Global Information Assurance Certification Paper

Securing the Corporate WLAN in a Healthcare Regulated Organization

James Pomeroy

RES 5500 GSEC Gold

Abstract

Wireless networks are a crucial component in the technology infrastructures of modern medical practices and have become an enabler of patient services in the healthcare industry.

Healthcare organizations deploy wireless diagnostic devices to provide critical information at the point of care. These devices provide data to medical decision-makers in real time to improve patient outcomes.

One of the challenges of integrating these new devices and services into the wireless networks of medical practices is wireless network security. Wireless networks have inherent risks, ranging from data leakage to availability issues in the event of a DoS (Denial of Service) attack or outage.

It is critical to secure a patient's personal information termed electronic protected healthcare information (ePHI) at all times. Protecting ePHI is a primary goal in designing wireless networks for a healthcare-focused organization. Wireless implementations must be designed to protect patient health information from breach or theft, while at the same time providing needed services to patients and clients.

The primary goal of this research project was to provide a healthcare-focused consulting organization with a secure and compliant wireless network. The network is to enable employee collaboration, facilitate client engagement, and accomplish the primary security goal of protecting the company's ePHI.

Introduction

In the healthcare sector, wireless networks are relied upon to provide critical patient care and client services. The healthcare industry's reliance on wireless networks is increasing at a frenetic pace, with more devices and applications being developed for deployment at the patient point of care (POC) in medical practices. Examples of medicine's reliance on wireless technology include: computerized provider order entry systems (CPOE) that enable healthcare professionals to enter medical orders into applications for direct dispatch to the patient point of care (in both inpatient and mobile medical settings).

Physicians and support staff are utilizing WiFi-connected mobile devices to access EHR (electronic health records) systems to provide immediate access to patient health records. Medical technicians are now able to utilize WiFi-connected portable devices (such as mobile ultrasound units) to more quickly diagnose a patient for treatment.

The challenge in medical practices and in other organizations that support the healthcare industry is that the reliance on wireless networks is complicating the job of protecting patients' personal healthcare information. Wireless networks, though enablers of technology and service, open an organization up to additional vulnerabilities and threats which can lead to the loss or theft of patient data.

The threat to patient data is a pressing one as patient health records currently one of the most lucrative items to sell on the black market. According to a report compiled by the IRTC (Identity Theft Resource Center), in the first half of 2017, 179 breaches had occurred in the healthcare sector. This number makes up 22.6 percent of all U.S. data breaches for the first half of 2017 ("At Mid-Year, U.S. Data Breaches", 2017). The number of individuals affected by the breaches is congruous with the number of healthcare records stolen in the first half of 2016. It

should be noted, however, that the actual number of breaches and affected individuals is probably much higher than reported, as the Department of Health and Human Services (which oversees healthcare security regulation) requires reporting only on breaches of 500 or more records ("At Mid-Year, U.S. Data Breaches",2017). With this in mind, security and infrastructure professionals must design wireless networks for healthcare organizations with the intent of protecting a patient's personal health information. At the same time, it must be relatively simple to enable critical wireless devices access to wireless network resources.

1. Regulatory Environment, HIPAA Background Information

The HIPAA (Health Insurance Portability and Accountability Act) of 1996 was enacted to ensure that the Federal Government develops regulations to protect the privacy and security of electronic protected health information (ePHI). The HIPAA Act is comprised of two primary components: the Privacy Rule, and the Security Rule. The Privacy Rule encompasses the control of who is authorized within an organization to access patient information, how information is handled, and when or if this information may be shared with third parties. The Security Rule specifies the mechanisms used to protect the privacy of patients' health information. The Security Rule covers the operational and technical controls an organization must implement to protect ePHI ("Summary HIPAA Security Rule" 2013).

The HIPAA Act was followed by the HIPAA HITECH (Health Information Technology for Economic and Clinical Health) Act of 2009, which defines the categories for security violations, the breach notification requirements, and the associated penalties to be levied on healthcare organizations that violate the regulations.

Organizations that provide healthcare services such as hospitals and clinics are defined as "Covered Entities" under the HIPAA Act. Entities that provide services to the healthcare

industry and are responsible for the management of ePHI are considered Business Associates. (HIPAA 45 CFR 45 CFR 160.103)

Covered entities and business associates that create, transmit, receive, or maintain PHI (protected health information) on their systems are required to make a good faith effort to protect the enterprise computing environment from anticipated threats, and vulnerabilities. The HIPAA regulatory framework requires the confidentiality, integrity, and security of electronic protected health information ("Breach Notification Rule", 2013).

In January of 2013, the Omnibus Final Rule was released, which included updates from the HIPAA HITECH Act. The Final Rule consists of three main components (sections) that specify the security and privacy requirements for the protection of ePHI. Specifically, Part 164, subpart C (Security Standards for the Protection of Electronic Protected Health Information §164.3xx) (Leyva, 2013). The wireless security design for the healthcare-focused organization described in this document is based primarily on this section.

2. Company Profile and Business Case

The organization whose network design is the basis for this project is considered under the HIPAA and HIPAA HITECH regulations as a Business Associate entity (i.e., the organization does not provide direct patient care). Before the HIPAA HITECH Act of 2009 business associates were not required to comply directly with the Security Rule provisions of the HIPAA regulations. After the enactment of the HITECH legislation, business associate entities are now expected fully to comply with the HIPAA Security Rule and with all the required security safeguards and practices.

The case study organization for this research is a consulting and accounting firm. The company provides financial auditing services to a client base that is comprised primarily of

healthcare entities. The company has an integrated consulting division that provides services to healthcare providers, as well as to health insurance companies. Due to concerns of anonymity, the company's name is not used throughout this research paper.

Due to the amount of ePHI housed on the company's information systems, the company's legal counsel as well as third-party auditors and consultants have recommended that the organization fully comport to the HIPAA regulatory framework (as a covered entity would do). Due to these recommendations, the company's executive management and the CISO have mandated that the company design its security measures in accordance with HIPAA regulatory requirements. With these factors in mind, the company determined that its new wireless environment must be designed and configured according to the HIPAA and NIST regulatory requirements and guidelines.

3. Protecting ePHI in a WiFi-Enabled Enterprise HIPAA Requirements

When determining the security design of the organization's WiFi network, the following question was posed to the internal security team and CISO:

How should a wireless network infrastructure be architected to allow an organization focused on serving the healthcare industry effectively protect electronic protected health information (ePHI) and at the same time enable employees, vendors, contractors, and clients to utilize company wireless resources for essential collaborative services required to produce client deliverables?

The initial research for this project was performed by the IS security team and CISO. As a first step, HIPAA-based policies for wireless network access to ePHI on the corporate network were developed and implemented. The policy documents were the first step in determining the design and security requirements of the wireless network.

To guide organizations in protecting ePHI assets, HIPAA relies on guidance from NIST (National Institute of Standards and Technology) to determine what is required to secure information systems and ePHI assets. The HIPAA Security Rule and HIPAA Privacy rules base many security assumptions on guidelines from NIST.

The HIPAA Security Rule does not have specific standards or guidelines related to securing wireless networks. Instead, the HIPAA regulations defer to NIST guidelines and publications. The challenge with this approach is NIST does not have a single set of documents to cover all aspects of wireless network security. To overcome this, security practitioners may combine NIST guidelines and publications related to different components of wireless network security to create a comprehensive security strategy and architecture for wireless device access to ePHI.

The NIST guidelines affecting wireless network security include, but are not limited to the following NIST publications:

- NIST SP 800-153 Guidelines for Security Wireless Local Area Networks (WLANs) (NIST, 2012)
- NIST Special Publication 800-97 “Establishing Wireless Robust Security Networks A Guide to IEEE 802.11i”
- NIST Special Publication 800-120 “Recommendation for EAP Methods Used in Wireless Network Access” Authentication
- NIST Special Publication 800-92 "Guide to Computer Security Log Management” Logging Requirements
- NIST Special Publication 800-122 Revision 3 Final, “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"

- NIST Special Publication 800-66 Revision 1, "A Resource Guide for Implementing The HIPAA Security Rule"

Many of these documents have direct mappings to HIPAA regulatory compliance regulations while others do not. They are all relevant to designing a secure and complaint wireless network.

Utilized together, the NIST publications and HIPAA requirements in the Privacy and Security Rules can be utilized as a blueprint for defining the security considerations for the organization's wireless network implementation (HIPAA Security Standards: Technical Safeguards, 2007).

4. HIPAA Security Compliant Wireless Network Design Considerations

In any HIPAA-regulated organization, a determinant of the organization's security posture is an initial risk analysis. The HIPAA Security Rule requires healthcare providers and business associates to perform an analysis of potential risks to the security of the ePHI that the organization is responsible for protecting. An organization must then develop, implement, and maintain the appropriate security measures to safeguard the confidentiality, integrity, and availability of ePHI.

When making security design decisions for this project, it was determined by the organization's security committee that the configuration must not only be HIPAA-compliant, but also must provide the highest degree of security for ePHI assets possible. Many design decisions were based on a third-party HIPAA risk assessment that was conducted on the organization's infrastructure. Any gap areas discovered during the risk assessment were addressed in the wireless security design.

The design aspects of a HIPAA-compliant wireless network architecture must address the primary components of the HIPAA Security rule that apply to protecting ePHI. The design does not cover every aspect required of a wireless network to comport to HIPAA regulations. It does however cover the design decisions that an organization should address when deploying a HIPAA-compliant wireless network. The components of the network design detail how the organization implemented specific HIPAA requirements.

4.1 Security Design Components

The specific design components integrated into the infrastructure are a result of annual HIPAA Risk Assessments. The components are broken down in this document as follows:

- **Identity and Access Management**
  - Wireless LAN Policy Management
  - Authentication and Access Methods
  - Role-Based Access Control (user role in organization)
  - Device Identity-Based Access (controlling permitted devices)
  - Device Profiling
  - Wireless Network Access Requirements
- **Network Authentication and Access Control**
  - Initial Access to Wireless Networks
  - Employee Laptop Access Wireless and ePHI 802.1x Authentication
  - Captive Portal with Active Directory Authentication BYOD access
  - Guest Access
- **WLAN Segmentation and Firewalling**
  - Network Segmentation

  - Firewalling Wireless Connections
  - Wireless Access Control and Device Profiling
- **Encryption and Data Protection**

4.2 Infrastructure Components

The systems chosen for this implementation were determined through a request for proposal (RFP) and proof of concept (POC) process. The company's security team reviewed and tested components from various vendors. The components devices were chosen based on the architectural and security needs of the organization.

Designing a wireless production network has many considerations, including redundancy, RF spectrum management, sizing, etc. The infrastructure components listed below are specific to the HIPAA wireless security design for this project:

- Aruba 7210 hardware-based wireless controllers in an active-passive redundant pair
- Aruba ClearPass CPPM (ClearPass Policy Manager) for network access control
- Cisco 3850 PoE Stackwise switching systems for AP to Ethernet connectivity
- Cisco 9000 Series Layer 3 switching systems – routing and core switching
- PaloAlto PA 3020 firewalls in an active-passive pair
- Microsoft PKI for certificate services
- Microsoft Active Directory for WiFi policy control and role-based access

The HIPAA Security Rule contains security objectives and protections. The rule is intentionally technology-neutral. This provides organizations the flexibility to choose the specific technologies they want to use in order to comply with the regulations. The Security Rule provides standards, and in some instances also provides specifications with which covered entities and business associates must comply.

This wireless security implementation, though not vendor-agnostic, may be implemented using similar components from different vendors. A diagram of the HIPAA Compliant WLAN Design – Base Overview can be found in Appendix A. Pg.64

4.3 Wireless Network Requirements

The wireless network must provide access to multiple types of client devices in addition to providing for different user access requirements. The network access requirements are based on the role of the user and the need to access ePHI.

The following wireless networks were defined for the initial deployment:

- Private Network – required for all corporate endpoint devices running the Windows 10 operating system and Microsoft Active Directory joined. Access to this network is to be controlled via 802.1x authentication in conjunction with multifactor authentication (MFA).
- Guest Network – required for the company's clients to use when onsite for business activities. Clients are primarily healthcare practitioners.
- Contractor Network – required for contractors on-site working on company hardware or software systems. Firewall rules for this network and access roles are not static, but are defined on a per engagement basis. Access to this network is to be controlled via captive portal technology
- BYOD Network –required for end-user iOS and Android-based devices as well as Microsoft Surface devices provided by the company.
- Administrative Network – required for devices that are not active directory joined, do not have access to ePHI network segments, and are needed for administrative functions.

Other networks are to be added after stress testing and security testing of the initial deployment. Due to Aruba Network's GRE-tunnel best practices, a maximum of three SSIDs were to be used in the wireless network configuration. Using more than three GRE-tunneled SSIDs would degrade performance, and add complexity to the design (Aruba, 2010).

5. Identity and Access Management

The HIPAA Security Rule safeguards place a high degree of emphasis on identity management, authentication, and authorization. HIPAA Title II contains an Administrative Simplification section; this section is where the base security requirements for protecting ePHI are specified.

NIST's publication, "NIST SP 800-66 Revision 1, Technical Safeguards 4.14.Access Control (§164.312(a)(1))" specifies the requirements for allowing access to ePHI. The HIPAA Security Rule stipulates that identity management must be used to identify and track all user access to ePHI, that all users have unique user IDs, and that all access to ePHI can be traced to specific users. These specifications were used as inputs for the security and authentication design.

5.1 Wireless LAN Policy Management

Access policy and authentication in this wireless security design are controlled by utilizing a centralized policy server to manage and control access to wireless network resources.

The policy server used in the network design is the Aruba Clear Pass Policy Manager (CPPM). The Aruba CPPM is an authentication and authorization control server with captive portal capabilities. The server can integrate with multiple directory services databases for user and group authentication and authorization.

Users, groups other objects from directory services servers (such as Microsoft Active Directory) are used as inputs to comprise roles on the authentication server and the wireless network controllers (termed mobility controllers in an Aruba-based architecture).

For Non-Active Directory Services authentication (such as guest users), a local user account database with onboarding capabilities is used to create role-based access control to guest wireless resources.

Instructions sent from the policy server to the wireless mobility controllers are used to manage and control all endpoint or user access on the wireless network. The mobility controllers are also used for internal network segmentation and firewalling between network segments.

The CPPM can use multiple authentication and authorization types. For example, the system can use the TACACS protocol to control access to the management plane (as it does in this design) and use the RADIUS protocol for authenticating users to the WLAN (also used in this design).

By using a central policy management server, all wireless access can be managed from a central administrative point in the security architecture. This allows a single security team to manage the wireless security policies, firewall configurations, and authentication mechanisms. All authentication and access requests for the wireless network are logged and tracked on the policy manager. Centrally logging authentication and access enables an organization to track every device and user in the wireless environment. The HIPAA Security Rule requires that all user access to ePHI is tracked and logged.

5.1.1 Wireless Policies

Wireless policies on the CPPM policy server are comprised of multiple components to enable administrators to control endpoint access decisions. The policy server construct that

controls access to the wireless network is termed a “Service”. Services are comprised of different object components that control user and device access to the network. The Service portion of the policy shown in Figure 1 is designed for wireless network authorization, and for profiling endpoint devices. Conditions within the Service determine what conditions the rule initially checks to begin the access decision process.

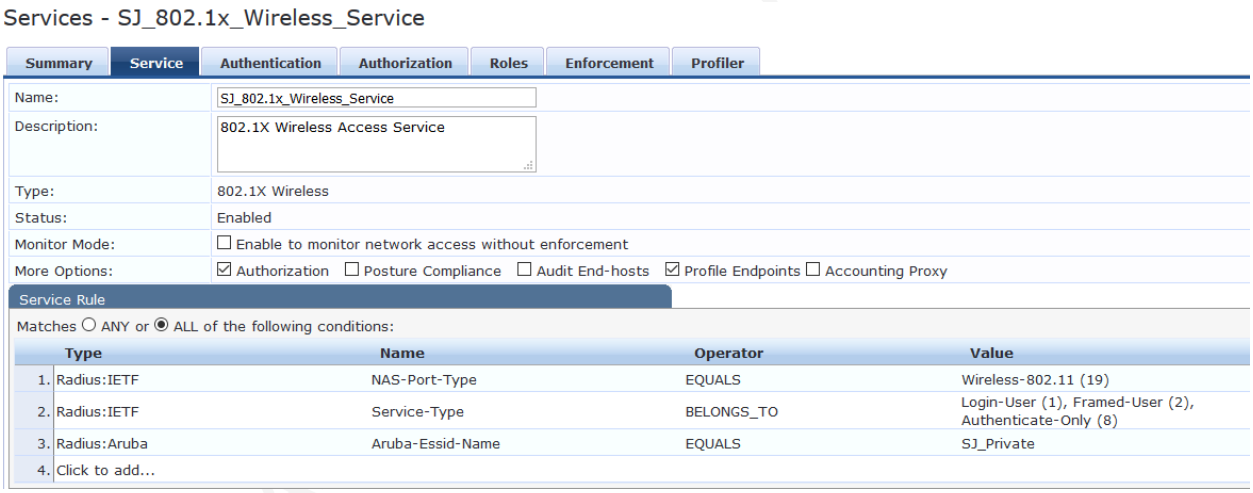


Figure 1: Wireless Service for 802.1x Service Component

Each Service consists of the following: service rules, authentication sources (such as the guest user repository for local authentication or Microsoft Active Directory), authorization methods, roles (user and device roles), enforcement policy rules and profiler endpoint classifications.

