FF F0 FF FE 18 0D 0A 50  61 73 73 77 6F 72 64 3A  .....Password:
000050  20 0D 0A 50 61 73 73 77  6F 72 64 3A 20          ..Password:
      fromAttacker:
000000  FF FD 03 FF FB 20 FF FB  1F FF FB 21 FF FD 01 FF  ..... ..!....
000010  FC 18 FF FA 1F 00 50 00  18 FF F0 FF FC 20 61 0D  .....P..... a.
000020  0A 61 0D 0A 61 0D 0A 0D  0A 25 20 42 61 64 20 70  .a..a....% Bad p
000030  61 73 73 77 6F 72 64          assword
    riskRatingValue: 56
    interface: fe0_0
    protocol: tcp

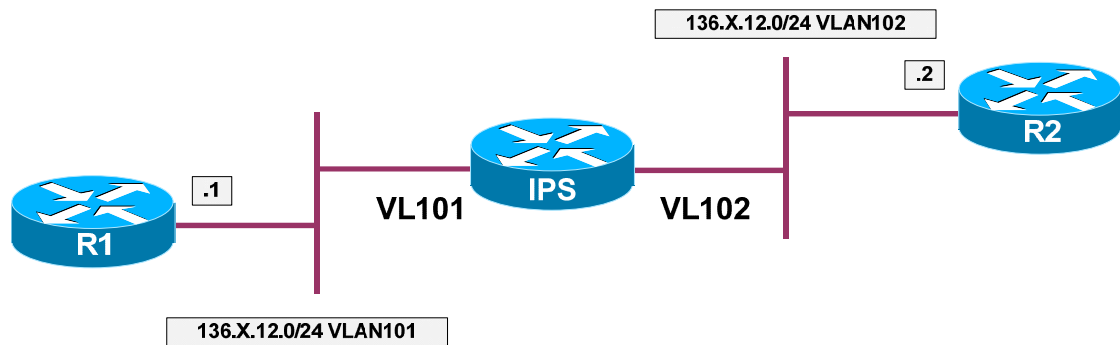
```

 **Further Reading**

[String TPC Engine Parameters](#)

Event Counting

Objective: Configure IPS to generate an alert once free unsuccessful login attempts have been performed in last 3 minutes



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario [“Creating Custom Signature”](#)
- Change signature 60005 settings as follows:
 - Enable Event Counting
 - Configure to respond with an alert on three consecutive events
 - Enable alert-interval, and set it to 3 minutes (180 seconds)

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# event-counter
Rack1IPS(config-sig-sig-eve)# event-count 3
Rack1IPS(config-sig-sig-eve)# specify-alert-interval yes
Rack1IPS(config-sig-sig-eve-yes)# alert-interval 180
    
```

Verification

```

R2:
line vty 0 4
 login
 password cisco

Fail logging-in three times in a row:

Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open
    
```

User Access Verification

```

Password:
Password:
Password:
% Bad passwords
    
```

[Connection to 136.1.12.2 closed by foreign host]

```

Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open
    
```

User Access Verification

```

Password:
Password:
Password:
% Bad passwords
    
```

[Connection to 136.1.12.2 closed by foreign host]

```

Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open
    
```

User Access Verification

```

Password:
Password:
Password:
% Bad passwords
    
```

