

Aruba

Intrusion Detection and Prevention System (IDPS)

aruba

a Hewlett Packard
Enterprise company

Copyright Information

© Copyright 2023 Hewlett Packard Enterprise Development LP.

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America.

Contents	3
About This Document	7
Intended Audience	7
Related Documents	7
Conventions	7
Terminology Change	9
Contacting Support	9
Overview of Aruba IDPS	10
Why Aruba IDPS?	10
Key Features and Benefits	10
How does Aruba IDPS Work?	11
Getting Started with Aruba IDPS	13
Gateway Provisioning Tasks for New Customers	13
Gateway Provisioning Tasks for Existing Customers without Aruba IDPS Supported Gateways	13
Gateway Provisioning Tasks for Existing Customers with Aruba IDPS Supported Gateways	14
Working with Aruba Central	15
Onboarding IDPS-Supported Aruba Gateways	16
Preparing to add the Aruba IDPS-Supported Gateways	16
Supported Aruba Gateways for Aruba IDPS	16
Best Practices	17
On-boarding Devices for an Evaluation Account	17
Upgrading the Firmware on a Device	17
Managing Subscription Keys	17
Assign Subscriptions to Aruba Gateways	18
Assign Gateways to a Group	18
Aruba Gateway Groups	18
Assigning a Group Role to an Aruba Gateway Group	19
Connecting Aruba Gateways to Aruba Central	19
Provisioning Aruba Gateways in Aruba Central	20
Different Modes of Configuring Gateways and Gateway Groups	21
Configure Aruba IDPS	22
Configuring IDPS at Global, Group, and Device Level	22
Enabling Traffic Inspection on Aruba Gateways	23
Updating Ruleset for Aruba IDPS	23
Configuring IDS on Aruba Gateways	23
Configuring IPS on Aruba Gateways	23
Manage Rules in Aruba IDPS Policies	23
Configuring a Fail Strategy for Traffic	23
Bypassing IDPS Inspection for Large Dataflows	24
Viewing the Rules	24
Manage Selective Inspection	24
Troubleshooting Aruba IDPS	25
Configure SIEM	25
Configure Aruba IDPS Alerts	25
Alert Aggregation	25
Alerts Acknowledgment	26
Alert Severity and Transition	27
Debugging Branch Gateways for Aruba IDPS	27
Troubleshoot Packet Drops	27

Monitoring Aruba IDPS	29
Data Filters	30
Filter	30
Time Filter	30
Threats List Filters	30
Threats List	30
Viewing Details of a Threat	31
Downloading the Threats List	32
Moving a Threat to Allow List	32
Gateway Intrusion Detection and Prevention Dashboard	32
IDPS Tab in Gateway Dashboard	36
Traffic Inspection Engine Status	36
Traffic Inspection Engine CPU Usage	37
Traffic Inspection Engine Memory Usage	37
Dropped Packets	37
Actions	38
Go Live	38
FAQs Aruba IDPS	39
Overview	39
Which traffic inspection engine is used in Aruba IDPS?	39
What is the performance of the traffic inspection engine?	39
Can I run the traffic inspection on a VPNC gateway in the Data Center?	39
Can I perform Sandboxing test on Aruba IDPS?	39
What are the types of protocol streams that are inspected by the traffic inspection engine?	40
Can I select protocol streams that can be inspected by the traffic inspection engine?	40
How extensive is the signature pack and what types of vulnerabilities does it capture?	40
How are the events reported when there is an attack on my network?	40
How do I quarantine the infected clients?	40
Who provides the threat intelligence to the traffic inspection engine?	40
How does Aruba IDPS work in conjunction with Zscaler Cloud Security Service for SD-Branch and AOS 10 Mobility Gateway?	40
How does the Aruba IDPS security solution work in conjunction with SD-Branch and AOS 10 Mobility Gateway?	41
How is the Aruba IDPS security solution different from security solutions offered by other competitors?	41
What are the software and hardware requirements to implement IDPS?	41
Can I evaluate the security features before using them in the production environment?	41
What is the advantage of an IDPS-enabled gateway?	41
How does Aruba IDPS help in improving network security?	41
Licensing	42
Which devices are supported by IDPS?	42
Is there any change in the workflow for new customers for on-boarding gateways and assigning subscriptions in IDPS?	42
How do I apply a license to evaluate the features of IDPS?	42
Is the Advance with Security evaluation license specific to IDPS-supported gateways?	42
Can I use the evaluation license on the production environment of IDPS?	42
What features are supported for evaluation license?	42
How do I move from an evaluation subscription to a paid subscription?	42
I am an existing customer and I am using a SD-WAN license. How do I upgrade to a security license?	42
I am an existing customer with IDPS supported gateways. How do I move the gateways from production cluster to beta cluster?	43
I am an existing customer without IDPS supported gateways. How do I upgrade to a security license?	43
Why does the gateway reboot when I apply a security license?	43
How to check the status of a subscription?	43
Can I rollback from a security license to a non-security license?	43
Is there any impact to IDPS licensing model and functionality after moving to Common Cloud Services Platform?	43
On-boarding IDPS Supported Gateways	43
What is the difference in on-boarding an IDPS-enabled gateway or other gateways?	43

Do I need to on-board devices to Aruba Central before assigning subscriptions?	43
How to on-board an IDPS gateway for a new customer?	44
How to on-board a gateway with IDPS support for an existing customer ?	44
How to on-board a gateway without IDPS support for an existing customer?	44
How do I upgrade the firmware on the device?	44
I see "single sign on enabled". How do I change or disable this?	44
Why do I see the "Server Details" drop-down menu with a list of names? Which one should I select?	44
I see a drop-down list on the top right where I can select languages. What other languages are supported?	45
Configuration	45
What is the hierarchy of configuration?	45
What are the different modes of traffic inspection available?	45
What happens when the inspection mode is set to IPS?	45
What does the ruleset version signify?	45
Can I bypass large dataflows from inspection?	45
Gateway Set Up	45
How do I set up a group for IDPS gateways?	45
Is there any difference in provisioning the gateways for IDPS?	46
What is the ideal way to group gateways?	46
Does 90xx secure gateway scan IPSec/ESP encrypted traffic?	46
Can I upgrade the 90xx IDPS secure gateway running IDPS engine 4.x to 6.x?	46
What new protocols are supported with IDPS 6.x engine version?	46
Rulesets and Policies	46
What are the different types of security policies?	46
How does enabling IDPS impact operation of the gateway?	46
Which is the default inspection mode in Gateway IDS/IPS?	46
What is the default security policy in IPS and IDS?	46
How do I stop traffic inspection for certain IDS or IPS rules?	47
How do I update the ruleset version at regular intervals?	47
What does the alert icon in the Ruleset version signify?	47
When does IDPS Supported gateways check for updated ruleset?	47
Can I view the list of gateways running 4.x and 5.x rulesets?	47
Can both 4.x and 6.x gateway engine versions co-exist in a single group?	47
Can I view the latest ruleset available timestamp information?	48
Can I perform signature allow listing separately for 4.x and 5.x gateway when they are in the same group?	48
Selective Inspection	48
Can I associate a policy to any T3 Bucket?	48
Can I edit the T3 Bucket name?	48
Does Selective Inspection support the downloadable user roles?	48
Does Threats List page have user role information?	48
How is bypass different in Selective Inspection and Bypass Inspection for Large Dataflows?	48
How is Selective Inspection buckets different from role-based ACLs?	48
Is it possible to selectively bypass or inspect specific trusted traffic?	49
Is there any limitation to the number of client roles that can be added to a T3 bucket?	49
Traffic has source and destination role, which one is considered for the Selective Inspection?	49
What is considered as trusted traffic?	49
What is the benefit of Selective Inspection?	49
Monitoring	49
Can I view the threat data for different durations?	49
Can I view the threat data for a duration of more than three months?	49
How do I view the threats that are identified?	49
How do I view the details of the most affected gateways?	50
How do I view the details of the most affected hosts?	50
What does HTTP and SMTP convey in the Threats chart?	50
What does % change convey in the Trends chart?	50
How do I view the details of the most threat generating sources and destinations?	50
How do I view the details of a particular threat?	50
How do I allow a rule?	50
How do I view the geolocation of the detected threats?	50
Where can I see the ruleset version?	51

Alerts and Events	51
What does the Alert & Events pane displays?	51
What are the alerts severity levels displayed?	51
What does Acknowledged Alerts mean?	51
What user role is needed to configure alerts?	51
Traffic Monitoring	51
How do I monitor the status of the traffic inspection engine?	51
What are the durations for which the Traffic Inspection Engine Status chart is available?	51
When will I be able to view the traffic inspection details in the monitoring dashboard?	52
What does the traffic inspection engine in the Gateway Details page convey?	52
How do I view the CPU usage of the traffic inspection engine?	52
How do I view the memory usage of the traffic inspection engine?	52
How do I view the number of packets dropped?	52
SIEM	52
What are the prerequisites for configuring SIEM server?	52
How do I send threat data to the SIEM server?	52
How do I stop sending the threat data to the SIEM server?	53
How do I verify the connectivity to the SIEM server?	53
How do I edit the SIEM server details?	53
How do I delete the SIEM server details?	53
Troubleshooting	53
How do I capture packet information for troubleshooting?	53
How do I troubleshoot when Aruba IDPS engine drops data packets without generating alerts?	53
How do I troubleshoot when Aruba IDPS engine generates threat alerts and drops data packets for normal traffic?	53
When doing a file sharing (SMB), the traffic is slow?	53
How do I capture the packets on the IDPS engine ports?	54
How to identify if the session is redirected to the IDPS engine?	54
Can I extend the traffic inspection time?	54
Threat events do not reach the Splunk server. What could be wrong?	54
Sometimes assigning or unassigning the Advanced with Security license does not enable or disable IDPS on the gateway. What is the solution?	54
Threat Categories	55

This document describes the Aruba Intrusion Detection and Prevention System (IDPS) in Software-Defined WAN (SD-WAN) and provides detailed instructions for setting up, configuring, and managing IDPS for SD-Branch and campus mobility gateways from Aruba Central.

Intended Audience

This guide is intended for network administrators who manage and monitor branch networks.

Related Documents

In addition to this document, see the following documents for more details on the SD Branch devices and Aruba Central:

- *Aruba Central Online Help* at <https://www.arubanetworks.com/techdocs/central/latest/content/home.htm>
- *ArubaOS User Guide*

Conventions

[Table 1](#) lists the typographical conventions used throughout this guide to emphasize important concepts:

Table 1: *Typographical Conventions*

Type Style	Description
<i>Italics</i>	This style is used to emphasize important terms and to mark the titles of books.
<code>System items</code>	This fixed-width font depicts the following: <ul style="list-style-type: none">▪ Sample screen output▪ System prompts
Bold	<ul style="list-style-type: none">▪ Keys that are pressed▪ Text typed into a GUI element▪ GUI elements that are clicked or selected

The following informational icons are used throughout this guide:



Indicates helpful suggestions, pertinent information, and important things to remember.



Indicates a risk of damage to your hardware or loss of data.



Indicates a risk of personal injury or death.

Terminology Change

As part of advancing HPE's commitment to racial justice, we are taking a much-needed step in overhauling HPE engineering terminology to reflect our belief system of diversity and inclusion. Some legacy products and publications may continue to include terminology that seemingly evokes bias against specific groups of people. Such content is not representative of our HPE culture and moving forward, Aruba will replace racially insensitive terms and instead use the following new language:

Usage	Old Language	New Language
Campus Access Points + Controllers	Master-Slave	Conductor-Member
Instant Access Points	Master-Slave	Conductor-Member
Switch Stack	Master-Slave	Conductor-Member
Wireless LAN Controller	Mobility Master	Mobility Conductor
Firewall Configuration	Blacklist, Whitelist	Denylist, Allowlist
Types of Hackers	Black Hat, White Hat	Unethical, Ethical

Contacting Support

Table 2: *Contact Information*

Main Site	arubanetworks.com
Support Site	asp.arubanetworks.com
Airheads Social Forums and Knowledge Base	community.arubanetworks.com
North American Telephone	1-800-943-4526 (Toll Free) 1-408-754-1200
International Telephone	arubanetworks.com/support-services/contact-support/
Software Licensing Site	lms.arubanetworks.com
End-of-life Information	arubanetworks.com/support-services/end-of-life/
Security Incident Response Team	Site: arubanetworks.com/support-services/security-bulletins/ Email: aruba-sirt@hpe.com

The Intrusion Detection and Prevention System (IDPS) monitors, detects, and prevents threats in the inbound and outbound traffic. The Intrusion Detection System (IDS) monitors the network for any malicious activity and generates threat events. The Intrusion Prevention System (IPS) has all the capabilities of IDS along with the ability to prevent intrusions by dropping malicious data packets. As an administrator, you can enable either IDS or IPS.

Aruba IDPS provides an extra layer of protection that actively analyzes the network and takes actions on the traffic flows based on live updated rules. These actions include alerting based on and blocking traffic flows. Aruba IDPS has the capability to inspect data packets that enter the network and act quickly to prevent threats in real time. All identified threats are logged for correlation and analysis.

Why Aruba IDPS?

