Advanced WIPS

Advanced WIPS

A Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless security system that

- uses advanced techniques for wireless threat detection and performance management
- enables the AP to detect threats and generate alarms, and
- combines network traffic analysis, topology information, signatures, and anomaly detection for comprehensive wireless threat prevention.

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 17.5.1	Advanced WIPS Signatures	Up to 15 additional signatures are supported.
Cisco IOS XE 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.

Advanced WIPS signatures and definitions

The table lists alarms introduced starting with Cisco IOS XE Bengaluru Release 17.5.1.

Table 2: Advanced WIPS signatures and definitions (Cisco IOS XE Bengaluru 17.5.1 and later)

Advanced WIPS signature	Definition
RTS Virtual Carrier Sense Attack	This alarm extends the RTS flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm triggers when an RTS frame with a large duration value is detected. An attacker can use these frames to exhaust airtime and disrupt wireless client services.
CTS Virtual Carrier Sense Attack	This alarm extends the CTS flood alarm introduced in Cisco IOS XE Bengaluru 17.4.x. The alarm triggers when a CTS frame with a large duration value is detected. An attacker can use these frames to exhaust airtime and disrupt wireless client services.
Deauthentication Flood by Pair	This alarm provides enhanced threat context by tracking both the source (attacker) and the destination (victim) involved in the attack.
Fuzzed Beacon	A fuzzed beacon occurs when an attacker introduces invalid, unexpected, or random data into a beacon frame and replays the modified frames over the air. This can cause unexpected behavior on the destination device, such as driver crashes, operating system crashes, and stack-based overflows, and may allow execution of arbitrary code.
Fuzzed Probe Request	A fuzzed probe request occurs when an attacker introduces invalid, unexpected, or random data into a probe request and replays the modified frames over the air.
Fuzzed Probe Response	A fuzzed probe response occurs when an attacker introduces invalid, unexpected, or random data into a probe response and replays the modified frames over the air.
PS Poll Flood by Signature	A PS poll flood occurs when an attacker spoofs the MAC address of a wireless client and sends a large number of PS poll frames. The access point sends buffered data frames to the client, which may cause the client to miss data frames while operating in power-save mode.
EAPOL Start Flood by Signature	An Extensible Authentication Protocol over LAN (EAPOL) start flood occurs when an attacker floods an access point with EAPOL start frames to exhaust its internal resources.

Advanced WIPS signature	Definition
Reassociation Request Flood by Destination	A reassociation request flood occurs when a device floods an access point with a large number of spoofed client reassociation requests to exhaust its resources, particularly the client association table. When the table overflows, legitimate clients cannot associate, resulting in a denial-of-service (DoS) attack.
Beacon Flood by Signature	A beacon flood occurs when stations receive a large number of beacons generated with different MAC addresses and SSIDs. This flood prevents clients from detecting beacons sent by corporate access points and can result in a denial-of-service (DoS) attack.
Probe Response Flood by Destination	A probe response flood occurs when a device floods clients with a large number of spoofed probe responses. This prevents clients from detecting valid probe responses sent by corporate access points.
Block Acknowledgement Flood by Signature	A block acknowledgement flood occurs when an attacker sends an invalid Add Block Acknowledgement (ADDBA) frame to an access point while spoofing a valid client MAC address. The access point then ignores valid traffic from the client until traffic outside the invalid frame range is received.
AirDrop Session	An AirDrop session uses Apple AirDrop to establish a peer-to-peer link for file sharing. This activity can introduce security risks by allowing unauthorized peer-to-peer networks to appear in the WLAN environment.
Malformed Association Request	A malformed association request occurs when an attacker sends a malformed request to an access point to exploit software defects, potentially resulting in a denial-of-service (DoS) attack.
Authentication Failure Flood by Signature	An authentication failure flood occurs when a device floods an access point with invalid authentication requests spoofed from a valid client, which can cause client disconnections.
Invalid MAC OUI by Signature	An invalid MAC OUI event occurs when a spoofed MAC address that does not contain a valid organizationally unique identifier (OUI) is used.
Malformed Authentication	Malformed authentication occurs when an attacker sends malformed authentication frames that may expose vulnerabilities in certain wireless drivers.

The table lists alarms introduced prior to Cisco IOS XE Bengaluru Release 17.5.1.

Table 3: Advanced WIPS signatures (prior to Cisco IOS XE Bengaluru 17.5.1)

Advanced WIPS signature
Authentication Flood Alarm
Association Flood Alarm
Broadcast Probe Flood Alarm
Disassociation Flood Alarm
Broadcast Disassociation Flood Alarm
Deauthentication Flood Alarm
Broadcast Deauthentication 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.
- From Cisco IOS XE 17.12.6 onwards, aWIPS profile download is supported when Cisco Catalyst Center is configured using the fully qualified domain name (FQDN). It strictly requires an IP name-server and a valid DNS record, as it bypasses local IP host entries.

