DATA SHEET

WEB CONTENT CLASSIFICATION (WEBCC) BUNDLE

(URL Filtering, IP Reputation, and Geolocation Filtering)

Aruba's WebCC service bundle is a subscription-based license available for ArubaOS controller-managed networks and Aruba Central cloud-managed APs. WebCC complements the application visibility and user-role based access control included within Policy Enforcement Firewall (PEF) for Dynamic Segmentation.

The WebCC bundle includes URL filtering, IP reputation, and geo-location filtering. The web dictionaries are continuously updated to provide up-to-date policy enforcement and rate-limiting actions.

URL FILTERING

The solution involves extracting the hostnames and URLs that users are browsing using the Aruba 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 network 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.

FEATURES AND BENEFITS

- Enhances policy enforcement with an expanded library of definitions
- 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

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.

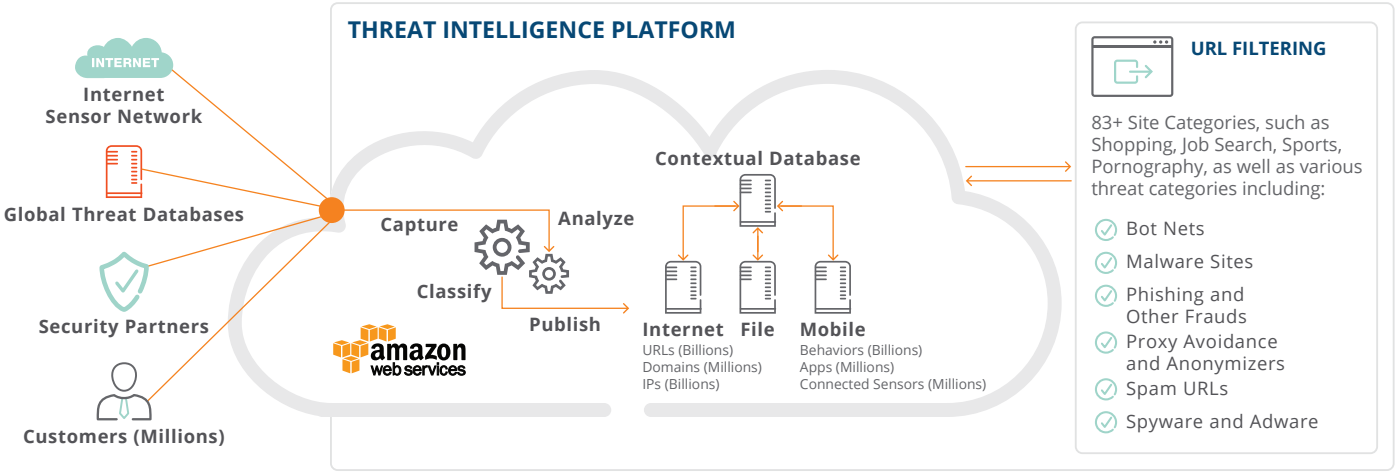

figure 1.0_071916_webcc-dsa

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, 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 contains BOT IPs and also the originating central server IP. This insight can help security administrators better understand incoming threats so they can take proactive measures.

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 allows 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.

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.

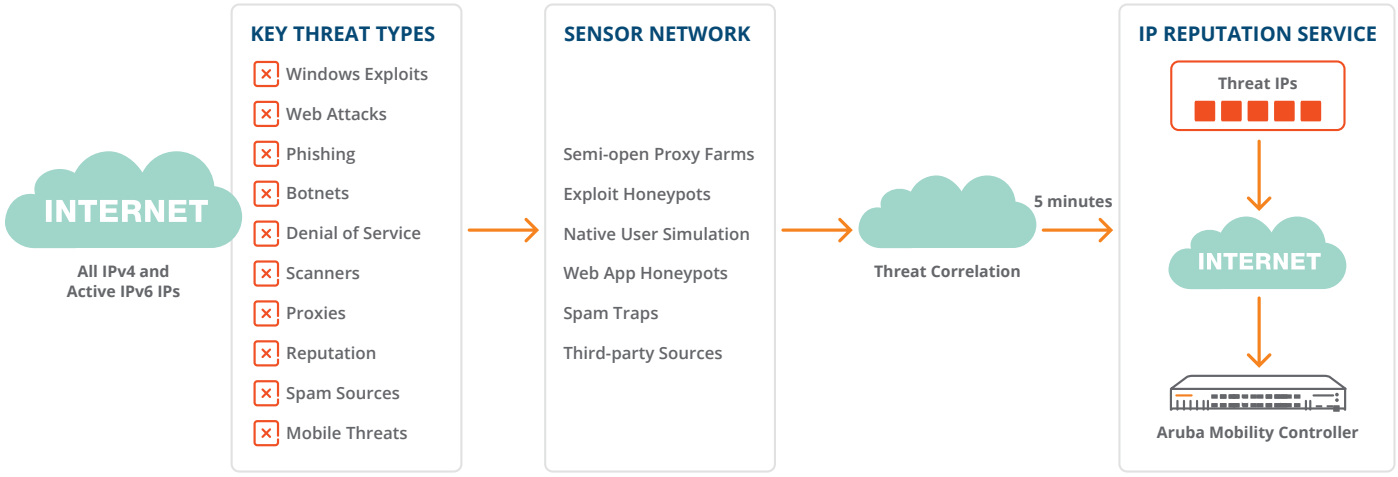

figure 2.0_071916_webcc-dsa

ORDERING INFORMATION*	
Part Number	**Description**
JY028AAE (SUB1-WebCC)	1 year subscription license for Aruba Mobility Controller WebCC Feature license per Access Point. The supported controllers include 70xx and 72xx running ArubaOS 6.5 and beyond including ArubaOS 8.x.
JY029AAE (SUB3-WebCC)	3 year subscription license for Aruba Mobility Controller WebCC Feature license per Access Point. The supported controllers include 70xx and 72xx running ArubaOS 6.5 and beyond including ArubaOS 8.x.
JY030AAE (SUB5-WebCC)	5 year subscription license for Aruba Mobility Controller WebCC Feature license per Access Point. The supported controllers include 70xx and 72xx running ArubaOS 6.5 and beyond including ArubaOS 8.x.
JY031AAE (SUB7-WebCC)	7 year subscription license for Aruba Mobility Controller WebCC Feature license per Access Point. The supported controllers include 70xx and 72xx running ArubaOS 6.5 and beyond including ArubaOS 8.x.
JY032AAE (SUB10-WebCC)	10 year subscription license for Aruba Mobility Controller WebCC Feature license per Access Point. The supported controllers include 70xx and 72xx ArubaOS 6.5 and beyond including ArubaOS 8.x.

DS_WebCC_SK_041520 a00073443enw