aruba
a Hewlett Packard
Enterprise company

EXECUTIVE OVERVIEW

MIGRATING FROM LEGACY AAA TO POLICY MANAGEMENT AND VISIBILITY

MOBILITY AND IOT IS CHANGING THE NETWORK ACCESS GAME ON WIRELESS AND WIRED NETWORKS

A quick look at why authentication, authorization and accounting – or AAA and RADIUS – were developed can easily take you back more than a decade.

Acronyms and phrases like modems, roaming between ISPs, UNIX, and AOL come to mind. Users had one device and IT managed everything – devices, applications and access to network resources.

Authentication for one user with one device, using very fixed criteria, is a thing of the past. In fact, the majority of users now have three or more devices. They access email and secure enterprise resources from anywhere at any time. This next-generation workforce, known as #GenMobile, is pushing the limits of IT and legacy AAA platforms.

So we are now faced with new challenges: What's the best way to implement policy management to enforce behavioral policies related to mobility and the use of personally-owned devices on the wireless or wired network? And how do you account for multiple types of devices per person?

One thing is certain – policy management is the key to enforcing secure mobility. It's more cost-effective and easier to manage than the tedious and complex rules associated with legacy AAA. And it accommodates armies of users with lots of mobile devices, or personal laptops on the wired network.

Similarly, Internet of Things (IoT) devices have been proliferating in the enterprise – everything from surveillance cameras, printers, temperature controls, and HVAC systems, which have created another problem on the wired side of the network – how do you create visibility for devices that have no common profile and how do you make sure that these devices are not compromised?

Automated policies

Older AAA rules sets have transitioned to policy management systems that leverage contextual data – user roles, device types, application flows and location – to dynamically enforce what resources can be accessed.

What's different and better is that policies can be created based on expected results as well as unexpected results. For example, a laptop that had been deemed compliant can change state overnight, requiring remediation or given limited access until resolved.

Visibility and profiling

Knowing what devices are connected to the network makes it easier for IT to define basic wireless and wired access policies. Device ownership is also important. It allows it to create more granular policies based on a specific type of device and as well as device ownership.

Consequently, an IT-issued laptop can be allowed to securely access a wider range of network resources or be given more bandwidth than a personally-owned smartphone used by the same employee.

IoT devices are much more difficult to discover and profile than smart devices due to the rapid adoption and development of new devices. However discovery is just as critical so that these devices can be controlled on the network as well. So it is critical to have a system that can allow for custom profiling.

Built-in services

This one's a game changer — it t can use baseline AAA and policy elements to automatically exchange data with third-party applications and implement self-service workflows. These capabilities do not exist in legacy AAA solutions and can impede the rollout of bring-your-own-device (BYOD) initiatives.

Today's policy management systems let users configure their own devices for secure Wi-Fi connectivity. Leveraging data from a mobile device management (MDM) or enterprise mobility management (EMM) solution makes it easy to detect if a device can securely connect to enterprise networks.

The same Exchange capability built into Aruba ClearPass will also work with other point security solutions such as perimeter firewalls, IPS, SIEM, and even other support services.

Guest authentication

Centralized management of guest policies also provides a big advantage over legacy AAA. Exhibiting greater flexibility, policy management systems can accommodate modules that enable IT to leverage authentication and enforcement methods and leverage an internal database.

They also allow IT to create security policies that separate guest traffic from enterprise traffic. It's even possible to define simple rules that determine when and how long guests can stay connected to the network and cache their authentication over that period of time so that they do not need to continually log in.

GET READY FOR POLICY MANAGEMENT AND VISIBILITY

Most it organizations currently rely on Active Directory or LDAP to assign and enforce security policies for users and devices. But what is missing are real-time enforcement and the use of contextual data. Both are essential to making pre and post-admission decisions based on the status or actions of users and devices. And these directories do not have associations with IoT devices.

Policy and AAA servers

So what's the most expedient way to roll out policy management? Migrating from legacy AAA to centralized policy management is best completed in phases. Best practices dictate that upcoming guest, employee BYOD, and IoT initiatives should be managed by the incoming policy management solution.

Policy management proxy services enable legacy AAA to support use cases that previously required lots of customization, such as wired VoIP implementations, surveillance cameras, and other IoT devices. Once IT becomes familiar with a policy management system's AAA capabilities, services from the legacy AAA server can be retired.

Network infrastructure

The best policy management systems can be implemented on existing wireless and wired networks and support 802.1X, standard RADIUS, change-of-authorization (CoA) RFC 3576 and external captive portals. Although most vendors support these features, software or hardware upgrades might be necessary if older equipment is utilized.

Mobile and IoT devices

Authentication services are fairly consistent between AAA and policy management systems. However, any form of health checks or device interrogation will require a policy management system.

A critical policy management capability entails making real-time decisions based on intelligence gathered from devices using NAC and/or MDM agents. The policy management system determines if a device can connect, if remediation is required, or if access should be denied.

Policy management must also be able to discover and control IoT devices on the network for the same security considerations as controlling personal devices on the network.

SUMMARY

Using policy management in a mobile environment, where users connect over wireless and wired networks throughout the day solves a set of entirely new challenges that didn't previously exist. If a device is denied access today, user and IT productivity is lost.

With the right policy management approach, IT organizations can ensure that the growing universe of #GenMobile workers get instant access to the apps, printers, and network services they're authorized to use, and that operational technology departments can deploy IoT devices to automate environmental and operational process without concern for the enterprise network security.

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