BUSINESS PAPER

aruba
a Hewlett Packard Enterprise company

Implementing Zero Trust Architecture and Comply-to-Connect Best Practices

How Aruba Built-in Network Security Protects Government Networks

TABLE OF CONTENTS

OVERVIEW

The US Government has recognized that network security challenges have significantly increased as users have become more decentralized, new IoT devices have flooded the network and attacks have become more sophisticated and persistent. Traditional security approaches that focused primarily on the perimeter of the network have become ineffective as a primary security strategy. Modern network security must accommodate an ever-changing, diverse set of users and devices, as well as much more potent threats targeting previously "trusted" parts of the network infrastructure.

To address this issue, two major network security initiatives were launched to help guide agencies in planning, designing and implementing more secure networks in support of their overall IT protection strategy. In the 2014 Federal Information Systems Management Act (FISMA), NIST was impaneled to develop a set of overall security guidelines and architecture that has evolved to a Zero Trust Architecture. In 2017, the Defense Authorization Act for Fiscal 2017 authorized the planning for "Comply-to-Connect" that focuses on endpoint conformance with security configuration standards as a condition of network access.

ZERO TRUST ARCHITECTURE AND COMPLY-TO-CONNECT—COMPLEMENTARY PROTECTION

One of the foundational principles of a Zero Trust Architecture is that access to IT resources should not be dictated solely by where or how a client connects. In other words, the network is inherently untrustworthy and an "overlay" security fabric must be added based on a well-defined, identity-based architecture that segments traffic to those paths and resources that have been explicitly permitted. In addition, a Zero Trust Architecture can manage the security "lifecycle" of an endpoint from authentication and authorization to continuous monitoring and attack response.

Comply-to-Connect starts with a focus on the security posture of the endpoint at time of IT access. The objective is to authenticate the client and then continuously compare its configuration and status to a defined set of acceptable security states to ensure that it will not introduce vulnerabilities.

Both frameworks address 5 key security challenges:

1. Eliminate network blind spots. Many IoT devices connect to the network outside the purview of the network and security team. The goal is to discover and profile all devices connected to the network.
2. Verify identity before allowing access. Starting with 802.1X there are a number of authentication techniques to ensure that only legitimate users and devices connect to the network.
3. Compare endpoint configuration to compliance baselines and remediate as needed. This is a crucial Connect-to-Comply step and it allows the security team to define and enforce configuration guidelines that reflect the application of the appropriate patches and updates.
4. Establish least privilege access to IT resources by segmenting traffic based on identity-based policies. Once identity and configuration compliance is confirmed, the user or device can be assigned a set of IT privileges dictated by pre-defined access policies that are enforced in the network infrastructure.
5. Continuously monitor the security state of the user and device and bi-directionally communicate with other elements in the security ecosystem. Once a user or device is connected to the network, if there are signs that it has been compromised or is participating in an attack, its access rights must be reduced or eliminated until the problem has been remediated.

From AI-powered analytics to built-in security controls, Aruba Networks IT solutions, anchored by the ClearPass family of access control solutions, provides the products and technologies needed to satisfy each of these requirements.

OVERVIEW OF ARUBA'S EDGE SERVICES PLATFORM ZERO TRUST ARCHITECTURE AND COMPLY-TO-CONNECT SOLUTIONS

The Aruba Edge Services Platform (ESP) supports Comply-to-Connect and Zero Trust Architecture by delivering device discovery, authentication, configuration enforcement, role-based access control, built-in policy based traffic segmentation and continuous threat protection, all from a single solution comprising:

Aruba Central Client Insights: Security and networking teams are constantly on the lookout for devices that are connected to the network outside the proper controls. CPDI uses a full range of passive and active discovery techniques along with AI fingerprinting to ensure that every device is located and profiled.

ClearPass Policy Manager: CPPM performs a wide range of Zero Trust Architecture and Comply-to-Connect functions. It starts with a range of authentication services to identify users and devices and based on that identity, CPPM will assign a set of access permissions that are enforced by the Aruba network.

Policy Enforcement Firewall/Dynamic Segmentation: PEF is a stateful, Layer 7 firewall that can be enabled on Aruba wireless access points, gateways, and controllers. PEF is the companion enforcement point for ClearPass policies and enforces policy-based per-user and per-device traffic segmentation for wired, wireless and WAN connectivity.

ClearPass OnGuard: The OnGuard performs advanced endpoint posture assessment and remediation to ensure security and compliance requirements are met prior to users and devices connecting to the network.

Aruba 360 Security Exchange: ClearPass Policy Manager is bi-directionally integrated with over 150 third party security and management products to provide identity-based information to the ecosystem and receive, threat and attack information to inform policy decisions.