In today's network environments, which are much larger and more complex than those in the past, applications and connections are vulnerable. In order to address these challenges, Aruba introduces IDPS that adds an additional layer of security that focuses on users, applications and network connections, integrated with your existing Aruba SD-Branch, WAN, or ArubaOS 10 solution. Aruba IDPS proactively prevents and protects the network from intrusions. This is a policy-driven intrusion prevention technology that operates efficiently with minimal manual intervention. IDPS protects the network from real-time attacks with an additional advanced security dashboard that provides Security Analysts with everything they need to manage an end-to-end zero trust, edge-to-cloud environment providing network-wide visibility, multi-dimensional threat metrics, threat intelligence data, correlation, and incident management.



When IDPS is enabled, certain scenarios in layer 3 high availability (L3HA) are not ideal. Therefore, please review before you choose L3HA with IDPS enabled.

Key Features and Benefits

The following are some of the key features and benefits of Aruba IDPS:

- Full Packet Inspection—Aruba IDPS offers a signature and usage pattern-based inspection that inspects every data packet for intrusion.
- North-South and East-West inspection—Monitors both LAN and WAN networks for all traffic flows, including traffic coming into the network and leaving the network as well as inter and intra VLAN segments.
- Multi-dimensional Threat Metrics—Enables you to identify and view threats from different dimensions such as different protocols, threat types, source and destination hosts, geographic locations, time of day, and so on.
- Allow listing—Allow the administrators to ignore or bypass traffic from being inspected for certain rulesets.

- **Threat Intelligence**—There are about 50 threat categories that include Command and control, Ransomware, Phishing, Malware, Spyware, Cryptomining, and so on.
- **Correlation and Incident Management**—In addition to monitoring usage patterns, tracking events, and analyzing event logs and data for any relationship to prevent attacks, threat events are also streamed to Security Information and Events Management (SIEM) systems such as Splunk Cloud as well as integrated with Central Alert Framework for notification and integration with third-party systems based on the configured threshold.
- **Simplified Configuration**—A user-friendly and intuitive user interface that allows you to configure IDPS for your SD-Branch network with ease. Aruba offers three types of threat profiles: Lenient, Moderate, and Strict for IDS and IPS modes.
- **Licensing**—The Foundation and Advanced Gateway licenses are offered an add-on Security license that provides IDPS feature.
- **Selective Inspection**—Handling any exceptions for the inspection based on your business requirement. **Selective Inspection** allows you to define a common traffic treatment type for a collection of client roles.

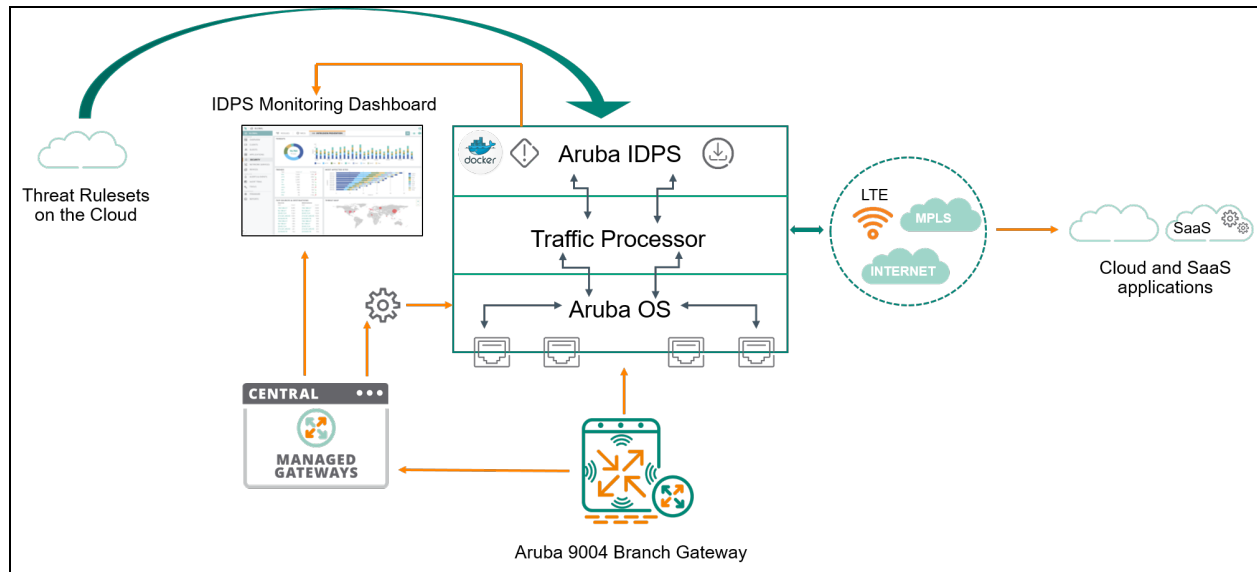
How does Aruba IDPS Work?

Aruba leverages an open source IDPS engine which is integrated as a Virtual Network Function (VNF) with the SD-Branch Gateway and VPNC gateways. This engine detects and prevents intrusion based on rules set by the user.

The following process describes the Aruba IDPS workflow to detect and prevent intrusions:

- **Download Threat Rulesets**—Aruba IDPS downloads threat rulesets from the cloud repository.
- **Enable Aruba IDPS**—Enable IDPS and configure an IDPS policy in Aruba Central.
- **Stream Realtime Events**—The events are streamed real-time based on preset event category.
- **Enrich Events**—Aruba IDPS enriches events with host, application, and location details.
- **Send Alerts and Block Traffic**—Sends alerts and notifications if IDS is selected and blocks traffic if IPS is selected as the mode of inspection.
- **Monitor Threats**—Monitor and move threats to the Allow List in the IDPS dashboard in Aruba Central.
- **Share Threat Data**—The threat data recorded in Aruba Central is shared with the SIEM server and the supported third-party integrations through Central Alert framework, if configured.

Figure 1 Aruba IDPS Architecture Diagram



To start using the SD-Branch solution, ensure that you have a valid Aruba Central subscription and licenses for the 9000 series gateway devices.

- If you are an existing Aruba Central customer with a valid subscription key and device licenses, access the Aruba Central UI and complete the provisioning tasks.
- If you are an existing Aruba customer with valid device licenses, but are not an Aruba Central customer, sign up for Aruba Central. After a successful registration, Aruba sends a verification email with a link to the Aruba Central portal. For more information, see *Aruba Central Online Help*.

Use one of the following workflows to get started. You can view, manage, onboard, and add subscription to all the devices in your account using the **Devices** option in HPE GreenLake platform.

For more information, see the **Devices** section in the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us

Gateway Provisioning Tasks for New Customers

Complete the following provisioning tasks to bring up your devices in the Aruba Central management interface:

1. **Step 1: Organize the setup for the Aruba IDPS Supported Gateways**
2. **Step 2: Connect and configure the Aruba IDPS Supported Gateways in Aruba Central**
3. **Step 3: Set up Aruba IDPS**
 - [Configure Aruba IDPS](#)

Gateway Provisioning Tasks for Existing Customers without Aruba IDPS Supported Gateways

Complete the following provisioning tasks to bring up your devices in the Aruba Central management interface:

1. **Step 1: Before you begin**
 - [Preparing to add the Aruba IDPS-Supported Gateways](#)
2. **Step 2: Organize the SD-Branch setup for the Aruba IDPS Supported Gateways**
3. **Step 3: Connect and configure the Aruba IDPS Supported Gateways in Aruba Central**
4. **Step 4: Set up Aruba IDPS**
 - [Configure Aruba IDPS](#)

Gateway Provisioning Tasks for Existing Customers with Aruba IDPS Supported Gateways

Complete the following provisioning tasks to bring up your devices in the Aruba Central management interface:

1. **Step 1: Before you begin**
 - [Preparing to add the Aruba IDPS-Supported Gateways](#)
2. **Step 2: Set up Aruba IDPS**
 - [Configure Aruba IDPS](#)



Chapter 4

Working with Aruba Central

This section provides information about how to access and start using Aruba Central. You can access Aruba Central from the HPE GreenLake portal.

For detailed steps, see the **Accessing Aruba Central Portal** section in the *Aruba Central Online Help*.

Chapter 5

Onboarding IDPS-Supported Aruba Gateways

The following sections explain how to on-board Aruba IDPS supported gateways:

- [Preparing to add the Aruba IDPS-Supported Gateways](#)
- [On-boarding Devices for an Evaluation Account](#)
- [Upgrading the Firmware on a Device](#)
- [Managing Subscription Keys](#)
- [Assign Subscriptions to Aruba Gateways](#)
- [Assign Gateways to a Group](#)
- [Assigning a Group Role to an Aruba Gateway Group](#)
- [Connecting Aruba Gateways to Aruba Central](#)
- [Provisioning Aruba Gateways in Aruba Central](#)

Preparing to add the Aruba IDPS-Supported Gateways

If you are an existing customer who wants to enable and use Aruba IDPS, and do not have Aruba IDPS-supported gateways, then you need Aruba IDPS-supported gateways and a gateway or SD-Branch security license.

If you are an existing customer who has Aruba IDPS-supported gateways deployed, then you need a gateway or SD-Branch security license to use Aruba IDPS.

Supported Aruba Gateways for Aruba IDPS

The following table lists the Branch Gateway models that support Aruba IDPS:

Table 3: *Supported Aruba Gateways*

Platform	Deployment Type	Minimum Supported Software Version	Latest Software Version	Recommended Software Version
Aruba 9004-LTE	Branch Gateway	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0
Aruba 9012	Branch Gateway	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0
	VPNC	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0	ArubaOS 8.7.0.0-2.3.0.0
Aruba 9004	Branch Gateway	ArubaOS 8.5.0.0-2.3.0.0	ArubaOS 8.6.0.4-2.2.0.0	ArubaOS 8.6.0.4-2.2.0.0

The IDPS-supported gateway reboots in the following scenarios:

- When you apply the security license to Aruba IDPS-supported gateways on the network, the gateways reboot to enable the traffic inspection engine.
- When a System IP is assigned to the gateway.
- When the image on Activate and that on the device are different.
- When you upgrade the software to the recommended version.



When the gateways reboot, there will be a considerable down time (approximately 4 minutes) in the network. It is recommended that you apply the security license to the existing Aruba IDPS-supported gateways during non-working hours.

Best Practices

The following are some of the best practices for configuring Aruba IDPS and get the IDPS-supported gateways up and running:

- Ensure that you set up the recommended firmware upgrade at the group level.
- Assign the gateway or SD-Branch security subscription before you start to configure the IDPS-supported gateway.
- Ensure that the device image is compliant with the image in Activate.
- Follow the given sequence of steps to configure Aruba IDPS on a IDPS-supported gateway:
 1. Upgrade firmware to ArubaOS 8.5.0.0 - 2.3.0.0.
 2. Apply a valid security subscription.
 3. Enable traffic inspection.

On-boarding Devices for an Evaluation Account

You can add your IDPS-supported Branch Gateway to Aruba Central using the **Devices** option in HPE GreenLake platform.

For more information, see the **Devices** section in the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us

Upgrading the Firmware on a Device

The device firmware for IDPS is not updated automatically.

For details on how to check for an available version on the image server in the cloud and upgrade the firmware, see **Upgrading the Firmware** section in the *Aruba Central Online Help*.

Managing Subscription Keys

The subscription keys are managed on the **HPE GreenLake** portal.

For more information, see **Devices** section in the *HPE GreenLake Edge to Cloud Platform User Guide*, using the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=a00120892en_us

Assign Subscriptions to Aruba Gateways

For Aruba gateways to start functioning, you must onboard them in your account using the **Devices** option in HPE GreenLake platform.

A valid subscription allows the gateway to be managed by Aruba Central.

For detailed information about the available licenses for Aruba IDPS, see the **Assign Subscriptions to Aruba Gateways** section in the *Aruba Central Online Help*.

Assign Gateways to a Group

A group in Aruba Central is a primary configuration element that acts like a container. In other words, groups are a subset of one or several devices that share common configuration settings. Aruba Central supports assigning devices to groups for the ease of configuration and maintenance. For example, you can create a common group for Branch Gateways that have similar configuration requirements.

Aruba Gateway Groups

The device groups in Aruba Central support the following features:

- Combining Branch Gateways of identical characteristics and configuration requirements under a single group.
- Creating groups according to your branch requirements.
 - You can create separate groups for the small, medium, and large sized branches.
 - You can also create separate groups for the branch sites in different geographical locations; for example, East Coast and West Coast branch sites. If these groups have similar characteristics with minor differences, you can create the first group and then clone it.
 - You can use either a single group for all the devices or deploy devices in multiple groups. For example, you can deploy 7008 controllers and Aruba 2930F Switch Series with 24 ports in a single group for every branch.
 - You can also deploy 7005 controller and Aruba 2930F Switch Series with 24 ports in one group and provision 7008 controller with Aruba 2930F Switch Series with 48 ports in another group.
- Provisioning Branch Gateways and VPN VPNCs in separate groups. As the configuration requirements for Branch Gateways and VPNCs are different, the Branch Gateways and VPNCs must be assigned to different groups.
- Combining different types of devices under a group. For example, a group can have Instant APs, switches, and SD-Branch gateways.
- Adding different gateways to the same group will not create any problems in case of CaaS. However, Aruba does not recommend this as it might lead to inefficient configuration management. For example, if you add 9012 and 9004 gateways to the same group, you cannot configure ports (0/0/4 - 0/0/11).

For detailed steps, see the **Assigning Gateways to a Group** section in the *Aruba Central Online Help*.

