Configuring IDS Signatures

Intrusion Detection System Signatures

You can configure intrusion detection system (IDS) signatures, or bit-pattern matching rules used to identify various types of attacks in incoming 802.11 packets, on the controller. When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller. If an attack is detected, appropriate mitigation is initiated.

Cisco supports 17 standard signatures. These signatures are divided into six main groups. The first four groups contain management signatures, and the last two groups contain data signatures.

- **Broadcast deauthentication frame signatures**—During a broadcast deauthentication frame attack, a hacker sends an 802.11 deauthentication frame to the broadcast MAC destination address of another client. This attack causes the destination client to disassociate from the access point and lose its connection. If this action is repeated, the client experiences a denial of service. When the broadcast deauthentication frame signature (precedence 1) is used to detect such an attack, the access point listens for clients transmitting broadcast deauthentication frames that match the characteristics of the signature. If the access point detects such an attack, it alerts the controller. Depending on how your system is configured, the offending device is contained so that its signals no longer interfere with authorized clients, or the controller forwards an immediate alert to the system administrator for further action, or both.
- **NULL probe response signatures**—During a NULL probe response attack, a hacker sends a NULL probe response to a wireless client adapter. As a result, the client adapter locks up. When a NULL probe response signature is used to detect such an attack, the access point identifies the wireless client and alerts the controller. The NULL probe response signatures are as follows:
  - NULL probe resp 1 (precedence 2)
  - NULL probe resp 2 (precedence 3)

Note Controller does not log historical NULL Probe IDS events within the Signature Events Summary output.

- **Management frame flood signatures**—During a management frame flood attack, a hacker floods an access point with 802.11 management frames. The result is a denial of service to all clients associated or attempting to associate to the access point. This attack can be implemented with different types of management frames: association requests, authentication requests, reassociation requests, probe requests, disassociation requests, deauthentication requests, and reserved management subtypes.

  When a management frame flood signature is used to detect such an attack, the access point identifies management frames matching the entire characteristic of the signature. If the frequency of these frames is greater than the value of the frequency set in the signature, an access point that hears these frames triggers an alarm. The controller generates a trap and forwards it to Cisco Prime Infrastructure.

  The management frame flood signatures are as follows:

  - Assoc flood (precedence 4)
  - Auth flood (precedence 5)
  - Reassoc flood (precedence 6)
  - Broadcast probe flood (precedence 7)
  - Disassoc flood (precedence 8)
  - Deauth flood (precedence 9)
  - Reserved mgmt 7 (precedence 10)
  - Reserved mgmt F (precedence 11)

    The reserved management frame signatures 7 and F are reserved for future use.

- **Wellenreiter signature**—Wellenreiter is a wireless LAN scanning and discovery utility that can reveal access point and client information. When the Wellenreiter signature (precedence 17) is used to detect such an attack, the access point identifies the offending device and alerts the controller.
- **EAPOL flood signature—**During an EAPOL flood attack, a hacker floods the air with EAPOL frames that contain 802.1X authentication requests. As a result, the 802.1X authentication server cannot respond to all of the requests and fails to send successful authentication responses to valid clients. The result is a denial of service to all affected clients. When the EAPOL flood signature (precedence 12) is used to detect such an attack, the access point waits until the maximum number of allowed EAPOL packets is exceeded. It then alerts the controller and proceeds with the appropriate mitigation.
- **NetStumbler signatures**—NetStumbler is a wireless LAN scanning utility that reports access point broadcast information (such as operating channel, RSSI information, adapter manufacturer name, SSID, WEP status, and the latitude and longitude of the device running NetStumbler when a GPS is attached). If NetStumbler succeeds in authenticating and associating to an access point, it sends a data frame with the following strings, depending on the NetStumbler version:

Version	String
3.2.0	“Flurble gronk bloopit, bnip Frundletrune”

Version	String
3.2.3	“All your 802.11b are belong to us”
3.3.0	Sends white spaces

When a NetStumbler signature is used to detect such an attack, the access point identifies the offending device and alerts the controller. The NetStumbler signatures are as follows:

- NetStumbler 3.2.0 (precedence 13)
- NetStumbler 3.2.3 (precedence 14)
- NetStumbler 3.3.0 (precedence 15)
- NetStumbler generic (precedence 16)

A standard signature file exists on the controller by default. You can upload this signature file from the controller, or you can create a custom signature file and download it to the controller or modify the standard signature file to create a custom signature.

Configuring IDS Signatures (GUI)

Uploading or Downloading IDS Signatures

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a Trivial File Transfer Protocol (TFTP) server available. Follow these guidelines when setting up a TFTP server:

- If you are downloading through the service port, the TFTP server must be on the same subnet as the service port because the service port is not routable, or you must create static routes on the controller.
- If you are downloading through the distribution system network port, the TFTP server can be on the same or a different subnet because the distribution system port is routable.
- A third-party TFTP server cannot run on the same computer as the Cisco Prime Infrastructure because the Prime Infrastructure built-in TFTP server and the third-party TFTP server require the same communication port.

