TECHNCIAL BRIEF

ADVANCED THREAT DEFENSE WITH ARUBA SD-BRANCH

PROTECTING THE BRANCH FROM TODAY'S EVOLVING THREATS

KEY BENEFITS

Advanced Threat Defense provides:

- Granular firewall policies based on users and application roles
- Real-time monitoring of external threats across all your sites
- Classification of threats by application, user, and traffic direction
- Information on the source and impact of all threats
- Incident management and response based on business impact

INTRODUCTION

As Gartner and other analysts have noted, security is a top concern for enterprises implementing WAN and SD-WAN solutions: it's a critical requirement to ensure continued network operations for IT staff responsible for managing multiple, geographically distributed locations.[1] And as enterprises increasingly connect to the Internet from branch offices, the requirements expand to include inspections such as intrusion detection and prevention (IDS/IPS), anti-virus, and anti-malware built into the gateway.

Aruba provides fully integrated SD-WAN security by establishing and enforcing policies with a stateful, application-aware firewall, including deep packet inspection (DPI) combined with application classification and web content filtering. Aruba then takes this a step further by detecting and preventing outside threats, which is a key objective of securing distributed enterprises. A traffic inspection engine built into Aruba 9000-series gateways provides extensive intrusion and detection functionality, ensuring continued operations.

SECURITY WITHOUT COMPROMISE FOR SD-BRANCH

While keeping the performance and cost benefits of SD-WAN, Aruba's security functions are handled at the edge rather than backhauled to the data center or campus. Security can be divided into assurances for the integrity of either the LAN or the WAN. The LAN requires assurances for East-West traffic and the WAN needs security for traffic across sites, also known as North-South traffic.

The state of the art in SD-WAN gateways should include routing, SD-WAN overlay creation, security, deep packet inspection, and other functions that had historically been handled in separate appliances.

[1] Gartner has discussed this in a report entitled, Address Security and Digital Concerns to Maintain SD-WAN Growth.

The following table explains the tools for securing these networks.

Table 1: Functionality to secure LAN and WAN traffic.

Security Feature	Details
Stateful, Application-Aware Layer 4-7 Firewall	User and application awareness with full policy enforcement
Intrusion Prevention	Integrated intrusion prevention with configuration capabilities by type of asset targeted
Web Content Filtering	Provides the ability to create policies based on categories of sites
IP Reputation	Automatically restricts traffic from known malicious sources
Cloud Security Ecosystem	Secures Internet breakout traffic
Security Dashboards and Drilldown	Includes threat metrics by type, geography and gateway
Security Event Streaming	Streams threat events to key security monitoring tools such as Security Information and Event Management (SIEM) systems

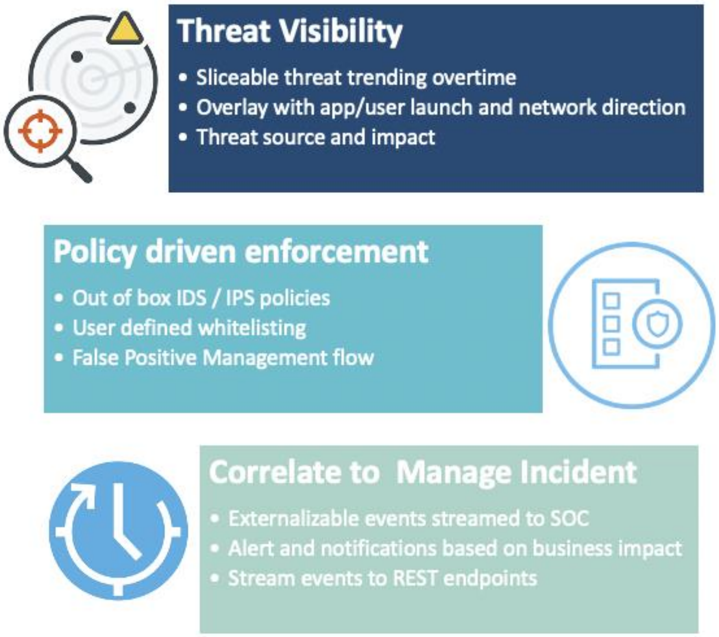
This table highlights the many different components that fall under the category of Unified Threat Management (UTM). UTM refers to a series of solutions combined into one appliance (in this case, the Aruba gateway). Aruba 70XX gateways support deep packet inspection (DPI), web content filtering, an application aware stateful firewall,[2] VPN overlays, and cloud security through integration with third party cloud security providers.[3]

With the 90XX gateways, the support is more comprehensive: there are many additional UTM features. These include IDS/IPS, security dashboards, and integration with SIEM systems. This functionality ensures security without compromise for SD-WAN and SD-Branch implementations.