Assigning a Group Role to an Aruba Gateway Group

The term persona in Aruba Central refers to a group role that you can set for the device groups. To deploy gateways for the SD-Branch or WLAN solution, you must configure a group role to designate gateways as Branch Gateways or VPNs.

For detailed steps, see the **Assigning a Group Role to an Aruba Gateway Group** section in the *Aruba Central Online Help*.



- Aruba Central does not support managing gateways at the MSP level. However, gateways can be configured and managed at the tenant account level. The persona of a default group at the tenant account level in MSP is set to **Branch Gateway**. The VPNC option is disabled.
- After you define a group role as a VPNC or Branch Gateway, Aruba Central does not allow you to edit or modify the group role.
- You can configure Aruba IDPS only on Aruba 9004 gateways. Aruba 9004 gateways can be deployed only as Branch Gateways.

Connecting Aruba Gateways to Aruba Central

The Aruba gateways have the ability to automatically provision themselves and connect to Aruba Central once they are powered on. The gateways also support multiple active uplinks for ZTP (also referred to as automatic provisioning). The supported ZTP ports for different hardware platforms are listed in the following table. All these ZTP ports are assigned to VLAN 4094.

Table 4: ArubaOS Hardware Platforms and Supported ZTP Ports

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba7005 Gateway	ALL ports except 0/0/1
Aruba7008 Gateway	ALL ports except 0/0/1
Aruba7010 Gateway	ALL ports except 0/0/1
Aruba7030 Gateway	ALL ports except 0/0/1
Aruba7024 Gateway	ALL ports except 0/0/1
Aruba7210 Gateway	ALL ports except 0/0/1
Aruba7220 Gateway	ALL ports except 0/0/1
Aruba7240 Gateway	ALL ports except 0/0/1
Aruba7280 Gateway	ALL ports except 0/0/1
NOTE: The minimum software version required for 7280 Gateway is ArubaOS 8.5.0.0 - 1.0.6.0.	

Table 4: ArubaOS Hardware Platforms and Supported ZTP Ports

ArubaOS Hardware Platform	Supported ZTP Ports
Aruba9004 Gateway NOTE: The minimum software version required for 9004 Gateway is ArubaOS 8.5.0.0 - 1.0.7.0.	ALL ports except 0/0/1
Aruba 9004-LTE Gateway	ALL ports except 0/0/1
Aruba 9012 Gateway	ALL ports except 0/0/1
Aruba 9240 Gateway	ALL ports except 0/0/1



Aruba7240 Gateway has attained end of life. For more information, see <https://www.arubanetworks.com/support-services/end-of-life/end-of-life-policy/>.

For detailed steps of how to automatically provision the gateways, see the **Connecting Aruba Gateways to Aruba Central** section in the *Aruba Central Online Help*.

After successfully connecting to Aruba Central, the gateways download the configuration from Aruba Central.



- From ArubaOS 8.7.0.0-2.3.0.0 release version onwards, Aruba SD-Branch Gateways no longer require additional reboot when they receive the gateway IP from Aruba Central after the ZTP process. Some services are restarted, resulting in an expected network impact, but the gateways do not reload for the second time. However, the gateways will reboot if there are any subsequent gateway IP changes.
- The gateways also include service ports that the technicians can use for manually provisioning devices in the event of ZTP failure. For more information on ports available for Aruba 7000 Series Mobility Controllers and Aruba 7200 Series Mobility Controllers, see *ArubaOS User Guide*.

Provisioning Aruba Gateways in Aruba Central

Aruba Central offers the following options to configure Gateways for SD-Branch deployments:

- **Groups**—You can create a logical subset of devices as groups. If you have devices that must share common configuration settings, ensure that you assign these devices to the same group. Any new device joining a group inherits the configuration that is already applied to the devices in a group. Similarly, you can also maintain separate groups for Branch Gateways and VPN Concentrators by assigning a group role for the devices.
- **Device-specific configuration**—If you have considerably lesser number of devices that do not have the same configuration requirements, you can apply configuration changes at the device level. In some cases, although the devices are assigned to a group, you may want to have a slightly different configuration to one specific device in a group. In such cases, you can modify the device configuration and apply changes at the device level. Aruba Central marks the discrepancies in the group and device configuration as overrides on the Configuration Audit page.

- Bulk Configuration—Aruba Central supports several bulk configuration options for Aruba Gateways:
 - Bulk Configuration Upload—Allows you to download a list of Aruba Gateways from Aruba Central in the CSV file format. You can add the configuration parameters for host name, system IP address, VLAN, and Ports, and then upload the CSV file to Aruba Central.
 - Gateway Pools—Allows you to create a common pool of IP addresses and enables automatic assignment of IP addresses to Aruba Gateways.
 - DHCP Pools—Allows you to configure a DHCP pool, using which Aruba Central automatically assigns a subnet to each Aruba Gateway for a given VLAN.
- APIs—Allows you to configure and monitor devices using NB APIs.

Different Modes of Configuring Gateways and Gateway Groups

Aruba Central supports the following methods for configuring Gateway groups and Gateways.

- **Guided Setup**—You can use the **Guided Setup** to quickly configure basic and essential parameters on Aruba Gateways for deploying the SD-Branch solution. The **Guided Setup** provides a wizard-based workflow for provisioning Gateways. The wizard allows you to configure Gateways at your own pace, pause, and resume when required. However, the Guided Setup will not be available after you complete the provisioning workflow for a Gateway group or a Gateway.
- **Basic Mode**—You can use the **Basic Mode** to configure your Gateways in a non-linear fashion. This mode allows you to make configuration changes after you provision your gateways for the first time using Guided setup.
- **Advanced Mode**—The Advanced mode allows you to configure advanced features for SD-Branch deployments.



Before you proceed with the configuration tasks, browse through the recommendations and best practices described in the *Aruba SD-Branch Fundamentals Guide* and *Aruba SD-Branch Security Hardening Guide*.

- **Configuration Templates**— You can provision Gateways using a configuration template.

For more information about configuring and provisioning Aruba Gateways, see *Aruba Central Online Help*.

You must configure Aruba IDPS to enable traffic inspection, threat detection, and threat prevention on the Aruba Branch Gateways and gateway clusters. Aruba Central provides an intuitive user interface that allows you to configure IDS or IPS with ease.

- **IDS**—IDS monitors the network for any malicious activity and generates an alert. IDS does not take any action on the identified threats. Configuring IDS will help detect the threats and capture the details of the threats detected.
- **IPS**—IPS monitors the network for malicious activity, generates alerts, and takes action based on a predefined rule. Configuring IPS will help detect the threats, create alerts, and drop the packets for the threats identified.

This chapter contains the following sections:

- [Configuring IDPS at Global, Group, and Device Level](#)
- [Enabling Traffic Inspection on Aruba Gateways](#)
- [Updating Ruleset for Aruba IDPS](#)
- [Configuring IDS on Aruba Gateways](#)
- [Configuring IPS on Aruba Gateways](#)
- [Manage Rules in Aruba IDPS Policies](#)
- [Manage Selective Inspection](#)
- [Troubleshooting Aruba IDPS](#)
- [Configure SIEM](#)
- [Configure Aruba IDPS Alerts](#)

Configuring IDPS at Global, Group, and Device Level

You can configure IDPS at Global, group, or device level to apply the configurations to a gateway, a group of gateways, or to a Security Incident and Event Management (SIEM) server.

The following details provide the specification for each level:

- If you select **Global** from the filter, you can configure a Security Incident and Event Management (SIEM) server provided by a third party such as Splunk. To configure Aruba IDPS, you have to select either a group or a gateway that supports Aruba IDPS configuration.
- If you select a **group** from the filter and configure Aruba IDPS, the configuration applies to all Aruba IDPS compatible gateways that are active in the group. The IDPS dashboard and threats list displays data for all Aruba IDPS compatible gateways that are active in the group.
- If you select a **device** from the filter and configure Aruba IDPS, the configuration applies only to the selected gateway, which is active in Aruba Central. The IDPS dashboard and threats list display data for only the selected Aruba IDPS supported gateways, which are active in Aruba Central.

Enabling Traffic Inspection on Aruba Gateways

You must configure traffic inspection to enable Aruba IDPS.

For detailed steps, see the **Enabling Traffic Inspection on Aruba Gateways** section in the *Aruba Central Online Help*.

- You have an active gateway subscription with security license.
- You must have on-boarded and connected the Aruba IDPS supported Branch Gateways or campus mobility gateways to Aruba Central successfully.

After traffic inspection is enabled, the Branch Gateways start detecting malicious events in the inbound and outbound data. IDS is selected as the default mode and IDS Strict is selected as the default policy. You can either configure IDS and IPS based on the requirement. Otherwise, the traffic inspection engine is set up to work on the default configuration.

Updating Ruleset for Aruba IDPS

To use the latest signatures, you must update the rulesets. After enabling traffic inspection, you can update the ruleset version. By default, the ruleset version is automatically updated every 24 hours.



The Aruba gateway (independent or part of a group) that you want to configure must support Aruba IDPS.

For detailed steps, see the **Updating Ruleset for Aruba IDPS** section in the *Aruba Central Online Help*.

Configuring IDS on Aruba Gateways

Configuring IDS enables traffic inspection engine to check the inbound and outbound data packets for threats and create alerts for the identified threats.

For detailed steps, see the **Configuring IDS on Aruba Gateways** section in the *Aruba Central Online Help*.

Configuring IPS on Aruba Gateways

Configuring IPS enables traffic inspection engine to check the inbound and outbound data for threats, create alerts, and drop packets for the threats identified.

For detailed steps, see the **Configuring IPS on Aruba Gateways** section in the *Aruba Central Online Help*.

Manage Rules in Aruba IDPS Policies

You can define a fail strategy for the traffic or enforce and apply Allow List rules for a policy. For detailed steps, see the **Managing Rules in Aruba IDPS Policies** section in the *Aruba Central Online Help*.

Configuring a Fail Strategy for Traffic

A fail strategy must be defined for any situation where the inspection engine is down, then how should the traffic be handled. You can either bypass or block the traffic. By default, the fail strategy is set to

Bypass, which means that traffic flow continues even when the Intrusion Prevention engine crashes and fails to inspect the traffic. When **Block** strategy is selected as the fail strategy, then traffic flow is blocked if it does not go through the inspection.

For detailed steps, see the **Configuring a Fail Strategy for Traffic** section in the *Aruba Central Online Help*.

Bypassing IDPS Inspection for Large Dataflows

Large dataflows sometimes cause latency or black hole in the traffic. Aruba Central allows you to bypass IDPS inspection for large SMB data transfers to avoid any drops, when large dataflows impact the traffic flow. Enable the **Bypass inspection for large dataflows** toggle switch. By default, the bypass inspection for large dataflow is disabled.

This option must be enabled only for gateways with huge SMB data transfers. When bypass is enabled, the inspection is not done for SMB traffic for the new and existing sessions. When bypass is disabled, the inspection is done for SMB traffic, but only for the new sessions.

For detailed steps, see the **Bypassing IDPS Inspection for Large Dataflows** section in the *Aruba Central Online Help*.

Viewing the Rules

Each and every rule is handled by a policy.

For detailed steps on how to view the rules, see the **Rules** section in the *Aruba Central Online Help*.

Manage Selective Inspection

The Risk-Oriented Traffic Inspection (ROTI) is a concept that aids the IDPS engine to process selective inspection. The **Selective Inspection** feature allows you to define a Traffic Treatment Type (T3) based on an identity. The **T3 Bucket** is the implementation of ROTI concept. T3 allows you to define a traffic treatment type for a group. The identity-based traffic inspection is introduced for client roles. Client roles are a combination of device or user roles.

Selective Inspection is introduced to handle any exceptions for the inspection based on your business requirement. **Selective Inspection** allows you to define a common traffic treatment type for a collection of client roles. The treatment type can be to either assign an inspection policy or bypass the inspection for a client role or roles. There are two pre-defined traffic treatment type buckets, namely **Risky** and **Safe**.

By default, the **Selective Inspection** is set to the **Risky** T3 bucket, that is, all the traffic for all client roles goes through inspection. If you have enabled IDS/IPS, the existing settings are inherited and all traffic passing through the gateway is inspected.

This feature is customizable according to your requirement. You can change the **T3 Bucket** name, choose which T3 bucket can be set as default, or change the policy for the **Risky** T3 bucket. Based on your requirement, if you have an exception for a client role, you can configure the default behavior and Aruba Central follows that for the selected roles. You can use different traffic treatment types for specific roles or choose to bypass the inspection for trusted roles.

The following scenarios serve as examples:

- If you want to retain the current behavior along with selective inspection, then do not change, keep the default as **Risky**. All the traffic is inspected for all roles. For example, the IoT devices are business critical, therefore must go through inspection. Critical users that are target for attacks are also strong

candidates for the inspection.

- If you want to bypass the inspection, then assign the client roles to the **Safe** T3 bucket. Traffic inspection is bypassed for the selected roles. For example, if you have vulnerability assessment tools that do not require inspection, then, you can assign that in the non-default bucket.
- If you do not want the default behavior, then assign client roles to the non-default bucket. For example, if your guest traffic does not consume any important resources, then assign that role to bypass the inspection.



Usually, anything connected to the trusted port does not get authenticated or get any role. Therefore, a policy cannot be assigned to it. In **Selective Inspection**, the **Trusted Traffic** is provided as a separate category and is available for assigning a role or policy.

