# Application Aware Firewall

This document describes how Zone Based FireWall policy is defined based on the applications that NBAR can detect and make Zone Based FireWall application aware. The Application FireWall inspects the traffic and blocks traffic based on applications, category, application-family or application-group. This application aware firewall feature provides the following benefits:

- Application visibility and granular control
- Classification of 1400+ layer 7 applications
- Allows or blocks traffic by application, category, application-family or application-group



# Feature Information for Application Aware Firewall

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.

| Feature Name | Releases | Feature Information |
|---|---|---|
| Application Aware Zone-based FW | Cisco IOS XE Fuji 16.9.1 | This document describes how Zone Based FireWall policy is defined based on the applications that NBAR can detect and make Zone Based FireWall application aware. The Application FireWall inspects the traffic and blocks traffic based on applications, category, application-family or application-group.<br>The following commands were introduced or modified:<br>**show class-map***avc-classmap-name*<br>**show policy-map type inspect zone-pair**<br>**show policy-map type inspect zone-pair sessions**<br>**show policy-map type inspect avc**<br>**show platform hardware qfpactive feature firewall drop** |

# Information About Application Awareness on Zone-Based FW

## Prerequisites for Application Aware Firewall

- Ensure that traffic is matched to the Layer3/Layer4 inspect class map. If the traffic does not match the firewall inspection, the AVC policy fails to see the traffic.
- Inspect DNS in the same class-map where the AVC service-policy is applied.

## Restrictions on Application Aware Zone-Based FW

- No support for traffic to self-zone.
- The AVC inspect policy should allow all and only deny certain application because many applications are interdependent and therefore allowing one application while denying all others do not work all the time.
- Each application class-map can have upto 16 filters (each match is considered a filter).
- The AVC policy-map can have upto 32 class-maps (including class-default).
- You cannot configure **match protocol attribute application-family** or **match protocol attribute application-group** if you specify the category using the **match protocol attribute category** command.

Before you configure class-map and policy-map, use the **parameter-map type inspect** configure the parameter-map type to log dropped packets:

```
Device (config)# parameter-map type inspect
Device (config-map)# log dropped-packets
```

## Policies Based on Network Layers L3/L4

Zone-based Firewall uses policies based on network layers L3/L4, for example, class maps are based on ACL and L4 protocolsTCP/UDP/ICMP or L7 protocolsFTP and SIP. Policies that are defined using the L7 protocol utilize the protocol's destination port to classify the packet. ZBF lacks application visibility, it supports FTP inspection through the FTP ALG, and only identifies the protocols that are based on port 21.

**Note** If an FTP control flow is opened on some random port, zone-based firewall cannot identify the application.

# How to Configure NBAR Based Application Awareness on ZBFW

## Configure Layer 4 Zone-Based Firewall

```
Device(config-profile)#class-map type inspect match-any cm1
Device(config-cmap)#match protocol http
Device(config-cmap)#match protocol https
Device(config-cmap)#match protocol dns
Device(config-cmap)#match protocol tcp
Device(config-cmap)#match protocol udp
Device(config-cmap)#match protocol icmp
Device(config-cmap)#exit
Device(config)#class-map match-any nbar-class1
Device(config-cmap)#match protocol yahoo-mail
Device(config-cmap)#match protocol amazon
Device(config-cmap)#match protocol attribute category consumer-internet
Device(config-cmap)#exit
```

## L7 Service Policy for Application Aware Firewall

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Configure the class-map for inspection.<br>**Example:**<br>`class-map type inspect match-any cm1`<br>` match protocol http`<br>` match protocol https`<br>` match protocol dns`<br>` match protocol tcp`<br>` match protocol udp`<br>` match protocol icmp` | Defines the protocols and category using the **class-map type inspect** and **match protocol** commands. |
| **Step 2** | Define the action, in this case the AVC, using the application firewall policy.<br>**Example:**<br>`policy-map type inspect avc nbar-policy1`<br>`class nbar-class1` | Uses the **deny** command to refuse the remote network management protocols listed in the `nbar-class1`class map. |