An example of the Enforcement Policy in a policy server Service

Policy enforcement is based on roles (machine and user) for role-based authentication, authorization, and network traffic control. The enforcement policy for the employee 802.1x authenticated network is shown in Figure 2. The rules are processed from top to bottom, just as firewall rules are processed.

Services - SJ_802.1x_Wireless_Service

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: SJ_Wireless_802.1x_Enforcement_Policy [Modify] Add new Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS SJ_Wireless_Admin_Role) AND (Tips:Role EQUALS [User Authenticated]) AND (Tips:Role EQUALS [Machine Authenticated])	SJ_Wireless_Domain_Admin_Enforcement_Profile, [Update Endpoint Known], SJ_Update_Domain_Endpoint_Information, [Aruba Terminate Session]
2.	(Tips:Role EQUALS [Machine Authenticated]) AND (Tips:Role EQUALS [User Authenticated])	[Update Endpoint Known], SJ_Wireless_Domain_Enforcement_Profile, SJ_Update_Domain_Endpoint_Information
3.	(Tips:Role EQUALS SJ_Wireless_Device_Role) AND (Tips:Role EQUALS [User Authenticated])	[Update Endpoint Known], SJ_Wireless_Domain_Enforcement_Profile, SJ_Update_Domain_Endpoint_Information
4.	(Tips:Role EQUALS [Machine Authenticated])	SJ_Wireless_Machine_Enforcement_Profile, [Update Endpoint Known], SJ_Update_Domain_Endpoint_Information
5.	(Tips:Role EQUALS [User Authenticated])	[Deny Access Profile]

Figure 2: Wireless Service for 802.1x Enforcement Polices

5.2 Role-Based Access Control Requirement

One of the requirements for the network design was the enforcement of RBAC (role-based access control) for all wireless network access (including guest and contractor access).

With role-based access control, users from a directory services environment such as Microsoft Active Directory or other authentication database sources are used to populate wireless access roles on a wireless policy server.

The use of roles in the environment is predicated on the requirement that the organization matches a user's network access with the user's file system access to ePHI. Roles based on user group enable the organization to control user access to ePHI via Active Directory group membership. It must be noted that RBAC is not a HIPAA requirement. However, role membership may be considered a component of identifying a group of users who have access to ePHI, and users in a role may be identified by their AD group membership.

For a user to be added to the membership of an AD security group with ePHI access, a principle (manager or partner) in the department that owns the ePHI data must sign off on a change control document permitting the user to attain group membership. With role-based access, the wireless administrator does not have to manage role/group membership. Instead, this

task will be delegated to a Help Desk technician. This process must also be followed in the case of new employee onboarding.

In this implementation, user's group-based roles are components of the wireless Services on the policy server. The Service rules are used to make decisions about what network a user is placed on and what firewall set is applied to the user's connection. Roles are also mapped to user groups that either are or are not permitted to have access to ePHI to control network access.

The Aruba policy server natively implements a role-based access scheme to authenticate users and devices. Roles are used as a component of the wireless Services. Wireless services are the top-level object in the rule configuration on the policy manager. Roles are key to the Service operation on the management server.

5.3 Device Identity-Based-Access

In an environment with ePHI to protect, it is incumbent on the security design not only to track which users are connecting to the environment, but also to determine what types of devices are accessing the network.

Devices that are not secured by the company's security team, or controlled by the company must be segregated from internal network segments that contain sensitive information. These unmanaged devices may contain rogue applications, and are not be protected by the company's security tools. It is incumbent on an organization protecting ePHI to shield network segments from unmanaged devices.

In a wired network, devices connect to resources in what is termed a "fixed edge" (users connecting a device with a network cable plugging into a switchport). In a fixed edge environment, device access security is applied at the switch port level to prevent unauthorized devices from connecting to the company's resources.

Secure connections to the wired network are controlled by a policy server and an 802.1x authentication process. In other organizations, standard port security on access layer switches may be used to lock a device's physical address to a particular switch port.

In wireless networks, users and devices seeking access to a network's resources and applications are not connecting to a fixed port. Because devices roam and are not statically connected, the network must be able to identify and track every user and device attempting to gain access to company resources and ePHI. Access policies are then applied to device/user combinations. This concept termed identity-based network access by Aruba is a crucial component of the authentication and authorization process for the wireless network design. Device Identity-based network access used in conjunction with device profiling enables the wireless policy server and controllers to track and trace every device on the wireless network and provide an audit trail.

Device identities are combined with user and machine roles on the policy server to control access at a granular level. To identify a device, it is necessary to profile that device.

5.4 Device Profiling

A primary component of identity-based access is the profiling of end-user devices and device attributes. Device profiling enables the policy servers to classify end user devices based on factors such as operating system, device type, hostname, etc. Profiling devices allow the security of the wireless network to be more granular and controlled.

Figure 3 illustrates the ability of the policy manager to profile connected devices. The devices shown are from the pilot of the production network for this project.

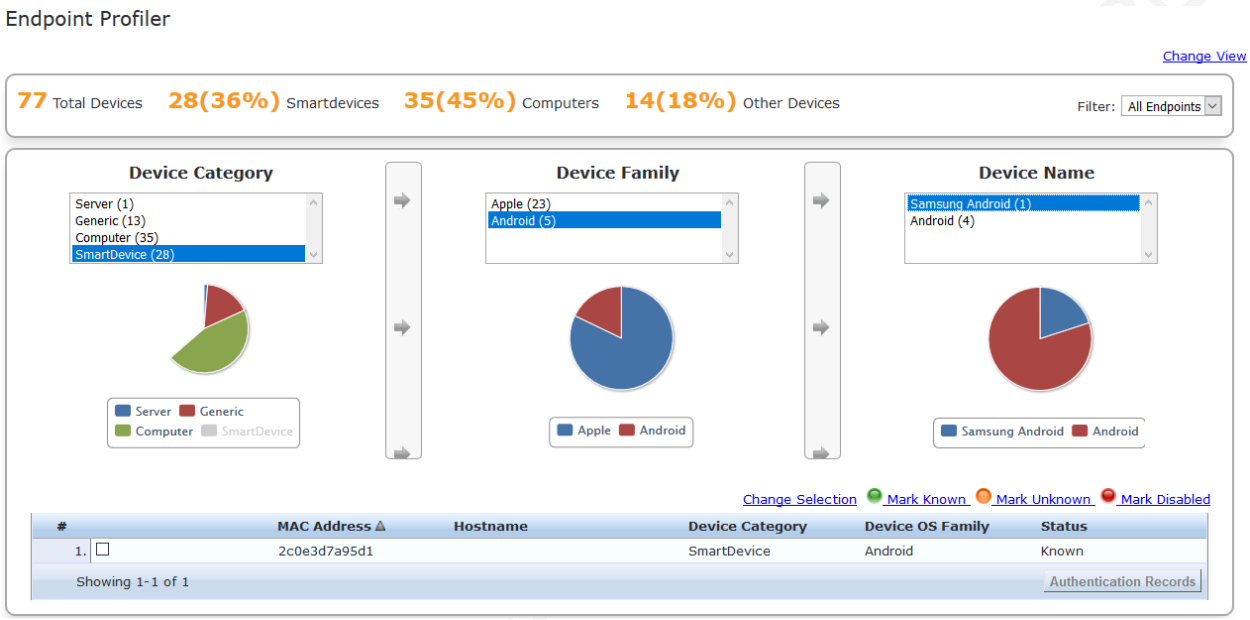


Figure 3: Endpoint Profiler Example.

The policy manager profiles devices by Device Category (computer, smart device), Device Family (operating system), and Device Name (hostname if available and resolvable via DNS).

Attributes are gleaned from operating system behavior detected by the policy server (operating system, version and services). Device fingerprinting is performed by comparing device attributes to attributes in the device profile database on the policy manger server.

Additional device attributes may be customized by an administrator and associated with devices (in the policy server database) when the device connects to the wireless network. These custom attributes allow for additional control of traffic and access management. In this environment, a custom attribute is added to corporate laptops as they join the network. The attribute is then used to match a rule condition to prevent corporate devices from joining the guest or BYOD networks.

With an understanding of identity-based access for authentication and authorization, the authentication and authorization design of the primary corporate network connecting to ePHI resources is next broken down.

5.5 Wireless Network Access Requirements (Devices and Users)

To properly segregate user roles and access to ePHI, and to control traffic to networks and applications for non-healthcare related network segments, the design breaks down the authentication and access methods (used in conjunction with role-based authentication) into three primary network and authentication / access types as follows:

- **802.1x authentication** – mutual authentication (machine and user) with multifactor authentication (MFA) as an authentication component.
- **Captive Portal with Active Directory** authentication (contractors, administration, BYOD devices, etc.)
- **Captive Portal with Local Authentication** (authentication from local database for guest access)

Each of these authentication requirements / methods are mapped to a wireless SSID advertised on the network. A maximum of three SSIDs are used to advertise company networks.

From an encryption and security standpoint, each SSID requires a separate GRE tunnel from the AP the endpoint is connecting to, through to the wireless mobility controller. Using more than three GRE tunnels could possibly cause performance issues on the mobility controllers (Aruba, 2010). Additionally, using more than three SSIDs in the environment was deemed confusing to the user population using the wireless network. This was determined by user feedback to the IS department Help Desk.

Figure 4 below shows connected clients on a wireless controller. The client device connections shown are connected to either the captive portal (for non-ePHI network access), or to the network segment containing ePHI via 802.1x.

Search Results

Clients All | IPv4 | IPv6 |

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
miller	iPhone	dc:0c:5c:9a:2a:da	10.0.92.25	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
grindle	iPhone	ac:fd:ec:11:01:ff	10.0.92.34	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
karmazin	iPhone	7c:04:d0:74:8d:37	10.0.92.140	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
jjohnson	Android	2c:0e:3d:7a:95:d1	10.0.93.103	SJ_Employee_BYOD_Admin_Role	MAC	SJ_Mobile
eitzmann	iPad	bc:ec:5d:11:d4:03	10.0.92.144	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
green	iPad	70:48:0f:a0:ab:45	10.0.92.31	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
SJSQ\HOFFMAN	Win 10	e4:a7:a0:64:6e:64	10.0.91.159	SJ_Employee_Domain_Role	802.1x	SJ_Private
suiter	iPhone	dc:a9:04:cc:0d:9b	10.0.92.22	SJ_Employee_BYOD_Role	MAC	SJ_Mobile
ahaluska	iPhone	dc:0c:5c:dc:18:76	10.0.93.100	SJ_Employee_BYOD_Admin_Role	MAC	SJ_Mobile
SJSQ\jshurtliff		e4:a7:a0:64:4e:0c	10.0.91.29	SJ_Employee_Domain_Role	802.1x	SJ_Private

Figure 4: Wireless Controller Logging Output

6. Network Authentication and Access Control

6.1 Initial Access to Wireless Networks

All wireless networks in the environment utilize WPA2 authentication with AES encryption for device association with the wireless access points in the environment. This scheme is used in conjunction with GRE tunneling from the access point to the controller (at layer2) to ensure encryption on all wireless traffic from the endpoint to the mobility controller.

The 802.1x authenticated network used for corporate portable computers uses WPA2 Enterprise. Captive portal-based SSIDs utilize WPA2-Personal for the initial connection and association with the captive portal. From that point, user identification and network access control is performed by a captive portal in conjunction with RADIUS authentication.

6.2 Employee Laptop Access, Wireless and ePHI 802.1x Authentication

In this design, only one employee facing wireless network SSID provides access to ePHI; all other wireless networks are segregated via policy, captive portal, and firewall rules from accessing any network segment containing ePHI.

However, certain groups of users who are non-employee users may have cause to access ePHI under certain circumstances. Examples include healthcare clients, and software and hardware consultants. Access for these users can be enabled temporarily if needed by applying a specific firewall rule set to the wireless access policy associated with the user's role when connecting. The access for these users is detailed in section 6.3.5 ePHI Access Exceptions with Captive Portal.

Company-owned laptop computers are required by policy to use 802.1x authentication to connect to company owned wireless resources and ePHI. 802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides a centralized authentication framework for client devices to authenticate to wired and wireless networks (Aruba, 802.1x Auth, 2017) 802.1x authentication enables the centralization of policies, access, and device management in the wireless infrastructure. The Aruba policy manager manages the 802.1x authentication process in the design used in this research.

6.2.1 Employee Laptop Access Requirements

The requirements defined by the company's IS Security Committee for corporate laptop wireless access to ePHI, internal facing applications, and other data are as follows:

- Wireless network access to company resources must be seamless to the user, i.e. users must not be required to use MFA tokens or smart cards to access the wireless network.
- Multifactor authentication (MFA) is a requirement for corporate device access to networks containing ePHI.
- Active Directory (AD)-joined laptops must be automatically joined to the primary company SSID without requiring user interaction.

- Access to ePHI wireless networks must be monitored and logged at all times through the wireless policy server. These logs are to be forwarded to the company's SIEM device for log archiving.
- Company AD joined laptop computers are not permitted to connect to any other wireless networks at the company location. The devices must be prevented from connecting to the guest or mobile (BYOD) networks by policy.
- Company laptops must be prevented from bridging network connections between wired and wireless networks.
- Company AD-joined laptops must be able to connect to non-company wireless networks when off premise (such as at a client's site).
- Encryption must be enforced from the endpoint through to the wireless controllers. The controllers terminate network connections in the data center.

6.2.2 Accounts Database and Device Attributes

In the company's network environment, Windows Active Directory is the primary user accounts database. Therefore, AD was the best choice to integrate with the policy server for computer and end user authentication. User and device attributes from Active Directory are used by the policy server to make wireless network authentication and authorization decisions.

Controlling access to the wireless networks, the policy server utilizes the following user and computer attributes from Active Directory in conjunction with digital certificates:

- Computer AD group membership (defines company-owned device)
- User Group Membership (defines network access for the user)
- User Account (end user authentication)

These attributes are specified in the policy server's service rule configuration. Matching these attributes determines what network access the user is granted.

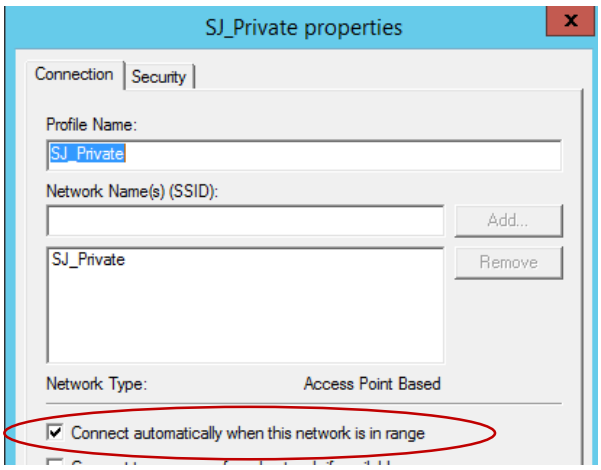
6.2.3 Active Directory Wireless Policy

In order to manage the wireless configurations on company-owned laptops centrally, the Active Directory group policy was used to specify wireless 802.11 policies. The wireless security configuration for connecting to the company's private network was specified in the policy. This was then deployed to the organizational units containing the company's laptop computers.