For detailed steps, see the **Managing Selective Inspection** section in the *Aruba Central Online Help*.

Troubleshooting Aruba IDPS

You can enable the Aruba IDPS engine to capture malicious data packets to analyze the root cause and troubleshoot.

For detailed steps, see the **Troubleshooting Aruba IDPS** section in the *Aruba Central Online Help*.

Configure SIEM

Aruba IDPS provides the option to send the threat event data to a third-party Security Incident and Event Management (SIEM) server such as Splunk, which allows you to perform advanced analysis and generate reports. SIEM provides a holistic picture of the security posture of your organization by aggregating and correlating data from disparate sources in the network. For information about how to set up HTTP event collector in Splunk web, see

<https://docs.splunk.com/Documentation/SplunkCloud/9.0.2208/Data/UsetheHTTPEventCollector>.



SIEM configuration is available only in the **All Devices** context. If configured, threat data from all 9004 Branch Gateways connected to Aruba Central are sent to the SIEM server.

For detailed steps to enable, add, edit, delete a SIEM server and the supported URL formats, see the **Configuring SIEM** section in the *Aruba Central Online Help*.

Configure Aruba IDPS Alerts

This topic explains how alerts are aggregated and the different scenarios when these alerts are triggered.

Alert Aggregation

Gateway Threat Count

Aggregation determines how alerts are collected based on the duration, customer, or the device. For example, the **Gateway Threat Count** alert is aggregated at the gateway level for a time duration. In the alert configuration page, you can set the time duration.

The following is a screenshot of a sample configuration:

Figure 2 An Example for Gateway Threat Count Alert Configuration

The screenshot shows the 'Gateway Threat count' configuration page. Under 'Rule 1', the 'Severity' section has four options: Critical (selected), Major, Minor, and Warning. Each option has a corresponding 'exceeds' value: Critical is 500, Major is 400, Minor is 300, and Warning is 200. The 'Duration' is set to 30 mins.

The dataset used to run this service will be from last 30 minutes. If you have configured the alert at 5:00 PM for a duration of 30 minutes. Then the dataset used to run this service is from 4:30 to 5:00 PM. Considering the present time is 5:05 PM, then the dataset used will be from 4:35 PM to 5:05 PM.

The aggregation of alerts happens at the Gateway level. It triggers an alert for every Gateway. The triggered alert is based on the total number of IDPS events for each gateway.

For example, if you have five gateways with IDPS enabled in your Aruba Central account. The total number of IDPS events is 250 for two gateways. Then as per the configuration in [Figure 2](#), two alerts are triggered with Alert Severity as **Warning**. The alert is triggered because the events count (250 count) has exceeded the severity threshold configured (200 count) for **Warning**. If the number of events for the other three gateways is 530. Then three alerts are triggered with alert severity as **Critical**.

If the number of events for the other three gateways crosses 250, a **Warning** alert will be raised. If the IDPS event count crosses 500 for any of the three gateways. Then the alert severity of the raised alert changes from **Warning** to **Critical**.

Gateway Threat Count per Signature

For this alert, the aggregation happens for every customer. If you have configured five IDPS gateways in your Aruba Central account and each of them have 50 IDPS events count for one signature, then only one alert is triggered. The alert severity is **Warning** because the total number of IDPS events sums up to 250 (which exceeds the events count configured for **Warning** in the example). Therefore, this alert does not consider the individual gateways. The alerts are aggregated that is based on the events pertaining to each signature.

Gateway Threat Count per User

For this alert, the aggregation happens every time a user exceeds the defined threshold of threat events. Configure the severity as **Critical**, **Major**, **Minor**, and **Warning** by specifying the value for number of threats for a specific duration. Set the rule for group, label, or site. When a user exceeds the threshold, a notification is sent as email or webhook. For example, when a user accessing the gateway with IDPS license exceeds the defined threshold for threats, an email alert is sent to the administrator. The message in the email alert states, **Threat events for user id <userid> exceeded the threshold 8 in last 5 minutes, triggering this WARNING Alert notification.**

Alerts Acknowledgment

- **Automatic acknowledgment**

Alerts are acknowledged automatically when the event count drops below the lowest severity threshold configured for the alert. For example, if the lowest severity value is set to 200 for **Warning**. The alert is acknowledged automatically when the event count falls below 200 in the previous 30 minutes.

- **Manual acknowledgment**

Users with admin access can acknowledge alerts irrespective of the severity configuration. As manually acknowledging an alert does not reset the count data, the alert service continues to aggregate events. When the number of new events meets the configured threshold, an alert is triggered again. The alert service will use the previous data along with new data x1 (if any) for aggregation. If the aggregated count meets the configured threshold, an alert will be raised again.

Alert Severity and Transition

Alert severity falls under one of the following categories:

- **Critical**
- **Major**
- **Minor**
- **Warning**

The alert severity changes based on the severity threshold set up for each category and the events count in the last span of time interval.



The severity configured for the alerts is different from the **Threat Lists** and **Threat Details** pages in the **Security > Gateway IDS/IPS** tab. The Severity value displayed in the **Gateway IDS/IPS** tab is specific to the threat signature.

Debugging Branch Gateways for Aruba IDPS

If you come across any of the following scenarios, you can collect logs to debug the gateway from Aruba Central:

- In the [IDPS Tab in Gateway Dashboard](#), the **Traffic Inspection Engine Status** displays as **Crashed**.
- The **Traffic Inspection Engine Status** displays as not in **Running** status, despite enabling traffic inspection.
- The gateway is not updating to a rule set selected in the **Gateway IDS/IPS > General** page.
- While debugging other errors such as incorrect packet drops.

For detailed steps, see the **Troubleshooting Branch Gateways for Aruba IDPS** section in *Aruba Central Online Help*.



After troubleshooting Aruba IDPS, ensure to delete the three **Logging Levels** that you added. To delete an entry, select the row and click the delete icon.

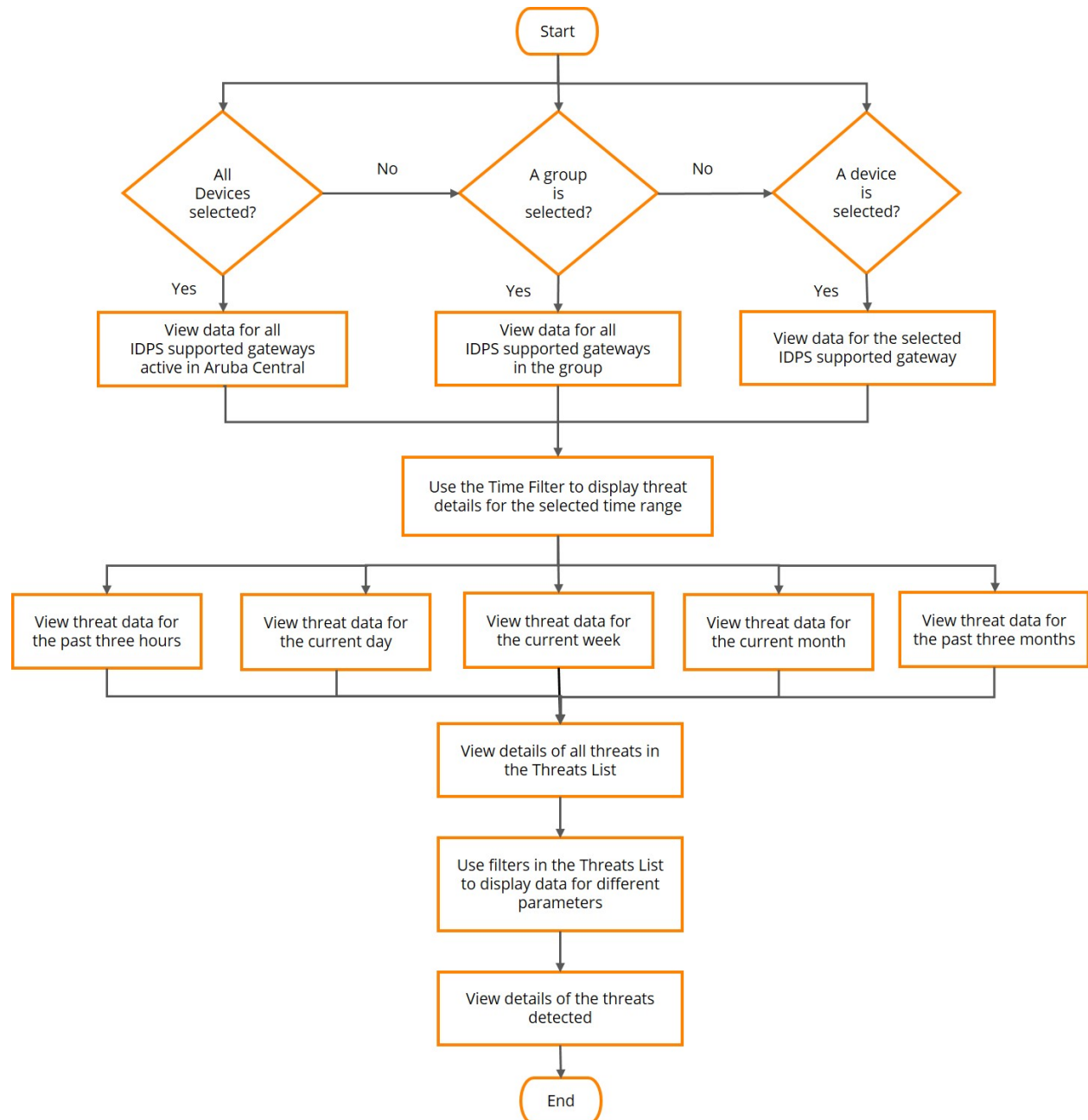
Troubleshoot Packet Drops

There might be instances when an IDPS engine incorrectly identifies legitimate traffic as malicious activity and drops packets. The following sections provide procedures to troubleshoot scenarios when legitimate data packets are dropped.

Packets dropped for legitimate traffic might or might not generate alerts. For detailed troubleshooting steps for such packet drops, see the **Troubleshooting Packet Drops** section in *Aruba Central Online Help*.

The **IDPS** dashboard provides all metrics about the threats information associated with the IDPS supported gateways connected to Aruba Central. The **IDPS** dashboard displays the threats detected by the traffic inspection engine in charts for different parameters.


The following flowchart shows how the threat data can be filtered and viewed.



Data Filters


The different data filters allow you to monitor and customize the threat data displayed on the charts.

Filter

The  filter option allows you to select a group or a IDPS supported gateway for performing specific configuration and monitoring tasks. If you do not select a group or a device, then the charts display data for all the IDPS supported gateways provisioned and managed through Aruba Central.




When you select a group from the filter, the IDPS dashboard displays threat data specific to the IDPS supported gateways within the group. When you select an individual IDPS supported gateway from the filter, the IDPS dashboard displays data specific to the hosts associated with the gateway.

Time Filter

The  time filter option allows you to set a time range to display threat details in the charts and threats list. You can set the filter to any of the following time ranges:

- **3 Hours**—The charts display the threat details for the past three hours.
- **1 Day**—The chart displays the threat details for the current day.
- **1 Week**—The chart displays the threat details for the current week.
- **1 Month**—The chart displays the threat details for the current month.
- **3 Months**—The chart displays the threat details for the past three months.

Threats List Filters

The  filters in the Threats List table allows you to filter data in the columns. The  and  icons allow you to sort the columns in either ascending or descending order.

Threats List

The Threats List provides details of the threats detected by the traffic inspection engine.

For detailed steps to navigate to the page, see the **Threats List** section in *Aruba Central Online Help*.

The **Threats List** table provides the following information:

- **Occurred On**—The timestamp of the gateway system clock specifying when the threat was detected.
- **Gateway**—Name of the gateway in which the threat was detected.
- **Model**—The gateway model number.
- **User Role**—The user role corresponding to the source where the threat is identified.
- **Ruleset Type**—The ruleset type currently running on the device. It is the IDPS engine version such as **4x** or **5x**.
- **Type**—The type of event in which the threat is identified.
- **Source**—The IP address of the host from where traffic is initiated.
- **Destination**—The IP address of the host where traffic is destined to.

- **Geo Location**—The geographic location details.
 - **Source**—The geographic location of the host that is initiating traffic.
 - **Destination**—The geographic location of target host that is receiving the traffic.
- **Severity**—The severity of the threat as classified by the ruleset.
- **Action**—The action defined in the ruleset.
- **Description**—The signature description of the threat event detected.

Viewing Details of a Threat

You can view the details of a threat in the packet info. For detailed steps to navigate to the packet info, see the **Threats List** section in *Aruba Central Online Help*.

The **Threat** details page provides the following information:

- **Timestamp**—The timestamp of when the threat was detected.
- **Signature**—The signature description of the detected threat.
- **Protocol**—The type of event in which the threat is identified.
- **Category**—The alert type under which the threat is categorized.
- **Source IP address**—The IP address of the host from where traffic is initiated.
- **Signature ID**—The ID associated with the signature.
- **Destination IP address**—The IP address of the host where traffic is destined to.
- **Severity**—The severity of the threat as classified by the ruleset.
- **Additional Details**—The detailed information about the alert.
 - **Alert**—The alert statement specifying that a alert was triggered due to a policy violation. The alert is triggered when a network traffic policy is violated based on threat categories. For more information, see alerts [Threat Categories](#).
 - **Description**—The description of the threat explaining more details such as how and where the violation has occurred.
 - **Impact**—The possible effect of the threat that may be caused on the network based on the severity of the alert.



