On-Device Management for Security Features

The On-Device Management for Security Features provides an intuitive and simple management interface, the Cisco Configuration Professional Express, to deploy a variety of security features. The security features available through the Cisco Configuration Professional Express are zone-based firewalls, VPN, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), URL filtering, and content scan.

The Cisco Configuration Professional Express uses existing zone-based firewall CLIs in conjunction with Network-Based Application Recognition 2 (NBAR2) CLIs to determine the application category, and position NBAR2 protocols supported by the firewall into the relevant application category.

This module provides a brief overview of the feature and describes in detail the enablement of NBAR2 for zone-based firewalls.

- Finding Feature Information, page 1
- Information About On-Device Management for Security Features, page 2
- How to Configure On-Device Management for Security Features, page 4
- Configuration Examples for On-Device Management for Security Features, page 8
- Additional References for On-Device Management for Security Features, page 8
- Feature Information for On-Device Management for Security Features, page 9

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 On-Device Management for Security Features

On-Device Management for Security Features Overview

The following features are available in the Cisco Configuration Professional Express for the on-device management of security features:

- Displays the default zone-based firewall policy assignment; the policy between the LAN zone and WAN zone.
- Configures other firewall policies, in addition to default firewall policy.
- Displays default zones (the LAN zone and WAN zone)
- Assigns or removes interfaces to/from a zone.
- Creates and customizes zones.
- Displays the default Intrusion Prevention System (IPS) configuration.
- Provides a knob to enable or disable IPS globally.
- Validates the IPS master signature file; cisco public key.
- Lists IPS signatures in use.
- Configures and manages filtering for specific domains or websites.
- Provides a listing of popular domains that are intended to be blocked.
- Informs users when their access to domains and websites are blocked.
- Provides filtering of HTTP and Secure HTTP (HTTPS)-based access to domains.

NBAR2 Enablement in Zone-Based Firewalls

In Cisco IOS Release 15.5(1)T and later releases, zone-based firewalls supports Network-Based Application Recognition 2 (NBAR2).

NBAR2, is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments. With the NBAR2, enablement in zone-based firewalls, the traffic flow classification is done by NBAR2.

NBAR2 classification of traffic flows happens once and the classification results are used by multiple features including the firewall; thus avoiding flow classification by multiple features and saving router resources. NBAR2 keeps updating the Protocol Description Language (PDL) to cater to new protocols and enhancements to existing protocols. With NBAR2 enablement, the firewall does not need to update application layer gateways (ALGs).

NBAR2 Protocol Signatures Overview

NBAR2 protocol descriptions are written in StILE (Stateful Inspection Language Engine) and NBAR2 signatures are written into Protocol Description Language (PDL) files, which have a .PDL extension. Typically, each protocol has one .PDL file. Each PDL has a set of handlers that define match conditions, such as well-known port, the regular expression available in a packet, and so on. Further checks to strengthen signatures can be added within the handlers. Port-based and regular expression-based match conditions are together termed as heuristics in NBAR2 terminology. NBAR2 supports dynamic loading of PDLs which define new protocols or update existing protocols.

The following match conditions are supported by the NBAR2 Enablement in Zone-Based Firewalls feature:

- Port-based: Based on the TCP or UDP port on which a packet is available.
- Regular expression or pattern-based: Based on a specific regular expression, or fixed patterns at specific offsets found in a packet. This check can be done on the first data packet of a traffic flow in either direction, or on all packets of a flow till the classification is successful.
- General: Based on general hooks; where all packets in a flow are checked until the classification is successful.

The following are some of the key functionalities of NBAR2:

- Matches protocol-specific fields for classification of packets.
- Uses derived flows (example, FTP data flows) that are based on application-specific information derived from packets.
- Flow table manipulation based on entries in the global flow cache. These entries are added, deleted or modified by using specific PDL constructs. These entries are directional, and typically, either half-tuple or full tuple-based.
- Dynamic CLI generation based on the **match protocol** *protocol-name* command for dynamically generating the protocol name options and other NBAR2 commands.
- Subport classification (or subclassification) based on the characteristics of a protocol, such as HTTP headers (example, URL, and host), or Citrix priority tags. A PDL that provides subclassification, can specify the set and type of parameters that it supports. Subport classification also results in the generation of dynamic CLI generation.
- Maintaining of cross-packet states using local tables.
- Classification of tunneled protocols (example, Yahoo messenger over HTTP).
- Limited support for field extraction.

How to Configure On-Device Management for Security Features

Enabling NBAR2 in Zone-Based Firewalls

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect global**
4. **nbar-classify**
5. **end**
6. **show parameter-map type inspect global**

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	**parameter-map type inspect global** **Example:** `Device(config)# parameter-map type inspect global`	Configures a global inspect type parameter map and enters parameter-map inspect configuration mode.
Step 4	**nbar-classify** **Example:** `Device(config-profile)# nbar-classify`	Configures Network-Based Application Recognition 2 (NBAR2) classification for the zone-based firewall inspection.
Step 5	**end** **Example:** `Device(config-profile)# end`	Exits parameter-map inspect configuration mode and returns to privileged EXEC mode.
Step 6	**show parameter-map type inspect global** **Example:** `Device# show parameter-map type inspect global`	Displays the global inspect type parameter map values.

