Advanced WIPS

Feature History for Advanced WIPS

This table provides release and related information for the features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

Table 1: Feature History for Advanced WIPS

Release	Feature Name	Feature Information
Cisco IOS XE Bengaluru 17.5.1	Advanced WIPS Signatures	Up to 15 additional signatures are supported.
Cisco IOS XE Bengaluru 17.6.1	Syslog Support for Advanced WIPs	From 17.6.1 release onwards: • Two additional signatures are supported. • Syslog support has been added to the controller for advanced WIPS.

Information About Advanced WIPS

The Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. The aWIPS uses an advanced approach to wireless threat detection and performance management. The AP detects threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.

With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both wired and wireless networks and use that network intelligence to analyze attacks from multiple sources to accurately pinpoint and proactively prevent attacks, rather than wait until damage or exposure has occurred.

The following table shows the alarms introduced from Cisco IOS XE Bengaluru 17.5.1 onwards:

Table 2: Advanced WIPS Signatures and Definitions: From Cisco IOS XE Bengaluru 17.5.1 Onwards

Advanced WIPS Signature	Definition
RTS Virtual Carrier Sense Attack	This is an addition to the existing RTS Flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm is triggered when an RTS with a large duration is detected. An attacker can use these frames to exhaust air time and disrupt wireless client service.
CTS Virtual Carrier Sense Attack	This is an addition to the existing CTS Flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm is triggered when a CTS with large duration is detected. An attacker can use these frames to exhaust air time and disrupt wireless client service.
Deauthentication Flood by Pair	In the enhanced context of threat, both the source (attacker) and the destination (victim) of attacks (Track by Pair) have visibility.
Fuzzed Beacon	Fuzzed beacon is when invalid, unexpected, or random data is introduced into the beacon and replays those modified frames into the air. This causes unexpected behavior on the destination device, including driver crashes, operating system crashes, and stack-based overflows. This in turn allows the execution of the arbitrary code of the affected system.
Fuzzed Probe Request	Fuzzed probe request is when invalid, unexpected, or random data is introduced into a probe request and replays those modified frames into the air.
Fuzzed Probe Response	Fuzzed probe response is when invalid, unexpected, or random data is introduced into a probe response and replays those modified frames into the air.

Advanced WIPS Signature	Definition
PS Poll Flood by Signature	PS poll flood is when a potential hacker spoofs a MAC address of a wireless client and sends out a flood of PS poll frames. The AP sends out buffered data frames to the wireless client. This results in the client missing the data frames because it could be in the power safe mode.
Eapol Start V1 Flood by Signature	Extensible Authentication Protocol over LAN (EAPOL) start flood is when an attacker attempts to bring down the AP by flooding the AP with EAPOL-start frames to exhaust the AP's internal resources.
Reassociation Request Flood by Destination	Reassociation request flood is when a specific device tries to flood the AP with a large number of emulated and spoofed client reassociations to exhaust the AP's resources, particularly the client association table. When the client association table overflows, legitimate clients are not able to associate, causing a DoS attack.
Beacon Flood by Signature	Beacon flood is when stations actively search for a network that is bombarded with beacons from the networks that are generated using different MAC addresses and SSIDs. This flood prevents a valid client from detecting the beacons sent by corporate APs, which in turn initiates a DoS attack.
Probe Response Flood by Destination	Probe response flood is when a device tries to flood clients with a large number of spoofed probe responses from the AP. This prevents clients from detecting the valid probe responses sent by the corporate APs.
Block Ack Flood by Signature	Block ack flood is when an attacker transmits an invalid Add Block Acknowledgement (ADDBA) frame to the AP while spoofing the MAC address of the valid client. This process causes the AP to ignore any valid traffic transmitted from the client until it reaches the invalid frame range.
Airdrop Session	Airdrop session refers to the Apple feature called AirDrop. AirDrop is used to set up a peer-to-peer link for file sharing. This might create a security risk because of unauthorized peer-to-peer networks created dynamically in your WLAN environment.
Malformed Association Request	Malformed association request is when an attacker sends a malformed association request to trigger bugs in the AP. This results in a DoS attack.

Advanced WIPS Signature	Definition
Authentication Failure Flood by Signature	Authentication failure flood is when a specific device tries to flood the AP with invalid authentication requests spoofed from a valid client. This results in disconnection.
Invalid MAC OUI by Signature	Invalid MAC OUI is when a spoofed MAC address that does not have a valid OUI is used.
Malformed Authentication	Malformed authentication is when an attacker sends malformed authentication frames that can expose vulnerabilities in some drivers.