[Connection to 136.1.12.2 closed by foreign host]

```

Rack1IPS# show events alert past 00:03:00
    
```

```

evIdsAlert: eventId=1168711179445317235 severity=medium vendor=Cisco
  originator:
    hostId: Rack1IPS
    appName: sensorApp
    appInstanceId: 331
  time: 1993/04/16 06:03:39 1993/04/16 06:03:39 UTC
  signature: description=My Sig id=60005 version=custom
    subsigId: 0
    sigDetails: My Sig Info
  interfaceGroup:
  vlan: 102
  participants:
    attacker:
      addr: locality=OUT 136.1.12.2
      port: 23
    target:
      addr: locality=OUT 136.1.12.1
      port: 11005
  context:
    fromTarget:
    
```

```

000000 FF FB 01 FF FB 03 FF FD 18 FF FD 1F 0D 0A 0D 0A .....
000010 55 73 65 72 20 41 63 63 65 73 73 20 56 65 72 69 User Access Veri
000020 66 69 63 61 74 69 6F 6E 0D 0A 0D 0A 50 61 73 73 fication....Pass
000030 77 6F 72 64 3A 20 FF FE 20 FF FD 21 FF FA 21 00 word: .. ..!..!.
000040 FF F0 FF FE 18 0D 0A 50 61 73 73 77 6F 72 64 3A .....Password:
000050 20 0D 0A 50 61 73 73 77 6F 72 64 3A 20 ..Password:
    
```

```
fromAttacker:
000000  FF FD 03 FF FB 20 FF FB 1F FF FB 21 FF FD 01 FF ..... !....
000010  FC 18 FF FA 1F 00 50 00 18 FF F0 FF FC 20 63 0D .....P..... c.
000020  0A 63 0D 0A 63 0D 0A 0D 0A 25 20 42 61 64 20 70 .c..c....% Bad p
000030  61 73 73 77 6F 72 64                                assword
    riskRatingValue: 56
    interface: fe0_0
    protocol: tcp
```

Wait for counters to reset (3 minutes) and fail logging just once:

```
Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open
```

User Access Verification

```
Password:
Password:
Password:
% Bad passwords
```

```
Rack1IPS# show events alert past 00:03:00
```

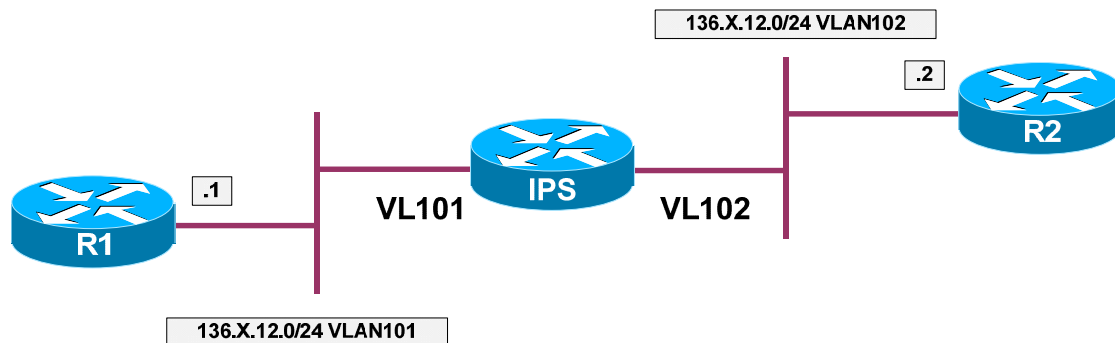


Further Reading

[Master Engine: General Parameters](#)

Inline Blocking

Objective: Configure IPS to block inline on event occurrence



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario “[Creating Custom Signature](#)”
- Change signature 60005 settings to respond with event-action “deny-attacker-inline”

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# engine string-tcp
Rack1IPS(config-sig-sig-str)# event-action deny-attacker-inline
Rack1IPS(config-sig-sig-str)# exit
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes?[yes]: yes
    
```

Verification

```

R2:
line vty 0 4
 login
 password cisco

Rack1R1#telnet 136.1.12.2
Trying 136.1.12.2 ... Open

User Access Verification

Password:
Password:
Password:
    
```

```
Rack1IPS# show statistics denied-attackers
Denied Attackers and hit count for each.
 136.1.12.2 = 11
Statistics for Virtual Sensor vs0
  Denied Attackers with percent denied and hit count for each.
      Attacker Address  Victim Address  Port  Protocol  Requested
Percentage  Actual Percentage  Hit Count
 136.1.12.2
100          11          100