The Pentagon Modernizes Wired and Wireless Connectivity, Across All Classification Levels, with Aruba Infrastructure

The Pentagon, headquarters of the United States Department of Defense (DoD), is modernizing its classified and unclassified networks to support tens of thousands of devices daily. Aruba's ESP-based architecture will provide the Pentagon an automated networking infrastructure that eliminates manual processes, like port mapping and initial switch configuration. It is also expanding its deployment of Aruba ClearPass Policy Manager, for secure network access control across its networks

KNOW WHAT'S ON YOUR NETWORK. DEVICE DISCOVERY AND PROFILING WITH CLEARPASS DEVICE INSIGHT

ClearPass Device Insight addresses the most stringent visibility requirements for the most diverse network environments. This includes the ability to broadly and accurately identify all wireless and wired devices connected to the network - from traditional IT managed devices to previously undetected IoT devices such as cameras, medical equipment, sensors and other hard to detect endpoints. ClearPass Device Insight utilizes a unique set of both active (NMAP, WMI, SNMP, SSH) and passive discovery methods (SPAN, DHCP, NetFlow/S-flow/IPFIX) in order to find and classify a wide range of device types. These capabilities are further enhanced through the use of deep packet inspection which provides additional context and behavioral information that can further identify difficult-to-detect devices connected to the network.

ClearPass Device Insight analyzes device attributes including communication and behavior patterns to dynamically build clusters of similar devices. Machine learning is used to constantly evaluate these attributes to dynamically update fingerprints and provide fingerprint recommendations.

ClearPass Device Insight also supports the critical Comply-to-Connect compliance requirement by providing device risk scoring that is calculated based on a comprehensive set of device security attributes. These attributes include potential vulnerabilities and related CVE scoring, as well as detailed information related to what security controls are enabled on each device, such as a host firewall.

Finally, in support of tight traffic segmentation, ClearPass Device Insight integrates with ClearPass Policy Manager for closed loop, end-to-end access control from visibility to automated enforcement. Devices that are discovered through ClearPass Device Insight can automatically be assigned access privileges based on a given policy or even quarantined in the event they are out of configuration compliance or behaving in a malicious or insecure manner.

KNOW WHO IS CONNECTING. AUTHENTICATION WITH CLEARPASS POLICY MANAGER

Once a user or device is known and profiled, the next step is to authenticate its identity each time it connects to the network. With ClearPass, organizations can deploy wired or wirelessly using standards-based 802.1X enforcement for secure authentication. ClearPass also supports MAC address authentication for IoT and headless devices that may lack support for 802.1X. For wired environments where RADIUS based authentication cannot be deployed, ClearPass offers an alternative using SNMP based enforcement.

Multiple authentication methods can be used to concurrently support a variety of use-cases including support for multifactor authentication based on log-in times, posture checks, and other context such as new user, new device, and more. Attributes from multiple identity stores such as Microsoft Active Directory, an LDAP-compliant directory, ODBC-compliant SQL databases, token servers and internal databases across domains can be used within a single policy for fine-grained control.

ClearPass Guest simplifies visitor workflow processes to enable employees, receptionists, and other non-IT staff to create temporary guest accounts for secure wireless and wired access. Highly customizable, mobile friendly portals provide easy-to-use login processes that include self-registration, sponsor approval, and bulk credential creation. Credentials can be delivered by SMS, email, printed badges, or input directly through cloud identity providers such as Facebook or Twitter

ENFORCE CONFIGURATION COMPLIANCE. ENDPOINT POSTURE AND REMEDIATION WITH CLEARPASS ONGUARD

Configuration compliance and security posture assessment is at the heart of Comply-to-Connect and in addition to the risk scoring provided by ClearPass Device Insight, ClearPass OnGuard provides the detailed and ongoing compliance checks and remediation that Comply-to-Connect requires.

Based on this, during the authorization process it is necessary to perform health assessments on specific devices to ensure that they adhere to IT-defined configuration standards including patch levels, anti-virus, anti-spyware and firewall policies. Devices not meeting compliance can either be automatically remediated with a persistent agent or redirected to a captive portal for further follow-up. ClearPass OnGuard features built-in capabilities that perform posture-based health checks to eliminate vulnerabilities across a wide range of computer operating systems. Whether agentless, or using persistent or dissolvable clients, ClearPass OnGuard can centrally identify compliant endpoints on wireless, wired and VPN infrastructures.