Click the  icon to download the packet info to your local setup for troubleshooting.

Figure 3 *Threat Details*

THREAT

TIMESTAMP

2022-07-13 22:46:12

SIGNATURE

Behavioral Unusual Port 445 traffic Potential Scan or Infection

PROTOCOL

ALERT

CATEGORY

SCAN

SEVERITY

SOURCE IP ADDRESS

SIGNATURE ID

DESTINATION IP ADDRESS

ADDITIONAL DETAILS

ALERT

Network or application scanning and reconnaissance attempt.

DESCRIPTION

An attacker has attempted to map a network, running applications, or services available. This is often benign, but can frequently indicate a more concerted attack is in progress.

IMPACT

Reconnaissance

Packet Info


Downloading the Threats List

You can download the data in the Threats List table into a .csv file. The file consists of Timestamp, Protocol, Source IP Address, Destination IP Address, Action, Source Country Name, Destination Country Name, Gateway ID, Source Latitude, Source Longitude, Destination Latitude, Destination Longitude, Severity, Signature ID, Description, Category, and Strategy information. For detailed steps of how to download, see the **Threats List** section in *Aruba Central Online Help*.

Moving a Threat to Allow List

A user can move a rule from the enforced list to the Allow List to allow the rule which identified the threat. When you move a threat to allow list, the corresponding rule is allow listed and alert is not generated for that rule, and it applies to all devices of the selected group.



When threat events are moved to allow list using the allow list  icon in the **Threats List** table, it signifies that rules associated with those threat events will not be used to inspect network traffic. When this action is performed at **Global** level, these rules cannot be brought back into the enforce list. You may revert the rules back to enforce list by choosing IDS/IPS policy that contain those rules from the group or device level.

You can also move threats to the allowed list in the policies. For more information, see [Manage Rules in Aruba IDPS Policies](#)

For detailed steps of how to move a threat to allow list, see the **Threats List** section in *Aruba Central Online Help*.

Gateway Intrusion Detection and Prevention Dashboard

The Gateway IDS/IPS dashboard displays the threat details associated with the gateways with IDPS license and the hosts connected to the gateways. The Gateway IDS/IPS dashboard displays the threats detected by the traffic inspection engine in different charts and tables.

For detailed steps on how to navigate to the page, see the **Gateway IDS/IPS Dashboard** section in *Aruba Central Online Help*.

The **Gateway IDS/IPS** dashboard displays the following charts and tables.

Threats Charts

The **Threats** charts display the number of threats detected by the traffic inspection engine for a selected duration, grouped by the type of protocol. This can be useful to identify the highest number of intrusions in the network traffic.


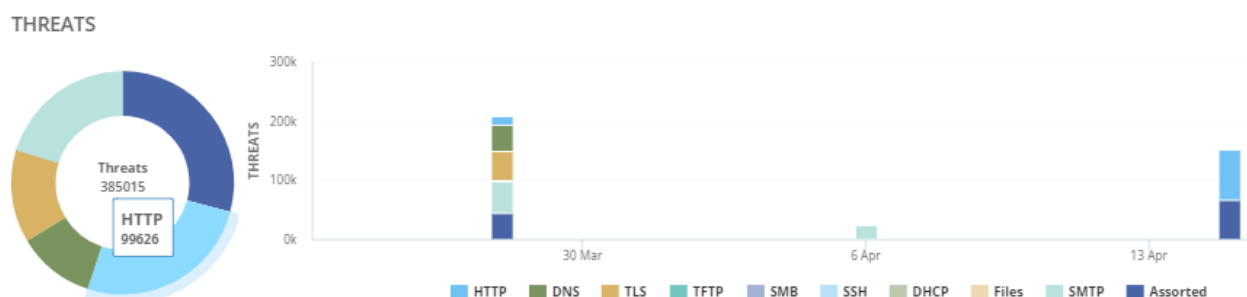
- **Threats pie chart**—The center of the chart displays the grand total number of threats detected for a selected duration. When you hover over the different regions on the chart, each region displays the total number of threats specific to the type of protocol for which the threat was detected. Click any region on the chart to view the threats for the particular type of protocol for the selected duration in the **Threats List**.
- **Threats bar chart**—The stacked vertical bars display the number of threats detected in a protocol for a selected duration. When you hover over a stacked vertical bar, it displays the timestamp and the number of threats for each type of protocol. Click any region on the stacked vertical bar to view threats for the particular type of protocol for the selected duration in the **Threats List**.
 - A legend is displayed for each type of protocol below the Threats bar chart. When you click a legend, the stacked vertical bar chart hides or shows the data for the selected type of protocol. By default, the stacked vertical bar displays the number of threats detected for all the protocols for a selected duration. For example, when you click **HTTP**, the stacked vertical bar chart hides or shows the number of threats detected for the **HTTP** protocol.
 - The  time filter allows you to set a time range to display threat details in the charts. You can set the filter to any of the following time ranges:
 - **3 Hours**—The bar chart is plotted on an hourly basis to display the threat details for the past three hours.
 - **1 Day**—The bar chart is plotted on an hourly basis to display the threat details for the current day.
 - **1 Week**—The bar chart is plotted on a daily basis to display the threat details for the current week.
 - **1 Month**—The bar chart is plotted on a daily basis to display the threat details for the current month.
 - **3 Months**—The bar chart is plotted on a weekly basis to display the threat details for the past three months.

Figure 4 Threats Pie and Bar Chart



Trends Table

The **Trends** table displays the threat type, number of threats, and the percentage of change in the number of threats of each type in comparison to the previous duration. This is useful to indicate a sudden change in the number of threats of a certain type from the previous duration to help identify a threat pattern. Click a threat type to view threats for the particular type in the **Threats List**.

Figure 5 Trends Table

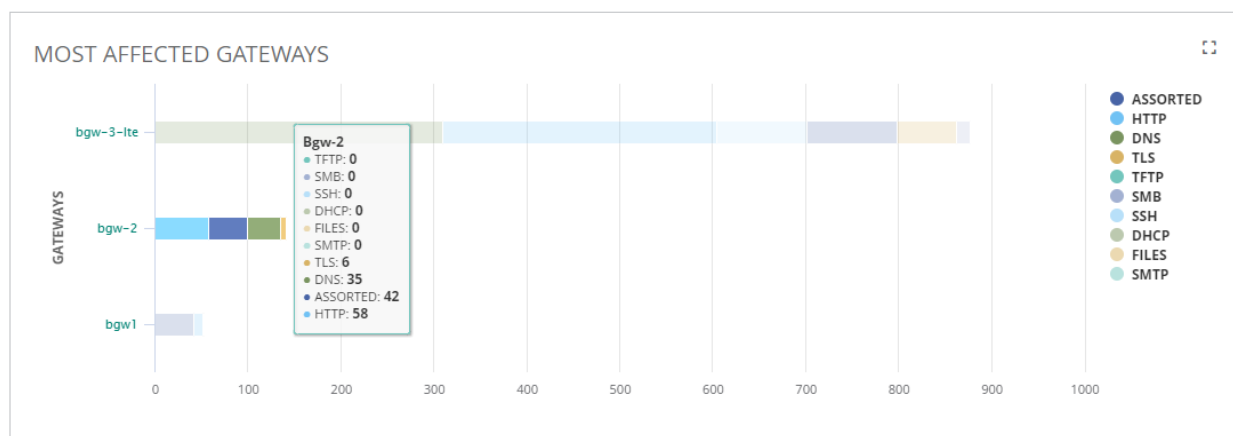
TRENDS

Type	Count	% Change
Assorted	112365	100% ↗
HTTP	99626	100% ↗
SMTP	77617	100% ↗
TLS	51660	100% ↗
DNS	43490	100% ↗
SMB	257	100% ↗

Most Affected Gateways or Hosts Chart

When you select **All Devices** in the filter, the chart displays the top 10 gateways with the number of threats detected in a stacked horizontal bar chart. When you hover over a horizontal stacked bar, it displays the number of threats for each type of protocol. Click a stacked horizontal bar to view threats for the particular type of protocol on the **Threats List** table. Click the legend for the threat type to show or hide the data for the threat type on the chart.

Figure 6 Most Affected Gateways Chart



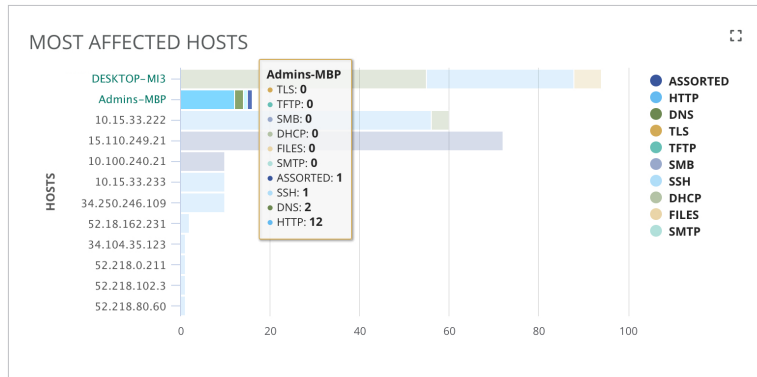
When you select a group or an IDPS supported gateway in the filter, the **Most Affected Gateways** chart is replaced by the **Most Affected Hosts** chart.

When you select a group in the filter, the chart displays the number of threats detected for the top 10 hosts connected to all IDPS supported gateways within a group. When you select an IDPS supported gateway in the filter, the chart displays the number of threats detected for the top 10 hosts associated with the gateway.



The host name is displayed on the chart only if the host name is configured, otherwise the source IP address is displayed. For more about configuring host name, see [Configuring or Renaming Gateway Hostname](#).

Figure 7 *Most Affected Hosts Chart*



Top Sources & Destinations Table

The **Top Hosts Sources** or **Destinations** table displays the top ten IP addresses of the source and destination hosts with the number of threats identified. Select either **Sources** or **Destinations** from the **Top Hosts** drop-down to view the host and corresponding threats. Click an IP address under **Sources** to view threats on the **Threats List** table for the selected source IP address. Click an IP address under **Destinations** to view threats in the **Threats List** table for the selected destination IP address.



The host name is displayed in the table only if the host name is configured, otherwise the source IP address is displayed. For more about configuring host name, see [Configuring or Renaming Gateway Hostname](#).

Figure 8 *Top Sources & Destinations Table*

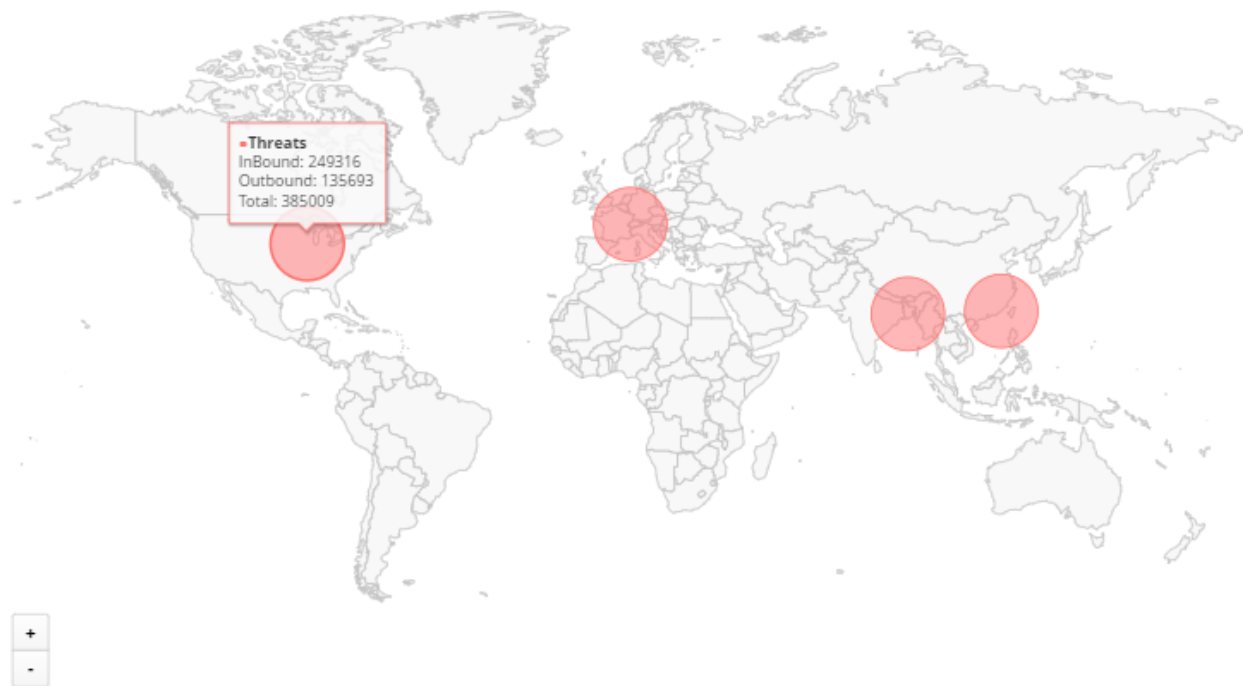
TOP HOSTS SOURCES ▼	
HOSTS	Count
91.0.0.2	364
DESKTOP-KG92P0B	251
81.0.0.3	215
81.0.0.4	180
91.0.0.110	177
91.0.0.111	175
81.0.0.6	171
81.0.0.5	170
91.0.0.128	166

Threat Map

The **Threat Map** displays the locations of the hosts, in which threats are detected. Hover over a location to view the number of inbound, outbound, and the total number of threats detected. Inbound displays the number of threats in the incoming traffic at a specific location. Outbound displays the number of threats in the outgoing traffic at a specific location. You can zoom in, zoom out, and move the map to view the threat details for a specific location. Click a location to view threats on the **Threats List** table.