Rack1IPS# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of
attackers currently being denied by the sensor.
Continue with clear? [yes]: yes
```

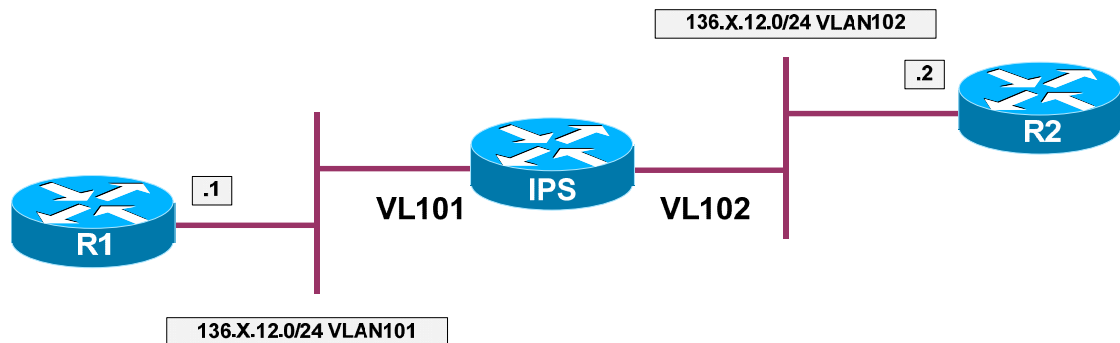


Further Reading

[Understanding the Deny Attackers Inline Event Action](#)

Event Action Override

Objective: Configure IPS to override event actions based on calculated Risk Rating



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario [“Creating Custom Signature”](#)
- Configure TVR (Target Value Rating) for IP address of R2 to “mission-critical”
- Change signature 60005 settings to have the value of SFR (signature fidelity rating) of 100 and Severity of “High”
- Configure Event Override to set action “deny-attacker-inline” for RR range 80-100

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service event-action-rules
Rack1IPS(config)# service event-action-rules rule0
Rack1IPS(config-rul)# target-value mission-crit target-add 136.1.12.2
Rack1IPS(config-rul)# overrides deny-attacker-inline
Rack1IPS(config-rul-ove)# risk-rating-range 80-100
Rack1IPS(config-rul-ove)# exit
Rack1IPS(config-rul)# exit
Apply Changes:[yes]: yes
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# alert-severity high
Rack1IPS(config-sig-sig)# sig-fidelity-rating 100
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes:[yes]: yes
    
```

Verification

R2:

```
line vty 0 4
 login
 password cisco
```

```
Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open
```

User Access Verification

```
Password:
Password:
Password:
```

```
Rack1IPS# show events alert past 00:03:00
```

```
evIdsAlert: eventId=1168711179445317245 severity=high vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
  time: 1993/04/16 06:57:27 1993/04/16 06:57:27 UTC
  signature: description=My Sig id=60005 version=custom
  subsigId: 0
  sigDetails: My Sig Info
  interfaceGroup:
  vlan: 102
  participants:
    attacker:
      addr: locality=OUT 136.1.12.2
      port: 23
    target:
      addr: locality=OUT 136.1.12.1
      port: 11008
  actions:
    deniedAttacker: true
  context:
    fromTarget:
000000 FF FB 01 FF FB 03 FF FD 18 FF FD 1F 0D 0A 0D 0A .....
000010 55 73 65 72 20 41 63 63 65 73 73 20 56 65 72 69 User Access Veri
000020 66 69 63 61 74 69 6F 6E 0D 0A 0D 0A 50 61 73 73 fication....Pass
000030 77 6F 72 64 3A 20 FF FE 20 FF FD 21 FF FA 21 00 word: .. !!!.
000040 FF F0 FF FE 18 0D 0A 50 61 73 73 77 6F 72 64 3A .....Password:
000050 20 0D 0A 50 61 73 73 77 6F 72 64 3A 20 ..Password:
    fromAttacker:
000000 FF FD 03 FF FB 20 FF FB 1F FF FB 21 FF FD 01 FF ..... !....
000010 FC 18 FF FA 1F 00 50 00 18 FF F0 FF FC 20 61 0D .....P..... a.
000020 0A 61 0D 0A 61 0D 0A 0D 0A 25 20 42 61 64 20 70 .a..a....% Bad p
000030 61 73 73 77 6F 72 64 password
    riskRatingValue: 100
    interface: fe0_0
    protocol: tcp
```

```
Rack1IPS# clear denied-attackers
```

```
Warning: Executing this command will delete all addresses from the list of
attackers currently being denied by the sensor.
Continue with clear? [yes]: yes
```

