Enabling ALGs and AICs in Zone-Based Policy Firewalls

Zone-based policy firewalls support Layer 7 application protocol inspection along with application-level gateways (ALGs) and application inspection and control (AIC). Layer 7 application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic that passes through a security module.

Prior to the introduction of Enabling ALGs and AICs in Zone-Based Policy Firewalls feature, the Layer 7 protocol inspection was automatically enabled along with the ALG/AIC configuration. With this feature you can enable or disable Layer 7 inspection by using the **no application-inspect** command.

This module provides an overview of the Enabling ALGs and AICs in Zone-Based Policy Firewalls feature and describes how to configure it.

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.

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.

Information About Enabling ALGs and AICs in Zone-Based Policy Firewalls

Application-Level Gateways

An application-level gateway (ALG), also known as an application-layer gateway, is an application that translates the IP address information inside the payload of an application packet. An ALG is used to interpret the application-layer protocol and perform firewall and Network Address Translation (NAT) actions. These actions can be one or more of the following depending on your configuration of the firewall and NAT:

- Allow client applications to use dynamic TCP or UDP ports to communicate with the server application.
- Recognize application-specific commands and offer granular security control over them.
- Synchronize multiple streams or sessions of data between two hosts that are exchanging data.
- Translate the network-layer address information that is available in the application payload.

The firewall opens a pinhole, and NAT performs translation service on any TCP or UDP traffic that does not carry the source and destination IP addresses in the application-layer data stream. Specific protocols or applications that embed IP address information require the support of an ALG.

Enabling Layer 7 Application Protocol Inspection Overview

Zone-based policy firewalls support Layer 7 protocol inspection along with application-level gateways (ALG) and application inspection and control (AIC). Layer 7 protocol inspection is automatically enabled along with the ALG/AIC configuration.

Layer 7 application protocol inspection is a technique that interprets or understands application-layer protocols and performs appropriate firewall or Network Address Translation (NAT) action. Certain applications require special handling of the data portion of a packet when the packet passes through the security module on a device. Layer 7 application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic that passes through the security module. Based on the configured traffic policy, the security module accepts or rejects packets to ensure the secure use of applications and services.

Sometimes, application inspection implementation issues can cause application packet drop and make networks unstable. Prior to the introduction of the Enabling ALGs and AICs in Zone-Based Policy Firewall feature, to disable application inspection you had to define an access control list (ACL) with the target Layer 7 protocol port define a class map that matches this ACL and matches either the TCP or UDP protocol to bypass the inspection for a specific Layer 7 protocol.

With the introduction of the Enabling ALGs and AICs in Zone-Based Policy Firewall feature, you can enable or disable Layer 7 protocol inspection for a specific protocol or for all supported Layer 7 protocols with the **application-inspect** command. Any configuration changes to a parameter map applies only to new sessions. For example, when you disable FTP Layer 7 inspection, the newly created sessions skip FTP Layer 7 inspection, while existing sessions before the configuration change will perform FTP Layer 7 inspection. For all sessions to perform the configuration change, you must delete all sessions and re-create them.

You can enable Layer 7 application protocol inspection for an individual parameter map or for a global firewall.

How to Enable ALGs and AICs in Zone-Based Policy Firewalls

Enabling Layer 7 Application Protocol Inspection on Firewalls

Application protocol inspection is enabled by default. Use the **no application-inspect** command to disable application protocol inspection.

Use the **application-inspect** command to reconfigure application protocol inspection, if you have disabled it for any reason. Configure either the **parameter-map type inspect** command or the **parameter-map type inspect-global** command before configuring the **application-inspect** command.

You can only configure either the **parameter-map type inspect** command or the **parameter-map type inspect-global** command at any time.

Use the

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **parameter-map type inspect** *parameter-map-name*
   - **parameter-map type inspect-global**
4. **application-inspect** {**all** | *protocol-name*}
5. **exit**
6. **class-map type inspect** {**match-all** | **match-any**} *class-map-name*
7. **match protocol** *protocol-name*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** {*class-map-name* | **class-default**}
11. **inspect** *parameter-map-name*
12. **exit**
13. **class** {*class-map-name* | **class-default**}
14. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	Do one of the following:
	• **parameter-map type inspect** *parameter-map-name*
	• **parameter-map type inspect-global**
	
	Example:
	`Device(config)# parameter-map type inspect pmap-fw`
	or
	`Device(config)# parameter-map type inspect-global`
		• (Optional) Enables an inspect-type parameter map for the firewall to connect thresholds, timeouts, and other parameters that pertain to the inspect action, and enters parameter-map type inspect configuration mode.
		• (Optional) Enables a global parameter map and enters parameter-map type inspect configuration mode.

Step 4	**application-inspect** {**all** | *protocol-name*} **Example:** `Device(config-profile)# application-inspect msrpc`	Enables application inspection for the specified protocols.
Step 5	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and returns to global configuration mode.
Step 6	**class-map type inspect** {**match-all** | **match-any**} *class-map-name* **Example:** `Device(config)# class-map type inspect match-any internet-traffic-class`	Creates an inspect type class map and enters class map configuration mode.
Step 7	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol msrpc`	Configures a match criterion for a class map based on the specified protocol.
Step 8	**exit** **Example:** `Device(config-cmap)# exit`	Exits class map configuration mode and returns to global configuration mode.
Step 9	**policy-map type inspect** *policy-map-name* **Example:** `Device(config)# policy-map type inspect private-internet-policy`	Creates an inspect type policy map and enters policy map configuration mode.