Figure 9 Threat Map

THREAT MAP



IDPS Tab in Gateway Dashboard

The **IDPS** tab under **Manage > Overview** in the gateway dashboard displays the following sections, in addition to the Actions and Go Live functions that can be performed:

- [Traffic Inspection Engine Status](#)
- [Traffic Inspection Engine CPU Usage](#)
- [Traffic Inspection Engine Memory Usage](#)
- [Dropped Packets](#)
- Actions
- Go Live

After you on-board the gateways and configure IDPS, you can view the IDPS traffic engine health and the number of packets dropped.

For detailed steps to navigate to the page, see the **Gateways > Overview > IDPS** section in *Aruba Central Online Help*.

You can change the time range for the **IDPS** tab by clicking the time range filter and selecting one of the available options: **3 hours**, **1 day**, **1 week**, **1 month**, and **3 months**.

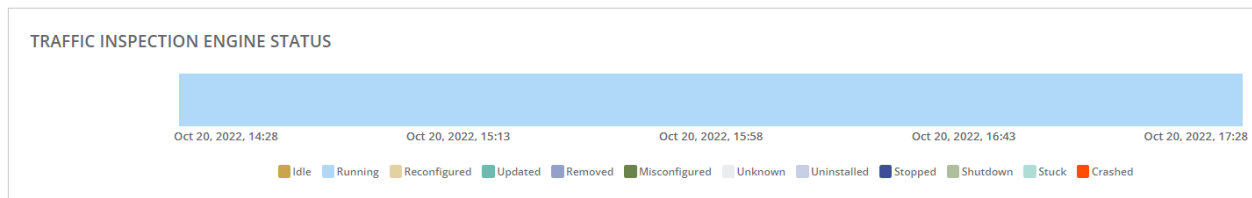
Traffic Inspection Engine Status

The **Traffic Inspection Engine Status** chart displays the status of the traffic inspection engine for the selected period in a timeline chart. Hover over the graph to view the status of the traffic inspection engine at a particular time. The legends represent different status of the traffic inspection engine.



The **Traffic Inspection Engine Status** chart is available for a period of 3 hours, 1 day, 1 week, or 1 month.

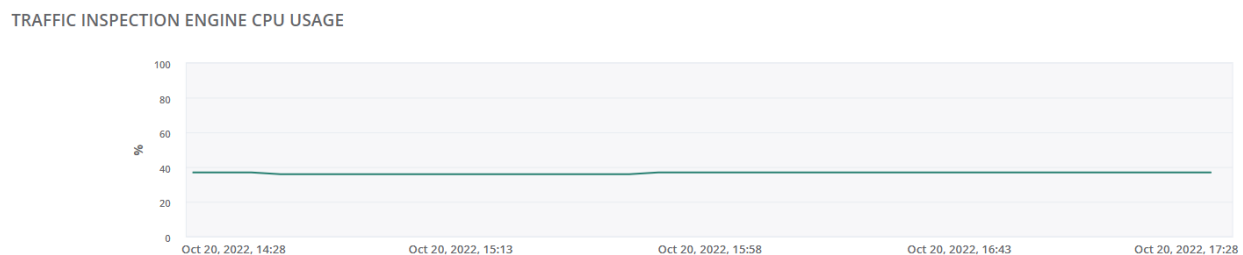
Figure 10 *Traffic Inspection Engine Status*



Traffic Inspection Engine CPU Usage

The **Traffic Inspection Engine CPU Usage** chart displays the CPU usage percentage of the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the CPU usage percentage at a particular time.

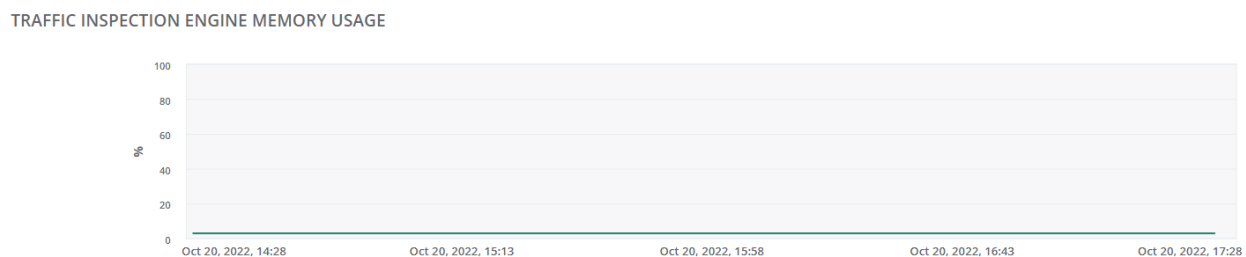
Figure 11 *Traffic Inspection Engine CPU Usage*



Traffic Inspection Engine Memory Usage

The **Traffic Inspection Engine Memory Usage** chart displays the percentage of memory usage by the traffic inspection engine for the selected period in a line chart. Hover over the graph to view the memory usage percentage at a particular time.

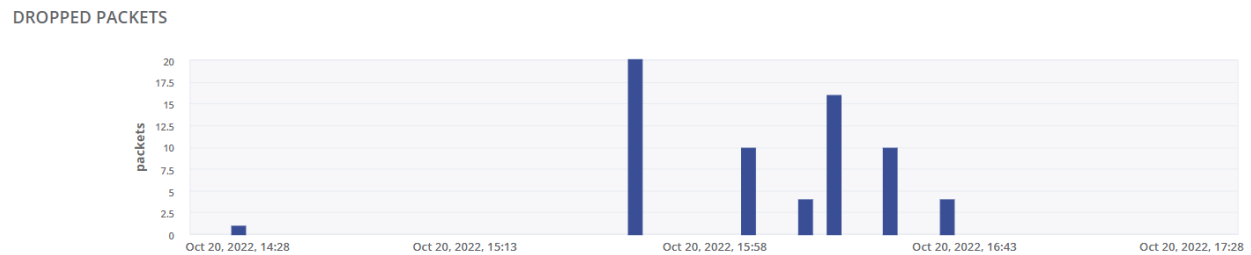
Figure 12 *Traffic Inspection Engine Memory Usage*



Dropped Packets

The **Dropped Packets** chart displays the number of packets dropped for the selected period in a vertical bar chart. Hover over the graph to view the packets dropped at a particular time.

Figure 13 *Dropped Packets*



Actions

The **Actions** drop-down list contains the following options (the **Clear IPsec SA**, and **Clear ISAKMP SA** options are available for tunnels only):

- **Reboot Gateway**—Reboots the gateway.
- **Open Remote Console**—Opens the remote console for a CLI session through SSH. The default user ID is admin, but you can edit and customize the user ID. This custom user ID must be mapped to the device.
- **Clear IPsec SA**—Clears the IPsec Security Associations (SA).
- **Clear ISAKMP SA**—Clears the ISAKMP SA.

Go Live

The **Go Live** link redirects to the **Manage > WAN > Summary** tab in the gateway dashboard.

The following is a list of FAQs related to Aruba IDPS categorized into different sections based on the functionality:

- [Overview](#)
- [Licensing](#)
- [On-boarding IDPS Supported Gateways](#)
- [Configuration](#)
- [Gateway Set Up](#)
- [Rulesets and Policies](#)
- [Selective Inspection](#)
- [Monitoring](#)
- [Traffic Monitoring](#)
- [SIEM](#)
- [Troubleshooting](#)

Overview

Which traffic inspection engine is used in Aruba IDPS?

Aruba IDPS uses an open source traffic inspection engine to detect and prevent intrusion in the inbound and outbound traffic.

What is the performance of the traffic inspection engine?

The performance of the traffic inspection engine for TCP Enterprise Mixed Throughput is Up to 920 Mbps in IPS mode and up to 950 Mbps in IDS mode.

Can I run the traffic inspection on a VPNC gateway in the Data Center?

Aruba Central version 2.5.3 and later support running Aruba IDPS in 9012 as a VPNC Gateway, and can be run in the Data Center. To run Aruba 9012 gateway as a VPNC, ensure that the 9012 gateway has ArubaOS 8.7.0.0-2.3.0.0 version installed and has all the required licenses and Aruba IDPS enabled.

Can I perform Sandboxing test on Aruba IDPS?

Sandboxing test can be performed on Aruba IDPS.

What are the types of protocol streams that are inspected by the traffic inspection engine?

All types of protocol streams are inspected by the traffic inspection engine on a 5x ruleset type. For example, HTTP, DNS, TLS, TFTP, SMB, SSH, DHCP, FILES, SMTP, SNMP, SIP, RFB, MQTT, RDP, and HTTP2.

Can I select protocol streams that can be inspected by the traffic inspection engine?

In the current release, the traffic inspection engine inspects all types of protocol streams. You can allow list the threat signatures or bypass inspection for large dataflows, if you do not want the threat signatures to be inspected by the traffic inspection engine.

How extensive is the signature pack and what types of vulnerabilities does it capture?

Aruba IDPS includes rulesets with rules and each rule contains signatures for different types of threat categories. Aruba IDPS includes three policies, namely lenient, moderate, and strict. The policies define rules to drop or allow packets that match a specific threat signature. The appendix provides description of some of the threat categories. For more information, see [Threat Categories](#).

How are the events reported when there is an attack on my network?

When there is an attack on the network, the events are reported in the **Gateway IDS/IPS** dashboard and the **Threats List**. Aruba Central also allows you to configure notifications for IDS and IPS alerts. For more information, see [Gateway Intrusion Detection and Prevention Dashboard](#).

How do I quarantine the infected clients?

Aruba IDPS provides the option to send threat event data to a third-party Security Incident and Event Management (SIEM) server such as Splunk. The correlation and incident management sends a request to Aruba ClearPass Policy Manager to move the infected client to quarantine. Aruba Central receives the notification delivery for all alerts through Webhooks configuration.

Who provides the threat intelligence to the traffic inspection engine?

The Aruba IDPS receives threat intelligence from a third-party service provider to monitor the inbound and outbound traffic for any malicious activity. For more information, see <https://www.proofpoint.com/us/products/advanced-threat-protection/et-intelligence>.

How does Aruba IDPS work in conjunction with Zscaler Cloud Security Service for SD-Branch and AOS 10 Mobility Gateway?

Aruba IDPS and Zscaler complement each other. Aruba IDPS inspects network traffic on the Branch Gateway at the edge driven by policies from Aruba Central. Zscaler or other Cloud Security services route the traffic based on their policy, to the Cloud Security Point of Presence (POP) in the Cloud and traffic is inspected based on the policy defined in the admin console. Additionally, Cloud Security

Services provide their own cloud native security services that may be used from across various environments.

How does the Aruba IDPS security solution work in conjunction with SD-Branch and AOS 10 Mobility Gateway?

The Aruba IDPS security solution is enabled on SD Branch Gateways. When IDPS is enabled, traffic in all directions, including east-west and north-south are inspected for any threat intrusion.

How is the Aruba IDPS security solution different from security solutions offered by other competitors?

The Aruba IDPS security solution prevents and protects the network from threat intrusions. It improves network security with features, such as full packet inspection, north-south and east-west inspection, allow listing, multi-dimensional threat metrics, threat intelligence, correlation and incident management, simplified configuration, and licensing.

What are the software and hardware requirements to implement IDPS?

For more information about the minimum supported software version and the recommended software version, see [Preparing to add the Aruba IDPS-Supported Gateways](#).

Can I evaluate the security features before using them in the production environment?

Yes, you can evaluate the IDPS security features using an **Advance with Security** evaluation license which expires after 90 days. It allows you to evaluate up to 10 devices with Aruba IDPS and advanced SD-Branch features on the IDPS-supported gateways.

What is the advantage of an IDPS-enabled gateway?

An IDPS-enabled gateway is entitled to security features. If you have IDPS-enabled gateway, you do not have to invest on another application to do the traffic inspection. It provides rich data that aids in monitoring such as CPU memory statistics, engine state, any drop in the packets, and so on.

How does Aruba IDPS help in improving network security?

Aruba IDPS helps the administrator to monitor, detect, and prevent malicious events for traffic in east-west and north-south directions, generates a threat event, and records details about these events. All identified threats are logged and can be sent to external systems (like Splunk Cloud) for correlation analysis. It provides an extra layer of protection that actively analyzes the network and takes actions on your traffic flows based on pre-configured rules.

Licensing

Which devices are supported by IDPS?

The Aruba 9004, 9004-LTE, and 9012 gateways support IDPS.

Is there any change in the workflow for new customers for on-boarding gateways and assigning subscriptions in IDPS?

Yes, there is a change in the workflow for new customers for on-boarding a gateway from Aruba Central 2.5.5. The features like adding devices and assigning licenses are available on HPE GreenLake. To use IDPS, you must assign **Advanced with Security** license to gateways.

How do I apply a license to evaluate the features of IDPS?

To evaluate the IDPS features, you must assign **Advance with Security** evaluation license to the gateways.

Is the Advance with Security evaluation license specific to IDPS-supported gateways?