Lower Severity and Fidelity for the custom signature:

```

Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# alert-severity low
Rack1IPS(config-sig-sig)# sig-fidelity-rating 10
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes:[yes]: yes

Rack1R1>telnet 136.1.12.2
Trying 136.1.12.2 ... Open

User Access Verification

Password:
Password:
Password:
% Bad passwords

[Connection to 136.1.12.2 closed by foreign host]

Rack1IPS# show events alert past 00:03:00

evIdsAlert: eventId=1168711179445317251 severity=low vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
time: 1993/04/16 07:01:53 1993/04/16 07:01:53 UTC
signature: description=My Sig id=60005 version=custom
  subsigId: 0
  sigDetails: My Sig Info
interfaceGroup:
vlan: 102
participants:
  attacker:
    addr: locality=OUT 136.1.12.2
    port: 23
  target:
    addr: locality=OUT 136.1.12.1
    port: 11009
context:
  fromTarget:
000000 FF FB 01 FF FB 03 FF FD 18 FF FD 1F 0D 0A 0D 0A .....
000010 55 73 65 72 20 41 63 63 65 73 73 20 56 65 72 69 User Access Veri
000020 66 69 63 61 74 69 6F 6E 0D 0A 0D 0A 50 61 73 73 fication...Pass
000030 77 6F 72 64 3A 20 FF FE 20 FF FD 21 FF FA 21 00 word: .. !...!
000040 FF F0 FF FE 18 0D 0A 50 61 73 73 77 6F 72 64 3A .....Password:
000050 20 0D 0A 50 61 73 73 77 6F 72 64 3A 20 ..Password:
  fromAttacker:
000000 FF FD 03 FF FB 20 FF FB 1F FF FB 21 FF FD 01 FF ..... !....
000010 FC 18 FF FA 1F 00 50 00 18 FF F0 FF FC 20 61 0D .....P..... a.
000020 0A 61 0D 0A 61 0D 0A 0D 0A 25 20 42 61 64 20 70 .a..a....% Bad p
000030 61 73 73 77 6F 72 64
  riskRatingValue: 5
  interface: fe0_0
  protocol: tcp

```

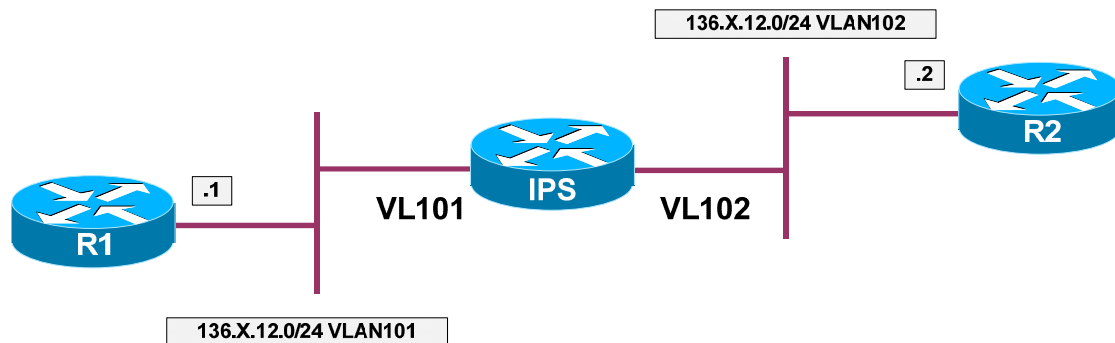



Further Reading

[Configuring Event Action Rules](#)

Event Action Filtering

Objective: Configure IPS to filter event actions based on calculated Risk Rating



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario “[Creating Custom Signature](#)”
- Set custom signature 60005 event-action to “deny-attacker-inline”
- Change signature 60005 settings to have the value of SFR (signature fidelity rating) of 50 and Severity of “Low”
- Configure TVR (Target Value Rating) for IP address of R2 to “Low”
- Configure Event Filter to subtract action “deny-attacker-inline” for RR range 0-40 and signature ID 60005

