WHITE PAPER

MULTI-FACTOR AUTHENTICATION FOR GOVERNMENT INSTALLATIONS

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

IDENTITY PROOFING NETWORK ACCESS TRANSACTIONS 3

WHERE ARUBA SOLUTIONS HELP 4

UNFORTUNATELY, WHAT HAPPENS TODAY? 5

HOW CLEARPASS HELPS 6

SUMMARY 7

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY 7

Military-Grade Security for Government

After a series of recent high profile hacks against government agencies, many of our customers are working to lock down their networks to prevent future attacks. There were nearly 70,000 information security incidents on federal government networks in fiscal year 2014, up 15 percent from fiscal year 2013. (source – Homeland Security and Governmental Affairs report) Although the days of users freely roaming internal networks are over, there are steps that can be taken to ensure military-grade security to mitigate risks. Policies can be customized to meet per-user requirements and enforced regardless if connecting to wireless, wired or VPN.

IDENTITY PROOFING NETWORK ACCESS TRANSACTIONS

One area of concern is the ease in which hackers have stolen username and password credentials in order to compromise internal network and computing systems.

This is an area that has been dealt with on the military side for years through the issuance and use of x.509 digital certificates on Common Access Cards (CAC). These cards are used to access computers and network elements alike and have largely eliminated password-based Active Directory accounts. Also, many network devices are still managed at the command line via TACACS+ or RADIUS username/password administrator accounts, but their days may be numbered as well.

When looking to upgrade wireless and wired authentication, NIST 800-63-2 Electronic Authentication Guideline state the directives that must be followed.

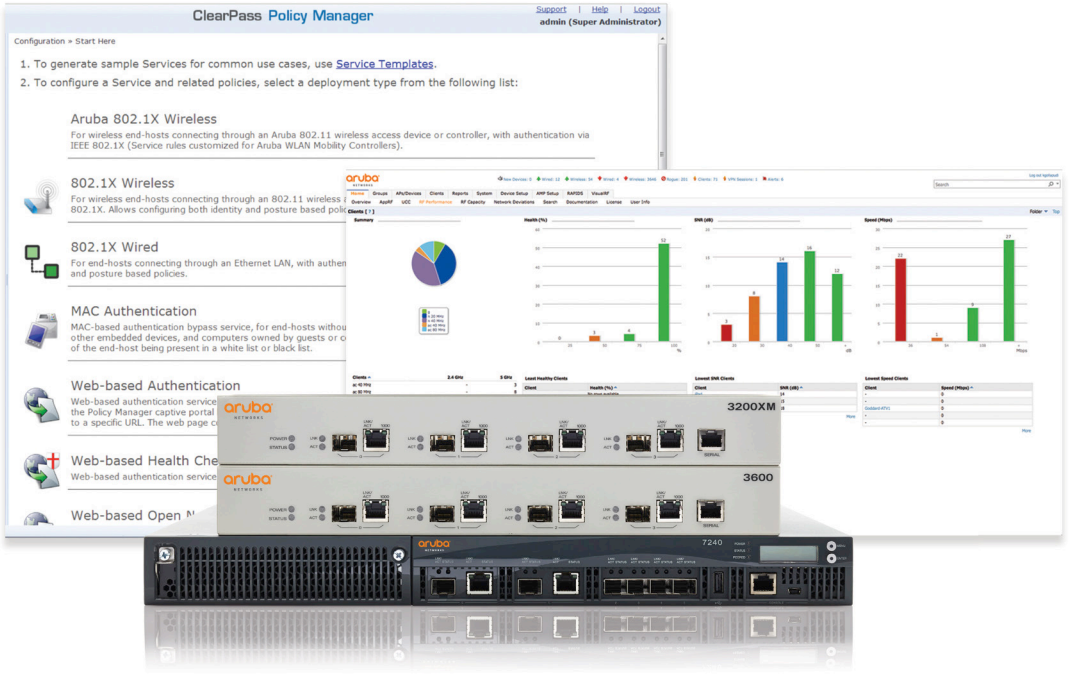
This document explains the requirements for the issuance and use of 2-factor authentication credentials, as well as 4 defined levels of assurance and where each level is appropriate. Each level is intended to protect a transaction that is classified in terms of its potential to cause harm by way of compromised privacy, safety, and financial loss.

- Most level 1 and level 2 transactions involve the public interacting with government web sites to obtain park permits, changing a mailing address, participating in citizen forums and so on.
- Level 3 and level 4 transactions involve employees and contractors accessing internal systems.

Common Access Cards (CAC)

In simple terms, level 3 allows the use of non-cryptographic token-based 2-factor solutions such as RSA and Safenet while level 4 requires the use of Personal Identity Verification (PIV) cards. These cards are the civilian equivalent of CAC cards and contain x.509 certificates with RSA 2048 bit key pairs.