Step 3 If you are downloading a custom signature file (*.sig), copy it to the default directory on your TFTP server.

Step 4 Choose **Commands** to open the **Download File to Controller** page.

Step 5 Perform one of the following:

- If you want to download a custom signature file to the controller, choose **Signature File** from the File Type drop-down list on the Download File to Controller page.
- If you want to upload a standard signature file from the controller, choose **Upload File** and then **Signature File** from the **File Type** drop-down list on the **Upload File from Controller** page.

Step 6 From the **Transfer Mode** drop-down list, choose **TFTP**, **FTP**, or **SFTP**.

The SFTP option was added in Release 7.4.

Step 7 In the **IP Address** text box, enter the IP address of the **TFTP**, **FTP**, or **SFTP** server.

Step 8 If you are downloading the signature file using a TFTP server, enter the maximum number of times that the controller should attempt to download the signature file in the **Maximum retries** text box.

The range is 1 to 254 and the default value is 10.

Step 9 If you are downloading the signature file using a TFTP server, enter the amount of time in seconds before the controller times out while attempting to download the signature file in the **Timeout** text box.

The range is 1 to 254 seconds and the default is 6 seconds.

Step 10 In the **File Path** text box, enter the path of the signature file to be downloaded or uploaded. The default value is "/."

Step 11 In the **File Name** text box, enter the name of the signature file to be downloaded or uploaded.

Note When uploading signatures, the controller uses the filename that you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 12 If you are using an FTP or SFTP server, follow these steps:

a. In the **Server Login Username** text box, enter the username to log into the FTP or SFTP server.

b. In the **Server Login Password** text box, enter the password to log into the FTP or SFTP server.

c. In the **Server Port Number** text box, enter the port number on the FTP or SFTP server through which the download occurs. The default value is 21.

Step 13 Choose **Download** to download the signature file to the controller or **Upload** to upload the signature file from the controller.

Enabling or Disabling IDS Signatures

Step 1 Choose **Security** > **Wireless Protection Policies** > **Standard Signatures** or **Custom Signatures** to open the Standard Signatures page or the Custom Signatures page.

The Standard Signatures page shows the list of Cisco-supplied signatures that are currently on the controller. The Custom Signatures page shows the list of customer-supplied signatures that are currently on the controller. This page shows the following information for each signature:

- The order, or precedence, in which the controller performs the signature checks.
- The name of the signature, which specifies the type of attack that the signature is trying to detect.
- The frame type on which the signature is looking for a security attack. The possible frame types are data and management.
- The action that the controller is directed to take when the signature detects an attack. The possible actions are None and Report.

- The state of the signature, which indicates whether the signature is enabled to detect security attacks.
- A description of the type of attack that the signature is trying to detect.

Step 2 Perform one of the following:

- If you want to allow all signatures (both standard and custom) whose individual states are set to Enabled to remain enabled, select the **Enable Check for All Standard and Custom Signatures** check box at the top of either the Standard Signatures page or the Custom Signatures page. The default value is enabled (or selected). When the signatures are enabled, the access points joined to the controller perform signature analysis on the received 802.11 data or management frames and report any discrepancies to the controller.
- If you want to disable all signatures (both standard and custom) on the controller, unselect the **Enable Check for All Standard and Custom Signatures** check box. If you unselected this check box, all signatures are disabled, even the ones whose individual states are set to Enabled.

Step 3 Click **Apply** to commit your changes.

Step 4 Click the precedence number of the desired signature to enable or disable an individual signature. The **Standard Signature (or Custom Signature) > Detail** page appears.

This page shows much of the same information as the Standard Signatures and Custom Signatures pages but provides these additional details:

- The tracking method used by the access points to perform signature analysis and report the results to the controller. The possible values are as follows:
  - Per Signature—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis.
  - Per MAC—Signature analysis and pattern matching are tracked and reported separately for individual client MAC addresses on a per-channel basis.
  - Per Signature and MAC—Signature analysis and pattern matching are tracked and reported on a per-signature and per-channel basis as well as on a per-MAC-address and per-channel basis.
- The pattern that is being used to detect a security attack

Step 5 In the Measurement Interval text box, enter the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 6 In the Signature Frequency text box, enter the number of matching packets per interval that must be identified at the individual access point level before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 7 In the Signature MAC Frequency text box, enter the number of matching packets per interval that must be identified per client per access point before an attack is detected. The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 8 In the Quiet Time text box, enter the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop. The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 9 Select the **State** check box to enable this signature to detect security attacks or unselect it to disable this signature. The default value is enabled (or selected).