	Command or Action	Purpose
Step 10	**class type inspect** {*class-map-name* | **class-default**} **Example:** `Device(config-pmap)# class type inspect internet-traffic-class`	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.
Step 11	**inspect** *parameter-map-name* **Example:** `Device(config-pmap-c)# inspect pmap-fw`	Enables stateful packet inspection.
Step 12	**exit** **Example:** `Device(config-pmap-c)# exit`	Exits policy-map class configuration mode and returns to policy map configuration mode.
Step 13	**class** {*class-map-name* | **class-default**} **Example:** `Device(config-pmap)# class class-default`	Specifies the default class so that you can configure or modify the policy.
Step 14	**end** **Example:** `Device(config-pmap)# end`	Exits policy map configuration mode and returns to privileged EXEC mode.

Configuring Zones for Enabling Layer 7 Application Protocol Inspection

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **zone security** {**default** | *security-zone*}
4. **exit**
5. **zone security** {**default** | *security-zone*}
6. **exit**
7. **zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone*
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **zone-member security** *security-zone*
12. **exit**
13. **interface** *type number*
14. **zone-member security** *security-zone*
15. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**zone security** {**default**	*security-zone*} **Example:** `Device(config)# zone security private`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode. • You need two security zones to create a zone pair: a source and a destination zone.
Step 4	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 5	**zone security** {**default** | *security-zone*} **Example:** `Device(config)# zone security internet`	Creates a security zone to which interfaces can be assigned and enters security zone configuration mode.
Step 6	**exit** **Example:** `Device(config-sec-zone)# exit`	Exits security zone configuration mode and returns to global configuration mode.
Step 7	**zone-pair security** *zone-pair* **source** *source-zone* **destination** *destination-zone* **Example:** `Device(config)# zone-pair security private-internet source private destination internet`	Creates a zone pair and enters security zone pair configuration mode.
Step 8	**service-policy type inspect** *policy-map-name* **Example:** `Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy`	Attaches a firewall policy map to the destination zone pair. • If a policy is not configured between a pair of zones, traffic is dropped by default.
Step 9	**exit** **Example:** `Device(config-sec-zone-pair)# exit`	Exits security zone pair configuration mode and returns to global configuration mode.
Step 10	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0/0`	Configures an interface and enters interface configuration mode.
Step 11	**zone-member security** *security-zone* **Example:** `Device(config-if)# zone-member security private`	Assigns an interface to a specified security zone. • When you make an interface a member of a security zone, all traffic into and out of that interface (except traffic bound for the device or initiated by the device) is dropped by default. To let traffic through the interface, you must make the zone part of a zone pair to which you apply a policy. If the policy permits traffic, traffic can flow through that interface.
Step 12	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 13	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/2/2`	Configures an interface and enters interface configuration mode.
Step 14	**zone-member security** *security-zone* **Example:** `Device(config-if)# zone-member security internet`	Assigns an interface to a specified security zone.
Step 15	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuration Examples for Enabling ALGs and AICs in Zone-Based Policy Firewalls

Example: Enabling Layer 7 Application Protocol Inspection on Firewalls

The following example shows how to enable Layer 7 application protocol inspection after configuring the **parameter-map type inspect** command. You can enable application inspection after configuring the **parameter-map type inspect-global** command also.

You can only configure either the **parameter-map type inspect** or the **parameter-map type inspect-global** command at any time.

```
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# application-inspect msrpc
Device(config-profile)# exit
Device(config)# class-map type inspect match-any internet-traffic-class
Device(config-cmap)# match protocol msrpc
Device(config-cmap)# exit
Device(config)# policy-map type inspect private-internet-policy
Device(config-pmap)# class type inspect internet-traffic-class
Device(config-pmap-c)# inspect pmap-fw
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap)# end
```

Example: Configuring Zones for Enabling Layer 7 Application Protocol Inspection

```
Device# configure terminal
Device(config)# zone security private
Device(config-sec-zone)# exit
Device(config)# zone security internet
Device(config-sec-zone)# exit
Device(config)# zone-pair security private-internet source private destination internet
Device(config-sec-zone-pair)# service-policy type inspect private-internet-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# zone-member security private
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/2/2
Device(config-if)# zone-member security internet
Device(config-if)# end
```

Additional References for Enabling ALGs and AICs in Zone-Based Policy Firewalls

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Firewall commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Enabling ALGs and AICs in Zone-Based Policy Firewalls

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 Enabling ALGs and AICs in Zone-Based Policy Firewalls

Feature Name	Releases	Feature Information
Enabling ALGs and AICs in Zone-Based Policy Firewalls	Cisco IOS XE Release 3.11S	Zone-based policy firewalls support Layer 7 application protocol inspection along with application-level gateways (ALGs) and application inspection and control (AIC). Layer 7 application protocol inspection helps to verify the protocol behavior and identify unwanted or malicious traffic that passes through security module. Prior to the introduction of Enabling ALGs and AICs in Zone-Based Policy Firewalls feature, the Layer 7protocol inspection was automatically enabled along with the ALG/AIC configuration. With this feature you can enable or disable Layer 7 inspection by using the no application-inspect command. In Cisco IOS XE Release 3.11S, this feature was introduced on Cisco ASR 1000 Series Aggregation Services Routers, Cisco 4400 Series Integrated Services Routers, and Cisco Cloud Services Routers 1000V. The following commands were introduced or modified: **application-inspect**, **show parameter-map type inspect**, and **show platform software firewall**.