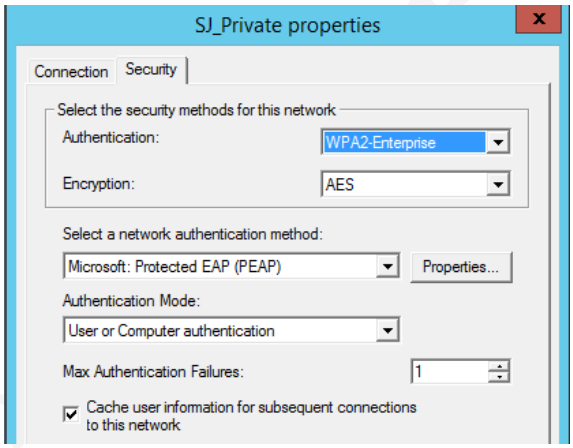
The policy consists of attributes that match up with the requirements for network access on the Aruba CPPM policy server. The policy specifies the authentication and encryption methods, as well as the network authentication methods. PKI certificate authorities that are trusted along with the handling of mutual authentication between clients and the policy server are also components of the policy. Appendix C. Pg. 72 contains a full breakdown of the Active Directory Wireless Policy used.

To enable corporate wireless endpoints to connect automatically to the wireless network when on premise the 'Connect automatically when this network is in range' is set in the policy, as seen in Figure 5 below.

Figure 5: Active Directory Policy Attributes



Authentication and encryption methods deployed in the wireless group policy (WPA2-Enterprise with AES). The authentication method is Microsoft Protected EAP (PEAP).



PEAP properties include server certificate verification for mutual authentication between client and server (policy server) Figure 6.

Trusted root certificate authorities are specified for the connection as well as attributes to warn the user if there is an issue with the server certificate or certificate authority. Note: both internal and external certificate authorities are used in the wireless security design.

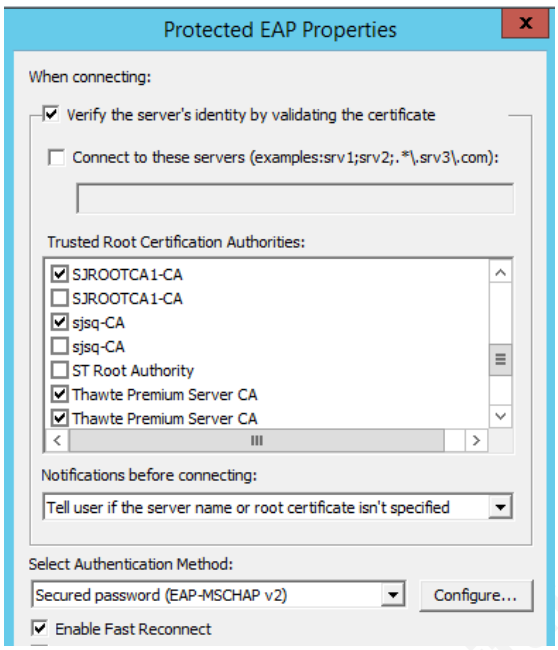


Figure 6: PEAP Properties of AD Group Policy

6.2.4 Authentication Sequence with the Policy Server (Machine and User Authentication and Authorization)

In order to ensure the security ePHI when company laptop computers connect, multiple authentication steps are required for a laptop and user to access a wireless network segment containing ePHI. This includes the use of multifactor authentication to meet the HIPAA security requirements for connecting to ePHI over a non-trusted network. In this configuration, the machine account (company laptop) performs the initial authentication step. Once the machine is authenticated to the policy server, user authentication may take place.

The decision to have both the laptop and the user authenticate in separate phases of the authentication sequence was made for security and manageability reasons. The machine portion of the authentication sequence utilizes multi-factor authentication (process detailed in section 6.2.5) and performs the initial association with the wireless access point. The user authentication component determines what network and firewall set the connection acquires from the policy server.

Additionally, computer authentication enables the policy server to identify the computer as an AD-joined company laptop. This ensures that only company owned AD-joined computers can connect to a wireless network that has access to ePHI.

The diagram below Figure 7 details the roles and steps in the authentication process for a company laptop and user to access a wireless network segment with access to ePHI. This diagram is also located in Appendix B. Pg.69

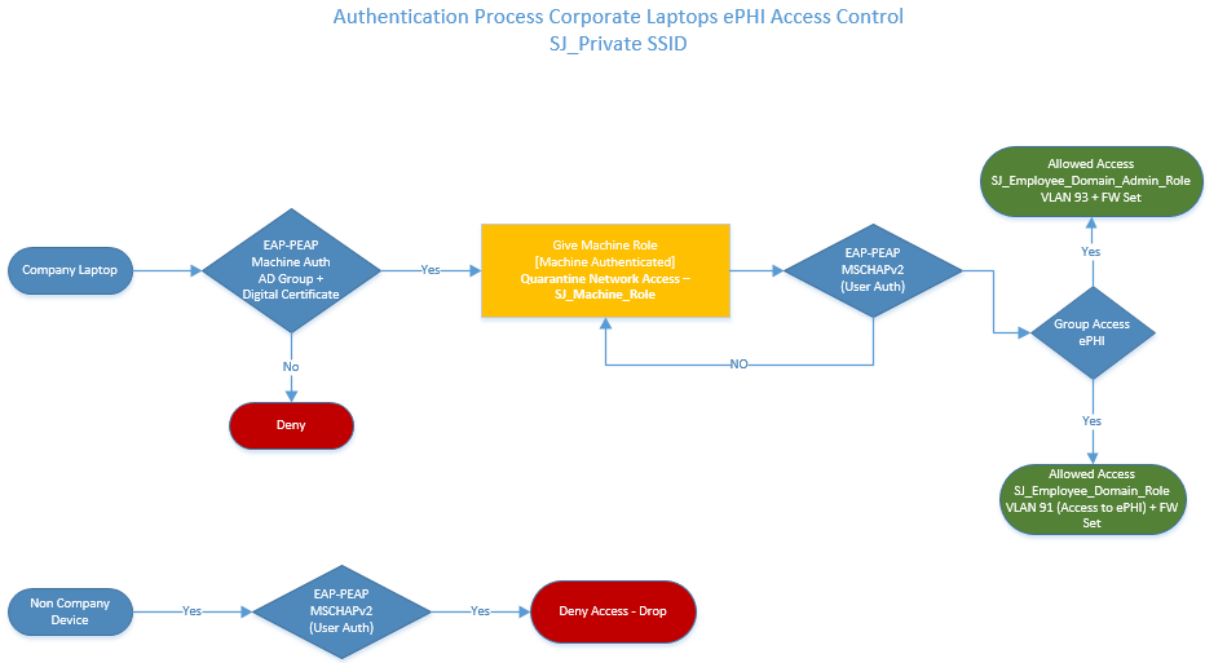


Figure 7: Authentication Process Corporate Laptops ePHI Access Control SJ_Private SSID

6.2.5 Machine Authentication

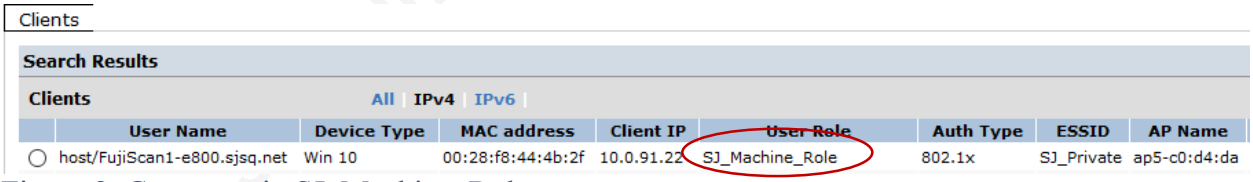
In the first phase of authentication, a company laptop connects to the wireless network (SJ_Private). This SSID is used to access internal networks with AD-joined laptop computers.

The policy server first authenticates the computer account via Active Directory. The computer's Active Directory group membership is queried by the policy server to make network access decisions.

Next, the computer's digital certificate is verified. The policy server verifies that the client certificate is deployed from the company's certificate authority, is valid, and that the hostname on the subject attribute is for the connecting machine.

If these attributes are correct and the digital certificate is valid, the computer is permitted to associate with the wireless network. The computer is then given the role: SJ_Machine_Role. In this role, the User Name attribute of the connection on the mobility controller log is the name of the computer that is connected as shown in Figure 8.

A machine in the SJ_Machine_Role is placed on a firewalled-VLAN with limited network access. Output from the wireless mobility controller's client monitor log after machine (computer) account authentication.


Clients

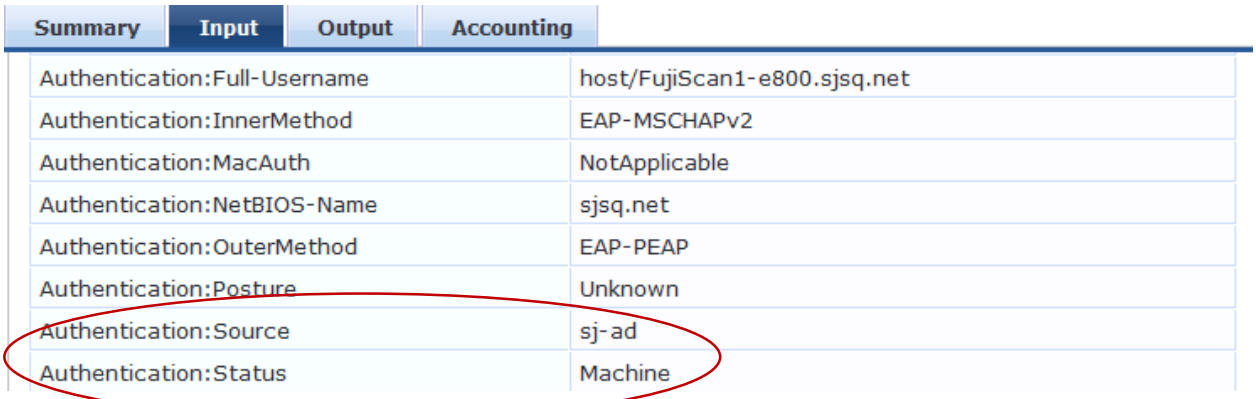
Search Results

Clients All | IPv4 | IPv6 |

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID	AP Name
host/FujiScan1-e800.sjsq.net	Win 10	00:28:f8:44:4b:2f	10.0.91.22	SJ_Machine_Role	802.1x	SJ_Private	ap5-c0:d4:da

Figure 8: Computer in SJ_Machine_Role

Attributes from the wireless policy server log are shown for a computer during the computer authentication phase of corporate machine wireless authentication. The authentication source sj-ad is mapped to an ldap connection on the policy server to the company's Active Directory domain controllers. The Authenticaton:Status is Machine at this point.


Summary | Input | Output | Accounting

Authentication:Full-Username	host/FujiScan1-e800.sjsq.net
Authentication:InnerMethod	EAP-MSCHAPv2
Authentication:MacAuth	NotApplicable
Authentication:NetBIOS-Name	sjsq.net
Authentication:OuterMethod	EAP-PEAP
Authentication:Posture	Unknown
Authentication:Source	sj-ad
Authentication:Status	Machine

The log output from the policy server Figure 9 shows the successful authentication of a computer (phase one for corporate machines). The Login Status ACCEPT shows that authentication for the connecting computer is completed.

#	Server	Source	Username	Service	Login Status
1.	10.0.4.183	RADIUS	host/FujiScan1-e800.sjsq.net	SJ_802.1x_Wireless_Service	ACCEPT

Figure 9: Output from ClearPass Policy Server Log for Authenticated Computer Account.

If the computer account does not have the proper AD group membership or if the computer's digital certificate is missing or has expired, the machine will be denied connection to the network and will be placed in a REJECT Login Status. The output of the policy server log during an authentication failure is shown below in Figure 10.

#	Server	Source	Username	Service	Login Status
1.	10.0.4.183	TACACS	pomeroy	SJ_CPPM_Login_Service	ACCEPT
2.	10.0.4.183	RADIUS	host/GBlum-zg3.sjsq.net	SJ_802.1x_Wireless_Service	ACCEPT
3.	10.0.4.183	RADIUS	host/JJOHNSON-ZBOOK.sjsq.net	SJ_802.1x_Wireless_Service	REJECT

Figure 10: Output from ClearPass Policy Server Log for a Rejected Computer Authentication Attempt

6.2.6 User Authentication

In the second phase of wireless network authentication for company-owned computers, user account authentication takes place when a user logs into their computer. If the computer is not connected to a wired connection, the user's credentials are passed to the wireless policy server automatically for authentication to the wireless network. User authentication to the wireless network also occurs when a user disconnects from a wired connection, and manually connects to the SJ_Private wireless SSID.

If the user is already logged on into a laptop and then the user connects to the SJ_Private SSID, the users Windows credentials are passed through to the policy server only after disconnection from a wired network connection. This mechanism is in place to prevent users

from bridging network connections between wired and wireless networks. This bridging prevention is controlled via an endpoint security agent on the laptop.

Shown below in Figure 11, is the log output from the policy server showing a successful login attempt by a user account.

#	Server	Source	Username	Service	Login Status
1.	10.0.4.183	RADIUS	host/pomeroy-z3g.sjsq.net	SJ_802.1x_Wireless_Service	ACCEPT
2.	10.0.4.183	RADIUS	SJSQ\jwhippet	SJ_802.1x_Wireless_Service	ACCEPT
3.	10.0.4.183	RADIUS	SJSQ\jwhippet	SJ_802.1x_Wireless_Service	ACCEPT

Figure 11: Output from ClearPass Policy Server Log for a Successful User Authentication

Attributes from the wireless policy server log are shown for a user during the user authentication phase of corporate machine wireless authentication. The Authenticaton:Status is User.

Authentication:Full-Username	SJSQ\jwhippet
Authentication:InnerMethod	EAP-MSCHAPv2
Authentication:MacAuth	NotApplicable
Authentication:NetBIOS-Name	SJSQ
Authentication:OuterMethod	EAP-PEAP
Authentication:Posture	Unknown
Authentication:Source	sj-ad
Authentication:Status	User
Authentication:Username	jwhippet
Authorization:Sources	sj-ad

Once the user and computer have authenticated, the policy server then checks the AD group membership of the user to determine on which VLAN the user should be placed.

The sequence below (Figure 12) shows the decision process after machine authentication has taken place and during user authentication. Currently there are two user groups with different access to ePHI on the network. The SJ_Employee_Domain_Admin_Role has expanded access to the ePHI networks. The full process is detailed in Appendix B. Pg.69

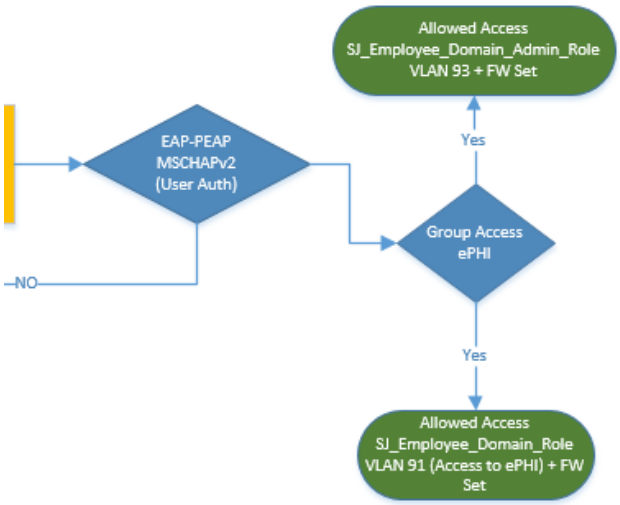


Figure 12: User Authentication Sequence (post machine authentication and authorization)

This authentication sequence is used whenever an AD joined company device or user connects to the wireless infrastructure. All user access is tracked on the wireless mobility controllers as well as on the policy server.

The log output from the controller client-tracking database Figure 13 shows completed connections. The users with the role SJ_Employee_Domain_Role applied are placed on VLAN 91 (network 10.0.91.0/24), with a firewall set applied to the connection. This network has access to ePHI.

Search Results

Clients All | IPv4 | IPv6

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID	AP Name
pomeroy	Win 10	cc:3d:82:85:a4:b2	10.0.93.112	SJ_Employee_BYOD_Admin_Role	MAC	SJ_Mobile	ap6-c0:d5:5c
SJSQ\austin	Win 10	e4:a7:a0:3f:79:24	10.0.91.149	SJ_Employee_Domain_Role	802.1x	SJ_Private	ap7-c0:d5:38
SJSQ\HOFFMAN	Win 10	e4:a7:a0:64:6e:64	10.0.91.159	SJ_Employee_Domain_Role	802.1x	SJ_Private	ap2-c0:d6:28

Figure 13: Mobility Controller Clients Mapped to SJ_Employee_Domain_Role

6.3 Captive Portal with Active Directory Authentication BYOD access

6.3.1 BYOD Network Access and Requirements

The BYOD network was designed to accommodate wireless network access for devices that are not Microsoft Active Directory joined. The devices are, however, authenticated and connected by using the Active Directory accounts database for user authentication.