No, the **Advance with Security** license gives all features of an **Advanced** subscription along with security license. You can use it as an evaluation license for IDPS-supported gateways. It allows you to evaluate up to 10 devices with Aruba IDPS and advanced SD-Branch features.

Can I use the evaluation license on the production environment of IDPS?

Yes, the evaluation license can be used on the production environment.

What features are supported for evaluation license?

The evaluation license supports all features of an **Advance with Security** license.

How do I move from an evaluation subscription to a paid subscription?

To move from an evaluation subscription to a paid subscription, you must assign a valid subscription to gateways in the **Subscription Management** page.

I am an existing customer and I am using a SD-WAN license. How do I upgrade to a security license?

To upgrade from a Foundation or an Advanced SD-WAN license to a security license, you must assign a valid subscription with security license.

I am an existing customer with IDPS supported gateways. How do I move the gateways from production cluster to beta cluster?

To move the gateways from production cluster to beta cluster for testing purpose, you must unassign the subscriptions from the devices, on-board the devices to the new cluster, and then assign valid subscriptions to the devices in the new cluster.

I am an existing customer without IDPS supported gateways. How do I upgrade to a security license?

To upgrade to a security license, you must on-board IDPS supported gateways and then assign a valid subscription with security license.

Why does the gateway reboot when I apply a security license?

When a security license is applied, the gateways reboots as the traffic inspection engine is activated for the first time. It is recommended that you apply the security license after business hours, as this might result in a downtime in the network.

How to check the status of a subscription?

You can check the status of the subscription using the **Devices** option in HPE GreenLake platform.

Can I rollback from a security license to a non-security license?

No, you must purchase a new valid subscription without security after the expiry of the current subscription.

Is there any impact to IDPS licensing model and functionality after moving to Common Cloud Services Platform?

No, there is no impact to the IDPS licensing model or functionality. However, managing subscriptions is done through the **HPE GreenLake** portal.

On-boarding IDPS Supported Gateways

What is the difference in on-boarding an IDPS-enabled gateway or other gateways?

There is no difference in on-boarding an IDPS-enabled gateway or other gateway. Only the IDPS-enabled gateway will require a reboot after the onboarding.

Do I need to on-board devices to Aruba Central before assigning subscriptions?

Yes, you must on-board devices to Aruba Central before assigning subscriptions.

How to on-board an IDPS gateway for a new customer?

For a new customer, the IDPS-supported gateways associated with your account are automatically retrieved. If the device you purchased does not show up in your account, you can manually add it.

To verify if the devices are added to the device inventory, see the **Managing Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

How to on-board a gateway with IDPS support for an existing customer ?

For an existing customer with IDPS supported gateways, you must remove the devices from the production cluster and then on-board the devices to the new cluster.

For more information, see the **Managing Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

How to on-board a gateway without IDPS support for an existing customer?

For an existing customer without IDPS supported gateways, you should purchase IDPS supported gateways and then on-board the devices to the new cluster.

For more information, see the **Managing Devices** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

How do I upgrade the firmware on the device?

You can manually upgrade or set the compliance for gateways in standalone mode to upgrade the firmware.

I see "single sign on enabled". How do I change or disable this?

If your email address is in the [arubanetworks.com](https://www.arubanetworks.com) or [hpe.com](https://www.hpe.com) domain, the single sign on is enabled. You can change or disable through SAML SSO configuration.

For more information, see the **HPE GreenLake Single Sign-On (SSO) Management** section in the HPE GreenLake Edge to Cloud Platform User Guide, using the following link:

<https://www.arubanetworks.com/techdocs/central/latest/content/nms/intro-pages/related-info.htm>

Why do I see the "Server Details" drop-down menu with a list of names? Which one should I select?

The **Registration** page displays a list of zones in which the Aruba Central servers are available for account creation. Based on the country you select, the Aruba Central server is automatically selected. If you want your account and Aruba Central data to reside on a server from another zone, you can select an Aruba Central server from the list of available servers. For more information, see *Aruba Central Online Help*.

I see a drop-down list on the top right where I can select languages. What other languages are supported?

Gateway IDS/IPS supports a total of seven different languages. The languages supported are English, Spanish, Brazilian Portuguese, French, German, Japanese, and Chinese.

Configuration

What is the hierarchy of configuration?

Aruba Central allows you to configure **Gateway IDS/IPS** at global, group, and device level. To configure SIEM on all IDPS-supported gateways added to Aruba Central, at a global level, select **Global** from the filter. Device configuration is done at the group and device level. To configure all IDPS-supported gateways at a group, select the group from the filter. To configure an individual IDPS-supported gateway, select a gateway from the filter.

What are the different modes of traffic inspection available?

In **Gateway IDS/IPS**, there are two modes of traffic inspection available, namely **IDS** and **IPS**.

What happens when the inspection mode is set to IPS?

When the inspection mode is set to **IPS**, the traffic engine enforces the IPS strict policy, which intrudes malicious traffic by dropping packets based on the rule match.

What does the ruleset version signify?

A ruleset version displays the current version of applied ruleset. It is recommended to keep the latest version for effective traffic inspection.

Can I bypass large dataflows from inspection?

Yes, you can bypass the large dataflows transfers or large dataflows using the **Bypass Inspection for Large Dataflows** toggle switch on the **Gateway IDS/IPS** configuration page. You must add the respective port number to bypass it from scanning. By default, the bypass inspection for large dataflow is disabled. For more information, see [Manage Rules in Aruba IDPS Policies](#).

Gateway Set Up

How do I set up a group for IDPS gateways?

Under **Maintain**, navigate to **Organization > Groups** on the **Aruba Central** app to set up a group for gateways.

Is there any difference in provisioning the gateways for IDPS?

No, there is no difference in provisioning the gateways.

What is the ideal way to group gateways?

The ideal way to group gateways is to assign all IDPS gateways to one group and other gateways to separate groups.

Does 90xx secure gateway scan IPSec/ESP encrypted traffic?

No, by default, IPSec/ESP encrypted traffic is not inspected. However, the pre-encryption and post-decrypted sessions are scanned for threats.

Can I upgrade the 90xx IDPS secure gateway running IDPS engine 4.x to 6.x?

Yes, you must install AOS 10.4.0.0 firmware version to upgrade.

What new protocols are supported with IDPS 6.x engine version?

Protocols like SNMP, SIP, RFB, MQTT, RDP, and HTTP2 are newly supported with the IDPS 6.x engine version.

Rulesets and Policies

What are the different types of security policies?

There are three different types of security policies for IDS and IPS, namely lenient, moderate, and strict.

How does enabling IDPS impact operation of the gateway?

For a new and an existing customer, enabling IDPS enhances the gateway operation with the added IDPS security features. However, for existing customers with IDPS supported gateways, the gateways reboot as the traffic inspection engine is activated for the first time. It is recommended that you apply the security license after business hours, as this might result in a downtime in the network.


Which is the default inspection mode in Gateway IDS/IPS?

In **Gateway IDS/IPS**, the default inspection mode is IDS.

What is the default security policy in IPS and IDS?

The default security policy for IPS is **IPS Strict**, and for IDS is **IDS Strict**.

How do I stop traffic inspection for certain IDS or IPS rules?

To stop traffic inspection for certain IDS or IPS rules, select the rules in the **Rules** table and click the  **Move to Allow List** icon. For more information, see [Manage Rules in Aruba IDPS Policies](#).

How do I update the ruleset version at regular intervals?

Select the **Automatically update the ruleset** check box in the Gateway IDS/IPS configuration page and set the day and time to update the ruleset version. For more information, see [Updating Ruleset for Aruba IDPS](#)

What does the alert icon in the Ruleset version signify?

The alert icon signifies that the ruleset version is not up-to-date and when the ruleset version of the device is older than the ruleset version of the group that it belongs to. To update the ruleset version, hover over the icon to know the latest version available, select the version from the **Update To** drop-down list, and click **Update** in the confirmation window.

When does IDPS Supported gateways check for updated ruleset?

The IDPS Supported gateways check for updated ruleset in the following scenarios:

- When you onboard IDPS Supported gateways to Aruba Central and enable Aruba IDPS, the IDPS Supported gateways check for updated ruleset version.
- The IDPS Supported gateways check for updated ruleset when the configured ruleset version does not match with the device ruleset version.
- When you configure the IDPS Supported gateways for automatic update of the ruleset version, the IDPS Supported gateways check for updated ruleset version at the schedule time.
- When IDPS Supported gateways reconnect to Aruba Central, the IDPS Supported gateways check for updated ruleset version.
- When IDPS Supported gateways fail to update due to network issues, the IDPS Supported gateways check for updated ruleset version every three minutes until it is successful.

Can I view the list of gateways running 4.x and 5.x rulesets?

Yes, you can view the version number in the **Ruleset Type** column under **Manage > Devices > Gateways**.

Can both 4.x and 6.x gateway engine versions co-exist in a single group?

Yes, it is possible.

Can I view the latest ruleset available timestamp information?

Yes, you can view the timestamp on the **Config > General** tab. For more information, see [Updating Ruleset for Aruba IDPS](#).

Can I perform signature allow listing separately for 4.x and 5.x gateway when they are in the same group?

Yes, you can allow list the signature belonging to a particular ruleset version.

Selective Inspection

Can I associate a policy to any T3 Bucket?

In Aruba Central 2.5.7 version, policy can be associated to only one bucket and other bucket has no policy. The Safe T3 bucket is a bypass inspection bucket and does not have any policy associated to it.

Can I edit the T3 Bucket name?

Yes, you can change the T3 Bucket name.

Does Selective Inspection support the downloadable user roles?

No, selective inspection does not support the downloadable user roles. It is not supported for ArubaOS 10.x.

Does Threats List page have user role information?

Yes, it has the **User Role** column. When there is a threat event match, the corresponding event displays the source role of the traffic in the **Threats List** table.

How is bypass different in Selective Inspection and Bypass Inspection for Large Dataflows?

Bypass Inspection for Large Dataflows is used only to bypass the inspection for the large SMB data transfers. For more information, see [Manage Rules in Aruba IDPS Policies](#).

Whereas, **Selective Inspection** is based on the administrator choice to bypass or inspect the traffic for client roles. When risky bucket is selected, then traffic is inspected. When the safe bucket is selected, then inspection is bypassed for the client roles assigned to it. For more information, see [Manage Selective Inspection](#).

How is Selective Inspection buckets different from role-based ACLs?

In the role-based ACL, only one role is selected for each ACL. In Selective Inspection, you can group the required client roles under the bucket and apply the inspection policy for multiple roles without having to define a separate ACL for each.

Is it possible to selectively bypass or inspect specific trusted traffic?

Aruba Central 2.5.7 does not support this.

Is there any limitation to the number of client roles that can be added to a T3 bucket?

No, there is no limit. Any number of client roles that are defined in the gateway page can be used.

Traffic has source and destination role, which one is considered for the Selective Inspection?

Only the source role is considered for the Selective Inspection.

What is considered as trusted traffic?

Anything connected to the trusted port does not get authenticated or get any role. Therefore, a policy cannot be assigned to it. In Selective Inspection, the Trusted Traffic is provided as a separate category and is available for assigning a role or policy. It cannot be deleted and the administrator must explicitly assign Trusted Traffic to one of the bucket.

What is the benefit of Selective Inspection?

Implicit benefit of Selective Inspection is the increased overall throughput of the gateway. Because, only a part of the traffic is inspected.

Monitoring

Can I view the threat data for different durations?

Yes, you can view the threat data for 3 hours, 1 day, 1 week, 1 month, and 3 months by selecting a duration in the time range filter.

Can I view the threat data for a duration of more than three months?

In the current release, you cannot view the threat data for a duration of more than three months.

How do I view the threats that are identified?

The **Gateway IDS/IPS** dashboard displays the threat details associated with the IDPS supported gateways with IDPS license and the clients connected to the IDPS supported gateways. The **Gateway IDS/IPS** dashboard displays the threats detected by the traffic inspection engine in different charts and tables. The charts and tables displayed are **Threats**, **Trends**, **Most Affected Gateways or Hosts**, **Top Sources & Destinations**, and **Threat Map**. For more information, see [Gateway Intrusion Detection and Prevention Dashboard](#) and [Threats List](#).

How do I view the details of the most affected gateways?

When you select **All Devices** in the filter, the **Most Affected Gateways** chart in the Gateway IDS/IPS dashboard displays the top 10 gateways with the number of threats detected in a stacked horizontal bar chart. For more information, see [Most Affected Gateways or Hosts Chart](#).

How do I view the details of the most affected hosts?

When you select a group in the filter, the **Most Affected Hosts** chart displays the number of threats detected for the top 10 hosts connected to all IDPS supported gateways within a group. When you select a IDPS supported gateway in the filter, the chart displays the number of threats detected for the top 10 hosts associated with the gateway. For more information, see [Most Affected Gateways or Hosts Chart](#).

What does HTTP and SMTP convey in the Threats chart?

In the **Threats** chart, the **HTTP** and **SMTP** are the types of protocols for which the threats are identified. When you click on a protocol, the bar chart hides or shows the number of threats detected for the selected protocol for the selected duration.


What does % change convey in the Trends chart?

In the **Trends** chart, the % change displays the percentage of change in the number of threats versus the previous time period.


How do I view the details of the most threat generating sources and destinations?

