TECHNICAL DOCUMENT

UNIFIED POLICY AND MANAGEMENT FOR THE DISTRIBUTED ENTERPRISE

HOW ARUBA SD-BRANCH SECURES AND SIMPLIFIES WIRED, WIRELESS AND WIDE AREA NETWORKS

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

KEY BENEFITS

- Dynamic micro-segmentation isolates users and devices to the smallest needed policy domain
- Branches are simplified by migrating from VLANs and static IP-based policies to role-based policies
- Policies are centrally defined and enforced across all branch gateways
- Users experience consistent access privileges at each branch
- Local wireless and wired roles and policies are extended to the WAN

INTRODUCTION: TRADITIONAL LAN SEGMENTATION

It has become a best practice in the wireless LAN (WLAN) world to authenticate all users and devices joining the network and to assign them roles. For instance, employees who join the network are assigned an employee role, guest users are assigned a guest role, and devices such as cameras are assigned camera roles. This is known as role-based authentication.

While Wi-Fi connectivity tends to be the most common way to join a network today, a large number of devices and users connect to wired networks. Groups of users are assigned to VLANs for traffic isolation based on device or traffic type. VLANs are a useful way to limit the scope of broadcast traffic, enforce security and privacy policies, and simplify access control.

For example, an IT department may support two groups of workers who must not use each other's shared printer or see other resources. VLANs in campus and branch networks are commonly used to group hosts into administrative domains, regardless of their physical locations in the network.

However, VLAN configuration remains a complex and error-prone process, because network administrators need to manually configure many individual network elements (i.e., switches) using device-level configuration. Furthermore, the VLAN approach brings with it the baggage of Access Control Lists (ACLs) that use hardwired IP address ranges, tied to specific VLANs. These ACLs may be configured on switches, routers and firewalls. Thus, extensive use of VLANs creates many challenges for network administrators.

The rise of workplace mobility creates an additional need for flexible, secure access, and Internet of Things (IoT) devices[1] are typically connected over physical wires to switch ports. As such, the usual way segmenting them is into their own separate VLAN. However, this results in VLAN sprawl, which adds further complexity to the LAN.

BRANCH OFFICE MANAGEMENT

Today, a medium-sized branch office contains many wired and wireless devices. These may include tablets, laptops, phones, lighting systems, door locks, Point-of-Sale (PoS) devices, inventory trackers, time clocks, and cameras, among others. To support these devices, the networking hardware may include a gateway, an access switch, and wireless access points.

Branch office personnel may include representatives from major company employee groups, such as general corporate staff, sales, security, contractors and guests.

Traditional VLAN Management

For these employee groups, a logical VLAN mapping often includes several VLANs on the switch and several more for the access points. For all of these, the administrator must track devices on individual ports, and add VLANs or ACLs to them when adding devices to the network. Moves, additions, and changes are difficult to manage and track.

Thus, traditional segmentation calls for quite a few managed VLANs for even a medium-sized branch office. Multiplying this by perhaps hundreds or thousands of branch offices illustrates the state of domain management in the age of distributed enterprises using mobility, IoT, and cloud services. As user roles change—for instance, an employee becomes an administrator, or a contractor becomes an employee—it is cumbersome to separately change switch and access point configurations to accommodate this.

[1] Common examples include cameras, door lock systems, HVAC systems, and many others.

This complexity is illustrated in Figure 1.