The SSID for this network is SJ_Mobile. All wireless network access on this SSID is controlled using captive portal technology. After initially connecting to the SSID, the user is presented with a captive portal web page in their browser. The user then simply logs in with an Active Directory username and password and agrees to the terms of service for the network. Access decisions as to what network to place the user on, as well as the firewall set applied to the connection, are made by the Aruba CCCM policy server.

The authentication and access decisions made by the wireless policy server are based on the Active Directory group membership of the connecting user. This enables devices such as mobile phones, tablets, and a contractor's personal laptop to connect to the wireless environment. Contractors are provided with a Microsoft Active Directory login and password for the duration of the time of their engagement with the company.

This network is designed for controlled wireless access for contractors, employee BYOD devices, and Administrative devices. It is also designed to scale out as different access needs are identified. The devices connecting by default do not have access to ePHI based on the VLAN and firewall rules applied to their connections.

The organization decided on captive portal for reasons of scalability, control, and the ability to properly firewall and segment a user's traffic based on the user's identification. By making access control decisions based on user id (AD user and group membership attributes), connections to specific network segments can be attributed to the user making the connection. This enables the connection tracking to be compliant with the HIPAA requirements for identity and access management, as well as network segmentation.

6.3.2 Captive Portal Authentication and Authorization Process

The diagram below (Figure 14) shows the workflow designed for captive portal network connectivity for wireless clients. At each step of the process, all connections are fully encrypted to the wireless controllers. The firewall sets applied at each role phase of the connection protect ePHI from access. A larger scale diagram is located in Appendix B. Pg.70

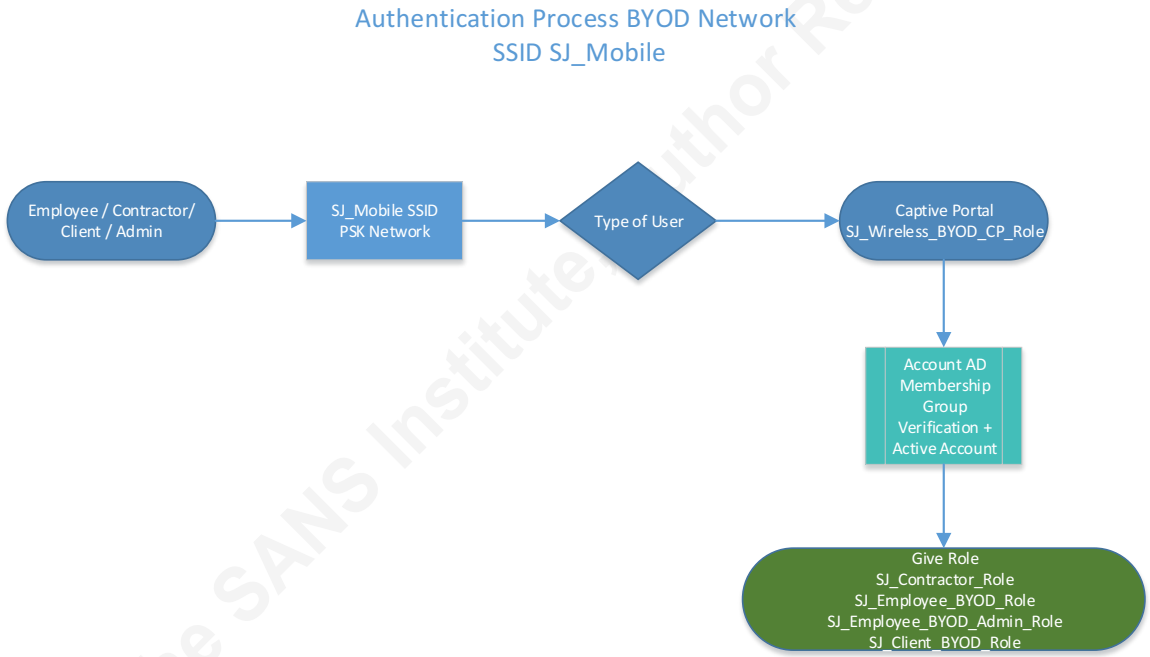


Figure 14: Authentication Process for BYOD Network

6.3.3 Captive Portal access controls

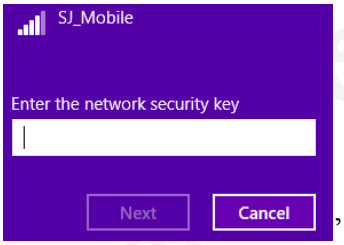
In some organizations, captive portals are designed with open access, allowing any device to connect to a login portal without an initial authentication requirement. The issue with this approach is that traffic sent between the endpoint device and the wireless access point is not encrypted. This is a major security problem with open access point usage.

To ensure the security of all aspects of the captive portal login process, and to accommodate multiple device types, WPA2 personal is used for the initial association between the connecting host machine and the wireless AP. With WPA2 personal, the user must input a shared password when connecting to the SSID prior to logging into the captive portal. This use

of a shared password enables the negotiation of an encrypted connection between the user's device and the wireless access point.

The example that follows is for a Contractor user; all other network access via employee mobile BYOD devices, Administrative users, and clients follows the same workflow and process, resulting in different access controls based on the user role assigned to the user after authentication.

The connection is initiated by a user connecting his or her device to the SJ_Mobile SSID. Once this connection is initiated, the user is prompted for a shared password. This shared password only permits the device to connect to the AP and allows it to be placed on a segregated VLAN with the default firewall set applied.



The default firewall set only allows the machine access to basic services in order to connect to the captive portal webpage. The policy server manages the initial WPA2 personal connection to the AP and places the connecting machine in a role on the controller. The initial role for any captive portal device that has not been user-authenticated is SJ_Wireless_BYOD_CP_Role

Mobility Controller log output from initial connection of a contractor device. The device has an IP on the default captive portal network (10.0.92.0/24). Note: the mac address for the computer is the username at this point (Figure 15).


Clients

Search Results

Clients All | IPv4 | IPv6

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID	AP Name	Phy Type
60:67:20:c2:01:bc	Win 8	60:67:20:c2:01:bc	10.0.92.148	SJ_Wireless_BYOD_CP_Role	MAC	SJ_Mobile	ap6-c0:d5:5c	802.11a-HT
suiter	iPhone	dc:a9:04:cc:0d:9b	10.0.92.22	SJ_Employee_BYOD_Role	MAC	SJ_Mobile	ap9-c0:d5:a4	802.11a-VHT
abaluska	iPhone	dc:0c:5c:dc:18:76	10.0.93.100	SJ_Employee_BYOD_Admin_Role	MAC	SJ_Mobile	ap6-c0:d5:5c	802.11a-VHT

Figure 15: Phase One Computer Authentication BYOD Network

The initial BYOD network firewall rules are applied to the connection to enable the device association with the network. This permits DHCP and DNS access for the wireless client (Figure 16).

Rules

IP Version	Source	Destination	Service/Application	Action	Log	Mirror
IPv4	user	any	udp 68	deny		
IPv4	any	any	svc-icmp	permit		
IPv4	any	any	svc-dns	permit		
IPv4	any	any	svc-dhcp	permit		
IPv4	any	any	svc-natt	permit		
IPv4	any	169.254.0.0 255.255.0.0	any	deny		
IPv4	any	240.0.0.0 240.0.0.0	any	deny		

Figure 16: Initial Firewall Rule Set SJ_Wireless_BYOD_CP_Role

Another firewall set is also applied (Figure 17). This firewall set enables the captive portal connection so that the user may login. The firewall sets on the connections are cumulative and work together to permit connectivity to resources required at this stage of authentication.

Rules

IP Version	Source	Destination	Service/Application	Action	Log	Mirror	Queue
IPv4	user	controller	svc-https	dst-nat 8081			Low
IPv4	user	any	svc-http	dst-nat 8080			Low
IPv4	user	any	svc-https	dst-nat 8081			Low
IPv4	user	any	svc-http-proxy1	dst-nat 8088			Low
IPv4	user	any	svc-http-proxy2	dst-nat 8088			Low
IPv4	user	any	svc-http-proxy3	dst-nat 8088			Low

Figure 17: Secondary Firewall Set SJ_Wireless_BYOD_CP_Role

The user is then presented with a login web page. The user input their AD credentials (Figure 18).

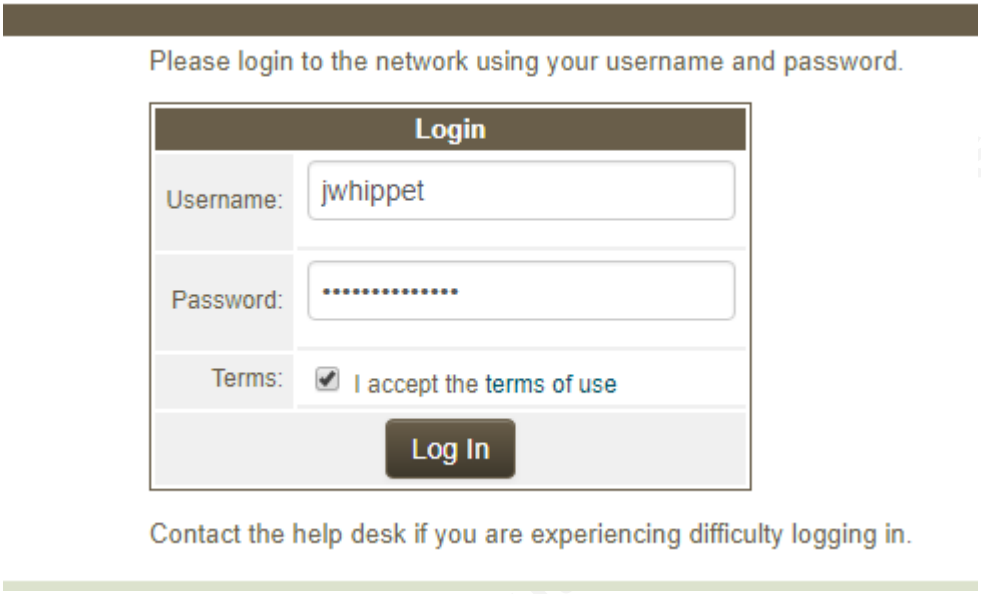


Figure 18: Captive Portal Login for BYOD Network

After logging into the captive portal, the user's computer is then given a new IP address on the subnet for which the user's role is associated. The original subnet in this example was subnet 10.0.92.0/24 the default for connecting devices to the captive portal. The user is also placed in a new role: in this, instance the SJ_Contractor_Role. Note the username has changed from the mac address of the machine to the AD username of the logged-in user.

Clients All | IPv4 | IPv6 |

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID	AP Name
jwhippet	Win 8	60:67:20:c2:01:bc	10.0.94.35	SJ_Contractor_Role	MAC	SJ_Mobile	ap6-c0:d5:5c

The firewall set associated with the connection also changes. Firewall sets are associated with roles. The firewall set for the SJ_Contractor_Role role is shown abridged (Figure 19)

Security > User Roles > Edit Role(SJ_Contractor_Role) > Edit Session (Contractor-User-ACLs)

User Roles | System Roles | Policies | Time Ranges | Guest Access | Branch Traffic

Rules

IP Version	Source	Destination	Service/Application	Action	Log	Mirror	Queue
IPv4	user	host 10.0.22.10	any	permit			Low
IPv4	user	host 10.0.22.11	any	permit			Low
IPv4	user	Clearpass	svc-http	permit			Low
IPv4	user	Clearpass	svc-https	permit			Low
IPv4	user	host 10.0.4.96	svc-icmp	permit			Low
IPv4	user	host 10.0.4.96	svc-dns	permit			Low
IPv4	user	10.0.2.0 255.255.255.0	any	deny			Low

Figure 19: Firewall Rule Set Applied to SJ_Contractor_Role

6.3.4 View from the Policy Server

During the authentication and authorization phase for the BYOD (SJ_Mobile) network all steps in the process are managed by the Aruba CPPM policy server. The policy server sends commands to the controller to change the user's role and access throughout the steps of the process. The controller relies on the policy server for all access decisions.

On the policy server, there are four separate authentication and authorization steps during captive portal authentication (Figure 20).

#	Server	Source	Username	Service	Login Status
1.	[redacted]				ACCEPT
2.	10.0.4.183	RADIUS	jwhippet	SJ_Wireless_BYOD_MAC_Authentication_Service	ACCEPT
3.	10.0.4.183	RADIUS	jwhippet	SJ_Wireless_BYOD_Web_Authentication_Service	ACCEPT
4.	10.0.4.183	RADIUS	jwhippet	SJ_Wireless_BYOD_Web_Authentication_Service	ACCEPT
5.	[redacted]				ACCEPT
6.	10.0.4.183	RADIUS	60:67:20:c2:01:bc	SJ_Wireless_BYOD_MAC_Authentication_Service	ACCEPT

Figure 20: Four Phases of Captive Portal Authentication for the BYOD Network (SJ_Mobile)

The four phases of authentication for captive portal clients are:

- machine authentication (shared key)
- user authentication (captive portal)
- group authentication (policy server pulls the group membership of the user from Active Directory)

- COA (change of authentication) the user's connection to the mobility controller is disconnected and reconnected as a new role is associated with the connection. The user is then placed in a different network with a new firewall set.

6.3.5 ePHI Access Exceptions with Captive Portal

While network access via captive portal does not have access to ePHI from any of the network segments that comprise the captive portal configuration, exceptions may be made in cases where contractors must have access to a host or system where ePHI is stored in order to perform maintenance tasks.

If this is required, the contractor is given an Active Directory login with membership in the AD group Contractor-WiFi (which is the group associated with access to the contractor network). This account is set to expire by the end of the engagement with the contractor.

A firewall set is then defined to allow the contractor access to only the systems required to do their work. All other firewall rules are kept in place to prevent access to any other systems in the environment. The firewall set that allows ePHI access is only associated with the contractor user's login and will not work for another contractor logging into the captive portal for wireless connectivity.

Before these configuration changes are made, a change control document is required from a company principal (or CISO) requesting access to a system hosting ePHI. As this is a small organization, this is easily controlled as a one-off situation.

To comport with HIPAA regulatory requirements, the contractor's company must have a current HIPAA BA (business associate agreement) on file with the company.

7. Guest Network Access and Requirements

Unlike many organizations, guest access for company clients is not in place as strictly a convenience. The guests in the environment are primarily clients (the majority of which are healthcare clients). The guest wireless network is designed to enable clients working with the company's professional staff, to collaborate on projects. This often requires guests to have access to their own remote systems.

Guests in this environment must be able to access systems outside of the wireless perimeter such as VPN's, cloud-based file storage sites (such as Google docs), and other (often non-standard) applications needed when on site working with the company's professional staff. Due to this requirement, the management of the firewall rules for this network is done by the firewall team, instead of the wireless team that manages all internal wireless firewall rulesets.

Guest devices are to be permitted access to the network for a 24-hour period by default. The IS department's Help Desk staff may log into the policy server and extend the guest user's access for a longer period if needed. This takes a manual override and a request from the principal (manager or company owner) or staff member sponsoring the guest's access.

Guest devices may not automatically join the guest network via an open access point. There must be an authentication and authorization sequence for guest users. The decision to use a captive portal with guest access was made to control access to the guest network and to enable the tracking of all guest access via a user account.

The accounts database for guest access is located locally on the wireless policy server. Guests can log in and create an account that is associated with their mobile device in order to gain access to the network.

The SSID for this network is SJ_Mobile. Only one network is connected to the SSID. The traffic on this network does not mingle with the traffic from any other network. Guest network traffic has no access to any internal resources.

7.2 Guest Portal Authentication and Authorization Process

The diagram below (Figure 21) shows the workflow designed for the guest portal network for wireless clients. At each step of the process, all connections are encrypted from the connecting endpoint device through to the wireless controllers.