Step 10 Click **Apply** to commit your changes. The Standard Signatures or Custom Signatures page reflects the signature's updated state.

Step 11 Click **Save Configuration** to save your changes.

Viewing IDS Signature Events (GUI)

Step 1 Choose **Security** > **Wireless Protection Policies** > **Signature Events Summary** to open the Signature Events Summary page.

Step 2 Click the Signature Type for the signature to see more information on the attacks detected by a particular signature. The Signature Events Detail page appears.

This page shows the following information:

- The MAC addresses of the clients identified as attackers
- The method used by the access point to track the attacks
- The number of matching packets per second that were identified before an attack was detected.
- The number of access points on the channel on which the attack was detected
- The day and time when the access point detected the attack

Step 3 Click the **Detail link** for that attack to see more information for a particular attack. The Signature Events Track Detail page appears.

- The MAC address of the access point that detected the attack
- The name of the access point that detected the attack
- The type of radio (802.11a or 802.11b/g) used by the access point to detect the attack
- The radio channel on which the attack was detected
- The day and time when the access point reported the attack

Configuring IDS Signatures (CLI)

Step 1 If desired, create your own custom signature file.

Step 2 Make sure that you have a TFTP server available.

Step 3 Copy the custom signature file (*.sig) to the default directory on your TFTP server.

Step 4 Specify the download or upload mode by entering the **transfer** {**download** | **upload**} **mode tftp** command.

Step 5 Specify the type of file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} **datatype signature** command.

Step 6 Specify the IP address of the TFTP server by entering the **transfer** {**download** | **upload**} **serverip** *tftp-server-ip-address* command.

Note Some TFTP servers require only a forward slash (/) as the TFTP server IP address, and the TFTP server automatically determines the path to the correct directory.

Step 7 Specify the download or upload path by entering the **transfer** {**download** | **upload**} *path absolute-tftp-server-path-to-file* command.

Step 8 Specify the file to be downloaded or uploaded by entering the **transfer** {**download** | **upload**} *filename filename.sig* command.

Note When uploading signatures, the controller uses the filename you specify as a base name and then adds "_std.sig" and "_custom.sig" to it in order to upload both standard and custom signature files to the TFTP server. For example, if you upload a signature file called "ids1," the controller automatically generates and uploads both ids1_std.sig and ids1_custom.sig to the TFTP server. If desired, you can then modify ids1_custom.sig on the TFTP server (making sure to set "Revision = custom") and download it by itself.

Step 9 Enter the **transfer** {**download** | **upload**} *start* command and answer y to the prompt to confirm the current settings and start the download or upload.

Step 10 Specify the number of seconds that must elapse before the signature frequency threshold is reached within the configured interval by entering this command:

config wps signature interval *signature_id interval*

where signature_id is a number used to uniquely identify a signature. The range is 1 to 3600 seconds, and the default value varies per signature.

Step 11 Specify the number of matching packets per interval that must be identified at the individual access point level before an attack is detected by entering this command:

config wps signature frequency*signature_id frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 12 Specify the number of matching packets per interval that must be identified per client per access point before an attack is detected by entering this command:

config wps signature mac-frequency *signature_id mac_frequency*

The range is 1 to 32,000 packets per interval, and the default value varies per signature.

Step 13 Specify the length of time (in seconds) after which no attacks have been detected at the individual access point level and the alarm can stop by entering by entering this command:

config wps signature quiet-time *signature_id quiet_time*

The range is 60 to 32,000 seconds, and the default value varies per signature.

Step 14 Perform one of the following:

- To enable or disable an individual IDS signature, enter this command:

  config wps signature {**standard** | **custom**} **state** *signature_id* {**enable** | **disable**}

- To enable or disable IDS signature processing, which enables or disables the processing of all IDS signatures, enter this command:

  config wps signature {**enable** | **disable**}

Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

Step 15 Save your changes by entering this command:

save config

Step 16 If desired, you can reset a specific signature or all signatures to default values. To do so, enter this command:

config wps signature reset {*signature_id* | *all*}

Note You can reset signatures to default values only through the controller CLI.

Viewing IDS Signature Events (CLI)

Procedure

- See whether IDS signature processing is enabled or disabled on the controller by entering this command:

  show wps summary

Note If IDS signature processing is disabled, all signatures are disabled, regardless of the state configured for individual signatures.

- See individual summaries of all of the standard and custom signatures installed on the controller by entering this command:

  show wps signature summary

- See the number of attacks detected by the enabled signatures by entering this command:

  show wps signature events summary

- See more information on the attacks detected by a particular standard or custom signature by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# summary**

- See information on attacks that are tracked by access points on a per-signature and per-channel basis by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-signature** *source_mac*

- See information on attacks that are tracked by access points on an individual-client basis (by MAC address) by entering this command:

  show wps signature events {**standard** | **custom**} **precedence# detailed per-mac** *source_mac*