aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

SECURING THE NEW WORLD OF WIRED CONNECTIVITY

Combine Aruba Switches and ClearPass Network Access Control for Optimized LAN Security and Network Efficiency

As the trend towards a more flexible, productive network topology continues to grow, the challenge is how to incorporate the strong security and control that a mobile-first architecture requires to cover both wired and wireless connectivity. How does the networking and security team define one policy and set of controls that follows the user or device whenever and wherever they connect?

In addition, organizations are now faced with an onslaught of headless devices and "things" connecting to the general IT infrastructure—many of whom are wired and all of which can be the starting point for a comprehensive attack on critical IT resources.

As a key element in the Aruba Mobile First Architecture, Aruba networking products have always featured strong embedded security, from device hardening to military grade encryption to embedded firewalls. And while ClearPass has always delivered outstanding visibility and protection for any network environment, it is especially optimized for Aruba networks.

Whether you are starting with Aruba switches to upgrade wired connectivity, or adding them to existing Aruba wireless networks, ClearPass secure network access control leverages these built-in security functions to provide the visibility, authentication, single point of control and proactive attack response that today's targeted, highly lethal attacks require.

ClearPass + Aruba Switches: Together Delivering Maximum Protection

Individually, ClearPass and Aruba switches provide extensive security capabilities. By adding ClearPass to Aruba wired infrastructure, the protection dramatically expands.

- **Comprehensive Discovery and Profiling.** Understanding which devices are connecting to the network and what their capabilities are is critical to building a secure network policy. This includes both Windows, macOS and most Linux distributions as well as printers, media players, building controls, sensors and other headless devices do not support any interactive authentication methods.
- **Range of Authentication Options.** Often times "enabling AAA on the switch" is equated with 802.1X, but that is not always the case. Wired AAA can mean 802.1X, MAC Authentication, web authentication or any combination depending on the switch's capabilities. That said, 802.1X, which is as straightforward to implement with Aruba switches as is it for wireless access, is the gold standard for secure port-based access control and is deployed by many Aruba customers. That framework offers the best possible mix of flexibility, security, user and device identification and dynamic policy changes based on changes in user or device status.
- **Precision Role-based Control.** Downloadable user roles (available on Aruba Mobility Controllers, Aruba Mobility Access Switches and ArubaOS-Switches) enable ClearPass to act as a centralized policy and enforcement definition point, up to and including application-level access control. Once the role and the privileges are defined, they follow the user or device across wired and wireless access. If conditions change (such as the user switches to an unknown device, or is on an unsecured network), the policy will automatically change to reduce access and privilege. This delivers an intelligent edge with greater flexibility and dynamic security, independent of the type of access.
- **One Network, One Policy, Total Protection.** For the highest level of security, visibility and control, Aruba switches and Aruba Wireless Mobility Controllers can be used together to offer stateful firewall processing, application visibility and bandwidth restrictions, and centralized policy enforcement using the Tunneled-Node capability. Tunneled-Node leverages the same user roles and policies defined for a wireless deployment, including the same client access VLANs. For example: if the guest/open SSID uses a specific guest VLAN on the controller, that same VLAN can be used for wired guests via Tunneled-Node.