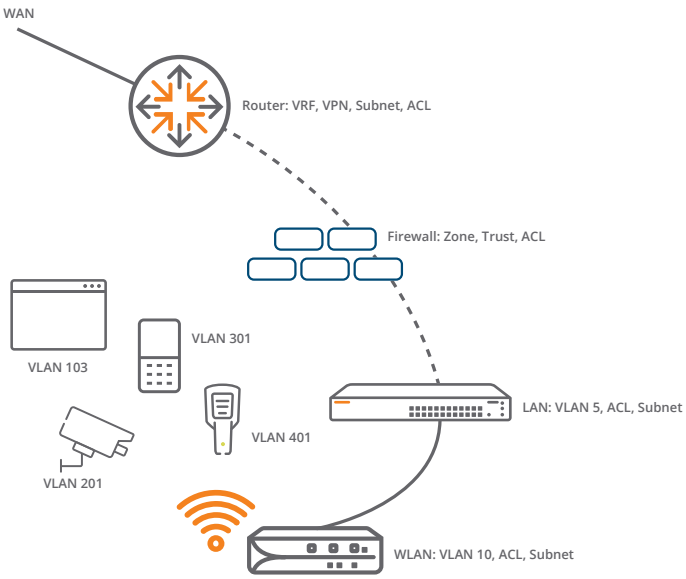

Figure 1: Static VLAN Management with Disaggregated Policy Enforcement

This simplified example shows how inflexible the traditional approach of segmenting and isolating these device types on their own VLANs can be.

Simplified LAN with Role-Based Access

By contrast, it is far simpler to manage this branch with a role-based approach, using Network Access Control (NAC) to set roles and policies, and then having a centralized policy enforcement point to dynamically segment traffic. Even with many employee groups and devices, the difference with role-based access is that devices and applications are dynamically mapped to a small set of roles.

These roles are defined in a single application for the whole network, and enforced at a single point (Figure 2) in each branch.[2]

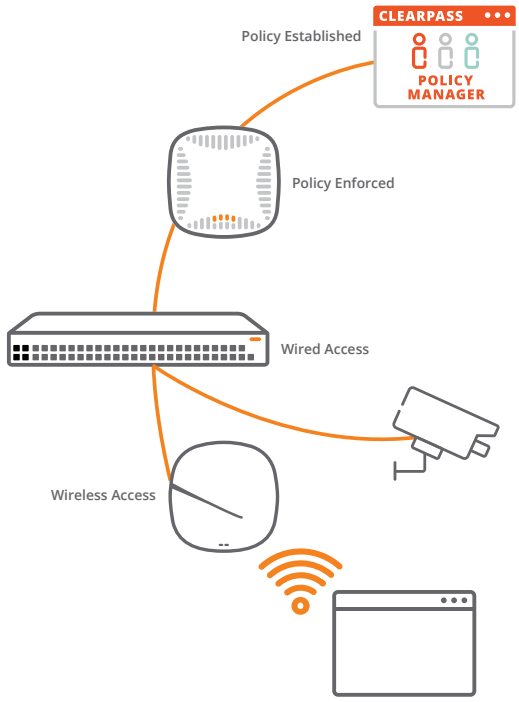

Figure 2: Role Based Access with Centralized Policy Establishment and Enforcement

[2] For more information on how this works, see the section below on Mechanisms for Role-Based Access and Policies.

Role-based access inherently simplifies the LAN: there is no need to segment the network into many VLANs. Every device is effectively micro-segmented into a separate tunnel, with the access rules dictating "who can talk to whom" (Figure 3).