The following table shows the alarms introduced prior to Cisco IOS XE Bengaluru 17.5.1:

Table 3: Advanced WIPS Signatures: Prior Cisco IOS XE Bengaluru 17.5.1

Advanced WIPS Signatures
Authentication Flood Alarm
Association Flood Alarm
Broadcast Probe Flood Alarm
Disassociation Flood Alarm
Broadcast Dis-Association Flood Alarm
De-Authentication Flood Alarm
Broadcast De-Authentication Flood Alarm
EAPOL-Logoff Flood Alarm
CTS Flood Alarm
RTS Flood Alarm

Guidelines and Restrictions

- In the aWIPS profile, Cisco Aironet 1850 Series Access Points, Cisco Catalyst 9117 Series Access Points, and Cisco Catalyst 9130AX Series Access Points can detect EAPOL logoff attack and raise alarms accordingly, only on off-channel. They can not detect EAPOL logoff attack and raise alarms on on-channel.
- aWIPS profile download is not supported when Cisco Catalyst Center is configured using the fully qualified domain name (FQDN).

Enabling Advanced WIPS

From Cisco IOS XE Release 17.5.1 onwards, aWIPS security gets a higher priority over Hyperlocation/Fastlocate. The following are the possible scenarios.

All Catalyst APs supporting Fastlocate can be used together with aWIPS depending on the configuration and regardless of the AP mode.

In modes other than the Monitor mode for Cisco Aironet 4800 AP, if both aWIPS and Hyperlocation are enabled, only aWIPS is available.

Hyperlocation/Fastlocate	Advanced WIPS	Cisco Aironet 4800 AP Mode	Cisco Aironet 4800 AP Effective Feature
Enable	Enable	Any Non-Monitor	aWIPS[1]
Enable	Disable	Any Non-Monitor	Hyperlocation/Fastlocate
Disable	Disable	Any Non-Monitor	Hyperlocation/Fastlocate and aWIPS are disabled.
Disable	Enable	Any Non-Monitor	aWIPS
Enable	Enable	Monitor	aWIPS and Hyperlocation[2]
Disable	Enable	Monitor	aWIPS[3]
Enable	Disable	Monitor	Hyperlocation/Fastlocate
Disable	Disable	Monitor	Hyperlocation/Fastlocate and aWIPS are disabled.

1 In modes other than the Monitor mode, if both aWIPS and Hyperlocation/Fastlocate are enabled, only aWIPS is available.
2 In Monitor mode, if both aWIPS and Hyperlocation/Fastlocate are enabled, both aWIPS and Hyperlocation/Fastlocate are available.
3 To monitor the status of aWIPS and Hyperlocation/Fastlocate simultanueously on AP, use the **show capwap client rcb** command.

Syslog Support for Advanced WIPS

This feature adds syslog support to the controller for Advanced WIPS.

The controller raises syslog messages when it receives alarms from an AP. The syslog messages go through throttling. If the same signature is detected from the same AP in a configured throttling interval, you must generate the syslog message for that alarm. For instance, if there were 100 occurrences of the same signature from the same AP within the throttling interval, say, 1 minute, you get to view only one syslog message in the controller in that 1-minute period instead of 100 messages.

Sample Syslog Format

The following is a sample syslog format:

```
Nov 18 20:45:23.746: %APMGR_AWIPS_SYSLOG-6-APMGR_AWIPS_MESSAGE: Chassis 1 R0/0: wncd: AWIPS
 alarm:(AP00B0.E19A.5720) 00b0.e19a.5720 Radio MAC 00b0.e19b.c300 detected Probe Response
Flood by Destination (10019)
```

The format covers the AP name, AP Ethernet MAC address, AP Radio MAC address, description (signature ID).

Note The syslog messages do not display any client information or context.

Advanced WIPS Solution Components

The aWIPS solution comprises the following components:

- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Aironet Wave 2 APs
- Cisco Catalyst Center

Because the aWIPS functionality is integrated into Cisco Catalyst Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

aWIPS supports the following capabilities:

- Static signatures

  From Cisco IOS XE, 17.4.1 onwards Cisco Catalyst Center can change threshold values and push new signature files to the AP.
- Enable or disable signature forensic capture from Cisco Catalyst Center.
- Standalone signature detection only
- Alarms only
- GUI support
- CLIs to view alarms
- Static signature file packaged with controller and AP image
- Export alarms to Cisco Catalyst Center through WSA channel

Note aWIPS alarm details such as the AP MAC address, alarm ID, alarm string, and signature ID are displayed on the Cisco Catalyst 9800 series wireless controller GUI.

Supported Modes and Platforms

aWIPS is supported on the following controllers:

- Cisco Catalyst 9800 Series Wireless Controllers
- Cisco Embedded Wireless Controller on Catalyst Access Points

Note aWIPS is not supported on Cisco IOS APs.