The firewall sets applied at each phase of the connection protect ePHI from access. This can be seen in detail in Appendix B. Pg. 71

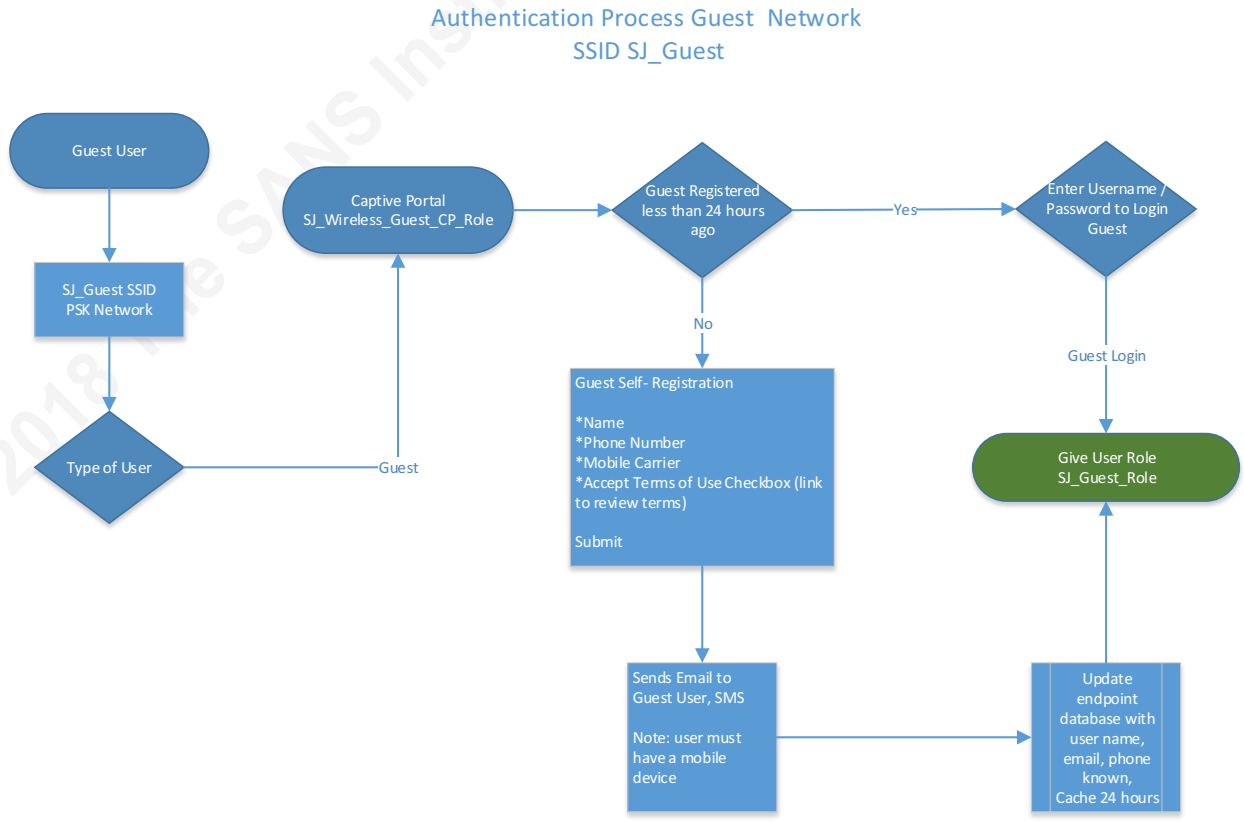


Figure 21: Authentication Process for the Guest Network

7.3 Guest Portal access controls

In many organizations, guest networks are designed as open access points, allowing any device to connect without authentication and authorization. While HIPAA regulations do not provide specific guidance on guest networks, it was determined that the design of the network must have HIPAA-based controls in place.

With this in mind and the fact that the majority of the company's clientele are healthcare entities that would be using the guest wireless network, controls were put in place for: user identification, encryption, traffic segmentation, and user activity logging.

Encryption throughout the connection is enabled using WPA2 personal authentication to create the initial connection between the guest's device and the wireless network. AES encryption is in place with WPA2 personal.

With WPA2 personal, the user must input a shared password when connecting to the SSID prior to logging into the captive portal. This use of a shared password enables the negotiation of an encrypted connection between the user's device and the wireless access point.

The example that follows is for a guest user connection. The connection is initiated by a user connecting his or her device to the SJ_Guest SSID. Once the connection is initiated, the user is prompted for a shared password. The shared password only permits the device to connect to the AP and to be placed on the guest VLAN with a default firewall set. For the guest network, the firewall set is in place to protect the policy manager's interface that resides on the guest network, as this network has no access to internal systems.

The policy server manages the initial WPA2 personal connection to the AP and places the connecting machine in a role on the controller. The initial role for guest network once the guest's device is associated with the network is the SJ_Guest_CP_Role.

Mobility Controller log output from initial connection of guest device (Figure 22). The device has an IP on the guest network. Note: the mac address for the computer is the User Name at this point in the connection. The initial role SJ_Guest_CP_Role is assigned to the machine.

Search Results

Clients All IPv4 IPv6

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
60:67:20:c2:01:bc	Win 8	60:67:20:c2:01:bc	10.0.99.31	SJ_Guest_CP_Role	MAC	SJ_Guest
miller	iPhone	dc:0c:5c:9a:2a:da	10.0.92.25	SJ_Employee_BYOD_Role	MAC	SJ_Mobile

Figure 22: Controller Log Output for Initial Guest Device Connection

The initial firewall sets from the Aruba controller prior to IP address assignment allow device association with the network (Figure 23).

Rules

IP Version	Source	Destination	Service/Application	Action
IPv4	user	any	udp 68	deny
IPv4	any	any	svc-icmp	permit
IPv4	any	any	svc-dns	permit
IPv4	any	any	svc-dhcp	permit
IPv4	any	any	svc-natt	permit
IPv4	any	169.254.0.0 255.255.0.0	any	deny
IPv4	any	240.0.0.0 240.0.0.0	any	deny

Figure 23: Pre-Authentication Firewall Set for Guest Captive Portal Access

The IP address configuration shown (Figure 24) is from a connected host before logging into the guest portal. DNS servers and DHCP addressing are being pulled from a PaloAlto firewall that manages the guest network subnet's connectivity.

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : 60-67-20-C2-01-BC
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f1dd:b642:aa76:2faa%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.0.99.31(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, February 7, 2018 2:00:10 PM
   Lease Expires . . . . . . . . . . : Thursday, February 8, 2018 3:08:42 PM
   Default Gateway . . . . . . . . . : 10.0.99.254
   DHCP Server . . . . . . . . . . . : 10.0.99.254
   DHCPv6 IAID . . . . . . . . . . . : 56649504
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-1B-70-A2-8E-38-EA-A7-FA-6D-7A
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       4.4.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Figure 24: Guest Network Connected Client Initial IP Configuration

Once the guest device has an IP address assignment, guest access to the policy server is then limited to the ports shown below (Figure 25). This firewall set also performs a destination NAT to forward captive portal traffic through the policy server to the guest captive portal pages. The firewall also manages connectivity between the endpoint and the wireless mobility controllers for session management.

Rules

IP Version	Source	Destination	Service/Application	Action	Log	Mirro
IPv4	user	controller	svc-https	dst-nat 8081		
IPv4	user	any	svc-http	dst-nat 8080		
IPv4	user	any	svc-https	dst-nat 8081		
IPv4	user	any	svc-http-proxy1	dst-nat 8088		
IPv4	user	any	svc-http-proxy2	dst-nat 8088		
IPv4	user	any	svc-http-proxy3	dst-nat 8088		

Add ▲ ▼ Delete

Figure 25: Initial Guest Network Firewall Rule Set Prior to Authentication

The guest user is then presented with a login web page (Figure 26). The user must input a user-name. This may be any name chosen by the guest user. A phone number is required to send the password to the guest via SMS. The mobile carrier is necessary to route the SMS message to the guest's mobile device.

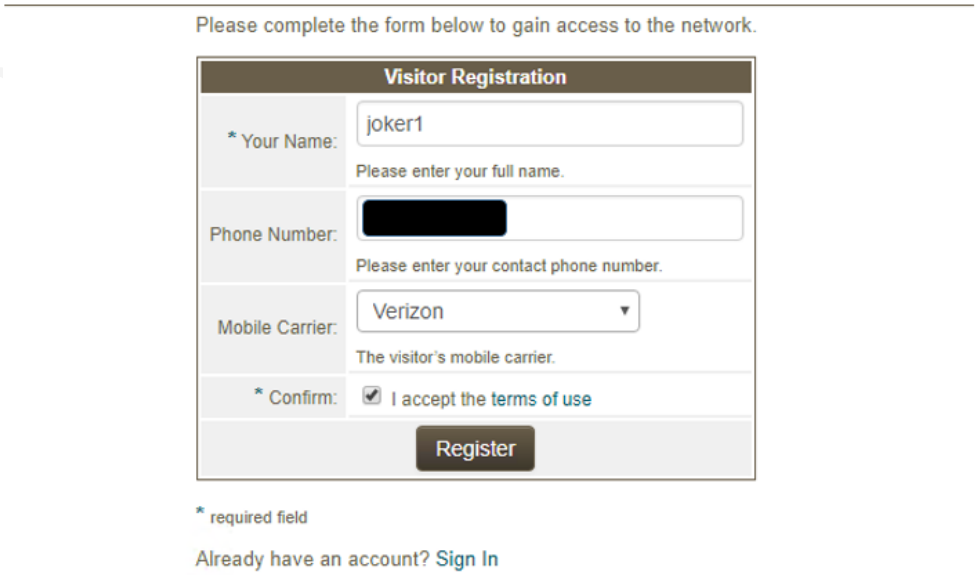
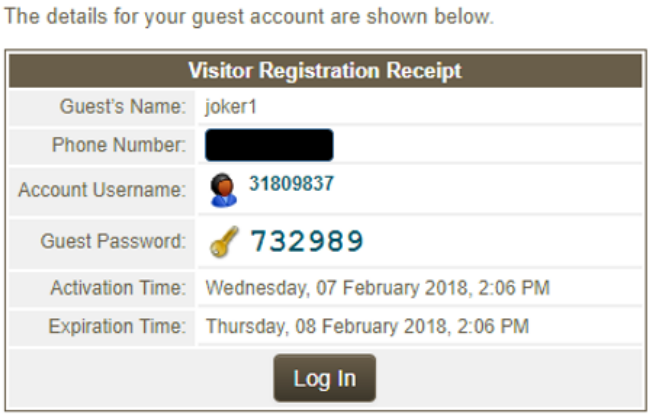


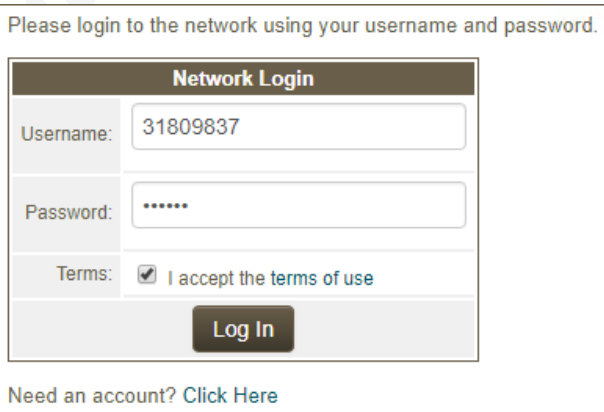
Figure 26: Guest Captive Portal Login

The guest user is then redirected to a login page to log on to the network. Initially the guest's login information is populated for the user. If the user connects subsequently (after leaving and returning), the user will need to input this information.

The guest will also require the account username that was created for the user in order to log in again. The name the guest specified when registering is not actually used for authentication. The actual user name for the guest account is generated by the policy server.



A returning guest will receive the following login prompt. To access the guest network the user will need to input the username and password furnished by the policy server.



The user's device is also placed in a new role, SJ_Guest_Role. Note the username has changed from the mac address of the machine to the Account Username provided to the user by the policy server (Figure 27).

Search Results

Clients All | IPv4 | IPv6 |

	User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
○	31809837	Win 8	60:67:20:c2:01:bc	10.0.99.31	SJ_Guest_Role	Captive Portal	SJ_Guest

Figure 27: Mobility Controller Log Authenticated Guest User

7.4 View from the Policy Server

During the authentication and authorization phase for the guest (SJ_Guest) network all steps in the process are managed by the Aruba CPPM policy server. Initially the user's device is connected with the mac address being used as the username for tracking the connection. This will change to a system assigned user id after the authentication sequence has completed (Figure 28).

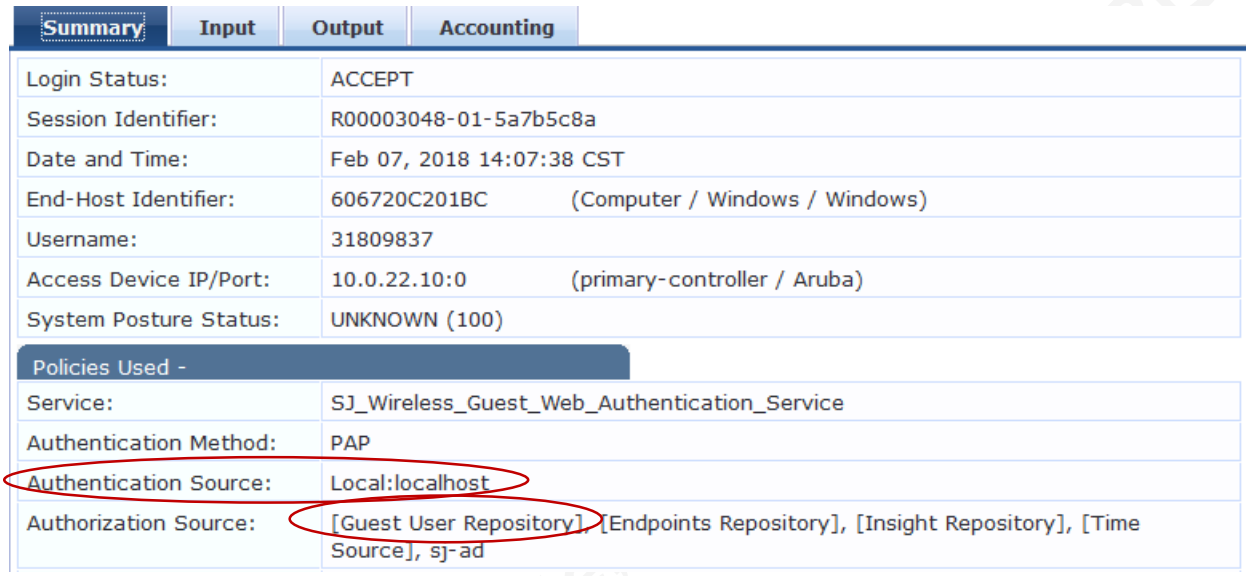
50.	10.0.4.183	RADIUS	31809837	SJ_Wireless_Guest_Web_Authentication_Service	ACCEPT
51.	10.0.4.183	RADIUS	60:67:20:c2:01:bc	SJ_Wireless_Guest_MAC_Authentication_Service	ACCEPT

Figure 28: Policy Server Log Entries for the Two Phases of Guest Authentication

The two phases of guest authentication for the guest captive portal are:

- machine authentication (shared key)
- user authentication (after registration to local accounts database)

Output from the second log entry (50) Figure 29 details the user authentication against the localhost (policy server) and authorization for the connection being managed by the Guest User Repository database.