Final Configuration

```

IPS:
Rack1IPS# conf t
Rack1IPS(config)# service signature-definition sig0
Rack1IPS(config-sig)# signatures 60005 0
Rack1IPS(config-sig-sig)# engine string-tcp
Rack1IPS(config-sig-sig-str)# event-action deny-attacker-inline
Rack1IPS(config-sig-sig-str)# exit
Rack1IPS(config-sig-sig)# sig-fidelity-rating 50
Rack1IPS(config-sig-sig)# alert-severity low
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes:[yes]: yes
Rack1IPS(config)# service event-action-rules rules0
Rack1IPS(config-rul)# target-value low target-address 136.1.12.2
Rack1IPS(config-rul)# filters insert FILTER1 begin
Rack1IPS(config-rul-fil)# signature-id-range 60005-60005
Rack1IPS(config-rul-fil)# risk-rating-range 0-40
Rack1IPS(config-rul-fil)# actions-to-remove deny-attacker-inline
Rack1IPS(config-rul-fil)# exit
Apply Changes:[yes]: yes
    
```

Verification

```

R2:
line vty 0 4
  login
  password cisco

Rack1R1#telnet 136.1.12.2
Trying 136.1.12.2 ... Open

User Access Verification

Password: a
Password: a
Password: a
% Bad passwords

[Connection to 136.1.12.2 closed by foreign host]

No event has been generated:

Rack1IPS# show events alert past 00:01:00

Rack1IPS# conf t
Rack1IPS(config)# service event-action-rules rules0
Rack1IPS(config-rul)# filters edit FILTER1
Rack1IPS(config-rul-fil)# show settings
  NAME: FILTER1
  -----
  signature-id-range: 60005-60005 default: 900-65535
  subsignature-id-range: 0-255 <defaulted>
  attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
  victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
  attacker-port-range: 0-65535 <defaulted>
  victim-port-range: 0-65535 <defaulted>
  risk-rating-range: 0-40 default: 0-100
  actions-to-remove: deny-attacker-inline default:
  deny-attacker-percentage: 100 <defaulted>
  filter-item-status: Enabled <defaulted>
  stop-on-match: False <defaulted>
  user-comment: <defaulted>
  -----
Rack1IPS(config-rul-fil)# filter-item-status disabled
Rack1IPS(config-rul-fil)# exit
Rack1IPS(config-rul)# exit
Apply Changes?[yes]: yes

Rack1R1#telnet 136.1.12.2
Trying 136.1.12.2 ... Open

User Access Verification

Password:a
Password:a
Password:a

Attack blocked:

Rack1IPS# show statistics denied-attackers

```

Denied Attackers and hit count for each.

136.1.12.2 = 12

Statistics for Virtual Sensor vs0

Denied Attackers with percent denied and hit count for each.

Attacker Address	Victim Address	Port	Protocol	Requested
Percentage	Actual Percentage	Hit Count		
100	136.1.12.2	12		100

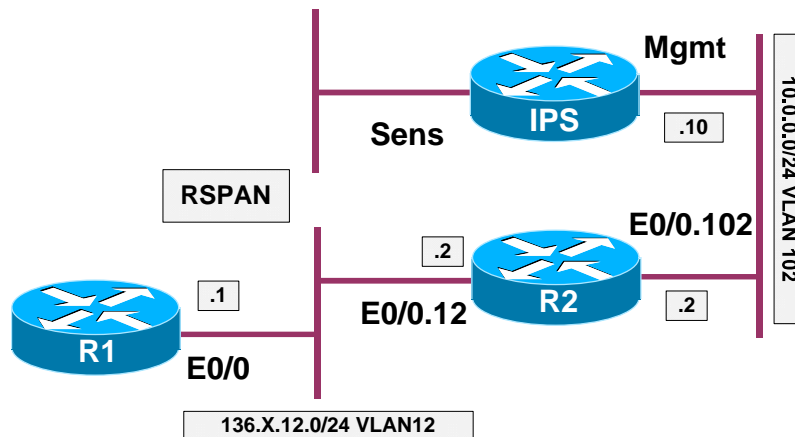


Further Reading

[Configuring Event Action Rules](#)

