Inspection of Router-Generated Traffic

Last Updated: November 27, 2012

The Inspection of Router-Generated Traffic feature allows Context-Based Access Control (CBAC) to inspect traffic that is originated by or destined to the router on which CBAC is configured. Previously, inspection of TCP, UDP, and H.323 connections initiated by or destined to the router were allowed.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Inspection of Router-Generated Traffic

- Configure CBAC.
- Configure Cisco Call Manager Express (CCME) or H.323 Gateway to configure the inspection of H. 323 connections to and from the router.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for Inspection of Router-Generated Traffic

- Inspection of router-generated traffic is supported only on the following protocols: H.323, TCP, and UDP.
- The Cisco IOS Firewall supports only Version 2 of the H.323 protocol. If CCME or the H.323 Gateway has inspection of H.323 router traffic enabled, enter the following commands so that it is configured to support only Version 2 features:

```
voice service voip
h323
session transport tcp calls-per-connection 1
h245 tunnel disable
h245 caps mode restricted
h225 timeout tcp call-idle value 0
```

Information About Inspection of Router-Generated Traffic

CBAC

CBAC is a Cisco IOS Firewall set feature that provides network protection by using the following functions:

Traffic Filtering

CBAC filters TCP and UDP packets based on application-layer protocol session information. You can configure CBAC to permit specified TCP and UDP traffic through a firewall only when the connection is initiated from within the network you want to protect. CBAC can inspect traffic for sessions that originate from either side of the firewall, and CBAC can be used for intranet, extranet, and Internet perimeters of your network.

Traffic Inspection

CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

Alerts and Audit Trails

CBAC generates real-time alerts and audit trails. Enhanced audit trail features use SYSLOG to track all network transactions; it records time stamps, the source host, the destination host, the ports used, and the total number of transmitted bytes, for advanced, session-based reporting. Real-time alerts send SYSLOG error messages to central management consoles upon detecting suspicious activity.

Using CBAC inspection rules, you can configure alerts and audit trail information on a per-application protocol basis. For example, if you want to generate audit trail information for HTTP traffic, you can specify that in the CBAC rule covering HTTP inspection.

Intrusion Detection

CBAC provides a limited amount of intrusion detection to protect against specific Simple Mail Transfer Protocol (SMTP) attacks. With intrusion detection, SYSLOG messages are reviewed and monitored for specific “attack signatures.” Certain types of network attacks have specific characteristics, or signatures. When CBAC detects an attack, it resets the offending connections and sends SYSLOG information to the SYSLOG server.

Inspection of Router-Generated Traffic Overview

Inspection of Router-Generated Traffic enhances CBAC’s functionality to inspect TCP, UDP, and H.323 connections that have a router or firewall as one of the connection endpoints. This enables CBAC to open pinholes for TCP, UDP, and H.323 control channel connections to and from the router, and to open pinholes for data and media channels negotiated over the H.323 control channels.

Inspection of TCP and UDP channels initiated from the router enables dynamic opening of pinholes on the interface access control list (ACL) to allow return traffic. You do not have to modify the ACL when a TCP connection such as Telnet is made from the router.

Inspection of local H.323 connections enables the deployment of CCME, H.323 gateway, and the Cisco IOS Firewall on the same router. This also simplifies ACL configuration on CCME’s interface through which H.323 connections are made. Before this feature, in addition to configuring ACLs to allow H.323 connections on a standard port (for example, port 1720), you had to configure ACLs to allow all dynamically negotiated data and media channels. With this feature you just configure the ACLs to allow H. 323 control channels on port 1720. The Cisco IOS Firewall inspects all the traffic on the control channel and opens pinholes to allow dynamically negotiated data and media channels.

To enable Inspection of Router-Generated Traffic, specify the **router-traffic** keyword in the **ip inspect name** command of the appropriate protocol. This allows inspection of traffic to the router and the traffic passing through the router..

How to Configure Inspection of Router-Generated Traffic

Configuring H.323 Inspection

To configure the H.323 protocol, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip inspect name** *inspection-nam* e {**TCP** | **UDP** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**router-traffic**][**timeout** *seconds*]
4. **interface** *type slot/port*
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip inspect name** *inspection-nam* e {**TCP** | **UDP** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}][**router-traffic**][**timeout** *seconds*] **Example:** `Router(config)# ip inspect name test H.323 router-traffic`	Defines a set of inspection rules.
Step 4	**interface** *type slot/port* **Example:** `Router(config)# interface FE 0/0`	Configures an interface type.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Configuring CBAC

To configure CBAC, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**deny** | **permit**} *source*[*source-wildcard*] [**log**]
4. **ip inspect name** *inspection-nam* e {**TCP** | **UDP** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**router-traffic**][**timeout** *seconds*]
5. **interface** *type slot/port*
6. **ip inspect** *inspection-name* {**in** | **out**}
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**access-list** *access-list-number* {**deny** | **permit**} *source*[*source-wildcard*] [**log**] **Example:** `Router(config)# access-list 121 permit tcp host 100.168.11.1 any eq 1720`	Defines a standard IP access list.
Step 4	**ip inspect name** *inspection-nam* e {**TCP** | **UDP** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}][**router-traffic**][**timeout** *seconds*] **Example:** `Router(config)# ip inspect name here H323 router-traffic timeout 180`	Defines a set of inspection rules.
Step 5	**interface** *type slot/port* **Example:** `Router(config)# Serial0/3/0`	Configures an interface type.