From the management perspective there are 2 authentication transactions that must be protected; SSH access for command line sessions and secure web access for Graphical User Interfaces (GUI) administration.



Aruba WLAN controllers, Airwave Management Servers, and ClearPass Policy Manager

WHERE ARUBA SOLUTIONS HELP

Let's look at the features Aruba, a Hewlett Packard Enterprise company delivers to enable Level 3 and 4 Identity Assurance. We'll also cover how Aruba's security model can provide a transitional solution for devices that may not be able to fully compliant with level 4 assurance.

Authentication services

As an option to standard username and password based authentication for administrative access, all Aruba WLAN controllers, Airwave Management Servers, and ClearPass Policy Manager appliances support CAC/PIV certificate-based authentication over https using the TLS protocol.

The Aruba equipment verifies the client certificate against the issuing Certification Authority (CA) and then looks up the user name via LDAP or RADIUS using an authorize-only transaction. This process ensures the user identity and authorizes them to access the system. During authorization, ClearPass may include information such as Active Directory group membership to determine access level privileges, such as read-only, operator, or administrator.

In practice this offers functionality very similar to the current paradigm of RADIUS or TACACS+ authentication for network operators and administrators. It doesn't require any local accounts and is easy to administer. For instance, if an employee leaves the organization the only thing needed to terminate their access would be to delete or deactivate their LDAP or Active Directory account.

Command line access

When it comes to the second protected transaction the solution is not as simple. Aruba, along with many other vendors, supports SSH with username/password or a public key authentication method for command line access.

SSH keys can be derived from RSA keys like those found on a PIV card but current SSH implementations do not send any user identity information linked to the key. This linkage between key and user identity is accomplished on the PIV card by use of an x.509 certificate. The certificate binds the user name to the public key in a package that is protected by a signature from the issuing Certification Authority. Without that bundle, each device must manually link a username to public key by creating a local account on the device and uploading each key.

Simply put, this is impractical for a network of any scale. Imagine a medium size government agency with several thousand network elements (switches, routers, firewalls) and several hundred administrators of various sorts. Adding an account for each administrator and manually uploading keys to every device is incredibly tedious, but also creates a vulnerability when accounts are not erased or updated in a timely manner.

In the long term, the solution comes in the form of RFC 6187 which updates the SSH protocol to support x.509 certificates. Once implemented, the network device could:

- Validate the client certificate against a CA
- Verify revocation status
- And, look up the name via RADIUS or LDAP to authorize the user and ultimately grant access

At that point the client may use a PIV card to access the CLI or GUI interface of a network element without the need to create local accounts. It will show clear advantages when code upgrades and new SSH clients support this throughout the network sometime in 2016.

UNFORTUNATELY, WHAT HAPPENS TODAY?

Let's look at NIST 800-63-2 guidelines which state:

The guidelines in this document assume the authentication and transaction take place across an open network such as the Internet. In cases where the authentication and transaction take place over a controlled network, agencies may take these security controls into account as part of their risk assessment.

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Years ago it was common to have an out-of-band (OOB) management network that was either completely disconnected from the enterprise or very nearly so. Accessing the management interface required physical presence on the network and was sometimes augmented by terminal servers connecting directly to device console ports.

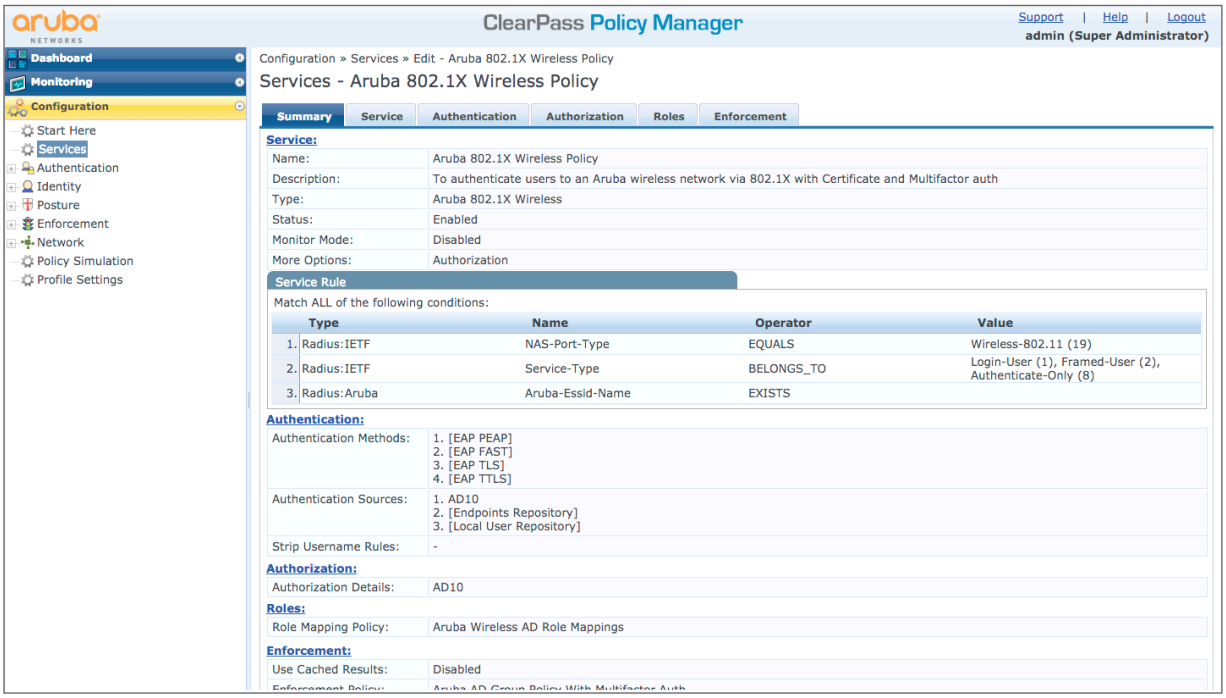
As stated above, such network control strategies can be considered mitigating factors in a risk assessment. Aruba APs and controllers can be used to create a controlled network for accessing network elements. This controlled network access meets the Level 4 requirements of NIST 800-63-2.