Summary	Input	Output	Accounting
Login Status:	ACCEPT		
Session Identifier:	R00003048-01-5a7b5c8a		
Date and Time:	Feb 07, 2018 14:07:38 CST		
End-Host Identifier:	606720C201BC	(Computer / Windows / Windows)	
Username:	31809837		
Access Device IP/Port:	10.0.22.10:0	(primary-controller / Aruba)	
System Posture Status:	UNKNOWN (100)		
Policies Used -			
Service:	SJ_Wireless_Guest_Web_Authentication_Service		
Authentication Method:	PAP		
Authentication Source:	Local:localhost		
Authorization Source:	[Guest User Repository], [Endpoints Repository], [Insight Repository], [Time Source], sj-ad		

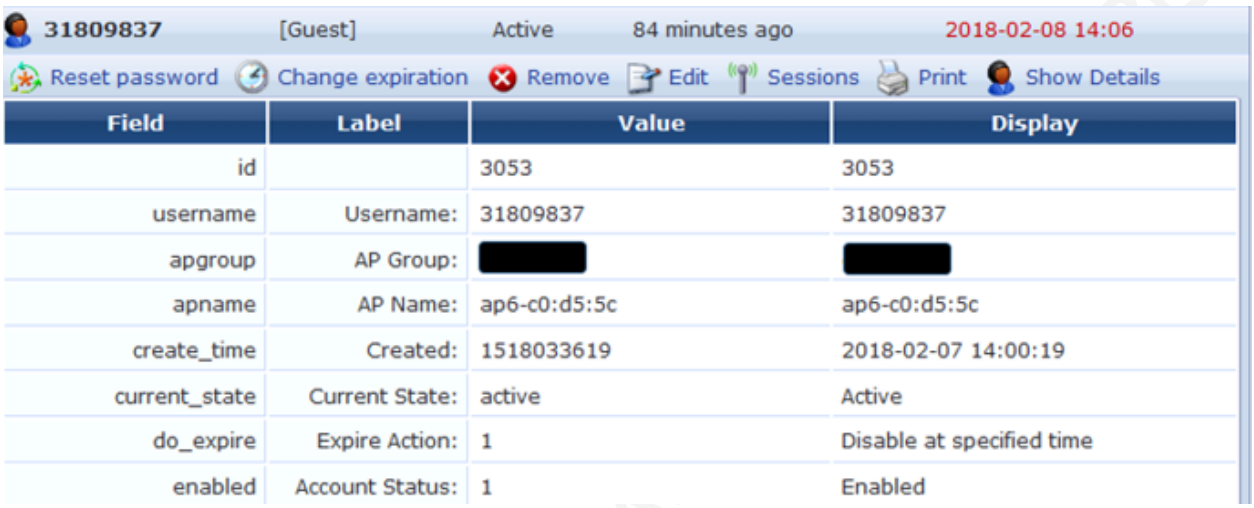
Figure 29: Detail of Log Entry for Authenticated Guest Account

7.5 Guest Access Accounting

Guest users are given randomly-generated numerical Account Usernames when they connect. These accounts are registered in the local accounts database of the Aruba ClearPass policy server, specifically in the Guest User Repository.

Guests are permitted access for a period of 24 hours. This can be manually changed by a Help Desk user, or by the policy server administrator. Like any other user in the wireless environment, all guest devices are tracked and user access to the wireless network is tracked.

The output from the guest user accounts database (below) shows a user account with some of the attributes associated with the account (Figure 30).



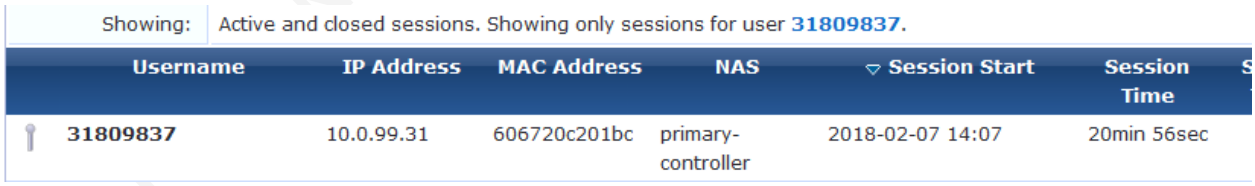
31809837 [Guest] Active 84 minutes ago 2018-02-08 14:06

Reset password | Change expiration | Remove | Edit | Sessions | Print | Show Details

Field	Label	Value	Display
id		3053	3053
username	Username:	31809837	31809837
apgroup	AP Group:	[redacted]	[redacted]
apname	AP Name:	ap6-c0:d5:5c	ap6-c0:d5:5c
create_time	Created:	1518033619	2018-02-07 14:00:19
current_state	Current State:	active	Active
do_expire	Expire Action:	1	Disable at specified time
enabled	Account Status:	1	Enabled

Figure 30: Guest User Account Detail in Guest User Repository

User session information is tracked in the policy manager as well as on the wireless controllers. Session data for guest wireless connections is forwarded to the company's SEIM for long-term retention and analysis.



Showing: Active and closed sessions. Showing only sessions for user 31809837.

Username	IP Address	MAC Address	NAS	Session Start	Session Time
31809837	10.0.99.31	606720c201bc	primary-controller	2018-02-07 14:07	20min 56sec

7.6 Guest Network Firewalling

Prior to a guest wireless client being authenticated and authorized firewalling of a device on the guest network is controlled by the Aruba mobility controller. Post authentication the firewall configuration for the guest network is controlled on the organization's PaloAlto firewall cluster. Traffic from the wireless mobility controllers for guest wireless traffic is placed on a subnet that is only available on the PaloAlto firewall. The PaloAlto firewall is the gateway for the network and controls all traffic from the guest network to the Internet.

This subnet is not routable in the company's routing and switching infrastructure and is fully segregated from any internal networks. The VLAN used for guest network access only

exists on the switch stack that is shared by interfaces from the Aruba wireless controllers and the PaloAlto high availability (HA) pair.

The Aruba ClearPass policy server has an interface in this network (the CPPM is a virtual machine running in a VMware environment), which accepts inbound connections from guest devices on the guest network. Therefore, no session or control traffic outside of the guest subnet is required.

All DHCP and DNS requests are handled on the PaloAlto firewall. URL filtering for the network is handled via an inline BlueCoat web proxy integrated with the PaloAlto Firewall. Thus, no web traffic passes into the internal network for processing.

This HIPAA guest WLAN Design – Base Overview, (Figure 31) diagram shows the traffic and firewalling overview for the guest wireless network. All guest traffic runs on VLAN 99, 10.0.99.0/24 network. See Appendix A Pg.65

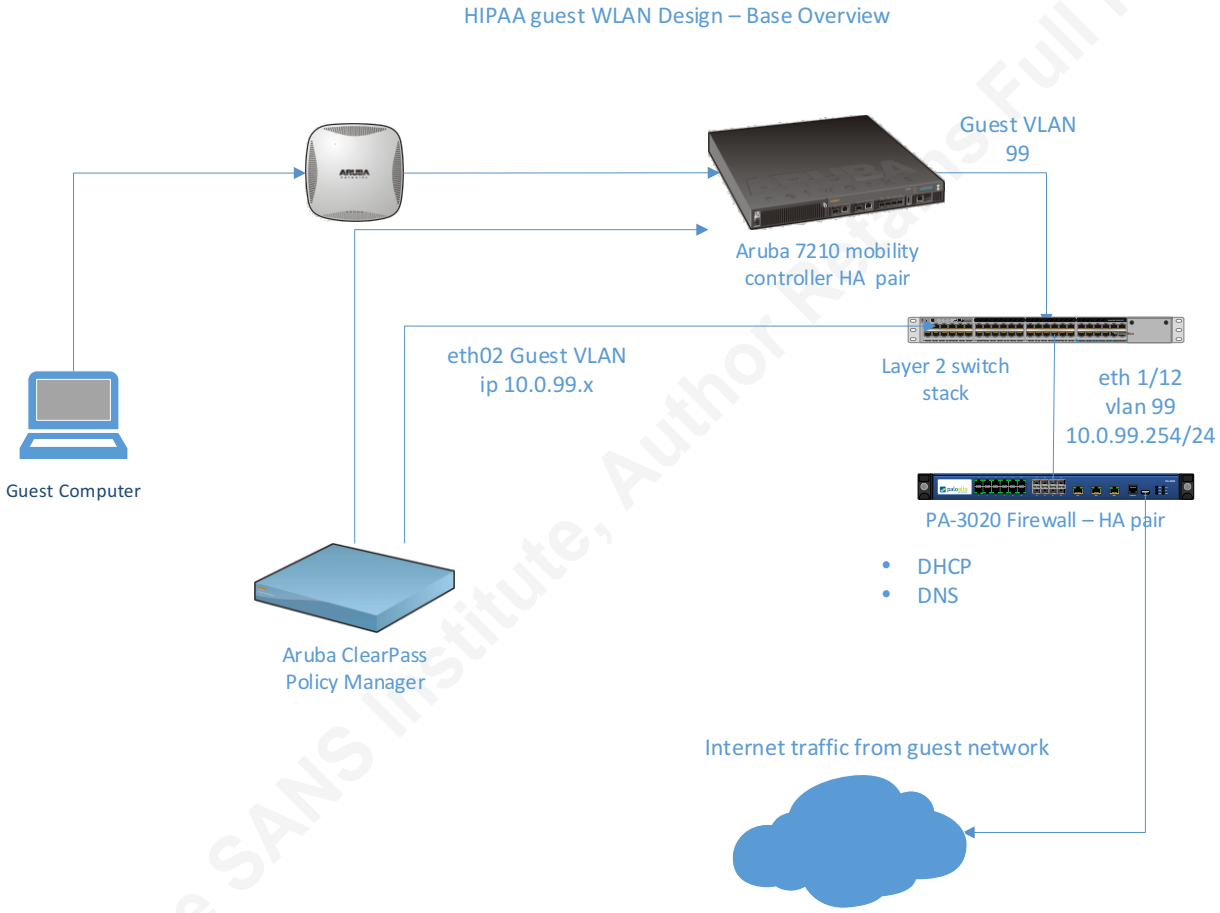


Figure 31: HIPAA Guest WLAN Design

8 WLAN Segmentation and Firewalling

Within any HIPPA-regulated organization, the Security Rule requires that the organization segments ePHI from other data and functions within an organization. When a company can isolate ePHI from other data in an effective manner, the organization will be more effective in controlling and protecting ePHI.

Access to ePHI in this company's environment is based on department and job role within the company. Therefore, security measures put in place must mimic this scheme.

ePHI access in this environment is to be protected from unauthorized access by employees, contractors, and client organizations that do not have a business-related need to access ePHI or a software application that handles ePHI (such as the financial auditing tools in this company).

8.1 Network Segmentation

On the wired network, the organization utilizes 801.1x authentication, authorization and access control to ePHI. Devices are only permitted access to particular network segments, information stores and applications. Connectivity to ePHI is controlled via a user's role in the company and the connections are firewalled as traffic leaves one segment and enters another.

When determining how to best segment a network, it is best practice not to rely on VLANs as a security mechanism. VLANs, though a necessary component of network segmentation, are not a reliable security device on their own.

In the HIPAA-compliant wireless access design, it was determined that the access control mechanisms should match up to those used for wired networks. The decision was made to use role-based access control (as on the wired network) to maintain secure access to ePHI.

All the wireless network configurations utilize user roles to determine what access users are given when connecting to the wireless network. Specifically, regarding users, access to ePHI 802.1x authentication was used in conjunction with user roles assigned to employees based on Microsoft Active Directory group membership. These roles and their access permissions are broken down in the decision diagrams in Appendix B Pg.69.

It must be noted that access to ePHI is also defined at the network share level, and in the role based access mechanisms of the company's document management system (DMS). These

layers of security further control access to ePHI at a granular level.

8.2 Firewalling Wireless Connections

To secure ePHI information stores on the company's network, segmentation policies are enforced by the wireless mobility controllers. The mobility controllers manage the terminating firewall rules on each wireless segment.

All wireless networks have application-based firewall sets applied to the network as traffic leaves the controller and enters the ethernet (wired network). Therefore, access to any host or network is restricted directly on the wireless network, prior to client traffic entering the wired portion of the subnet. The ability to firewall wireless connections before they leave the wireless network enables the company to simplify the management of wireless traffic.

The Firewalling Base Design Example diagram (Figure 32), illustrates the location where firewall rules are applied in the wireless network design. The user/computer is assigned a role (associated with an AD group and device profile). This role is then passed to the wireless controller after the user is authenticated. The role for the user on the mobility controller is then assigned to a subnet (VLAN pool) and a firewall set (which is applied before traffic enters the ethernet network). See Appendix A. Pg.67

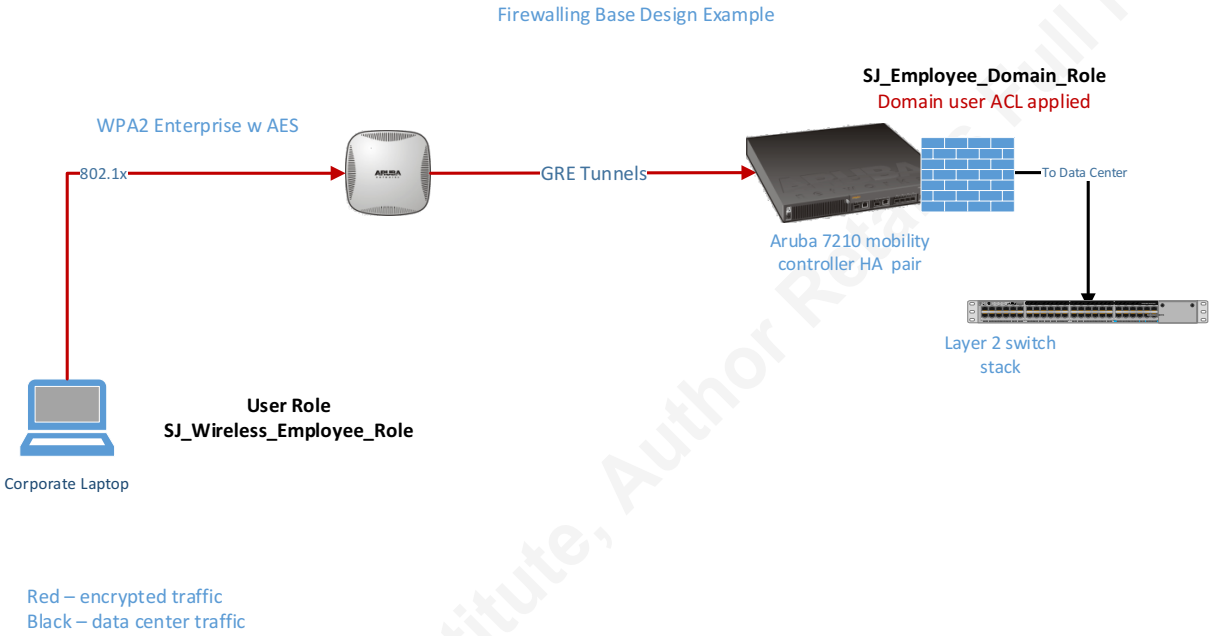


Figure 32: Firewalling Base Design Example

Thus, role-based access is used to apply firewall sets and access control policy.

8.3. Device Profiling to Control Network Access

One of the goals of protecting ePHI resources in the network design is the prevention of corporate endpoints from connecting to the other SSIDs on the company's wireless network. Corporate laptops are permitted to connect to a single on premise SSID (the SJ_Prvate SSID). These devices are never to be permitted access to the guest or BYOD / consultant networks.

A complication in controlling the WiFi networks accessed by company laptops is that these devices are used both on and off premise by the staff members assigned to the devices. Laptops used to access ePHI and other network resources are therefore used in the field by audit staff (on client networks, and for remote office work). These devices must be able to access other wireless networks when off site.

To control corporate endpoint access to other networks, corporate devices are fingerprinted using the device profiling capabilities of the wireless policy management server. By using device-profiling services to control devices, traffic and network access may be controlled by any attribute of the connecting device.

When a corporate laptop first connects to the network utilizing the machine authentication / user authentication combination (802.1-x authentication), the device is placed into the local database of the policy management server.

The devices' attributes (active directory group membership, digital certificate, operating system etc.) are analyzed and stored in an endpoints database. The attributes assigned to endpoints that have connected to the policy server are then used to make network access decisions through policy. This process is described as follows:

Corporate endpoints connected to the wireless controllers are shown below (Figure 33). The output shows the device types, addresses, roles assigned to the endpoint as well as authentication type and SSID.

Search Results

Clients All | IPv4 | IPv6 |

User Name	Device Type	MAC address	Client IP	User Role	Auth Type	ESSID
SJSQ\VSalcido	Windows	e4:a7:a0:64:6e:50	10.0.91.33	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\DHeaston	Windows	a4:34:d9:a6:10:bc	10.0.91.27	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\TGehring	Windows	e4:a7:a0:ae:8f:a3	10.0.91.167	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\RMerrill	Windows	e4:a7:a0:ae:8d:50	10.0.91.171	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\AEllwanger	Windows	e4:a7:a0:ae:8d:fa	10.0.91.30	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\MBlome	Windows	e4:a7:a0:ae:8f:0d	10.0.91.48	SJ_Employee_Domain_Role	802.1x	SJ_Private
SJSQ\JJudds		e4:a7:a0:9d:cc:9a	10.0.91.164	SJ_Employee_Domain_Role	802.1x	SJ_Private

Figure 33: Mobility Controller Device Log Output

Using the first device in the list (from figure 34), the attributes of this device are shown from the policy sever database.

