Overview

HPE Aruba Networking Controller Subscription Licenses

(URL Filtering, IP Reputation, and Geolocation Filtering)

Product Overview

As an add on feature for HPE Aruba Networking's Mobility Controllers, the WebCC service bundle bolsters network security and complements the existing application visibility and role-based security for mobile enterprises already included with the Policy Enforcement Firewall (PEF) feature in the Mobility Controller.

The WebCC bundle includes URL Filtering IP reputation, geolocation filtering. This continuously updated data is used in the PEF enforcement actions and rate limiting based on policy.

Standard Features

Features and Benefits

- Deploys an automated algorithm to identify suspicious IPs
- Examines and correlates by the IP
- Applies built-in rules to test the IP
- Determines if and how long to restrict the IP
- Releases the restrictions on the IP but keeps it under watch

URL Filtering

The solution involves extracting the hostnames and URLs that users are browsing using the HPE Aruba Networking DPI engine. The URLs are then looked up in a locally cached database that contains commonly used and recently accessed web sites. If the user's site is not on the list, the Mobility Controller makes a request for the category, classification, and reputation of the web site from the threat intelligence engine that classifies and scores an average of 2500+ URLS per second.

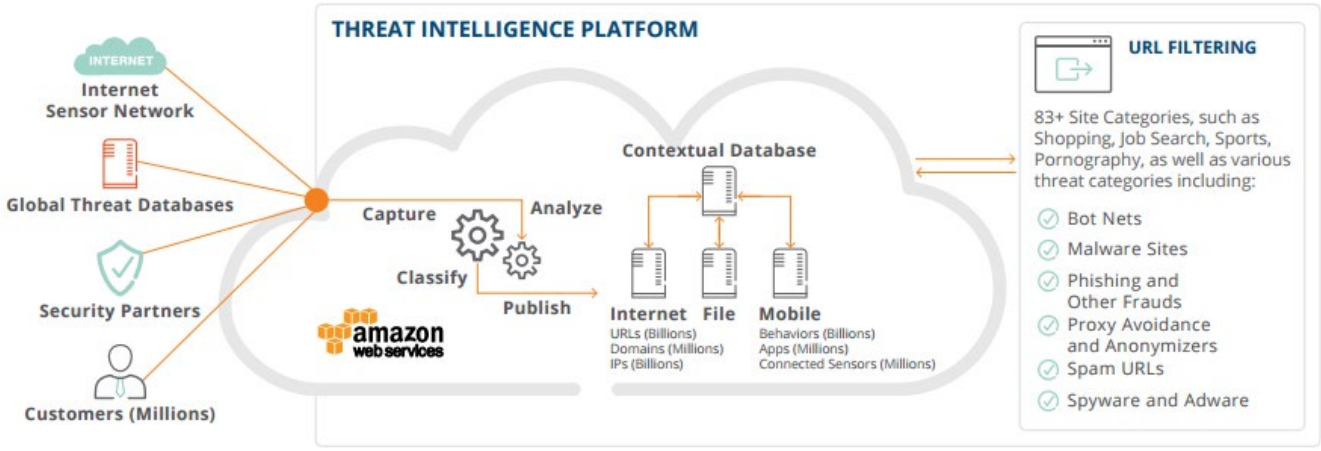


figure 1.0_071916_webcc-dsa

IP Reputation

The IP Reputation helps augment security posture by adding a dynamic IP reputation service to existing defenses. This service provides a real time feed of known malicious IP addresses broken down into 10 categories so IT security administrators can easily identify threats by type. These categories are Windows Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, Proxies, Reputation, Spam Sources, and Mobile Threats.

Security is increased with this service as the time required to identify new and existing IP threats is drastically reduced. Not only does the service decrease the time it takes to research IP addresses, but it also provides visibility into the types of threats, as well as historical and geolocation data to help security admins make better threat decisions.
The service uses a big data architecture to provide the most comprehensive and accurate threat intelligence available today, including up-to-the-minute intelligence on IPs of emerging threats. This includes a dynamic list of approximately 12 million dangerous IPs at any given time.

This intelligence can be used to block traffic from TOR nodes, proxies, botnets, and other malicious actors. In addition, customers can also access a rich set of meta data for investigative purposes. For example, proxies have been used for more than just obfuscation but also to launch short span DDoS attacks. Similarly, botnet command and control contain BOT IPs and the originating central server IP. This insight can help security administrators better understand incoming threats so they can take proactive measures.