Figure 1 shows high level business use cases supported by Aruba branch security.

[2] For more information, see the Unified Policy for the Distributed Enterprise technical document and the Policy Enforcement Firewall Technical Brief.

[3] See the Aruba Central online documentation for Zscaler integration.



Threat Visibility
• Sliceable threat trending overtime
• Overlay with app/user launch and network direction
• Threat source and impact
Policy driven enforcement
• Out of box IDS / IPS policies
• User defined whitelisting
• False Positive Management flow
Correlate to Manage Incident
• Externalizable events streamed to SOC
• Alert and notifications based on business impact
• Stream events to REST endpoints

Figure 1: Aruba Branch security business use cases.

Aruba's security features solve for these use cases in both East-West (LAN) and North-South (WAN) scenarios:

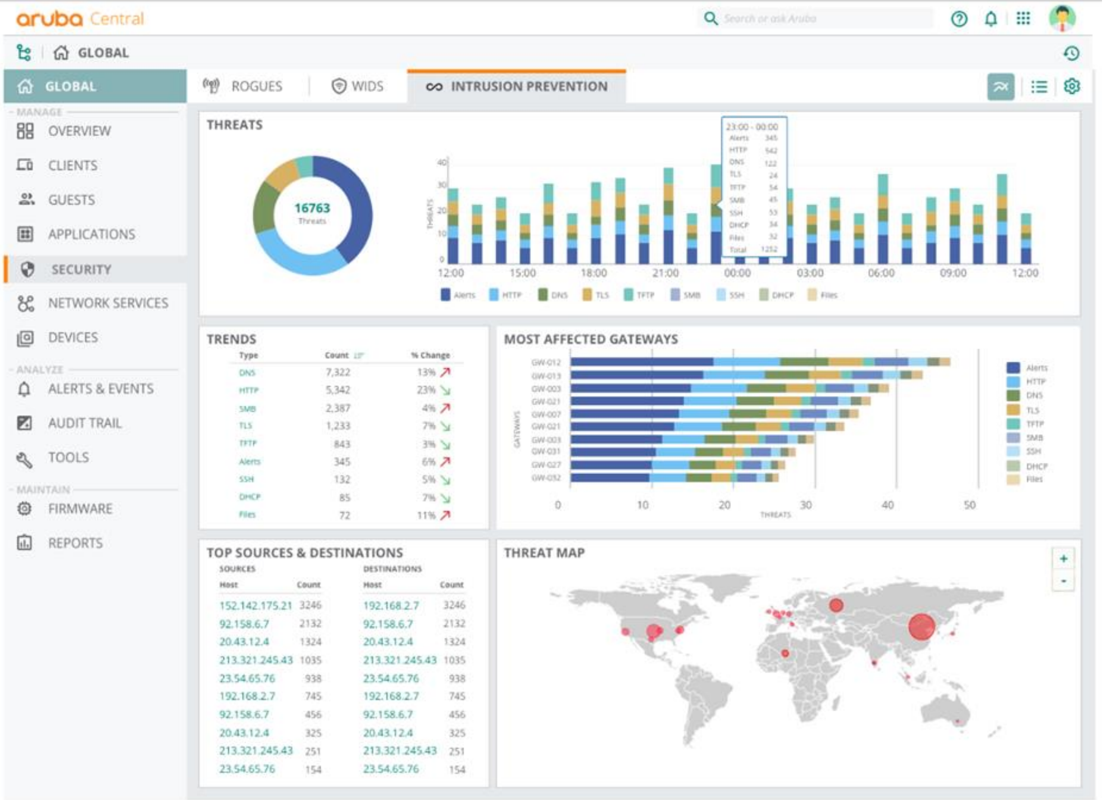
In the LAN, administrators get visibility into the lateral spread of threats across VLANs within branches through security dashboards. Actions are enforced using role-based ACLs and intrusion prevention policies. Subsequently, administrators can respond to the incident by quarantining using ClearPass, correlating with other security incidents, or taking action using third-party solutions such as SIEM (e.g., Splunk), ticketing systems (such as ServiceNow) and messaging systems (such as Slack or PagerDuty).