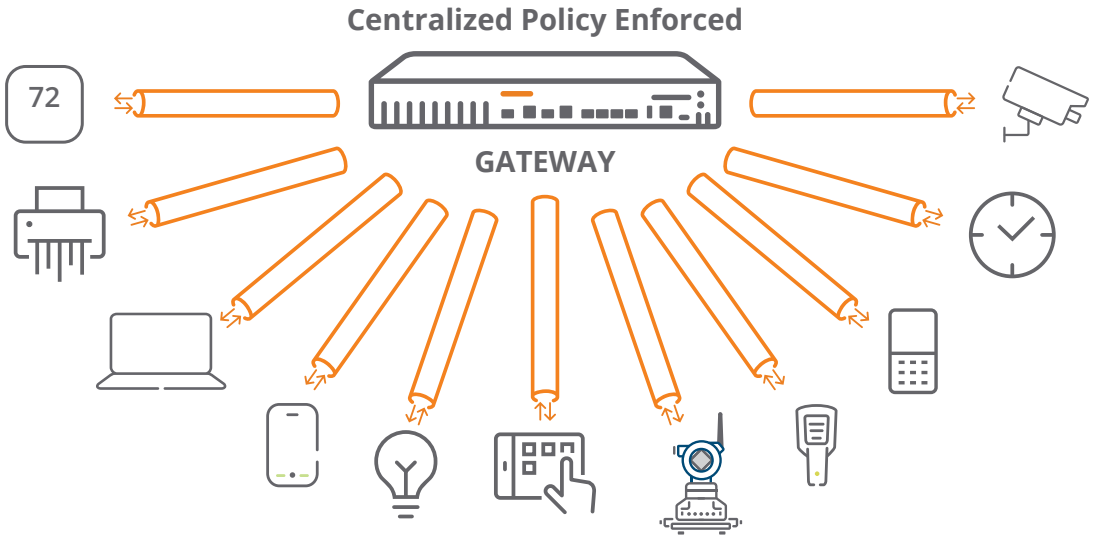

Figure 3: Devices and Users are placed in Secure Tunnels Rather than VLANs

Role-based access with centralized policy enforcement dramatically simplifies the network. The differences between segmenting communications in this manner rather than with static ACL assignments and VLANs is illustrated in Table 1.

TABLE 1: BENEFITS OF ROLE-BASED OVER TRADITIONAL ACCESS

Traditional Access	Role-Based Access
Intra-VLAN communication is permitted	Policy can selectively deny Intra-VLAN communication (micro-segmentation)
VLAN is assigned only once (manually, statically)	Flexible, continuous end-point profiling
VLAN assigned based on physical port	Role-assigned based on authentication and profiling
New services require new VLAN deployment	Faster deployment of new services (ZTP)
Ports are open by default, allowing accidental access	All ports are secured – no accidental access
DHCP scope is fragmented per VLAN	Single DHCP scope per branch
WAN policy is defined by distributed routing	WAN policy is centrally defined by user and application, and dynamic path steering (DPS) is permitted

Note that the above model also works in branch topologies with multiple gateways to support High Availability.

ROLE-BASED POLICY FOR THE DISTRIBUTED ENTERPRISE

A distributed enterprise needs a secure approach to managing not only the WAN but also the various LAN networks in branch offices. A key foundation for this is based on consistent, unified policies and common management across the enterprise. Aruba's SD-Branch solution provides this unification and simplification.

With SD-Branch, roles and policies are established using Aruba ClearPass[3] for all users and devices admitted to the network. This zero-trust access control provides visibility and context for profiling and onboarding. Following that, Aruba gateways ensure that these policies are enforced across the enterprise (Figure 4).

Figure 4: Aruba SD-Branch Policy and Security Approach

The Aruba gateways enforce LAN, WAN, and security policies at the WAN edge. Secure connectivity is extended from the branch across the WAN with SD-WAN secure overlay VPNs. This leads to secure branch offices and secure traffic across the distributed enterprise.

MECHANISMS FOR ROLE-BASED ACCESS AND POLICIES

Aruba ClearPass Policy Manager (CPPM) authenticates and assigns roles to all devices joining wired and wireless networks. Once all entities joining the network are authenticated and assigned a role, that role becomes the common policy construct (regardless of the means of access) to provide unified treatment (Figure 5).