In the **Gateway IDS/IPS** dashboard, the **Top Sources and Destinations** chart displays source and destination of the top threat generating traffic. For more information, see [Gateway Intrusion Detection and Prevention Dashboard](#).

How do I view the details of a particular threat?

In the **Threats List** table, select a threat and click the  **View Packet info** icon to view the details of the selected threat. The **Additional Details** section displays the description of the alert along with impact. For more information, see [Threats List](#).

How do I allow a rule?

In the **Threats List** table, select a threat and click the  **Move threat to allow list** icon to allow a threat. For more information, see [Threats List](#).

How do I view the geolocation of the detected threats?

In the **Gateway IDS/IPS** dashboard, the **Threat Map** displays the geolocation details of the detected threats and on the threats table. For more information, see [Gateway Intrusion Detection and Prevention Dashboard](#) and [Threats List](#).

Where can I see the ruleset version?

You can view the ruleset version under **Manage > Devices > Gateways**. The **Ruleset Type** column displays the version that is currently running on the device such as 4.x or 5.x.

Alerts and Events

What does the Alert & Events pane displays?

The **Alerts & Events** pane displays all types of alerts and events generated for events pertaining to device provisioning, configuration, and user management in the **List** view. Click the **Summary** view to see a detailed graph pertaining to each device type.

- **Summary** View—Allows you to view a detailed graph pertaining to each device type.
- **List** View —Allows you to view the list of total alerts and events generated. You can also filter the alerts based on the severity level by clicking the severity level tabs.
- **Config** View—Allows you to configure different types of alerts.

What are the alerts severity levels displayed?

- Critical
- Major
- Minor
- Warning

What does Acknowledged Alerts mean?

Acknowledged alert means that the admin has acknowledged or worked on a specific alert raised against an event. It means that the admin is now ready to start alerting on that event again.

What user role is needed to configure alerts?

Only network administrators or users those who have an admin role can configure alerts.

Traffic Monitoring

How do I monitor the status of the traffic inspection engine?

The **Traffic Inspection Engine Status** chart in the **IDPS** tab displays the status of the traffic inspection engine for the selected period in a timeline chart. Hover over the graph to view the status of the traffic inspection engine at a particular time. The legends represent different status of the traffic inspection engine. For more information, see [Traffic Inspection Engine Status](#).

What are the durations for which the Traffic Inspection Engine Status chart is available?

The **Traffic Inspection Engine Status** chart is available only for 3 hours, 1 day, 1 week, and 1 month.

When will I be able to view the traffic inspection details in the monitoring dashboard?

To view the traffic inspection details in the monitoring dashboard, you have to wait at least 15 minutes after the traffic flow is initiated.

What does the traffic inspection engine in the Gateway Details page convey?

In the **Gateway Details** page, the traffic inspection engine monitors the traffic between a set of one or more clients using a specific protocol.

How do I view the CPU usage of the traffic inspection engine?

The **Traffic Inspection Engine CPU Usage** chart in the **IDPS** tab displays the usage percentage of the traffic inspection engine's CPU for the selected period in a line chart. Hover over the graph to view the CPU usage percentage at a particular time. For more information, see [Traffic Inspection Engine CPU Usage](#).

How do I view the memory usage of the traffic inspection engine?

The **Traffic Inspection Engine Memory Usage** chart in the **IDPS** tab displays the usage percentage of the traffic inspection engine's memory for the selected period in a line chart. Hover over the graph to view the memory usage percentage at a particular time. For more information, see [Traffic Inspection Engine Memory Usage](#).

How do I view the number of packets dropped?

The **Dropped Packets** chart in the **IDPS** tab displays the number of dropped packets for the selected time period in a vertical bar chart. For more information, see [Dropped Packets](#).

SIEM

What are the prerequisites for configuring SIEM server?

Before you configure a SIEM server, you must have an active subscription with Splunk, a third party SIEM provider and obtain the server URL, an index, and the authentication token details.

How do I send threat data to the SIEM server?

To report threats to the SIEM server, in the **SIEM** tab, you must select the **Enable reporting of threats to SIEM systems** check box, and add the SIEM server details.

How do I stop sending the threat data to the SIEM server?

To stop reporting threats to the SIEM server, in the **SIEM** tab, you must deselect the **Enable reporting of threats to SIEM systems** check box.

How do I verify the connectivity to the SIEM server?

To verify the connectivity to the SIEM server, enter valid details to connect to the SIEM server and click **Test Connection**. For more information, see [Configure SIEM](#).

How do I edit the SIEM server details?

To edit the SIEM server details, see [Configure SIEM](#).

How do I delete the SIEM server details?

To delete the SIEM server details, see [Configure SIEM](#).

Troubleshooting

How do I capture packet information for troubleshooting?

To capture packet information for troubleshooting, select the **Enable packet capture** check box in the **General** tab. For more information, see [Troubleshooting Aruba IDPS](#).

How do I troubleshoot when Aruba IDPS engine drops data packets without generating alerts?

To troubleshoot when data packets are dropped without generating alerts, you need to connect to IDPS supported Branch Gateway through SSH and execute the debugging CLI commands. For more information, see [Troubleshoot Packet Drops](#).

How do I troubleshoot when Aruba IDPS engine generates threat alerts and drops data packets for normal traffic?

To troubleshoot when Aruba IDPS generates threat alerts and drops data packets for normal traffic, you must allow the threat signature for the traffic to flow. After allowing the threat signatures, contact Aruba Technical Support for further assistance. For more information, see [Troubleshoot Packet Drops](#).

When doing a file sharing (SMB), the traffic is slow?

If you experience slow SMB file transfers on 9xxx platforms that are IDPS enabled, you can prefer to skip the inspection for SMB traffic by enabling the **Bypass Inspection for Large Dataflows** option under the **Gateways IDS/IPS > Policies** tab. For more information, see [Manage Rules in Aruba IDPS Policies](#).

How do I capture the packets on the IDPS engine ports?

You can use the `idps extended packet capture` CLI.

How to identify if the session is redirected to the IDPS engine?

Use `show datapath session` CLI in the device to see if it has the Z flag for sessions redirected to the engine.

Can I extend the traffic inspection time?

Yes, you can extend inspection time by another 10 minutes by clicking the **Refresh Extended Packet Capture** button. For more information, see [Troubleshooting Aruba IDPS](#).

Threat events do not reach the Splunk server. What could be wrong?

Check the configured SIEM URL format. For more information, see [Configure SIEM](#).

Sometimes assigning or unassigning the Advanced with Security license does not enable or disable IDPS on the gateway. What is the solution?

Try unassigning and re-assigning as a workaround and it will resolve the issue.

Chapter 9

Threat Categories

This section lists the various threat categories and their descriptions in a table. This information helps you to understand and troubleshoot issues while monitoring and analyzing threats in your **Gateway IDS/IPS** dashboard.

Table 5: *Threat Categories*

Category	Description
Activex	Rules that detect attacks and vulnerabilities related to ActiveX.
Adware-PUP	Rules that are not explicitly malware, but might indicate software that is used for Ad tracking or other types of spyware related activity.
Attack Response	Responses that could indicate an intrusion. These rules are designed to detect the results of a successful attack. For example, error messages that indicate an intrusion.
Botcc (Bot Command and Control)	Rules autogenerated from several sources of known and confirmed active Botnet and other Command and Control hosts. The primary data source is shadowserver.org .
Botcc Portgrouped	Botcc rules that are grouped by destination port. Rules grouped by ports offer higher fidelity.
Chat	Rules to detect traffic related to numerous chat clients, Internet Relay Chat (IRC), and possible check-in activity.
CIArmy	IP rules generated by Collective Intelligence to block traffic.
Coinmining	Rules to detect activities related to coinmining such as coinmining for Bitcoin. Rules in this category mostly detect malware that perform coinmining.
Compromised	Rules to identify threats from a list of known compromised hosts that are confirmed and updated daily. This is a compilation of several private, but highly reliable data sources.
Current Events	Rules for active and short lived campaigns. This category covers exploit kits and malware that will be aged and removed quickly due to the short lived nature of the threat. These are rules that we don't intend to keep in the ruleset for long, or that need to be tested before they are considered for inclusion. For example, these rules contain simple signatures for Storm binary URL of the day signatures to detect CLSIDs of newly found vulnerable apps.
Decoder events	Rules to log normalization events related to decoding.
Deleted	Rules removed from the ruleset.
DNS	Rules to detect attacks and vulnerabilities related to DNS. This category includes abuse of the service for things such as tunneling.

Category	Description
DOS	Rules to detect Denial of Service (DOS) attempts, intended to detect inbound DOS activities, and outbound indications.
Drop	Rules to block spamhaus DROP (Don't Route or Peer) listed networks. This list is updated daily. For more information, see http://www.spamhaus.org .
Dshield	IP-based rules for Dshield Identified attackers. This list is updated on a daily basis. For more information, see http://www.dshield.org .
Exploit	Rules to detect direct exploits that are not covered in specific service category. For example, Windows exploit and Veritas are categorized as Exploit. While intrusions such as SQL injection are categorized as Exploits, they have their own category.
Exploit-Kit	Exploit Kit rules are used specifically to detect activity related to Exploit Kits, their infrastructure, and delivery.
FTP	Rules for attacks, exploits, and vulnerabilities related to FTP. This category includes basic non-malicious FTP activities such as login for logging purposes.
Games	Rules for identifying gaming traffic and attacks against those games.
HTTP Events	Rules to log HTTP protocol specific events.
Hunting	Rules that may match legitimate traffic or require intensive matching, but is useful for threat hunting because they provide indicators which are useful when matched with other rules.
ICMP	Rules for attacks and vulnerabilities related to ICMP. This category includes rules that detect basic activities of the protocol for logging purposes.
ICMP Info	Rules to log ICMP protocol specific events.
IMAP	Rules to identify attacks and vulnerabilities related to IMAP protocol. This category includes rules to detect basic activities of the protocol for logging purposes.
Inappropriate	Rules to identify pornography related activities.
JA3	Rules that support the mechanism to fingerprint malicious SSL certificates based on parameters that are in the SSL handshake negotiation by both clients JA3 and Servers JA3S. These signatures have a higher propensity for False Positives but are great for Threat Hunting or Malware Detonation Environments.
Malware	Rules for malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and anything that can be detected on the wire.
Mobile Malware	Rules specific to mobile platforms. This includes rules for malware and spyware related activities.
Netbios	Rules to identify attacks, exploits, and vulnerabilities related to Netbios. This category includes rules that detect basic activities of the protocol for logging purposes.
P2P	Rules to identify peer-to-peer traffic and attacks. These are not labeled as malicious, but might not be appropriate for all networks and environments.

Category	Description
Phishing	Rules that detect Credential Phishing activity including landing pages exhibiting credential phishing as well as successful submission of credentials into credential phishing sites.
Policy	Rules for applications like DropBox and Google Apps. This category covers off port protocols, basic DLP such as credit card numbers and social security numbers. Rules to block applications that are not allowed based on organizational policy.
POP3	Rules to identify, attacks, and vulnerabilities related to the POP3 protocol. This category includes rules to detect basic activities of the protocol for logging purposes.
RPC	Rules to detect attacks, vulnerabilities, and protocol related to RPC. This category includes rules to detect basic activities of the protocol for logging purposes.
SCADA	Rules for SCADA attacks, exploits, and vulnerabilities, and protocol detection.
SCADA_special	Rules for SCADA preprocessor based on Snort Digital Bond.
SCAN	Rules to detect reconnaissance and probing.
Shellcode	Rules for Remote Shellcode detection. Remote shellcode is used when an attacker wants to target a vulnerable process running on another machine on a local network or intranet. If successfully executed, the shellcode can provide the attacker access to the target machine across the network. Remote shellcodes normally use standard TCP/IP socket connections to allow the attacker access to the shell on the target machine. Such shellcodes can be categorized based on how the connection is set up. If the shellcode can establish the connection, it is called a "reverse shell" or a connect-back shellcode because the shellcode connects back to the attacker's machine.
SMTP	Rules for attacks, exploits, and vulnerabilities related to SMTP. This category includes rules to detect basic activities of the protocol for logging purposes.
SMTP events	Rules that log SMTP operations.
SNMP	Attacks, exploits, and vulnerabilities related to SNMP. This category includes rules to detect basic activities of the protocol for logging purposes.
SQL	Attacks, exploits, and vulnerabilities related to SQL. This category includes rules to detect basic activities of the protocol for logging purposes.
Stream events	Rules to identify intrusions through TCP stream engine events.
TELNET	Rules that detect attacks and vulnerabilities related to the TELNET service. This category includes rules to detect basic activities of the protocol for logging purposes.
TFTP	Rules that detect attacks and vulnerabilities related to the TFTP service. This category includes rules to detect basic activities of the protocol for logging purposes.
TLS events	Rules for identifying LS events and anomalies.
TOR	IP-based rules to identify traffic to and from Tor exit nodes.
Trojan	Malicious software that has clear criminal intent. Rules here detect malicious software that is in transit, active, infecting, attacking, updating, and anything that can be detected on the wire.
User Agents	User agent identification and detection.

Category	Description
VOIP	Rules that detect attacks and vulnerabilities related to VOIP environment. For example, intrusion using protocols such as SIP and RTP.
Web Client	Web-client-side attacks and vulnerabilities.
Web Server	Rules that detect attacks and vulnerabilities against web servers.
Web Specific Apps	Rules for specific web applications.
WORM	Traffic indicative of network-based worm activity.