In the WAN, administrators gain visibility into external attacks by connecting to multiple external sites and services through security dashboards, an application visibility dashboard, a firewall session dashboard, and web reputation dashboard. Enforcement actions use application classification, content and URL filtering, next generation firewall rules, route-based ACLs with intrusion prevention policies and cloud security policies. As with the LAN scenario, administrators respond to the incident by correlating with other security incidents and taking action using third-party solutions such as SIEM (e.g., Splunk), ticketing systems (such as ServiceNow) and messaging systems (such as Slack or PagerDuty).

Operational ease-of-use and cost are contributing factors for choosing UTM for smaller sites. Depending on the applications, some enterprises may choose to deploy a cloud security solution. However, the cost and performance of connecting remote sites to a cloud security provider can be much higher than simply having a branch appliance manage the threats locally.

INTRUSION PREVENTION: ARUBA CENTRAL SECURITY DASHBOARD

Intrusion prevention functionality is accessed and managed under Security Management in Aruba Central (*Figure 2*).



23:00 - 00:00

Alerts	345
HTTP	542
DNS	122
TLS	24
TFTP	54
SMB	45
SSH	53
DHCP	34
Files	32
Total	1252

TRENDS

Type	Count	% Change
DNS	7,322	13% ↗
HTTP	5,342	23% ↘
SMB	2,387	4% ↗
TLS	1,233	7% ↘
TFTP	843	3% ↘
Alerts	345	6% ↗
SSH	132	5% ↘
DHCP	85	7% ↘
Files	72	11% ↗