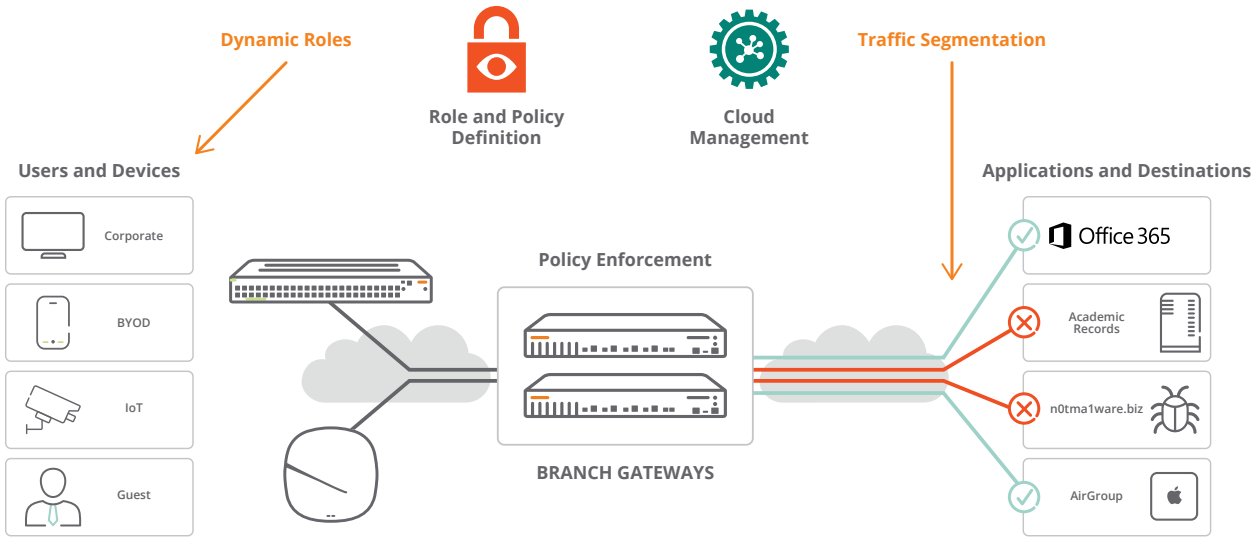

Figure 5: Framework for Assigning Policies and Roles

[3] Alternatives to a centralized role-based policy mechanism such as ClearPass invariably require many separately licensable and proprietary components.

CPPM assigns roles to users (such as employees, administrators or guests) and devices (such as cameras, phones or laptops). These roles are communicated as part of the device onboarding process using RADIUS VSAs (Vendor Specific Attributes). Aruba gateways dynamically learn these roles since they are in-line participants of the authentication exchange.

Policies are then created based on these roles and are configured and enforced at the gateways by Aruba Central. These policies allow authorization to access applications or destinations, and also to access each other (such as inter-user communication or access to devices).

THE GATEWAY'S ROLE IN POLICY ENFORCEMENT

In order to achieve this flexibility, traffic (wired or wireless) is tunneled from each access port of the switch to one or more gateways, which serve as the central policy enforcement point at the branch. The gateway learns the role assigned to the end point (whether connected to the wired or wireless network) during the authentication process.

All of the tunneled traffic that connects "things" (IoT devices) within the branch is inherently untrusted, and therefore will be inspected by the policy enforcement firewall. The gateway, therefore, becomes the security enforcement point.

Figure 6 illustrates the role of the gateway as a policy enforcement point.

After ClearPass establishes context through user and device authentication and policy assignment, the policies are pushed to the firewall within the gateway. User sessions are tracked and inspected by the firewall, and policies are enforced.

The green and red lines are examples of these enforced policies:

- The camera can communicate with the video recorder (green line)
- An employee cannot access the camera (red line)

However, if the employee in question subsequently is assigned administrative authority, this is a simple, centralized change. Administrators can define as many roles and policies as they need in this way.