Standard Features

The service analyzes and correlates data to create a predictive risk score, which falls into one of five rating bands ranging from trustworthy to malicious. The IP Reputation Index provides scores ranging from 1 to 100, with tiers split into Trustworthy, Low Risk, Moderate Risk, Suspicious, and High Risk (see chart below). Numerically lower scores (higher risk) indicate IPs that are more likely to be or become bad and are monitored at a greater frequency than trustworthy IPs.

The reputation tiers allow for enterprises to finely tune their security settings based on risk tolerance and business needs. For example, a highly security conscious bank may choose to block anything with a score lower than 80, while others may choose to accept traffic from IPs with scores higher than 60, as long as the site being accessed is affiliated with a partner.

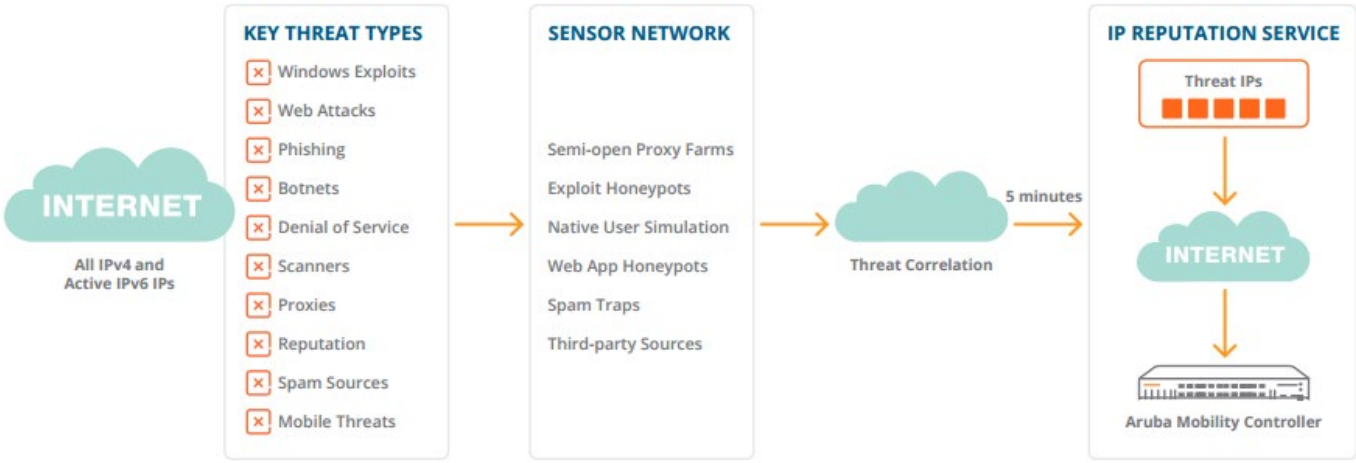


figure 2.0_071916_webcc-dso

Geolocation Filtering

The Geolocation filtering service allows an organization to associate source/destination IP addresses with location. PEF can be leveraged to apply policies to permit or drop inbound or outbound communications with certain known malicious countries.

Configuration Information

Ordering Information

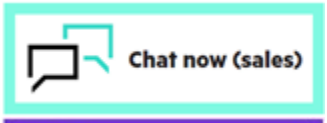
Description	SKU
HPE Aruba Networking Controller Web Content Classification 1-year Subscription E-STU	JY028AAE
HPE Aruba Networking Controller Web Content Classification 3-year Subscription E-STU	JY029AAE
HPE Aruba Networking Controller Web Content Classification 5-year Subscription E-STU	JY030AAE
HPE Aruba Networking Controller Web Content Classification 7-year Subscription E-STU	JY031AAE
HPE Aruba Networking Controller Web Content Classification 10-year Subscription E-STU	JY032AAE

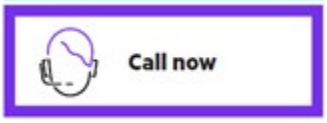
Summary of Changes

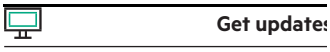
Date	Version History	Action	Description of Change
16-Dec-2024	Version 4	Changed	Summary of changes section was updated
22-Jan-2024	Version 3	Changed	Series name was updated.
23-Oct-2017	Version 2	Changed	HPE Aruba Networking information updated
01-Nov-2016	Version 1	Created	Document creation.

Copyright

Make the right purchase decision.
Contact our presales specialists.







Hewlett Packard Enterprise

To learn more, visit**: http://www.hpe.com/networking**

c05272742 - 15723 - Worldwide - V4 - 16-December-2024