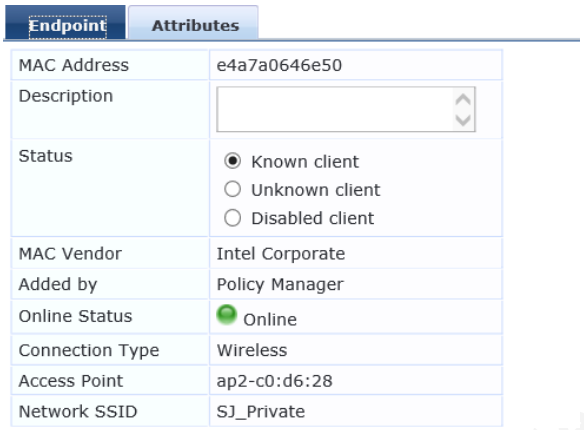
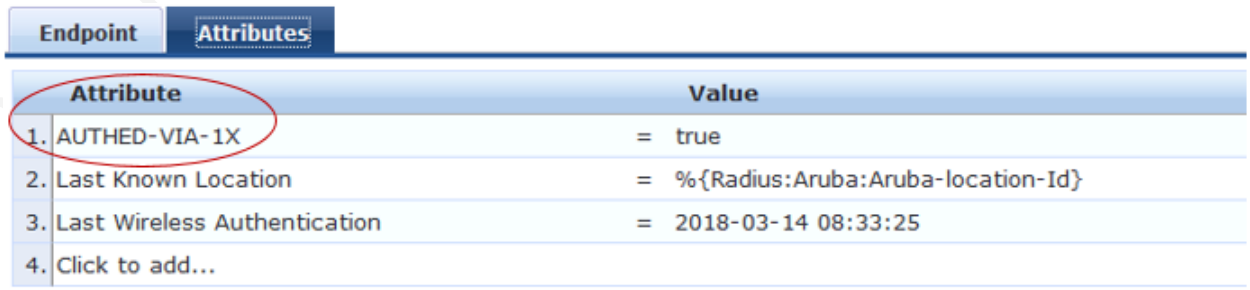


Figure 34: Endpoint Attributes from the Endpoint Database

Since this device is profiled as a corporate device (authenticated with 802.1x), the device has a custom attribute added to its object in the endpoints database of the policy server. The attribute AUTHED-VIA-1X is added to the device's database entry. Only company laptops that are AD joined use 802.1x authentication, therefore only those devices are tagged with the AUTHED-VIA-1X attribute.



Enforcement profiles on the policy server (Figure 35) are used to enforce access rules for endpoint network access or to manipulate device attributes to control network access. The enforcement profile below is used to add this AUTHED-VIA -1X attribute to corporate endpoints once they are initially authenticated. Additional attributes are also added such as Last Wireless Authentication (date and time).

Enforcement Profiles - SJ_Update_Domain_Endpoint_Information

Summary | Profile | Attributes

Profile:

Name:	SJ_Update_Domain_Endpoint_Information
Description:	
Type:	Post_Authentication
Action:	
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Endpoint	Last Known Location	=	%{Radius:Aruba:Aruba-location-Id}
2.	Endpoint	Last Wireless Authentication	=	%{Date:Date-Time}
3.	Endpoint	AUTHED-VIA-1X	=	true

Figure 35: Enforcement Profile Example

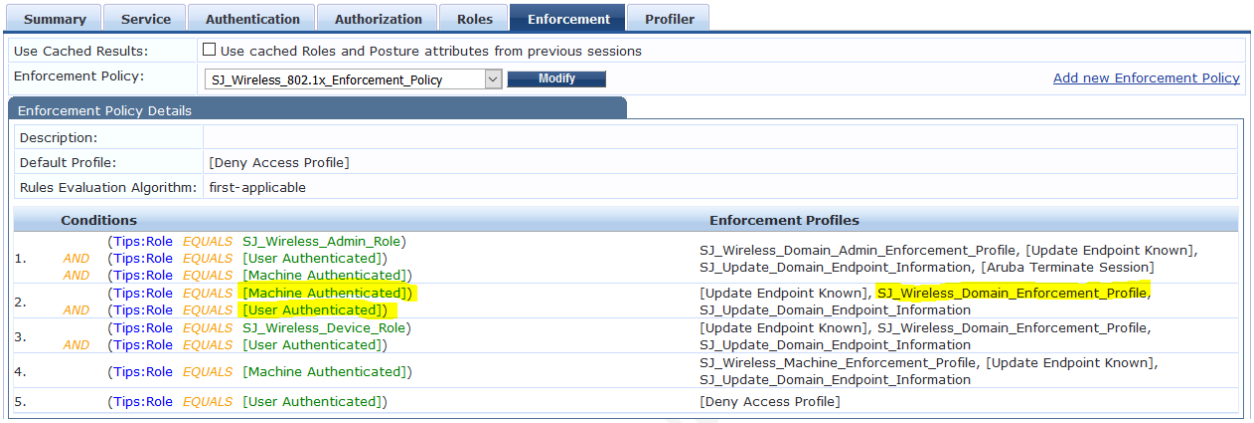
8.3.1 Permitting a Device with Device Profiling

When a device is authenticating to the policy server for access to a wireless network, a policy management service is used to evaluate whether a machine is permitted onto a specific wireless network or not.

When a device connects to the wireless network it is evaluated against multiple access enforcement policies in a Service. These policies are evaluated like firewall rules from top to bottom. An endpoint must match the proper criteria to be allowed onto a wireless network.

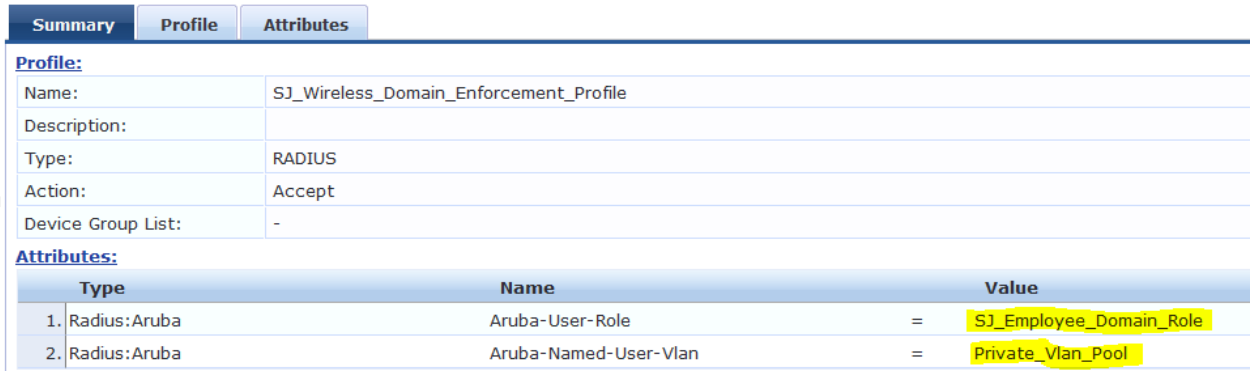
The enforcement policy below (a component of the SJ_802.1x_Wireless_Service) shows the attributes necessary to connect to the SSID for the corporate WiFi network that has access to internal ePHI resources. If the following conditions are met [Machine _ Authenticated] and [User_ Authenticated], the enforcement profile SJ_Wireless_Domain_Enforcement_Profile will be applied to the device.

Services - SJ_802.1x_Wireless_Service



The enforcement profile that is applied by the service is the SJ_Wireless_Domain_Enforcement_Profile (below). This enforcement profile applies the role SJ_Employee_Domain_Role to the endpoint connection and assigns the VLAN (Private_Vlan_Pool) to the connection on the wireless controller. The endpoint will now have access to the network containing ePHI.

Enforcement Profiles - SJ_Wireless_Domain_Enforcement_Profile



8.3.2 Denying a Device with Device Profiling

If this same endpoint attempts to connect to another SSID such as the BYOD SSID (SJ_Mobile), the enforcement portion of the wireless service associated with that SSID will block the device from accessing the network.

The policy condition at the top (SJ_Deny_802.1X_To_Other_Networks) denies access to this network for any device tagged with the corporate device attribute (AUTHED-VIA-1X.) The enforcement places the device in the SJ_Wireless_CaptivePortal_Enforcement_Profile.

Services - SJ_Wireless_BYOD_Web_Authentication_Service

Summary | Service | Authentication | Authorization | Roles | Enforcement

Use Cached Results: ☐ Use cached Roles and Posture attributes from previous sessions

Enforcement Policy: SJ_Wireless_Web_Authentication_Enforcement | Modify | Add new Enforcement Polic

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Tips:Role EQUALS SJ_Deny_802.1X_To_Other_Networks)	SJ_Wireless_CaptivePortal_Enforcement_Profile
2.	(Tips:Role EQUALS SJ_Wireless_Admin_Role) AND (Tips:Role EQUALS [User Authenticated])	SJ_Wireless_Employee_Admin_Enforcement_Profile, [Update Endpoint Known], SJ_Update_Password_Expiration, [Aruba Terminate Session], SJ_Wireless_Employee_Admin_MAC_Caching_Profile
3.	(Tips:Role EQUALS SJ_Wireless_Employee_Role) AND (Tips:Role EQUALS [User Authenticated])	SJ_Wireless_Employee_Enforcement_Profile, [Update Endpoint Known], SJ_Wireless_Employee_MAC_Caching_Profile, SJ_Update_Password_Expiration, [Aruba Terminate Session]
4.	(Tips:Role EQUALS SJ_Wireless_Contractor_Role) AND (Tips:Role EQUALS [User Authenticated])	SJ_Wireless_Contractor_Enforcement_Profile, SJ_Wireless_Contractor_MAC_Caching_Profile, [Update Endpoint Known], SJ_Update_Password_Expiration, [Aruba Terminate Session]
5.	(Tips:Role EQUALS SJ_Wireless_Guest_Role) AND (Tips:Role EQUALS [User Authenticated])	SJ_Wireless_Guest_MAC_Caching_Enforcement_Profile, [Update Endpoint Known], SJ_Wireless_Guest_Enforcement_Profile
6.	(Tips:Role EQUALS No Role Mapping Match)	SJ_Wireless_CaptivePortal_Enforcement_Profile

The SJ_Wireless_CaptivePortal_Enforcement_Profile then places the connection into a role where the device is segregated on a VLAN that the user and device have no authenticated access to. This role SJ_Guest_CP_Role will not allow the endpoint to authenticate. Therefore, the device is captive in this role until the user changes the SSID on the endpoint.

Enforcement Profiles - SJ_Wireless_CaptivePortal_Enforcement_Profile

Summary | Profile | Attributes

Profile:

Name:	SJ_Wireless_CaptivePortal_Enforcement_Profile
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	SJ_Guest_CP_Role

9. Encryption and Data Protection

HIPAA Safeguard 164.312(a)(1)(2)(iv) Encryption and Decryption, specifies the requirement of encrypting ePHI data. In accordance with this requirement, it is incumbent on organizations to encrypt data at every possible step in the transmission and management of ePHI.

In the wireless network designs, encryption requirements were considered for each network design. The specifics of each network's encryption configuration are as follows:

- For the employee laptops, accessing ePHI all data is secured using AES encryption. The initial connection to the wireless network is encrypted using WPA2 Enterprise authentication in conjunction with AES encryption.
- For the Captive Portal with Active Directory Authentication BYOD access as well as the Guest access wireless network, WPA2 personal with AES is used to negotiate and encrypt the connections between the APs and the client endpoints.

While WPA2 with AES is utilized for encryption from the endpoint to the AP, encryption from the Access Point to the data center is required by HIPAA regulations. In many wireless network designs, encryption is only enforced between the endpoint and the AP. Once the data exits the access point (and is placed on the wire), the data is decrypted while in transit to storage or application servers.

It was determined in this design that all data must be encrypted from the connecting device through to the data center. With this requirement all data between the wireless access points and the wireless controllers was to be encrypted.

To do this, the controller model was chosen that enabled the use of encrypted GRE tunnels at layer 2 of the architecture. This encryption design thus would enable the data to be encrypted through to the data center for maximum data protection over the wireless infrastructure.

The encryption architecture for the WLAN

In the diagram below (Figure 36), all traffic that is encrypted appears in red. Traffic sent from the wireless network to the data center appears in black. No data traffic passes between the Aruba ClearPass policy manager and the Aruba mobility controllers. The connections between the policy server and the controller contain device control traffic only.

It must be noted that for each SSID that connects between the access point (that carries that SSID) and the controller, there is a separate GRE tunnel. Therefore, in this design, there are three GRE tunnels between each AP and the mobility controllers. See Appendix A Pg.66

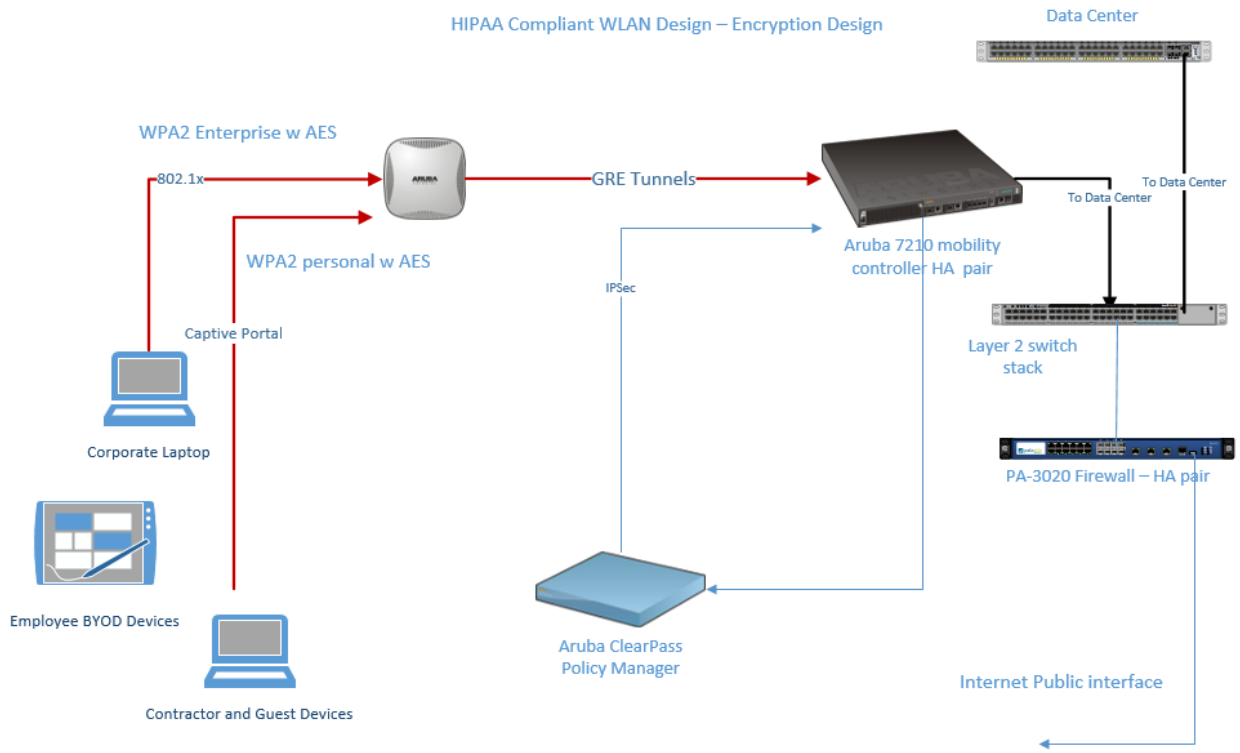


Figure 36: HIPAA Compliant WLAN Design – Encryption Design

The Aruba mobility controllers are connected via layer 2 directly to the data center where company ePHI resides. All WLAN traffic on the distribution layer of the network (between APs and controllers) is encrypted from the client device to the ethernet connection to the data center.

The Aruba wireless mobility controllers can use IPSec tunnels for secured connections to file servers, data stores, and database management systems that support the protocol. Utilizing IPSec tunnels to servers containing ePHI on the wired side of the network, the entire data stream from the client to the data store can be encrypted. This configuration is outside of the scope of this design.

10. Conclusion

The wireless network security design detailed in this paper is intended to be scalable. While this project was implemented in a smaller organization, the architecture will translate to larger healthcare organizations and hospital settings.

In designing, a wireless network's security based on the roles of the users in an organization, the wireless design will work in tandem with other aspects of an organization's security posture for ePHI. For example, if an organization has defined data governance protections in place for ePHI, user roles associated with data access can be carried over to the wireless network for role-based access to ePHI.

Wireless security in the healthcare industry is becoming of paramount concern. Organizations must invest the time and money secure wireless networks from breaches to ePHI. With the explosion of IoT (Internet of Things) devices in the healthcare arena, this is only going to get worse. Going forward, device profiling and interrogating devices that attach to a wireless network for the devices security posture will become the norm.