Examples of advanced health checks that provide extra security:

- Handling of peer-to-peer applications, services, and registry keys
- Determination of whether USB storage devices or virtual machine instances are allowed
- Managing the use of bridged network interfaces and disk encryption

LEVERAGE IDENTITY TO ENFORCE ACCESS PRIVILEGES. DYNAMIC SEGMENTATION OF NETWORK TRAFFIC WITH ARUBA POLICY ENFORCEMENT FIREWALL

At the heart of the NIST Zero Trust Architecture is a collaboration of two key components:

- A Policy Engine/Administrator that defines the conditions under which a user or device can connect to the network and what access privileges they are entitled to, based on the authentication and compliance process they must go through.
- A Policy Enforcement Point that interprets and enforces the access instructions delivered by the Policy Engine.

This kind of control cannot be added in after the fact to a network that has not considered how to manage and enforce identity-based access. For twenty years Aruba has built-in the support for Dynamic Segmentation, which provides the enforcement for identity-based access control across wired, wireless and WAN connectivity. Aruba Dynamic Segmentation maps to the NIST Zero Trust Architecture framework as follows:

- ClearPass Policy Manager is the Policy Engine/ Administrator
- The Aruba Policy Enforcement Firewall (PEF) is the policy enforcement point and can run on Aruba wireless access points and gateways. For switches, Aruba's Colorless Port functionality means that network teams no longer have to statically pre-configure access ports to vlans. Switched access ports can automatically apply a role/policy required to support the connected device in real-time.

As the name implies, Dynamic Segmentation delivers two main benefits:

- **Dynamic:** Points to Aruba's ability to assign policy (roles) on the fly to a wired port or wireless connection based on such things as access method of a client. When incorporated with ClearPass, additional context is available such as time-of-day, type-of-machine, etc. IT staff's no longer have to pre-configure access-ports to vlan and uplinks or wireless access privileges.
- **Segmentation:** Brings focus to the ability to segment client traffic based on the permissions included in the ClearPass access policy. This provides enhanced security and performance benefits, all based on better visibility.

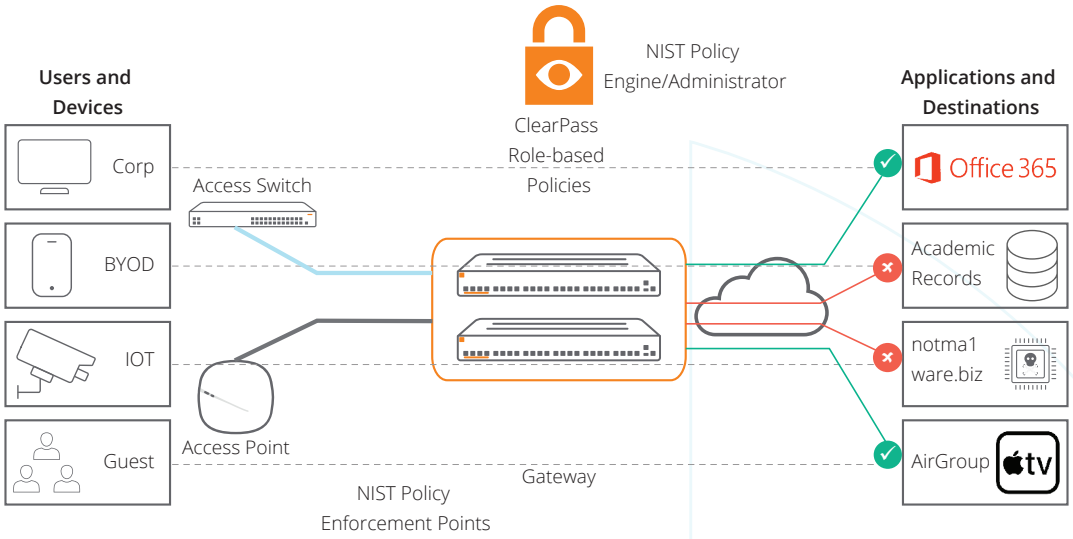

Figure 1: Trust enforced by dynamic segmentation

When VLAN's are Not Enough. Using EVPN-VXLAN to Extend Network Segmentation on a Global Scale

The proliferation of endpoints due to BYOD, workplace mobility, and IoT is driving a need for more fine-grained segmentation strategies to separate different profiles of users, devices, and traffic on global basis—beyond what traditional VLANs can offer. The Aruba CX family of network switches has expanded configuration and policy enforcement choices to include industry standards such as EVPN-VXLAN for more flexibility, global scale and third party interoperability. EVPN-VXLAN enables businesses to connect geographically dispersed locations using layer 2 virtual bridging and has emerged as a popular networking framework largely due to the limitations of traditional VLAN-based networks. VXLAN encapsulates layer 2 Ethernet frames in layer 3 UDP packets, meaning virtual layer 2 subnets can span underlying layer 3 networks and extend Dynamic Segmentation across physical locations.