Enable advanced WIPS

From Cisco IOS XE Release 17.5.1 onward, aWIPS security has higher priority than Hyperlocation/Fastlocate.

These are the possible scenarios.

All Catalyst APs that support Fastlocate can operate with aWIPS regardless of AP mode or configuration.

When both aWIPS and Hyperlocation are enabled on Cisco Aironet 4800 APs in any mode except Monitor mode, only aWIPS is available.

Table 4: Feature availability for Cisco Aironet 4800 AP (All Modes)

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

Hyperlocation/Fastlocate	Advanced WIPS	Cisco Aironet 4800 AP Mode	Cisco Aironet 4800 AP effective feature
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 simultaneously on AP, use the **show capwap client rcb** command.

Syslog messages for advanced WIPS

A syslog message for advanced WIPS is a controller notification mechanism that

- logs alarms sent from APs
- applies throttling to prevent redundant messages during configured intervals, and
- omits client-specific information from logs to protect privacy.

Sample syslog message format

A typical syslog message for advanced WIPS includes key elements such as:

- AP name
- AP Ethernet MAC address
- AP Radio MAC address
- Alarm description (signature ID)

```
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)
```

Additional notes

- When an AP sends an alarm to the controller, the controller raises the corresponding syslog message.

- Throttling ensures that if the same signature is detected from the same AP within a set interval (e.g., 1 minute), only one syslog message is generated for that period, regardless of the number of occurrences.
  - For example, 100 occurrences of the same signature from an AP within a minute will result in only one syslog message for that interval.
- Syslog messages generated for advanced WIPS do not display any client device information or context.

Advanced WIPS solution components and capabilities

The aWIPS solution comprises these components and capabilities.

Solution components

The aWIPS solution comprises these components

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

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

Capabilities

aWIPS supports these capabilities

- Static signatures

  Beginning with Cisco IOS XE version 17.4.1, 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
- Only alarms are supported.
- GUI support
- CLI to view alarms
- The static signature file is packaged with the 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 these controllers:

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

Note aWIPS is not supported on Cisco IOS APs.

Enable advanced WIPS (GUI)

Enable advanced WIPS features on your access points for improved network security.

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 return to the **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**.

Advanced WIPS and forensic features are enabled for the selected AP profile.

Enable advanced WIPS (CLI)

Enable advanced WIPS to enhance network security and ensure proper priority over location services.

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

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the default AP profile.

Example:

```
Device(config)# ap profile ap-profile-name
```

Step 3 Enable aWIPS.

Example:

```
Device(config-ap-profile)# awips
```

Note
aWIPS is disabled by default on the controller.

Step 4 Enable forensics for aWIPS alarms.

Example:

```
Device(conf-ap-profile)# awips forensic
```

Step 5 Enable Hyperlocation/Fastlocate on all the supported APs that are associated with this AP profile.

Example:

```
Device(config-ap-profile)# hyperlocation
```

Step 6 Return to privileged EXEC mode.

Example:

```
Device(config-ap-profile)# end
```

The controller is now configured with advanced WIPS and forensics, and prioritizes aWIPS above Hyperlocation/Fastlocate features on AP.

Configure syslog threshold for advanced WIPS (CLI)

Set the syslog throttle interval for advanced WIPS, so you can manage syslog message frequency and reduce unnecessary log volume.

Procedure

Step 1 Enter global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the syslog threshold for aWIPS.

Example:

```
Device(config)# awips-syslog throttle period syslog-throttle-interval
```

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 Return to privileged EXEC mode.

Example:

```
Device(config)# end
```

The syslog throttle interval for advanced WIPS is configured. Syslog messages for WIPS events will now be generated according to the specified interval.

View advanced WIPS alarms (GUI)

Identify and analyze current and historical WIPS alarms.

Procedure

Step 1 Navigate to **Monitoring** > **Security** > **Advanced Wireless Intrusion Prevention System (aWIPS)** .

Step 2 To view the details of the alarms in the last five minutes (0.08 hours), click the **Current Alarms** tab.

Step 3 To view the alarm count for longer periods such as hourly or daily (24 hours), click the **Historical Statistics** tab.

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

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

Advanced WIPS alarms appear according to the selected criteria. You receive real-time and historical data for security monitoring and analysis.

Verify 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:

Verify syslog configuration for advanced WIPS

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

```
Device# show awips syslog throttle

Syslog Throttle Interval (seconds)

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

38
```