Configuring Intrusion Detection System

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 <TBD>

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

Information About Intrusion Detection System

The Cisco Intrusion Detection System/Intrusion Prevention System (CIDS/CIPS) instructs controllers to block certain clients from accessing the wireless network when attacks involving these clients are detected at Layer 3 through Layer 7. This system offers significant network protection by helping to detect, classify, and stop threats including worms, spyware/adware, network viruses, and application abuse. Two methods are available to detect potential attacks:

- IDS sensors
- IDS signatures

IDS sensors can be configured to detect various types of IP-level attacks in the network. When the sensors identify an attack, they can alert the controller to shun the offending client. When a new IDS sensor is added, the IDS sensor should be registered with the controller so that the controller can query the sensor to get the list of shunned clients.

When an IDS sensor detects a suspicious client, it alerts the controller to shun this client. The shun entry is distributed to all controllers within the same mobility group. If the client to be shunned is currently joined to a controller in this mobility group, the anchor controller adds this client to the dynamic exclusion list, and the foreign controller removes the client. The next time that the client tries to connect to a controller, the anchor controller rejects the handoff and informs the foreign controller that the client is being excluded.

How to Configure Intrusion Detection System

Configuring IDS Sensors

SUMMARY STEPS

1. **configure terminal**
2. **wireless wps cids-sensor** *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*]
3. **wireless wps cids-sensor** *index*
4. [**default exit fingerprint interval no port shutdown**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Controller# configure terminal`	Enters global configuration mode.
Step 2	**wireless wps cids-sensor** *index* [**ip-address** *ip-addr* **username** *username* **password** *password_type password*] **Example:** `Controller(config)# wireless wps cids-sensor 2 231.1.1.1 admin pwd123`	Configures the IDS sensors that holds and internal index number. The index parameter determines the sequence in which the controller consults the IDS sensors. The controller supports up to five IDS sensors. • **ip-address**– [optional] Provide the IP address for the IDS. • **username**– [optional] Configures the username for the IDS. • **password**– [optional] Configures the password for the respective username.
Step 3	**wireless wps cids-sensor** *index* **Example:** `Controller(config)# wireless wps cids-sensor 1`	Enters the IDS configuration submode.
Step 4	[**default exit fingerprint interval no port shutdown**] **Example:** `Controller(config-cids-index)# default`	Configures various IDS parameters. • **default**– [optional] Sets a command to its default. • **exit**– [optional] Exits the submode.

	Command or Action	Purpose
		• **fingerprint**– [optional] Configures the sensor's TLS fingerprint. • **interval**– [optional] Configures the sensor's query interval. The range is between 10-3600 seconds. • **no**– [optional] Negates a command or set its defaults. • **port**– [optional] Configures the sensor's port number. • **shutdown**– [optional] Shuts down the intrusion detection sensor.

Step 5	**end**
	Example:
	`Controller(config)# end`
		Returns to privileged EXEC mode. Alternatively, you can also press **Ctrl-Z** to exit global configuration mode.

Monitoring Intrusion Detection System

Table 1: Commands for Monitoring Wireless Multicast

Commands	Description
show wireless wps cids-sensor *index*	Displays the IDS configuration of the IDS sensor with the mentioned index value.
show wireless wps cids-sensor summary	Displays the list of all the configured IDS with their respective values like index, ip-address, port number, interval value, status and last query.
show wireless wps shun-list	Displays the list of the IDS shun list.