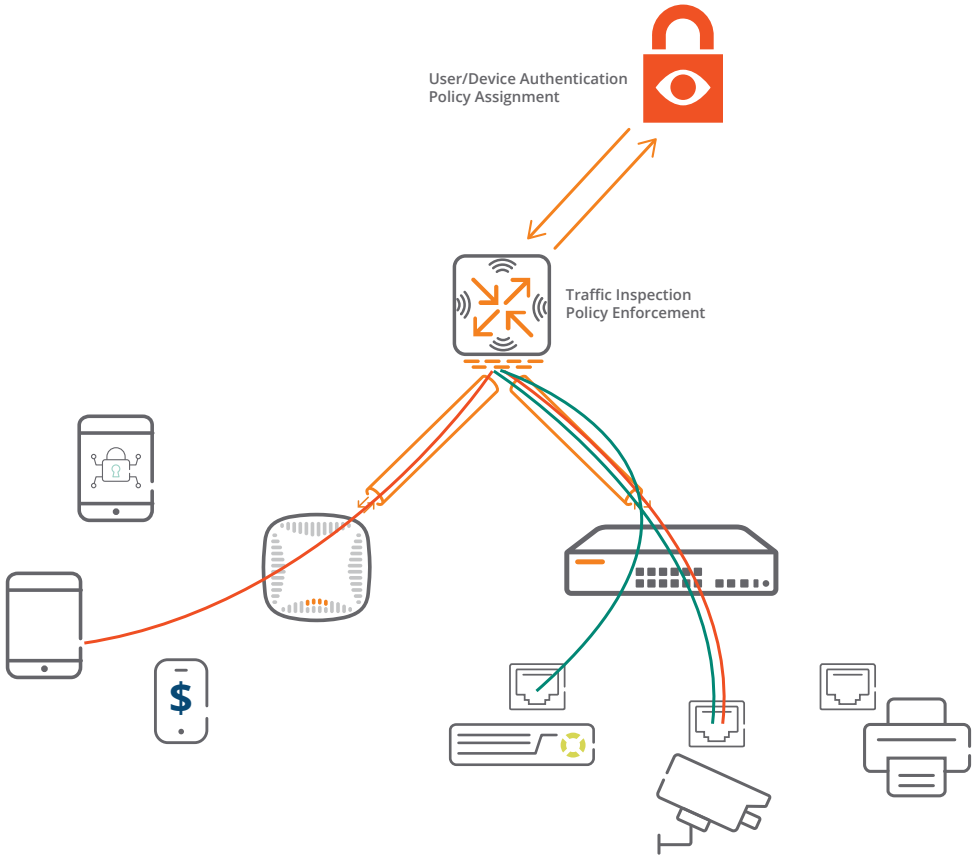

Figure 6: Gateway as Centralized Policy Enforcement Point

EXTENDING ROLE-BASED POLICIES TO THE WAN

Role-based policies are used not only to enforce security but also to define WAN policies (Figure 7).

In this context, roles are a way to segment and classify common sets of attributes (users, devices, applications, locations, and WAN state) for policy enforcement and security. This is a far more elegant and efficient approach than the use of numerous VLANs. Policies are ultimately used for a simplified micro-segmentation of the network. They have similar influences in the LAN, WLAN, and WAN, and in how they establish security.

The policy clearly defines the intent without specifying VLANs and IP addresses, allowing the policies to be defined once centrally for all branch sites, with the gateways enforcing the policy per location. By treating every endpoint as a segment of one, the gateway enforces fine grain segmentation policies; for example, Payment Card Industry (PCI) traffic isolation can be enforced effectively.

In the WAN, roles may influence path steering of traffic; for instance, guest roles may not have access to MPLS links, whereas employees use MPLS for voice applications. The enforcement of these rules may be partly influenced by WAN state; for example, in some cases employee roles may in fact selectively be modified to access Internet for unified communications if the MPLS links are not providing adequate quality.

Aruba Central also provides a single location to configure policies both for routing and access control. Since these policies are coordinated with end points and roles (rather than being tied to ports and hard-wired IP addresses), role information learned in the access layer can carry out performance routing in the WAN layer.

This capability provides many other advantages, including heightened security. For example, an administrator may discover (through the news or other means) the existence of malware in a particular brand of camera. To isolate the camera (and the traffic it generates) with traditional means, the administrator would need to make static changes to access lists with hard-coded IP addresses for each of the affected cameras. With ClearPass, on the other hand, the administrator can split the "Camera" role into two roles: one for normal operations and one for the malware brand. For the "Malware" role, the administrator simply applies a rule to black-hole the traffic.