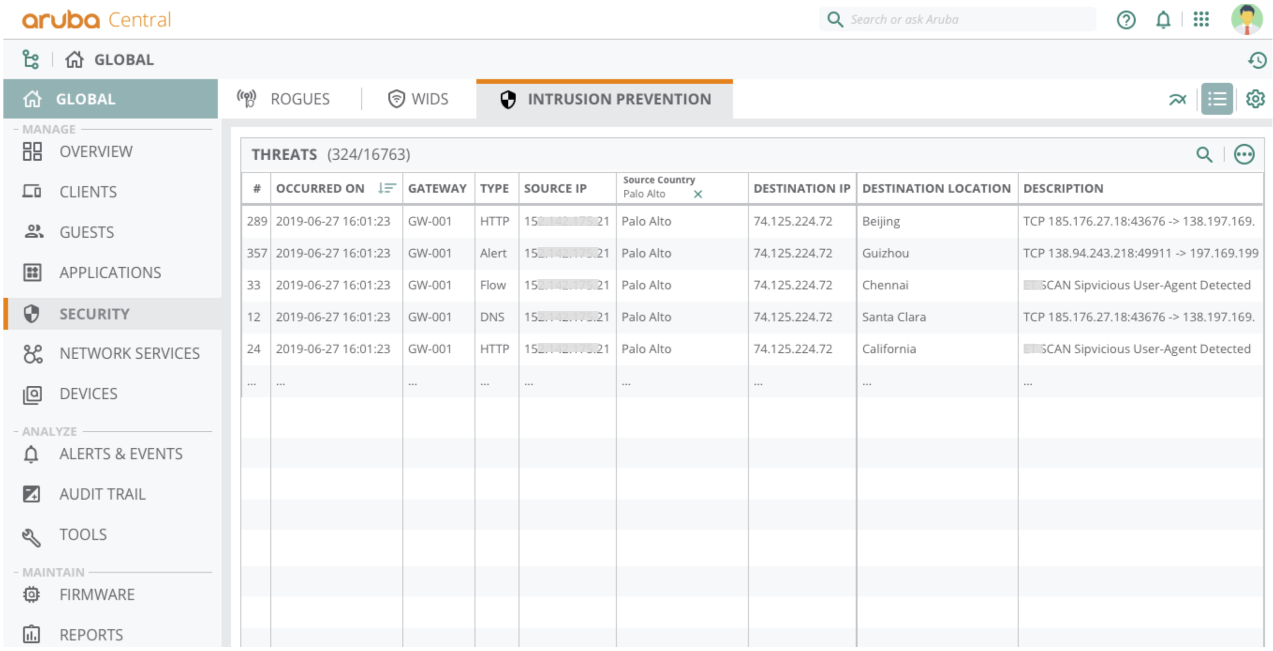
TOP SOURCES & DESTINATIONS

SOURCES		DESTINATIONS	
Host	Count	Host	Count
152.142.175.21	3246	192.168.2.7	3246
92.158.6.7	2132	92.158.6.7	2132
20.43.12.4	1324	20.43.12.4	1324
213.321.245.43	1035	213.321.245.43	1035
23.54.65.76	938	23.54.65.76	938
192.168.2.7	745	192.168.2.7	745
92.158.6.7	456	92.158.6.7	456
20.43.12.4	325	20.43.12.4	325
213.321.245.43	251	213.321.245.43	251
23.54.65.76	154	23.54.65.76	154

Figure 2: Intrusion prevention security dashboard under Aruba Central.

Perceived threats, including alerts, are collated and presented in the top tile. The threats are categorized according to how they enter the branch (for instance, through an HTTP or DNS request). From this dashboard, you can see threats over time, mapping user and application traffic to threats. You can also see trends for different types of threats.

The metrics used are by threat category, the type and severity of the threats, along with threat prevalence. You can also drill down to impacted users and devices and the source and level of the impact. *Figure 3* shows all the threats affecting one particular device.