| | Command or Action | Purpose |
|---|---|---|
| | deny<br>class class-default<br>allow | |
| **Step 3** | Log the dropped packets using the application firewall policy.<br>**Example:**<br>policy-map type inspect pm1<br>class type inspect cm1<br>inspect<br>service-policy avc nbar-policy1<br>class class-default<br>drop log<br>Traffic from amazon, in nbar-class1, is denied by the policy. For example, a dropped packet is shown in the following drop log message:<br>Oct 17 12:44:08.101: %IOSXE-6-PLATFORM: R0/0:<br>cpp_cp:<br>QFP:0.0 Thread:000 TS:00000002517650404876<br>%FW-6-DROP_PKT:<br>Dropping dns/amazon pkt from GigabitEthernet3<br>171.70.168.183:53 =><br>171.10.1.101:50877(target:class)<br>-(in_to_out:cm1) due to AVC Policy drop:classify<br>result with ip ident 65434 | |

### What to do next

Add the **ip nbar protocol-discovery ipv4** command on the ingress interface. Then use the **show ip nbar protocol-discovery interface** [**intf-name**] command to see the application classification.

# Example: Application Aware Show Commands

In this example, the **show policy-map type inspect zone-pair** command shows the policy map statistics and other information including information about the sessions existing on a specified zone pair. The line following `Class-map: nbar-class1 (match-any)` includes the packet counter value (`7 packets`), which increases whenever traffic matches the nbar-class1 class.

```
Device# show policy-map type inspect zone-pair

Zone-pair: in_to_out
Service-policy inspect : pm1

Class-map: cm1 (match-any)
Match: protocol http
Match: protocol https
Match: protocol dns
Match: protocol tcp
Match: protocol udp
Match: protocol icmp
Inspect
Packet inspection statistics [process switch:fast switch]
tcp packets: [0:485]
dns packets: [0:51]
```

```
Session creations since subsystem startup or last reset 21
Current session counts (estab/half-open/terminating) [13:0:0]
Maxever session counts (estab/half-open/terminating) [13:2:0]
Last session created 00:00:00
Last statistic reset 00:00:19
Last session creation rate 151
Last half-open session total 0

Service-policy inspect avc : nbar-policy1

Class-map: nbar-class1 (match-any)
7 packets, 1449 bytes
30 second offered rate 1000 bps, drop rate 0000 bps
Match: protocol amazon
Match: protocol yahoo-mail
Match: protocol attribute category consumer-internet
Deny

Class-map: class-default (match-any)
211 packets, 94091 bytes
30 second offered rate 27000 bps, drop rate 0000 bps
Match: any
Allow

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

```
Device# show platform hardware qfp active feature firewall drop
-------------------------------------------------------------------------------
Drop Reason                                                            Packets
-------------------------------------------------------------------------------
AVC Policy drop:classify result                                             38
```

```
Device# show platform hardware qfp active feature firewal datapath scb
[s=session  i=imprecise channel c=control channel  d=data channel A/D=appfw action allow/deny]
Session ID:0x0000DA5B  171.10.1.101 64204 171.70.168.183 53 proto 17 (0:0) (1456:0xd000208)
 [scA]
Session ID:0x0000DA18  171.10.1.101 58836 74.125.199.103 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5A  171.10.1.101 64206 8.8.8.8 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA11  171.10.1.101 58833 74.125.199.84 443 proto 6 (0:0) (1440:0xd000210)
 [sdA]
Session ID:0x0000DA57  171.10.1.101 64205 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA2C  171.10.1.101 58839 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA59  171.10.1.101 64203 173.36.131.10 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
Session ID:0x0000DA0B  171.10.1.101 58831 74.125.199.94 443 proto 6 (0:0) (1456:0xd000208)
 [sdA]
Session ID:0x0000DA5C  171.10.1.101 64207 8.8.4.4 53 proto 17 (0:0) (0:0xd000001) [sc]
Session ID:0x0000DA58  171.10.1.101 64203 171.70.168.183 53 proto 17 (0:0) (1761:0xd00033f)
 [scD]
```

# Additional References for Firewall Stateful Interchassis Redundancy

### Related Documents

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

### 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 |