There are many other ways in which this degree of flexibility provides granular and dynamic control of traffic. For instance, YouTube traffic used for employee training may need to be treated very differently than YouTube traffic from guest devices. Even among employees, you might want to offer different treatment to your finance, marketing, engineering, HR, and sales teams based on the applications they tend to access (for instance, prioritizing Salesforce access for sales, Business Intelligence applications for Finance, Workday for HR, etc.). There are over 3100 applications that can be identified, classified, and associated with users in this way.

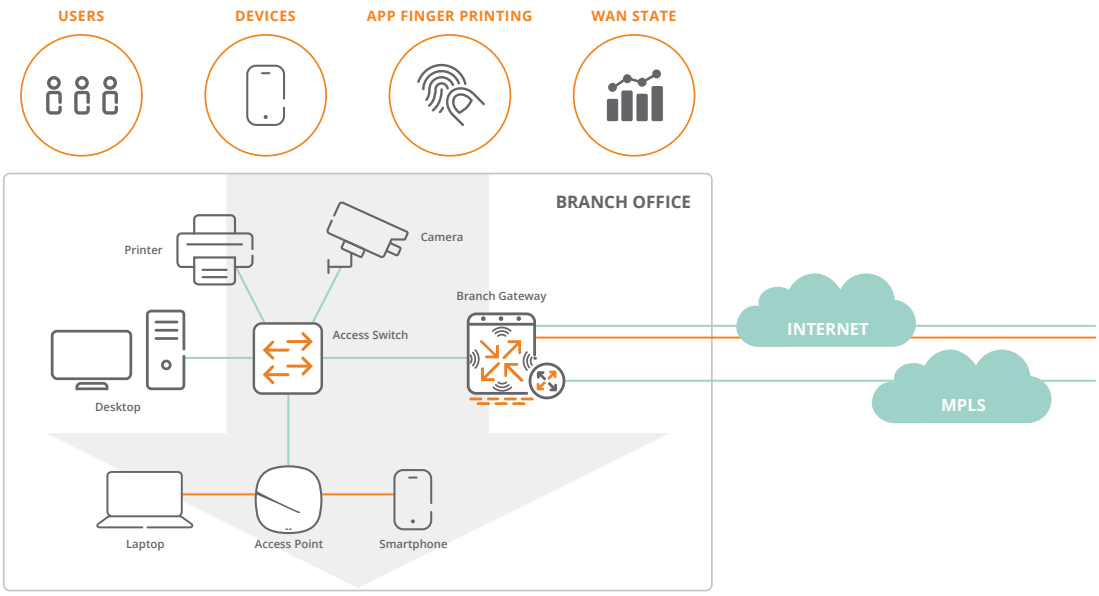

Figure 7: Role Based Policies for LAN, WAN, and Security

By using roles and applications to classify traffic, you have the power to provide differentiated treatment in the selection of WAN paths, setting QoS precedence, selecting different SD-WAN SLA policies, and segmenting the traffic into different tunnels within the SD-WAN overlay.

CONCLUSION

Policy is a major focus for Aruba SD-Branch. Accordingly, Aruba branch gateways include role-based, stateful firewalls to enforce policies across the distributed enterprise. This functionality includes the following:

- Role-based policies where policy is dynamic and follows the end-point, regardless of the access medium
- Identity management and authorization, with CPPM to create roles
- Deep Packet Inspection (DPI) and Web Content Classification (WebCC) for enforcement and classification on the gateway
- Network segmentation into "microsegments of one" with clear, plain-language policies to specify "who is allowed to talk to whom."

A key value proposition of SD-Branch is the coordination of data across the LAN, WLAN, WAN and Security layers to provide new insights and help with rapid troubleshooting. Furthermore, role information learned in the access layer can carry out performance routing in the WAN layer. This is the promise of unified policy and management.

TD_UnifiedPolicyManagement_103119 a00091523enw