aruba
a Hewlett Packard Enterprise company

SOLUTION BRIEF

ACCESS CONTROL OPTIONS FOR WIRED NETWORKS

INTRODUCTION

When policy and access control are discussed, there's usually an immediate association with wireless and unmanaged devices such as smartphones and IoT devices. As these devices are often used outside of the workplace and normally connect over the air, policy controls and device profiling efforts have been solely focused on wireless access. This has led to wired access controls being overshadowed or not configured at all, leading to security gaps in many organizations. And as IT Security experts are well aware, networks are only as strong as their weakest link.

As the modern workplace is full of external personnel such as temporary workers, contractors, and guests who may use their personal devices within the workplace, identity and device visibility have become valuable components during the authentication and authorization phase. This data is then used to enforce policies on wireless and wired networks. But, the growth of IoT devices, that are not associated with a specific user or group, is now causing security concerns on the wired network.

Without consistency on the wired network, malicious users can connect and access corporate resources easily. For instance, depending on the access switch configuration, users may be able to access the wired network through an authenticated device such as an IP phone's built-in switch port. Even though there is some form of authentication, it may not necessarily apply to the devices connected through the IP phone.

This paper discusses options that bring wired networks closer to the same level of control that have been on wireless networks, regardless of access control method, either through secure means or non-AAA enforcement.

OPTION 1: NON-AAA ENFORCEMENT

With non-AAA enforcement, the goal on a wired network is to minimize the effort it takes to deploy a policy enforcement service. Endpoints do not require a supplicant or agent, which makes it convenient for laptops, printers, and IoT devices – many of which do not support an 802.1X supplicant. And, there is minimal configuration required on the actual switches.

When a device plugs into a wired port, the policy engine can be notified of the new device, and profiling techniques such as DHCP Fingerprinting or Windows Management Instrumentation (WMI) can be used to identify the type of device and the user. With this information, we can validate this device and user against the Active Directory or a device database so that appropriate policies can be applied to the switch port. This means that every device connecting to the wired network is profiled and evaluated providing much needed visibility.

Profiling consists of fingerprinting each device as well as the ability to perform device assessments to better understand the posture of a device. Methods of profiling and assessment include DHCP fingerprinting, SNMP scans, NMAP scans, Link Layer Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP), Windows Management Instrumentation (WMI), and more. For Windows laptops, you can perform basic assessments like seeing if required services exist and if they are running on each device.

The advantage of using non-AAA enforcement is that there is minimal configuration, and it allows IT to quickly meet internal or external audit or compliance demands. You're also able to build a comprehensive database of all devices connecting to the wired network, which becomes more important as IoT devices emerge in greater numbers.

OPTION 2: IDENTITY-BASED 802.1X AUTHENTICATION

802.1X is the most secure option and provides real-time certificate or login and password based authentication. You also benefit by performing authentication before a device receives an IP address. In the non-AAA model, devices receive limited access to the network before any authentication.

Using 802.1X also provides better options for the authorization of device privileges. Instead of just VLAN placement, the use of ACLs, downloadable ACLs, and roles can be used to define access when the status of a device changes. The ability to use granular identity-based enforcement also makes it easier to share user information with firewalls and other security components for enhanced downstream policies and threat prevention.

But as with anything related to security, there is an inverse relationship between convenience and the level of effort needed from IT to implement a model with secure policy management.

There are three components that must be in place and configured for 802.1X to work; a supplicant, an authenticator, and an authentication server. The supplicant resides on the endpoint device, the authenticator is the switch in a wired network, and the authentication server is a AAA component that typically uses the RADIUS protocol. In today's world, the AAA server resides within a policy management solution.

For a wired environment, 802.1X eliminates port VLAN configuration issues as each device that connects can initiate a session for that specific connection. A user can't unplug a printer, connect a laptop and gain access to the printer VLAN. The workflow, once a laptop is connected, would be to establish the identity of the user and device and perform a role-based enforcement for that user or device. Differentiated privileges can be granted based on user and device role, location, posture of the device, and more. For devices that do not support 802.1X, you can also use MAC address based authentication to enable connectivity to the wired network.

The profiling data that can be captured is similar to what can be collected in the non-AAA model, but enforcement options are greater as collected attributes can then be used to perform runtime changes of authorization based on changes of a device's status.

Another advantage is that 802.1X supports logins and passwords, or the use of device certificates, which provide a higher level of security. Certificates can't be spoofed. Today, onboarding services can automate the configuration of endpoint supplicants and create a database for use when performing authorization and enforcement. This can be used on wired, wireless and VPN networks to provide a consistent user experience.

Other advantages include the ability to change the privileges of connected devices based on their behavior. If multiple devices are connected behind a switch port, a change of authorization (CoA) to adjust security policies would not affect all devices, only the target device.

RECOMMENDATIONS

IT security administrators have spent a considerable amount of time securing the wireless network due to personal devices, guests, visitors, and contractors requesting Internet access. However, the wired network has often been overlooked due to lack of resources. Today, the growth of IoT and compliance requirements are driving the need for wired networks to receive the same level of attention.

Given that more and more security breaches are targeting IoT devices on wired networks, our recommendation is to deploy an option that makes sense for both wired and wireless networks. For this reason, Aruba ClearPass supports both non-AAA and secure 802.1X policy enforcement for wired, as well as wireless networks. ClearPass OnConnect allows for non-AAA wired enforcement so that customers can start down the policy and access control path. All devices can be profiled with user based authorization, all with minimal configuration on the switching infrastructure.

The more secure 802.1X enforcement model should be considered for greater policy enforcement options. As it will require more planning and configuration, if 802.1X is already being used for a wireless service, ClearPass provides mechanisms to unify policy enforcement across different network transport types, all from a single solution.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com