IPS Network Access Control (Shunning)

Objective: Configure IPS respond to attack by configuring blocking rule in a router



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario “[IPS Initial Setup](#)”
- Configure the devices per the “Intrusion Prevention/Basic Configuration” scenario “Promiscuous Mode Monitoring with RSPAN”
- Create VLAN100 and configure IP address for the link between the IPS management interface and R2, using subinterface for VLAN 100 at R2
- Configure R2 for remote access as follows:
 - Terminal line should ask for password “CISCO”
 - Enable password should be “CISCO”
- Configure user profile named R2_PROFILE on the IPS to match those requirement
- Configure router device on the IPS to access R2 (IP 10.0.0.2) and associate it with user profile named R2_PROFILE. Use telnet to access R2
- This router device should block ingress on Ethernet 0/0.12
- Tune signature 2152 (ICMP Flood) to respond with “request-block-host”

Final Configuration

```

SW1:
vlan 100
!
interface FastEthernet 0/10
 switchport mode access
 switchport access vlan 100

R2:

```

```

interface Ethernet 0/0.100
  encapsulation dot1q 100
  ip address 10.0.0.2 255.255.255.0
  !
  ! Access Control
  !
no aaa new-model
enable secret CISCO
!
line vty 0 4
  password CISCO
  login

IPS:
!
! Create a user profile
!
Rack1IPS# conf t
Rack1IPS(config)# service network-access
Rack1IPS(config-net)# user-profiles R2_PROFILE
Rack1IPS(config-net-use)# password
Enter password[: CISCO
Re-enter password: CISCO
Rack1IPS(config-net-use)# enable-password
Enter enable-password[: CISCO
Re-enter enable-password: CISCO
Rack1IPS(config-net-use)# exit
!
! Configure router device
!
Rack1IPS(config-net)# router-devices 10.0.0.2
Rack1IPS(config-net-rou)# profile-name R2_PROFILE
Rack1IPS(config-net-rou)# communication telnet
Rack1IPS(config-net-rou)# block-interfaces E0/0.12 in
Rack1IPS(config-net-rou-blo)# exit
Rack1IPS(config-net-rou)# exit
Rack1IPS(config-net)# exit
Apply Changes:[yes]: yes
!
! Tune Signature 2152
!
Rack1IPS(config-sig)# signatures 2152 0
Rack1IPS(config-sig-sig)# engine flood-host
Rack1IPS(config-sig-sig-flo)# event-action request-block-host
Rack1IPS(config-sig-sig-flo)# exit
Rack1IPS(config-sig-sig)# exit
Rack1IPS(config-sig)# exit
Apply Changes:[yes]: yes

```

Verification

```
Rack1R1#ping 136.1.12.2 repeat 100
```

Type escape sequence to abort.

Sending 100, 100-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:


```
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
time: 1993/04/17 08:06:51 1993/04/17 08:06:51 UTC
shunInfo:
  host: connectionShun=false
  srcAddr: 136.1.12.1
  vlan: 0
  destAddr: 136.1.12.2
  protocol: numericType=1 other
  timeoutMinutes: 30
evAlertRef: hostId=Rack1IPS

evStatus: eventId=1168711179445317323 vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: nac
  appInstanceId: 274
time: 1993/04/17 08:06:51 1993/04/17 08:06:51 UTC
shunEntryAdded:
  description: Router [10.0.0.2] has added a block to the ACL.
  shunInfo:
    host:
      srcAddr: 136.1.12.1
      srcPort: 0
      destAddr: 136.1.12.2
      destPort: 0
      protocol: numericType=1
      vlan: 0
      interface:
      timeoutMinutes: 30

evIdsAlert: eventId=1168711179445317324 severity=informational vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
time: 1993/04/17 08:07:05 1993/04/17 08:07:05 UTC
signature: description=ICMP Echo Request id=2004 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: locality=OUT 136.1.12.1
  target:
    addr: locality=OUT 136.1.12.2
summary: final=true initialAlert=1168711179445317307 summaryType=Regular 100
alertDetails: Regular Summary: 100 events this interval ;
riskRatingValue: 50
interface: fe0_0
protocol: icmp

Rack1R2#show ip access-lists
Extended IP access list IDS_E0/0.12_in_1
 10 permit ip host 10.0.0.10 any
 20 deny ip host 136.1.12.1 any (21 matches)
 30 permit ip any any

Rack1R2#sh run int eth 0/0.12
```



```
Building configuration...
Current configuration : 130 bytes
!
interface Ethernet0/0.12
 encapsulation dot1Q 12
 ip address 136.1.12.2 255.255.255.0
 ip access-group IDS_E0/0.12_in_1 in
```