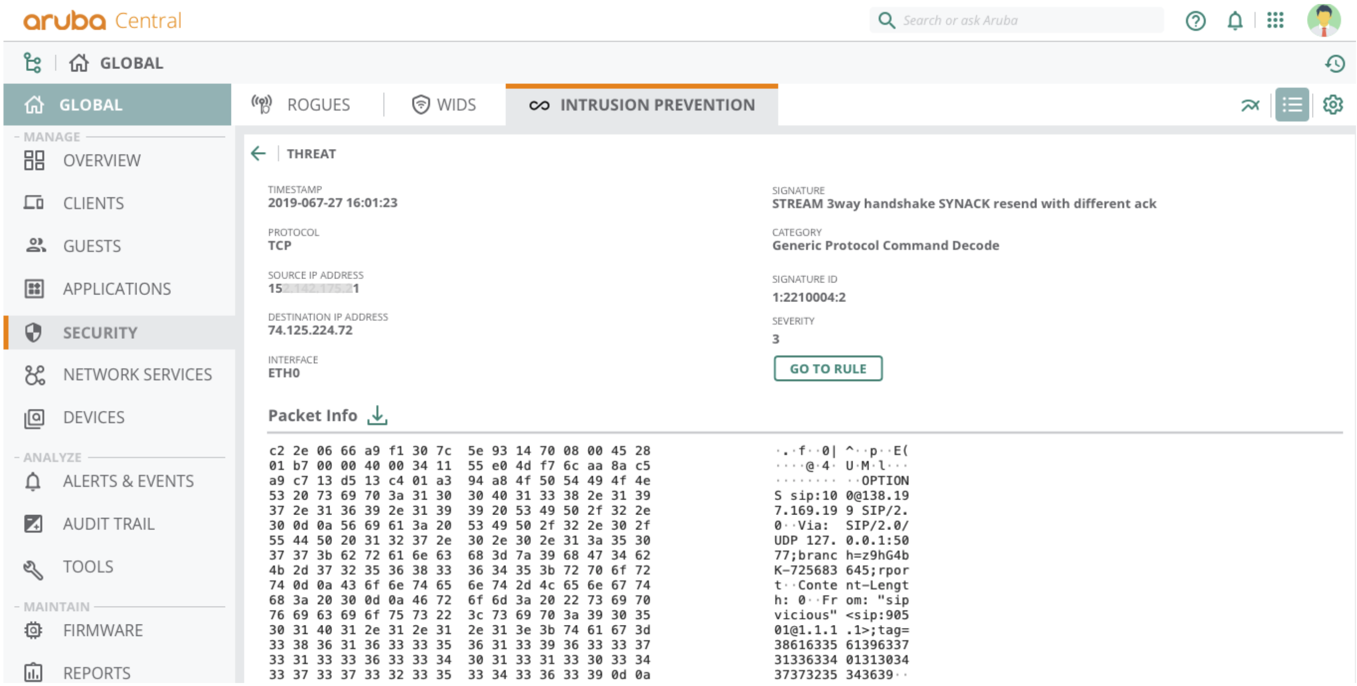


THREATS (324/16763)

#	OCCURRED ON	GATEWAY	TYPE	SOURCE IP	Source Country Palo Alto	DESTINATION IP	DESTINATION LOCATION	DESCRIPTION
289	2019-06-27 16:01:23	GW-001	HTTP	15[redacted]21	Palo Alto	74.125.224.72	Beijing	TCP 185.176.27.18:43676 -> 138.197.169.
357	2019-06-27 16:01:23	GW-001	Alert	15[redacted]21	Palo Alto	74.125.224.72	Guizhou	TCP 138.94.243.218:49911 -> 197.169.199
33	2019-06-27 16:01:23	GW-001	Flow	15[redacted]21	Palo Alto	74.125.224.72	Chennai	[redacted]SCAN Sipvicious User-Agent Detected
12	2019-06-27 16:01:23	GW-001	DNS	15[redacted]21	Palo Alto	74.125.224.72	Santa Clara	TCP 185.176.27.18:43676 -> 138.197.169.
24	2019-06-27 16:01:23	GW-001	HTTP	15[redacted]21	Palo Alto	74.125.224.72	California	[redacted]SCAN Sipvicious User-Agent Detected
...	...	...	...	...	...	...	...	...

Figure 3: Threat list for single device obtained by drilling down from dashboard.

In addition to the date, this table shows the gateway through which the threat entered the branch, along with the type of threat, its source, and a description. For any particular threat, you can drill down further to look at the details (*Figure 4*).