Enabling Advanced WIPS(GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.
Step 2 Click **Add**. The **Add AP Join Profile** window is displayed.
Step 3 In the **Add AP Join Profile** window, click the **Security** tab.
Step 4 Under the **aWIPS** section, check the **aWIPS Enable** check box.
Step 5 Click **Apply to Device**. You will go back the to **General** tab.
Step 6 Click the **Security** tab.
Step 7 Under the **aWIPS** section, check the **Forensic Enable** check box.
Step 8 Click **Apply to Device**.

Enabling Advanced WIPS (CLI)

To enable aWIPS from the controller and ensure that aWIPS has higher priority than Hyperlocation/Fastlocate, perform the following:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**ap profile** *profile-name* **Example:** `Device(config)# ap profile ap-profile-name`	Configures the default AP profile.
Step 3	**awips** **Example:** `Device(config-ap-profile)# awips`	Enables aWIPS. **Note** aWIPS is disabled by default on the controller.

	Command or Action	Purpose
Step 4	**awips forensic** **Example:** `Device(conf-ap-profile)# awips forensic`	Enables forensics for aWIPS alarms.
Step 5	**hyperlocation** **Example:** `Device(config-ap-profile)# hyperlocation`	Enables Hyperlocation/Fastlocate on all the supported APs that are associated with this AP profile.
Step 6	**end** **Example:** `Device(config-ap-profile)# end`	Returns to privileged EXEC mode.

Configuring Syslog Threshold for Advanced WIPS (CLI)

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**awips-syslog throttle period** *syslog-throttle-interval* **Example:** `Device(config)# awips-syslog throttle period 38`	Configures the syslog threshold for aWIPS. *syslog-throttle-interval*: Enter the syslog throttle interval, in seconds. The range is from 30 to 600. **Note** The default throttling interval is 60 seconds.
Step 3	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Viewing Advanced WIPS Alarms (GUI)

Procedure

Step 1 Navigate to **Monitoring** > **Security** > **aWIPS**.

Step 2 To view the details of the alarms in the last 5 minutes, click the **Current Alarms** tab.

Step 3 To view the alarm count over an extended period of time, either hourly, for a day (24 hours) or more, click the **Historical Statistics** tab.

Step 4 Sort or filter the alarms based on the following parameters:

- **AP Radio MAC address**
- **Alarm ID**
- **Time Stamp**
- **Signature ID**
- **Alarm Description**
- **Alarm Message Index**

Verifying Advanced WIPS

To view the aWIPS status, use the **show awips status** *radio_mac* command:

```
Device# show awips status 0xx7.8xx8.2xx0

AP Radio MAC  AWIPS Status  Forensic Capture Status   Alarm Message Count
--------------------------------------------------------------------------------
0xx7.8xx8.2xx0      ENABLED       CONFIG_NOT_ENABLED  14691
```

The various aWIPS status indicators are:

- `ENABLED`: aWIPS enabled.
- `NOT_SUPPORTED`: The AP does not support AWIPS.
- `CONFIG_NOT ENABLED`: aWIPS is not enabled on the AP.

To view details of specific alarm signatures, use the **show awips alarm signature** *signature_id* command:

```
Device# show awips alarm signature 10001

AP Radio MAC    AlarmID   Timestamp          SignatureID    Alarm Description     Message
Index
-------------------------------------------------------------------------------------------------------------
0xx7.8xx8.2f80   1714    11/02/2020 13:02:19   10001       Authentication Flood     3966
```

To view alarm message statistics, use the **show awips alarm statistics** command:

```
Device# show awips alarm statistics
```

To view a list of alarms since the last clear, use the **show awips alarm ap** *ap_mac* **detailed** command:

```
Device# show awips alarm ap 0xx7.8xx8.2f80 detailed
AP Radio MAC    AlarmID     Timestamp              SignatureID   Alarm Description

-------------------------------------------------------------------------------------------------------------
0xx7.8xx8.2f80    2491    08/02/2022 17:44:40       10009         RTS Flood
```

To view detailed alarm information, use the **show awips alarm detailed** command:

```
Device# show awips alarm detailed
```

```
AP Radio MAC    AlarmID  Timestamp   SignatureID Alarm Description
-----------------------------------------------------------------------------------------------
7xx3.5xxd.d360  1        10/29/2020  23:21:27    10001 Authentication Flood by Source
dxxc.3xx5.9460  71       10/29/2020  23:21:27    10001 Authentication Flood by Source
7xx3.5xxd.d360  2        10/29/2020  23:21:28    10002 Association Request Flood by
Destination
dxxc.3xx5.9460  72       10/29/2020  23:21:28    10002 Association Request Flood by
Destination
```

To view the alarms on a specific AP, use the **show awips alarm ap** *radio_mac* **detailed** command:

Verifying Syslog Configuration for Advanced WIPS

To verify the syslog configuration for aWIPS, use the following command:

```
Device# show awips syslog throttle

Syslog Throttle Interval (seconds)

-----------------------------------------------------------------------------------------------

38
```