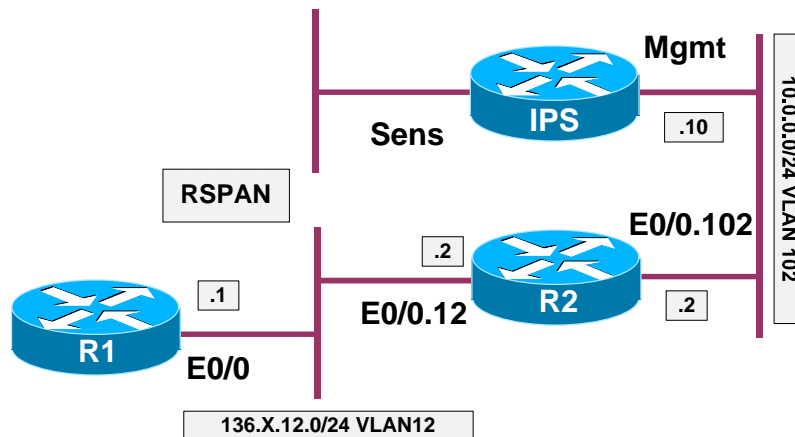


Further Reading

[Configuring Attack Response Controller for Blocking and Rate Limiting](#)

Rate Limiting with IPS

Objective: Configure IPS respond to attack by configuring rate-limit settings in a router



Directions

- Configure devices per the “Intrusion Prevention/Basic Configuration” scenario “[IPS Initial Setup](#)”
- Configure the devices per the “Intrusion Prevention/Basic Configuration” scenario “Promiscuous Mode Monitoring with RSPAN”
- Create VLAN100 and configure IP address for the link between the IPS management interface and R2, using subinterface for VLAN 100 at R2
- Configure R2 for remote access as follows:
 - Terminal line should ask for password “CISCO”
 - Enable password should be “CISCO”
- Configure user profile named R2_PROFILE on the IPS to match those requirement
- Configure router device on the IPS to access R2 (IP 10.0.0.2) and associate it with user profile named R2_PROFILE. Use telnet to access R2
- This router device should block ingress on Ethernet 0/0.12
- This router device should be able to respond to rate-limit requests
- Tune signature 2152 (ICMP Flood) to respond with “request-rate-limit”. Additionally configure rate-limit type to be based on percentage, and set percentage to 10%

Final Configuration

```
SW1 :
vlan 100
!
```

```

interface FastEthernet 0/10
  switchport mode access
  switchport access vlan 100

R2:
interface Ethernet 0/0.100
  encapsulation dot1q 100
  ip address 10.0.0.2 255.255.255.0
!
! Access Control
!
no aaa new-model
enable secret CISCO
!
line vty 0 4
  password CISCO
  login

IPS:
!
! Create a user profile
!
Rack1IPS# conf t
Rack1IPS(config)# service network-access
Rack1IPS(config-net)# user-profiles R2_PROFILE
Rack1IPS(config-net-use)# password
Enter password[]: CISCO
Re-enter password: CISCO
Rack1IPS(config-net-use)# enable-password
Enter enable-password[]: CISCO
Re-enter enable-password: CISCO
Rack1IPS(config-net-use)# exit
!
! Configure router device
!
Rack1IPS(config-net)# router-devices 10.0.0.2
Rack1IPS(config-net-rou)# profile-name R2_PROFILE
Rack1IPS(config-net-rou)# communication telnet
Rack1IPS(config-net-rou)# response-capabilities rate-limit
Rack1IPS(config-net-rou)# block-interfaces E0/0.12 in
Rack1IPS(config-net-rou-blo)# exit
Rack1IPS(config-net-rou)# exit
Rack1IPS(config-net)# exit
Apply Changes?[yes]: yes
!
! Tune Signature 2152
!
Rack1IPS(config-sig)# signatures 2152 0
Rack1IPS(config-sig-sig)# engine flood-host
Rack1IPS(config-sig-sig-flo)# event-action-settings
Rack1IPS(config-sig-sig-flo-eve)# external-rate-limit-type percentage
Rack1IPS(config-sig-sig-flo-eve-per)# external-rate-limit-percentage 10
Rack1IPS(config-sig-sig-flo-eve-per)# exit
Rack1IPS(config-sig-sig-flo-eve)# exit
Rack1IPS(config-sig-sig-flo)# event-action request-rate-limit
Rack1IPS(config-sig-sig-flo)# exit
Rack1IPS(config-sig-sig)# exit