THREAT

TIMESTAMP
2019-067-27 16:01:23

PROTOCOL
TCP

SOURCE IP ADDRESS
15[redacted]1

DESTINATION IP ADDRESS
74.125.224.72

INTERFACE
ETH0

SIGNATURE
STREAM 3way handshake SYNACK resend with different ack

CATEGORY
Generic Protocol Command Decode

SIGNATURE ID
1:2210004:2

SEVERITY
3

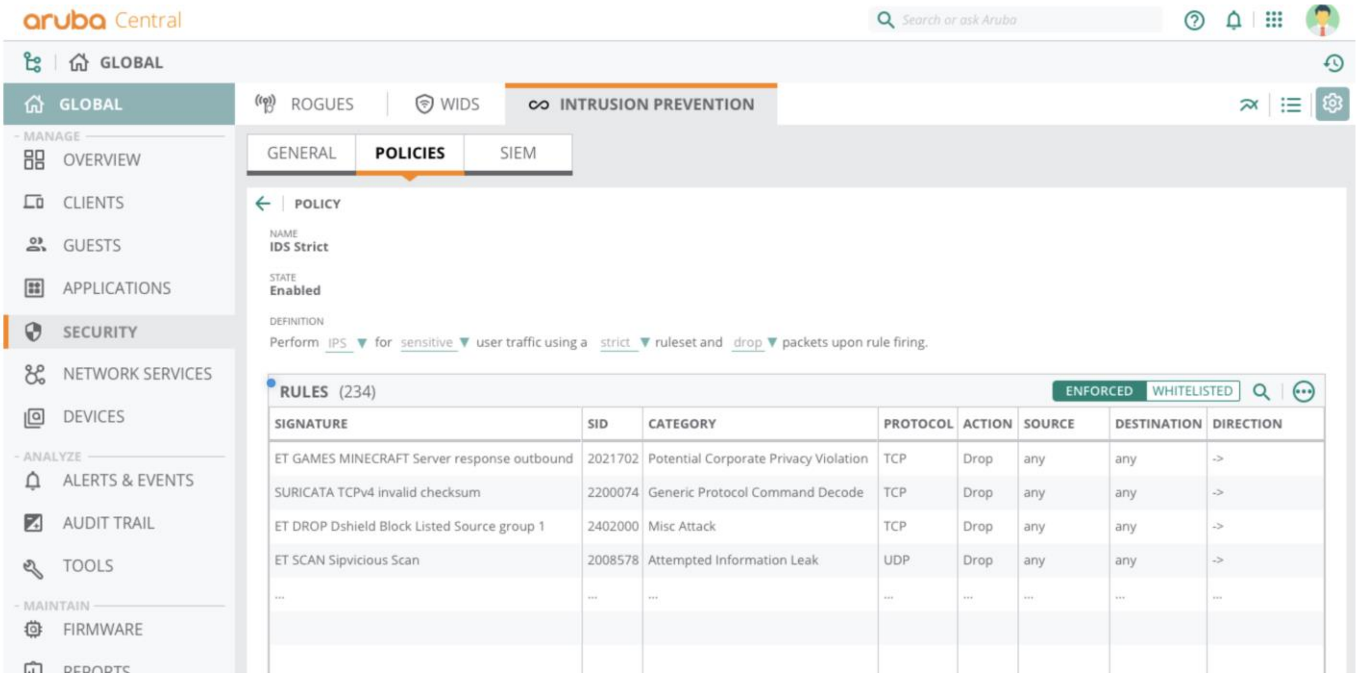
Packet Info

```
c2 2e 06 66 a9 f1 30 7c  5e 93 14 70 08 00 45 28    ·.·f··0| ^··p··E(
01 b7 00 00 40 00 34 11  55 e0 4d f7 6c aa 8a c5    ····@·4· U·M·l···
a9 c7 13 d5 13 c4 01 a3  94 a8 4f 50 54 49 4f 4e    ········ ··OPTION
53 20 73 69 70 3a 31 30  30 40 31 33 38 2e 31 39    S sip:10 0@138.19
37 2e 31 36 39 2e 31 39  39 20 53 49 50 2f 32 2e    7.169.19 9 SIP/2.
30 0d 0a 56 69 61 3a 20  53 49 50 2f 32 2e 30 2f    0··Via:  SIP/2.0/
55 44 50 20 31 32 37 2e  30 2e 30 2e 31 3a 35 30    UDP 127. 0.0.1:50
37 37 3b 62 72 61 6e 63  68 3d 7a 39 68 47 34 62    77;branc h=z9hG4b
4b 2d 37 32 35 36 38 33  36 34 35 3b 72 70 6f 72    K-725683 645;rpor
74 0d 0a 43 6f 6e 74 65  6e 74 2d 4c 65 6e 67 74    t··Conte nt-Lengt
68 3a 20 30 0d 0a 46 72  6f 6d 3a 20 22 73 69 70    h: 0··Fr om: "sip
76 69 63 69 6f 75 73 22  3c 73 69 70 3a 39 30 35    vicious" <sip:905
30 31 40 31 2e 31 2e 31  2e 31 3e 3b 74 61 67 3d    01@1.1.1 .1>;tag=
33 38 36 31 36 33 33 35  36 31 33 39 36 33 33 37    38616335 61396337
33 31 33 33 36 33 33 34  30 31 33 31 33 30 33 34    31336334 01313034
33 37 33 37 33 32 33 35  33 34 33 36 33 39 0d 0a    37373235 343639··
```

Figure 4: Threat details.

This view tells you the type of threat (Category) and provides the threat signature. Aruba's threat intelligence includes an extensive signature pack and rule set with tens of thousands of rules and dozens of categories. Furthermore, the rule set is always growing: submissions are received from all over the world covering previously unseen threats. The signature pack ensures optimum performance and accurate detection.

You can edit the policies based on the information you see on the Threat Details page (*Figure 5*).