DEEP INTEGRATION WITH SECURITY ECOSYSTEM. BI-DIRECTIONAL COMMUNICATION AND STATUS CHECKING

As is emphasized in both the NIST Zero Trust Architecture and Comply-to-Connect, organizations must ensure that their entire security ecosystem communicates and coordinates attack awareness and response.

A critical advantage of the ClearPass Policy Manager is that customers can leverage their existing security investments by seamlessly integrating 360 Security Exchange-sourced products with Aruba solutions. Unlike other infrastructure providers that lock customers into costly upgrades and a single source of products, the Aruba 360 Secure Fabric provides the best elements of a unified solution with the flexibility of an open architecture.

Support for the Aruba 360 Security Exchange Program is an integrated component of ClearPass Policy Manager. Features such as REST-based APIs, RADIUS Accounting Proxy, and Syslog ingestion help facilitate workflows with orchestration, SIEM, firewalls, help-desk systems and more. Context is shared between each component for end-to-end policy enforcement and visibility. The ClearPass Ingress Event Engine provides 3rd party systems the means to share information in real-time using Syslog. This enables ClearPass to respond to changing threats for users and devices after they have authenticated to the network. By utilizing an open dictionary approach, anyone can write a parsing ruleset without the need for costly add-ons or closed vendor ecosystems.

ClearPass Policy Manager provides advanced reporting capabilities via customizable templates. Information about authentication trends, profiled devices, guest data, on-boarded devices, and endpoint health can also be viewed in an easy to use dashboard. Aruba Central Client Insight also has support for granular alerts and a watch list to monitor specific authentication failures.

An Extra Layer of Protection: Aruba Advanced Cryptography

Approved by the U.S. National Security Agency (NSA), the Commercial National Security Algorithm (CNSA) Suite is a set of publicly available algorithms that serve as the cryptographic base for unclassified information and most classified information. The NSA has authorized the use of CNSA to facilitate the sharing of sensitive and classified information among multiple departments as well as to bring secure mobility to commercial laptops, tablets, and smartphones.

The Aruba Advanced Cryptography (ACR) module delivers CNSA cryptography, enabling user mobility and secure access to networks that handle controlled unclassified, confidential and classified information.

SUMMARY

Networking solutions from Aruba start with built-in support for Zero Trust Architectures and Comply-to-Connect. Without this comprehensive support for all five of the major Zero Trust Architecture and Comply-to-Connect requirements, organizations are faced with assembling complicated, unintegrated solutions that leaves gaps in their protection.

Requirement	Zero Trust Architecture Approach[1]	Comply-to Connect Approach[2]	Aruba Solution
1. Know what's on the network	An organization protects resources by defining what resources it has	Single platform to discover, identify, categorize, classify, and profile all devices	✓ Aruba Central ClearPass Device Insight
2. Authenticate all users and devices	Create, store, and manage enterprise user accounts and identity records	Authenticate all connecting devices utilizing 802.1x or equivalent standards	✓ ClearPass Policy Manager
3. Ensure configuration and compliance guidelines are followed	Gather information about the enterprise asset's current state and apply updates to configuration and software components	Assess the device compliance with guidelines imported from DoD authoritative source; automatically remediate deviations from established required compliance baselines	✓ ClearPass OnGuard
4. Assign and enforce access policies in the network	All resource authentication and authorization are dynamic and strictly enforced before access is allowed via coordination between a Policy Engine and a Policy Enforcement Point	Perform or orchestrate network segmentation actions at a variety of policy enforcement points in the network (e.g., host, access switch, wireless access point, network firewall)	✓ ClearPass Policy Manager, Policy Enforcement Firewall and Dynamic Segmentation with Aruba Access Points and Gateways
5. Communicate bi-directionally with the security ecosystem and respond to attacks	Provide real-time (or near real-time) feedback on the security posture of enterprise information systems; integrate with Security Information and Event Management systems.	Integrate/orchestrate functions and bi-directional information sharing with multiple security and management tools to enable automated proactive and/or responsive security and management operations	✓ ClearPass Policy Manager/360 Security Exchange

[1] From NIST Special Publication 800-27

[2] From the Defense Information Systems Agency (DISA), Development and Business Center (DBC) Endpoint Division (ID3) Comply-to-Connect (C2C) Request for Information

BP_ZeroTrustArchitecture_SK_011222 a00120128new

Contact us at www.arubanetworks.com/contact