```

```
Rack1IPS(config-sig)# exit
Apply Changes?[yes]: yes
```

Verification

```
Rack1R1#ping 136.1.12.2 repeat 100
```

```
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/4/20 ms
```

```
Rack1IPS# show events past 00:05:00
```

```
evIdsAlert: eventId=1168711179445317351 severity=informational vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
time: 1993/04/17 08:48:24 1993/04/17 08:48:24 UTC
signature: description=ICMP Echo Request id=2004 version=S1
  subsigId: 0
interfaceGroup:
vlan: 0
participants:
  attacker:
    addr: locality=OUT 136.1.12.1
  target:
    addr: locality=OUT 136.1.12.2
riskRatingValue: 50
interface: fe0_0
protocol: icmp
```

```
evShunRqst: eventId=1168711179445317352 vendor=Cisco
originator:
  hostId: Rack1IPS
  appName: sensorApp
  appInstanceId: 331
time: 1993/04/17 08:48:24 1993/04/17 08:48:24 UTC
shunInfo:
  rateLimit:
    protocol: icmp
    rate: 10
    destAddr: 136.1.12.2
    data: echo-request
    timeoutMinutes: 30
  evAlertRef: hostId=Rack1IPS
```

<output omitted>

```
Rack1R2#sh running-config interface ethernet 0/0.12
Building configuration...
```

```
Current configuration : 135 bytes
!
interface Ethernet0/0.12
  encapsulation dot1Q 12
  ip address 136.1.12.2 255.255.255.0
```

```
service-policy input IDS_RL_POLICY_MAP_0

Rack1R2#show policy-map IDS_RL_POLICY_MAP_0
Policy Map IDS_RL_POLICY_MAP_0
  Class IDS_RL_CLASS_MAP_icmp-xxBx-8_0
    police cir percent 10
      conform-action transmit
      exceed-action drop

Rack1R2#show class-map
Class Map match-any class-default (id 0)
  Match any

Class Map match-any IDS_RL_CLASS_MAP_icmp-xxBx-8_0 (id 1)
  Match access-group name IDS_RL_ACL_icmp-xxBx-8_0

Rack1R2#show ip access-list IDS_RL_ACL_icmp-xxBx-8_0
Extended IP access list IDS_RL_ACL_icmp-xxBx-8_0
  10 permit icmp any host 136.1.12.2 echo

Rack1R1#ping 136.1.12.2 repeat 100


Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 136.1.12.2, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/5 ms

Rack1R2#show policy-map interface ethernet 0/0.12
Ethernet0/0.12

Service-policy input: IDS_RL_POLICY_MAP_0

Class-map: IDS_RL_CLASS_MAP_icmp-xxBx-8_0 (match-any)
  100 packets, 11800 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: access-group name IDS_RL_ACL_icmp-xxBx-8_0
    100 packets, 11800 bytes
    5 minute rate 0 bps
  police:
    cir 10 %
    cir 1000000 bps, bc 31250 bytes
    conformed 100 packets, 11800 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps

Class-map: class-default (match-any)
  12 packets, 1080 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
```

 **Further Reading**

[Configuring Attack Response Controller for Blocking and Rate Limiting](#)