NAME
IDS Strict

STATE
Enabled

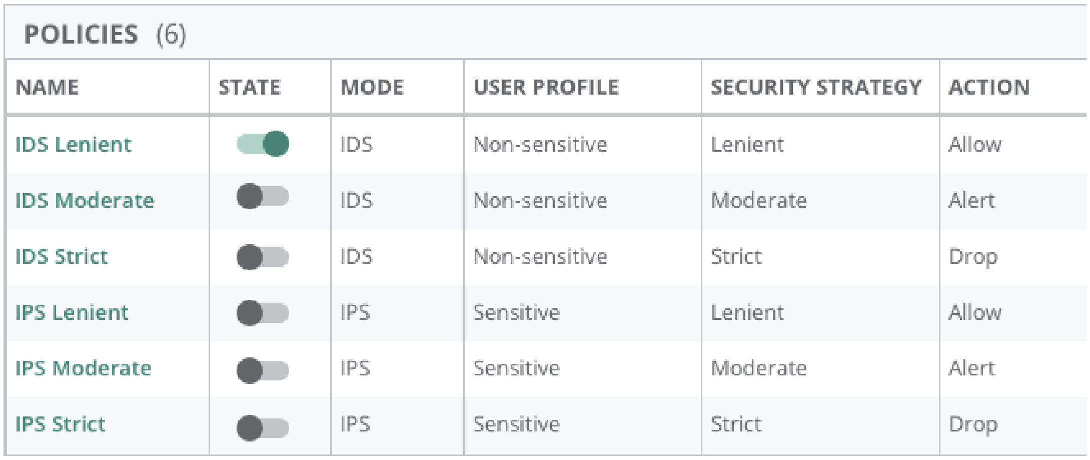
DEFINITION
Perform IPS ▼ for sensitive ▼ user traffic using a strict ▼ ruleset and drop ▼ packets upon rule firing.

RULES (234)

SIGNATURE	SID	CATEGORY	PROTOCOL	ACTION	SOURCE	DESTINATION	DIRECTION
ET GAMES MINECRAFT Server response outbound	2021702	Potential Corporate Privacy Violation	TCP	Drop	any	any	->
SURICATA TCPv4 invalid checksum	2200074	Generic Protocol Command Decode	TCP	Drop	any	any	->
ET DROP Dshield Block Listed Source group 1	2402000	Misc Attack	TCP	Drop	any	any	->
ET SCAN Sipvicious Scan	2008578	Attempted Information Leak	UDP	Drop	any	any	->
...	...	...	...	...	...	...	...

Figure 5: Edit policy rules for a set of threats.

There are built-in policies that define rules to drop or allow packets that match a specified threat signature. These are shown in *Figure 6*.



POLICIES (6)

NAME	STATE	MODE	USER PROFILE	SECURITY STRATEGY	ACTION
IDS Lenient	●	IDS	Non-sensitive	Lenient	Allow
IDS Moderate	○	IDS	Non-sensitive	Moderate	Alert
IDS Strict	○	IDS	Non-sensitive	Strict	Drop
IPS Lenient	○	IPS	Sensitive	Lenient	Allow
IPS Moderate	○	IPS	Sensitive	Moderate	Alert
IPS Strict	○	IPS	Sensitive	Strict	Drop

Figure 6: Built-in policies for threat management.

For both IDS and IPS, the security strategies may be lenient, moderate, or strict. These settings will allow, issue alerts, or drop traffic.

CONCLUSION

Aruba gateways provide a variety of mechanisms for securing the distributed enterprise. This functionality includes sophisticated threat management with intrusion detection and prevention, complete with policies to streamline the handling of these threats.

RESOURCES

The following resources are available for more information:

- Unified Policy For the Distributed Enterprise: Role-based policy and security across LAN and WAN
- Policy Enforcement Firewall Technical Brief: Functionality of the gateway's stateful firewall
- Aruba 360 Security Page: Aruba's integrated framework for visibility, control and AI-powered insights
- Aruba SD-WAN Home Page: Functionality and benefits of Aruba's SD-WAN solution
- Aruba SD-Branch Home Page: Functionality and benefits of Aruba's SD-Branch solution
- Aruba SD-WAN Datasheet: Includes ordering information for Aruba Virtual Gateways
- Software-Defined Branch for Dummies: Aruba SD-Branch Solution

aruba
a Hewlett Packard Enterprise company