This controlled network consists of a small number of VLANs connecting to an interface on each network element. These interfaces are blocked by firewall or access control lists from the enterprise network and can only be accessed by devices providing two-factor authentication via 802.1X.

Administrators requiring management access must first authenticate over 802.1X with their PIV card and are granted limited access to the devices they are allowed to manage. This limited access is enforced by Aruba's Common Criteria validated firewall, which allows each user to be assigned a unique set of access rules.

Ideally each user also joins the controlled management network over an encrypted link. Encryption eliminates the risk of address spoofing and provides something known as non-repudiation; strong evidence that user X sent packet Y because the encrypted key is derived from their PIV card.

This model of two-factor authentication, individual role-based firewalling, and strong encryption is what Aruba has been implementing via WPA2 and wireless for over 10 years. Combined with PIV cards issued in accordance with NIST 800-63-2 it provides Level 4 assurance for all users connected to the controlled management network.



ClearPass RADIUS-based wireless authentication service

HOW CLEARPASS HELPS

When an administrator authenticates to the controlled network via Wi-Fi, ClearPass can use attributes such as Active Directory group membership to authorize access to some devices but not others via Aruba's wireless controller's role-based firewall.

For instance if user A authenticates using their PIV card and the LDAP lookup identifies them as members of "Switch Admins" group, ClearPass can return the "User-Role" attribute "Switch-Admins". This attribute tells the Aruba Controller to assign a firewall rule-set allowing access to all switch management addresses but blocking that user from reaching firewalls, routers, or storage arrays.

Additionally, user A could log into switches via SSH and use a traditional username/password or a non-cryptographic two-factor solution such as RSA tokens. This is Level 4 Assurance at the network access layer to control the risk inherent in username/password management access.

Wired controls

While great for agencies that have pervasive wireless access but how are controls extended to a wired network? The most obvious way is to enable 802.1X for wired users as well. Once using 802.1X on switched ports you have 2-factor verification for all users, all connection types. For devices such as printers that may not be capable of 802.1X can exist in a heavily firewalled set of VLANs with no access to critical resources.

In order to segment wired users in 802.1X environments you can send down Role information derived from group membership or other user attributes. If the switch does not support this capability, it is possible to dynamically send a user firewall rule set in the form of a downloadable ACL (dACL). The use dACLs is supported by many newer switches from popular enterprise switch providers.

Worst case you can send down a VLAN assignment using RADIUS and implement access control at the default gateway router.

All of the policy controls described can be utilized by modern RADIUS/TACACS+ servers like the Aruba ClearPass Policy Manager.

New security mandates and bills

The federal government has recently enacted a number of new statutes to improve Federal network security and authorize and enhance the existing intrusion detection and prevention system for civilian Federal networks.

- S.1869 (July 27, 2015) – This Act may be cited as the "Federal Cybersecurity Enhancement Act of 2015".

The guidelines outlines best practices for encryption of login sessions and data, single sign-on, remote access controls, and data storage.

- NIST 800-82 revision 2 – section 5-15 outlines that authorization privileges should be enforced by some access control mechanism.

In general, authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes.

SUMMARY

The days where users freely roam the internal network are over. In addition to multi-factor authentication, Aruba offers traditional layer 3-4 and application firewalling. Security controls can also take into consideration the apps used and websites visited using URL and content categorization.

Policies can be customized to meet per-user requirements and enforced regardless if connecting to wireless, wired or VPN. A two-factor authentication access strategy using these tools can protect your management assets and will serve as the foundation of good network security policy going forward. This also sets the foundation for future device two-factor authentication services.

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com.

To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.

aruba
a Hewlett Packard Enterprise company

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

www.arubanetworks.com