Security of the Arista Cloud

Introduction

Across enterprises and public sectors alike, migrating in-house data processing to the cloud has become an accepted strategy among IT departments. This often raises eyebrows within the security department because data security controls that were traditionally managed in-house now move into the hands of third parties. Cloud managed WiFi is no exception to this dogma. Hence, Arista has taken proactive steps to build a robust security program for the cloud that strengthens its WiFi access and security solution. The Arista cloud security program comprises multiple pillars as described throughout this paper.

Local data plane and cloud management plane

In the Arista cloud architecture, the wireless data plane (A) is kept local to the enterprise network, while the management plane lives in the cloud (B). Wireless data transacted through Arista access points (APs) does not flow to the Arista cloud; rather it is routed locally on the enterprise network based on the enterprise's routing controls. This also facilitates local enforcement of datasecurity controls such as content filtering and forensic logging. The authentication and authorization functions of the data plane are also kept local to the enterprise network.

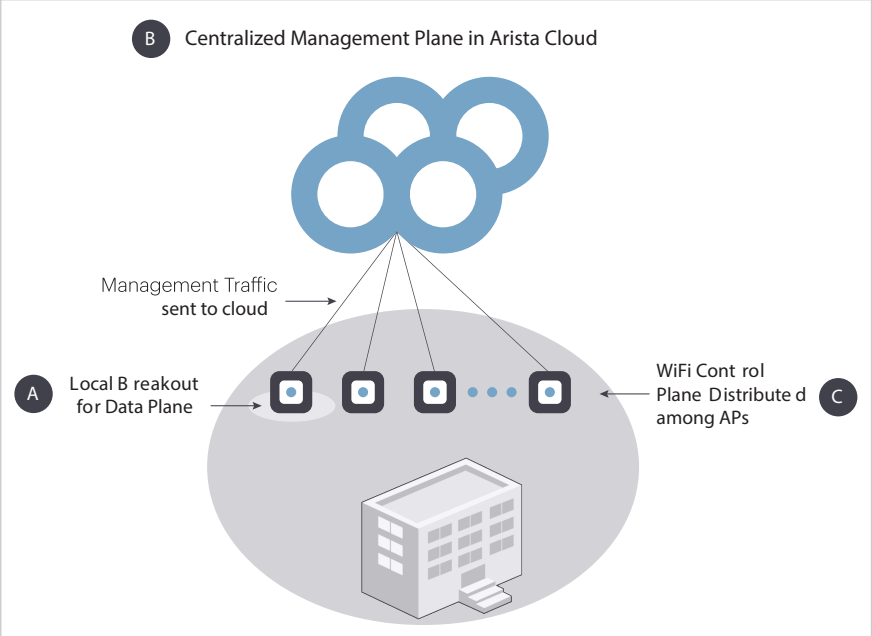

Figure 1: Arista Cloud WiFi Architecture

The management console used to configure and monitor the wireless network is provided from the Arista cloud. This console also provides security monitoring of the WiFi environment at the enterprise to detect and contain any undesirable activity in that air space. The control plane operates locally in the enterprise network among APs (C). This plane implements inter-AP messaging for handoffs, load balancing, RF optimization etc. and does not require constant input from the management plane past its initial configuration.

Data collected by cloud management plane

The cloud management plane collects and stores MAC and IP addresses of devices in the enterprise network that are seen by APs deployed within the network. It also collects metadata about devices such as their layer 2 wireless activity (probing, associations), OS, hostnames, applications usage, locations to the level of proximity to APs, and 802.1x login identities that are transmitted over the air in order to connect to the WiFi network.

It's important to note that employee passwords used for 802.1x authentication are not collected or stored in the cloud, as they are validated from the local enterprise RADIUS servers. 802.1x user passwords are also not readable by the APs as these are only passed between the client and the authentication servers.

For Guest WiFi, the cloud management plane also collects and stores identities of guest users used during WiFi authentication, to facilitate security audits of guest visitors. Enterprises can, if they wish, implement a Guest WiFi network with anonymous login as well.

AP-to-Cloud Communication

There are three security measures in place to ensure proper protection for AP-to-Cloud communication.

Mutual authentication: This occurs anytime an AP initiates a connection with the cloud. This is always an insideout request, and both the AP and cloud authenticate to one another in the process. This verifies the identity of both parties.

Per message authentication: This uses an HMAC SHA-1 authentication code for every message sent from an AP to the cloud. This ensures the integrity of the communication by confirming the message is sent by the correct entity and is not changed in transit.

AES encryption: This is used throughout AP-to-cloud communication. This ensures the messages remain confidential and cannot be intercepted.

Cloud environment in AWS data center

The Arista cloud is deployed as a virtual private cloud (VPC) in the Amazon Web Services (AWS) data center. In the VPC architecture, the Arista cloud environment is logically isolated from environments of other players that co-exist within the AWS data center. The physical and environmental security for the VPC is provided by AWS (1). Multiple subnets are provisioned inside the Arista VPC that host Arista application servers. Each subnet has a network ACL (Access Control List) to only allow certain protocols in and out of the subnet (2). The application server virtual machines are deployed as EC2 (Elastic Compute Cloud) instances and are connected to these subnets. Each EC2 instance that Arista deploys has a host based firewall that is configured to only allow protocols required for corresponding applications in and out of the server (3). The Arista applications that run on these EC2 virtual machines themselves are port hardened to ensure that unwarranted services and ports are not accessible on them (4).

The Arista cloud is deployed in AWS data centers located around the globe, and the footprint is rapidly growing as Arista acquires more global customers.