	Command or Action	Purpose
Step 6	**ip inspect** *inspection-name* {**in** | **out**} **Example:** `Router(config-if)# ip inspect test in`	Enables the Cisco IOS Firewall on an interface.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the CBAC Configuration

To verify the CBAC configuration, perform the following task.

SUMMARY STEPS

1. **show ip inspect name** *inspection-name*
2. **show ip inspect config**
3. **show ip inspect interfaces**
4. **show ip inspect session detail**
5. **show ip inspect all**

DETAILED STEPS

Step 1 **show ip inspect name** *inspection-name*

Use this command to show a particular configured inspection rule. The following example configures the inspection rule myinspectionrule. The output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

Example:

```
Router# show ip inspect name myinspectionrule
Inspection Rule Configuration
 Inspection name myinspectionrule
  tcp timeout 3600
  udp timeout 30
  ftp timeout 3600
```

Step 2 **show ip inspect config**

Use this command to show the CBAC configuration, including global timeouts, thresholds, and inspection rules.

Example:

```
Router# show ip inspect config
```

```
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
 Inspection Rule Configuration
  inspection name myinspectionrule
  tcp timeout 3600
  udp timeout 30
  ftp timeout 3600
```

Step 3 **show ip inspect interfaces**

Use this command to show the interface configuration with respect to applied inspection rules and access lists.

Example:

```
Router# show ip inspect interfaces

Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

Step 4 **show ip inspect session detail**

Use this command to display existing sessions that CBAC is currently tracking and inspecting. The following sample output shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic.

Example:

```
Router# show ip inspect session
 detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1
```

Step 5 **show ip inspect all**

Use this command to show all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.

Example:

```
Router# show ip inspect all

Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
    tcp timeout 3600
```

```
    udp timeout 30
    ftp timeout 3600
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (30.0.0.1:46065)=>(40.0.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (40.0.0.1:20)=>(30.0.0.1:46072) ftp-data SIS_OPEN
```

Configuration Examples for Inspection of Router-Generated Traffic

Example Configuring CBAC with Inspection of H.323 Traffic

These commands create the ACL. In this example, TCP traffic from subnet 100.168.11.1, 192.168.11.50, and 192.168.100.1 is permitted.

```
access-list 120 permit tcp host 100.168.11.1 any eq 1720
access-list 121 permit tcp host 192.168.11.50 host 100.168.11.1 eq 1720
access-list 121 permit tcp host 192.168.100.1 host 100.168.11.1 eq 1720
```

These commands create the CBAC inspection rule LOCAL-H323, allowing inspection of the protocol traffic specified by the rule. This inspection rule sets the timeout value to 180 seconds for each protocol (except for RPC). The timeout value defines the maximum time that a connection for a given protocol can remain active without any traffic passing through the router. When these timeouts are reached, the dynamic ACLs that are inserted to permit the returning traffic are removed, and subsequent packets (possibly even valid ones) are not permitted.

```
ip inspect name LOCAL-H323 tftp timeout 180
ip inspect name LOCAL-H323 h323 router-traffic timeout 180
```

These commands apply the inspection rule and ACL. In this example, the inspection rule LOCAL-H323 is applied to traffic at interface Serial0/3/0.

```
interface Serial0/3/0
 ip address 11.168.11.2 255.255.255.0
 ip access-group 121 in
 ip access-group 120 out
 ip inspect LOCAL-H323 in
 ip inspect LOCAL-H323 out
 encapsulation frame-relay
frame-relay map ip 11.168.11.1 168 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
CBAC	*Cisco IOS Security Command Reference* "Configuring Context-Based Access Control"
H.323	*Cisco IOS H.323 Configuration Guide*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Inspection of Router-Generated Traffic

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1 Feature Information for Inspection of Router-Generated Traffic

Feature Name	Releases	Feature Information
Inspection of Router-Generated Traffic	12.3(14)T	The Inspection of Router-Generated Traffic feature allows Context-Based Access Control (CBAC) to inspect traffic that is originated by or destined to the router on which CBAC is configured. Previously, inspection of Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and H. 323 connections initiated by or destined to the router were allowed.