The following sample output from the **show parameter-map type inspect global** command displays the NBAR2 configuration along with configurations available in the global parameter map:

```
Device# show parameter-map type inspect global

alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets disabled
  log summary disabled
  max-incomplete low 18000
  max-incomplete high 20000
  one-minute low 2147483647
  one-minute high 2147483647
  tcp reset-PSH disabled
  exporter not-configured
  nbar-classify
```

Configuring NBAR2 Protocols in a Class Map

To enable web application traffic such as Facebook, Twitter, LinkedIn and so on, you must enable basic web application protocols such as HTTP, Secure HTTP (HTTPS), or Domain Name System (DNS) to inspect traffic. For example, to enable facebook traffic, you must enable either HTTP, HTTPS or DNS traffic. When the web application uses the well-known port of a protocol; for example, port 80 that is assigned to HTTP, the initial traffic session is classified as HTTP protocol, based on the Layer 4 port. However, if subsequent packets match the web application protocol signature, the session is reclassified as the web application protocol.

```
class-map type inspect c1
 match protocol http
 pass
!
class-map type inspect c2
 match protocol facebook
 drop
!
 class-default
  drop
```

Multiple classes are needed to drop traffic from a web application, and inspect or pass the remaining traffic. The web application desired to be dropped needs to be set to drop in a separate class. In the configuration example below, if NBAR classifies traffic as "twitter"/"linkedin" firewall hits the class-default. In class-default if parent protocol is set to pass it will continue to do the parent class action, instead of dropping the packet. To explicitly drop, user should add drop action for each protocol need to be dropped.

You must remove the NBAR2 protocol match statements from the class map, before you disable NBAR2 using the **no nbar-classify** command.

Before You Begin

Prerequisites
You must enable Network-Based Application Recognition 2 (NBAR2) for zone-based firewalls by using the **nbar-classify** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type inspect** *class-map-name*
4. **match protocol** *protocol-name*
5. **exit**
6. **class-map type inspect** *class-map-name*
7. **match protocol** *facebook*
8. **exit**
9. **policy-map type inspect** *policy-map-name*
10. **class type inspect** *class-map-name*
11. **pass**
12. **exit**
13. **class type inspect** *class-map-name*
14. **drop**
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	**class-map type inspect** *class-map-name* **Example:** `Device(config)# class-map type inspect cmap1`	Specifies the traffic class on which an action is to be performed and enters the class map configuration mode.
Step 4	**match protocol** *protocol-name* **Example:** `Device(config-cmap)# match protocol http`	Configures a match criterion for a class map on the basis of a specified protocol.
Step 5	**exit** **Example:** `Device(config-cmap)# exit`	Exits class map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**class-map type inspect** *class-map-name* **Example:** `Device(config)# class-map type inspect cmap-new`	Specifies the traffic class on which an action is to be performed and enters the class map configuration mode.
Step 7	**match protocol** *facebook* **Example:** `Device(config-cmap)# match protocol facebook`	Configures a match criterion for a class map on the basis of a 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 pmap1`	Creates a Layer 3 and Layer 4 inspect type policy map and enters policy map configuration mode.
Step 10	**class type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect cmap1`	Specifies the traffic class on which an action is to be performed and enters the policy-map class configuration mode.
Step 11	**pass** **Example:** `Device(config-pmap-c)# pass`	Allows packets to be sent to the device without firewall 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 type inspect** *class-map-name* **Example:** `Device(config-pmap)# class type inspect cmap-new`	Specifies the traffic class on which an action is to be performed and enters policy-map class configuration mode.
Step 14	**drop** **Example:** `Device(config-pmap-c)# drop`	Configures a traffic class to discard packets that belong to a specific class.
Step 15	**end** **Example:** `Device(config-pmap-c)# end`	Exits policy-map class configuration mode and returns to privileged EXEC mode.

Configuration Examples for On-Device Management for Security Features

Example: Enabling NBAR2 in Zone-Based Firewalls

```
Device# configure terminal
Device(config)# parameter-map type inspect global
Device(config-profile)# nbar-classify
Device(config-profile)# end
```

Example: Configuring NBAR2 Protocols in a Class Map

```
Device# configure terminal
Device(config)# class-map type inspect cmap1
Device(config-cmap)# match protocol http
Device(config-cmap)# exit
Device(config)# class-map type inspect cmap-new
Device(config-cmap)# match protocol facebook
Device(config-cmap)# exit
Device(config)# policy-map type inspect pmap1
Device(config-pmap)# class type inspect cmap1
Device(config-pmap-c)# pass
Device(config-pmap-c)# exit
Device(config-pmap)# class type inspect cmap-new
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

Additional References for On-Device Management for Security Features

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security 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

Related Topic	Document Title
Cisco Configuration Professional	http://www.cisco.com/c/en/us/support/cloud-systems-management/configuration-professional/tsd-products-support-series-home.html

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 On-Device Management for Security Features

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 On-Device Management for Security Features

Feature Name	Releases	Feature Information
On-Device Management for Security Features	Cisco IOS Release 15.5(1)T	The On-Device Management for Security Features provides an intuitive and simple management interface, the Cisco Configuration Professional Express, to deploy a variety of security features. The security features available through the Cisco Configuration Professional Express are zone-based firewalls, VPN, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and URL filtering. This module provides a brief overview of the feature and describes how to enable NBAR2 for zone-based firewalls. The following commands were introduced or updated for this feature: **nbar-classify** and **show parameter-map type inspect global**.