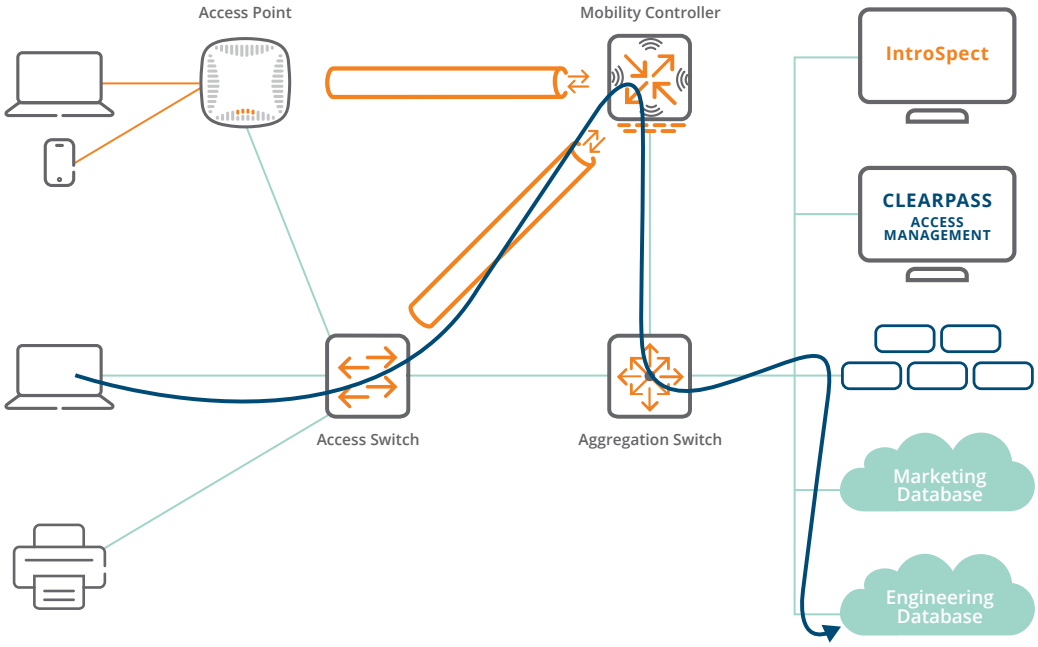


Figure 1: Tunnel-node

All firewall policies, bandwidth contracts and other traffic restrictions are enforced by the mobility controller. Here are some sample use cases:

- Branch scenarios where all wired and wireless traffic is processed by a Mobility Controller
- Regulatory or high-risk environments where all wired traffic must traverse a firewall
- Areas with high numbers of headless/IoT devices like building infrastructure head-ends or maintenance facilities
- Temporarily providing access during an event using an unmanaged switch

Switch-based Advanced Threat Detection. By virtue of ClearPass' position as gatekeeper to the network, its rich policy engine can be used to respond to attacks for users and devices already on the network. For example, all Aruba switches take advantage of complete traffic visibility to profile user and device activity and flag anomalies that are often indicative of an attack in progress. This includes:

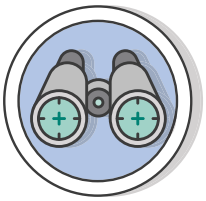
- MAC Spoofing
- IP Spoofing
- Rogue DHCP Server
- IP subnet sweep
- Server port scan
- IPv6 Spoofing
- Rogue DHCPv6 server
- ARP Poisoning

These alerts can be delivered to ClearPass (or any other security product, such as SIEM) where policy-based actions ranging from re-authentication to bandwidth control to quarantine to outright block can be executed to protect the organization.

This attack response mission for ClearPass applies to any source of an attack alert, including Aruba's IntroSpect behavioral analytics-based attack detection solution and for many of the over 120 third party technology partners in the Aruba 360 Security Exchange program.

Integrated TACACS+ Support. Every attacker tries to compromise the infrastructure as a path to extracting critical business or personal information. That is why ClearPass includes TACACS+ support to ensure that switch administration is monitored and secured.

BENEFITS OF USING CLEARPASS TO PROTECT ARUBA WIRED NETWORK



VISIBILITY

- As devices and users connect in an "anywhere, anytime, anyplace" environment, knowing what's on the network is the first step towards greater security.
- User and/or device identification is the key to effective access control policies that comprehend properties such as organizational structure, owner, time of day, location, etc.
- Device profile information is also important for detecting unauthorized access to the network. If a user were to change the MAC address of their laptop to match a previously authenticated device, like a printer, for example, ClearPass will detect a profile change and trigger a conflict state.

PROTECTION

- The ClearPass policy manager provides precision control over who and under what circumstances users and device can access IT resources. Contextual information from the network and infrastructure can be evaluated to help make a dynamic access decision—including individual application access. Some examples of contextual data sources include the user identity store, enterprise mobility management solutions, endpoint security solutions, asset management tools, etc.
- Integrated TACACS+ support ensures that switches will remain in their desired state and that all administration is performed with strict controls.
- Aruba switches now signal security issues directly to the ClearPass policy engine for rapid attack containment.

EFFICIENCY

- One Policy, One Network. Because roles and policies follow users and devices, the networking and IT teams do not have to adjust access control based on type of access.
- Closed-loop Attack Response. With the Aruba switches and ClearPass working together to detect and respond to attacks, pre-determined actions can be defined in user and device roles and policies to save crucial seconds in dealing with a propagating exploit.
- Better Port Utilization. Because control and policy enforcement is delivered via the role and not the port definition, networking teams can avoid the high-overhead task of assigning specific ports for specific purposes. Port utilization is significantly improved while maintaining the appropriate level of security.

SUMMARY

No matter what the network architecture, switches are still a critical component and with the flood of IoT devices attaching via switches to the network, that trend will continue. If you are using Aruba switches, add ClearPass secure network access control to realize maximum protection as well as significant operational efficiencies.

SB_ClearPassWiredConnectivity_011519