Vulnerability scanning

Arista regularly performs three types of vulnerability scans on the cloud hosted applications as follows.

Port scans: As compute instances are launched in different parts of the data center, it is essential to validate that the access to them is restricted to only those ports that are essential for accessing the application functionality. This reduces the attack surface considerably. Arista performs regular port scans on its cloud environment.

WAS (Web Application Security) scans: WAS scans focus on finding vulnerabilities at the web application level. Since the cloud application is accessible over HTTPS (port 443) and thus the Internet at large, the objective of a WAS scan is to ensure that

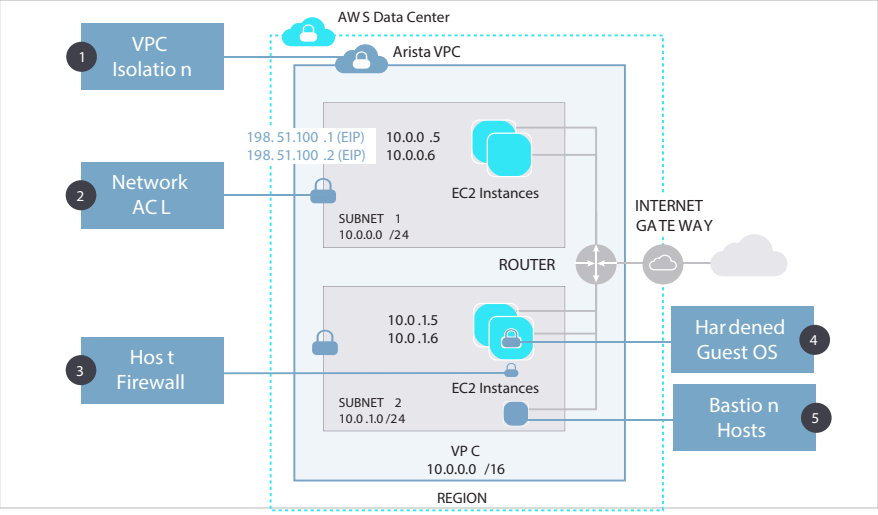

Figure 2: Arista VPC in Amazon Data Center

there are no exploitable vulnerabilities if an unauthorized user attempts to access the application. Another important objective is to prevent an authorized (authenticated) user from breaching application security controls, such as injection attacks, privilege levels, multi-tenancy, and so on. Arista deploys 24x7 automated WAS scanning using WhiteHat Security services and complements it with twice a year manual (deep) scans by WhiteHat Security experts.

Penetration Tests

Arista signs up third parties to perform penetration testing on the external facing interface of the cloud. Penetration tests are performed by security experts using multiple toolsets to try to find exploitable weaknesses in the system's workflow, configuration and implementation.

Software components scans

These scans are performed to audit software modules in the application for any missing security patches, stale versions, and misconfigurations. Arista performs software component scans on all its cloud applications at least once a quarter using the Nessus Enterprise tool.

Data encryption

Arista encrypts data in transit using AES. This includes management GUI (HTTPS) communication between the Arista AP and the cloud and all interactions between different Arista servers and applications in the cloud (HTTPS).

AES encryption is also applied to data at rest. Database backups of Arista applications in the cloud are stored in AWS S3 and Glacier that are also AES encrypted. The live database of Arista Wireless Manager, the flagship application that provides the wireless management console, resides in AWS EBS (Elastic Block Storage) and is also AES encrypted.

Access control

Arista personnel need to access cloud applications for the purposes of provisioning, maintenance and resolving trouble tickets. Arista implements access control mechanisms to limit Arista personnel access to customer accounts to a basic minimum. Privilege escalation for any task that requires higher level of access is subject to the

customer's permission and available for a temporary period of time. Employees who might work with such privileges must pass background screening first.

Maintenance access to EC2 server has to go through the bastion hosts. Login into the bastion hosts requires SSH and is allowed only from specific IP addresses. Bastion hosts implement strong access control and auditing functions to prevent unauthorized maintenance access.

All access interfaces to the cloud require two-factor authentication and enforce strong password policies.

Compliance certifications

Arista pursues security compliance certifications that include third party scrutiny (audit) and validation of the Arista cloud security controls geared towards confidentiality, integrity, and availability (the CIA triad).

WiFi Vendor SSAE SOC 2

Arista Networks has received SOC 2 Type 1 and Type 2 attestation for security, availability, and confidentiality of the Arista Cloud-managed WiFi solution. This establishes Arista as the first and only cloud WiFi vendor to achieve such attestation for practices in cloud-based WiFi management (SaaS).

Of course, the AWS data center (IaaS) where Arista applications are hosted are already SSAE 16 SOC 2 certified. The shared responsibility model for cloud security requires both IaaS security and SaaS security. In other words, data center SSAE certification by itself isn't adequate to guarantee comprehensive cloud security for the customers because it only covers IaaS practices such as physical security, environmental protection, and logical security (cybersecurity) up to the server boundary. There are a number of cloud operations that are handled by SaaS providers that are beyond the scope of SSAE certification of the data center itself such as vulnerability scans, change management, access control, disaster recovery preparedness, and change control management. The Arista Cloud-managed WiFi solution is certified for both Arista SaaS and AWS IaaS.

EU GDPR

Arista Networks provides General Data Protection Regulation (GDPR) compliant Arista Cloud WiFi to its partners, resellers, and customers in the European Union. The Arista Cloud acts as a GDPR Processor of personal data.

Arista SaaS and AWS IaaS

- ✓ Highest-level Cloud Security Certification
- ✓ AWS Data Center SSAE SOC 2
- ✓ Arista Vendor WiFi SSAE SOC 2

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062