Wireless device security in healthcare is going to be an issue for some time to come. A properly thought out security design and proper planning for device growth are paramount to keeping patients data secure.

References

Agency for Healthcare Research and Quality: Computers Provider Order Entry. Retrieved November 26, 2017, from https://healthit.ahrq.gov/key-topics/computerized-provider-order-entry

Aruba Airheads Community. (2009). Encrypting Guest Traffic. Retrieved December 15, 2017, from https://community.arubanetworks.com/t5/Security/Encrypting-Guest-traffic/m-p/2911

Aruba Airheads. (2011, December 19). User role based VLAN assignment. Retrieved November 27, 2017, from http://community.arubanetworks.com/t5/Security/User-role-based-VLAN-assignment/td-p/20690

Aruba Networks. (2012). Secure Wi-Fi For Healthcare Applications. Retrieved November 27, 2017, from http://www.arubanetworks.com/assets/wp/WP_Healthcare_WLAN.pdf

Aruba Networks. (2010). Aruba Mobility Controllers and Deployment Models Validated Reference Design. Retrieved November 26, 2017, from http://www.4gon.co.uk/documents/aruba_mobility_controllers_deployment_models.pdf

Cappalli, Tim. (2014, March 3). Using ClearPass to steer users to secure networks. [Blog post]. Retrieved November 27, 2017, from http://community.arubanetworks.com/t5/Security/Guide-Using-ClearPass-to-steer-users-to-secure-networks-mhc/td-p/144823

Ciarlone, John (2014). Waiting Room WiFi: How Doctors Can Stay HIPAA Compliant. Retrieved October 10, 2017, from https://info.hummingbirdnetworks.com/blog/waiting-room-wifi-how-doctors-can-stay-hipaa-compliant

Cision PR Newswire. (2017). At Mid-Year, U.S. Data Breaches Increase at Record Pace. Retrieved October 12, 2017, from http://www.prnewswire.com/news-releases/at-mid-year-us-data-breaches-increase-at-record-pace-300489369.html

Department of Health and Human Services. (2003). Business Associates. Retrieved December 10, 2017, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf

Department of Health and Human Services. (2007). HIPAA Security Series, Security Standards: Technical Safeguards. Retrieved November, 26 2017, from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf

Department of Health and Human Services (2013). Breach Notification Rule. Retrieved November 26, 2017, from https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Department of Health and Human Services (2013). Summary of HIPAA Security Rule. Retrieved November 26, 2017, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Department of Health and Human Services. (2017). Guidance on Risk Analysis. Retrieved December 28, 2017, from https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Department of Health and Human Services. (2017). HITECH Act Enforcement Interim Final Rule. Retrieved December 28, 2017, from https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

DHHS Office for Civil Rights (2016) HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Retrieved November 20, 2017, from https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

FindLaw (2017). HIPAA and WiFi: Regulatory Tangles for Wireless Health Care Networks. Retrieved October 10, 2017, from http://corporate.findlaw.com/litigation-disputes/hipaa-and-wifi-regulatory-tangles-for-wireless-health-care.html

Hewlett Packard Enterprise Support Center. (2016). Aruba Wireless - Guest Access Best Practices. Retrieved February 26, 2018, from https://support.hpe.com/hpsc/doc/public/display?docId=mmr_kc-0134121

HIT Infrastructure (2017). Security in Healthcare: Bolstering Connectivity and Protecting Patients. Retrieved October 12, 2017, from https://hitinfrastructure.com/resources/white-papers/security-in-healthcare-bolstering-connectivity-and-protecting-patients

Larsen, Michelle. (2014, March 24). AUTHENTICATION CALLED FOR BY PCI DSS, HIPAA/HITECH, AND GLBA/FFIEC. [Blog post]. Retrieved November 28, 2017, from https://info.townsendsecurity.com/bid/70520/Authentication-Called-For-By-PCI-DSS-HIPAA-HITECH-and-GLBA-FFIEC

Leyva, Carols. (2013). HIPAA Omnibus Rule Summary. Retrieved November 30, 2017, from http://www.hipaasurvivalguide.com/hipaa-omnibus-rule.php

Meraki Networks. (2015). HIPAA Compliance for the Wireless LAN. Retrieved October 10, 2017, from https://meraki.cisco.com/lib/pdf/meraki_whitepaper_HIPAA.pdf

NIST. (2007). Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

Retrieved October 12, 2017, from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf

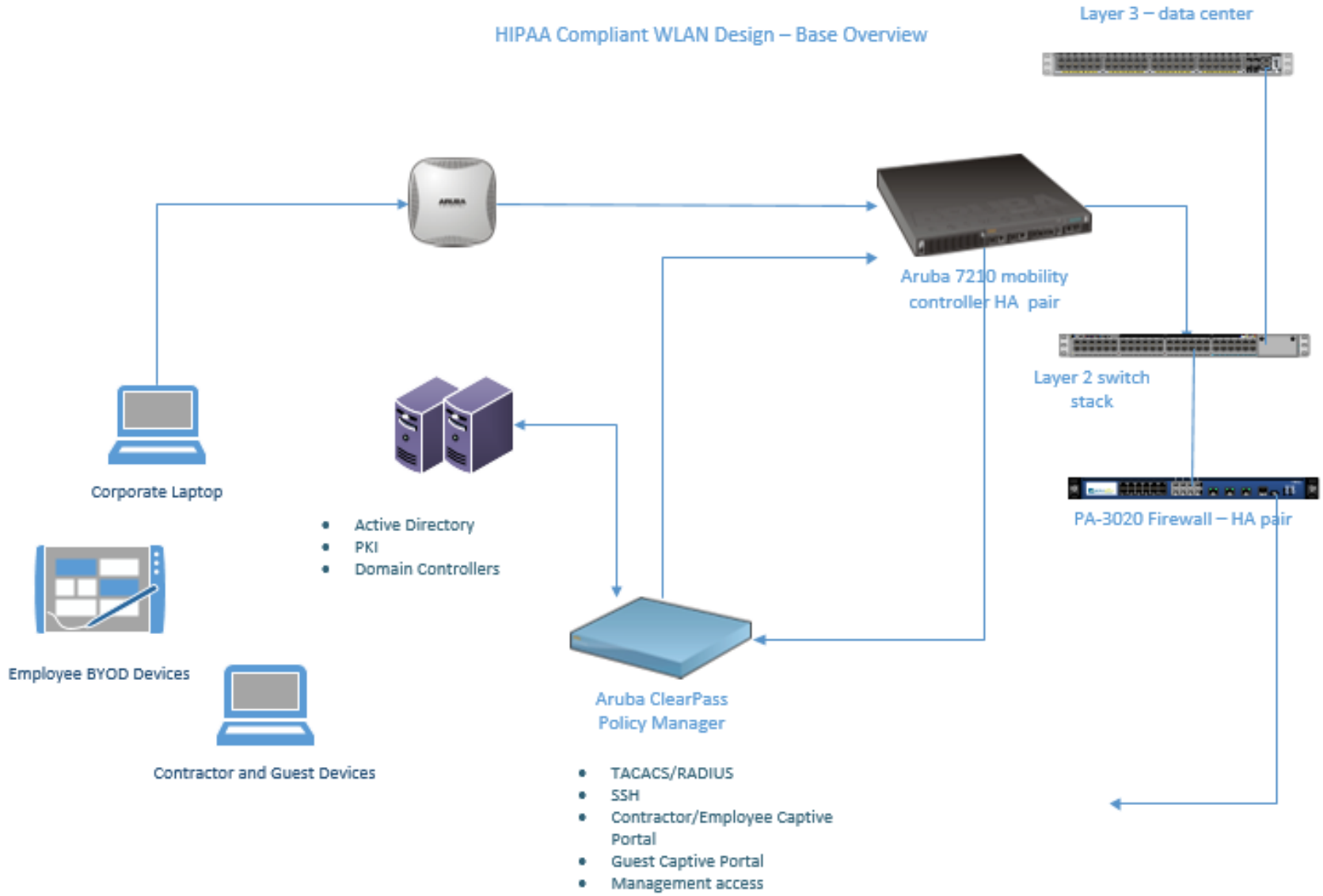
NIST. (2009). Recommendation for EAP Methods Used in Wireless Network Access Authentication. Retrieved October 12, 2017, from https://csrc.nist.gov/publications/detail/sp/800-120/final

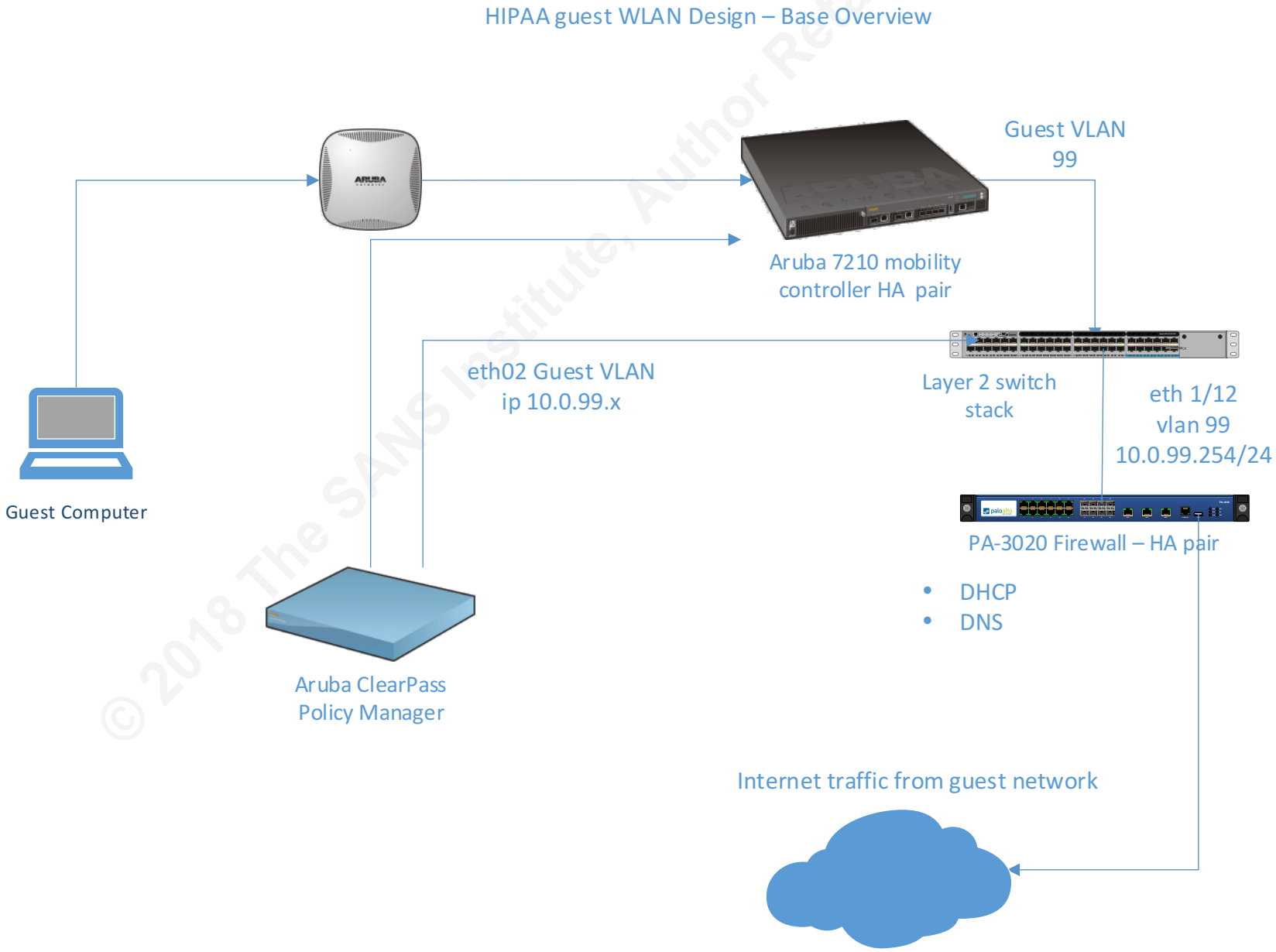
Nosowsky, Rachel. "ABA Health ESource." (June 2009). HITECH Implications for Business Associate Agreements: What Should You Do and When Should You Do It? Retrieved December 10, 2017, from https://www.americanbar.org/newsletter/publications/aba_health_esource_home/Volume5_10_Nosowsky.html

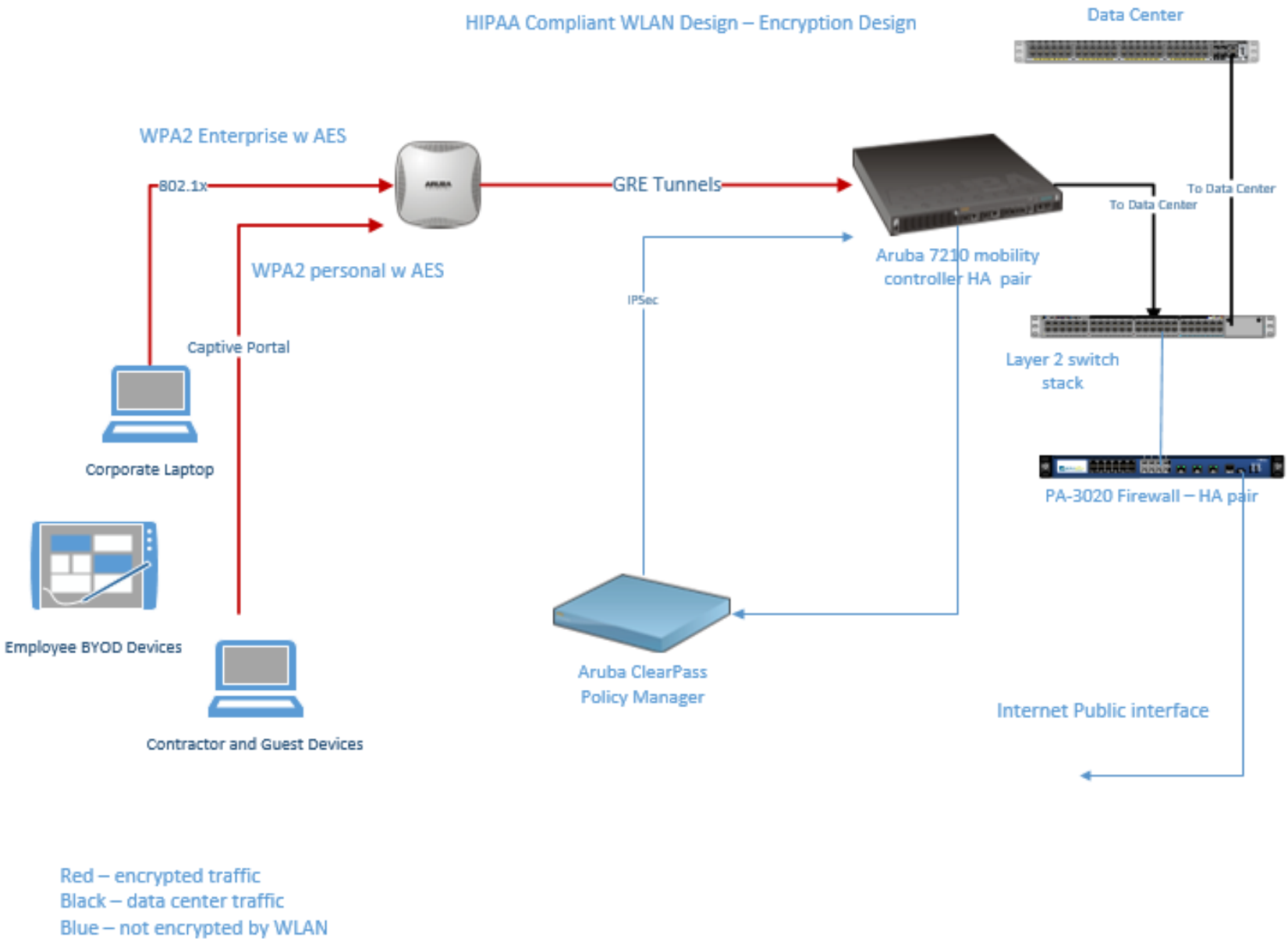
Wheeldon, Gavin. (2015). How WiFi is changing the Healthcare Industry. Retrieved December 13, 2017, from https://www.itproportal.com/2015/06/13/how-wifi-changing-healthcare-industry/

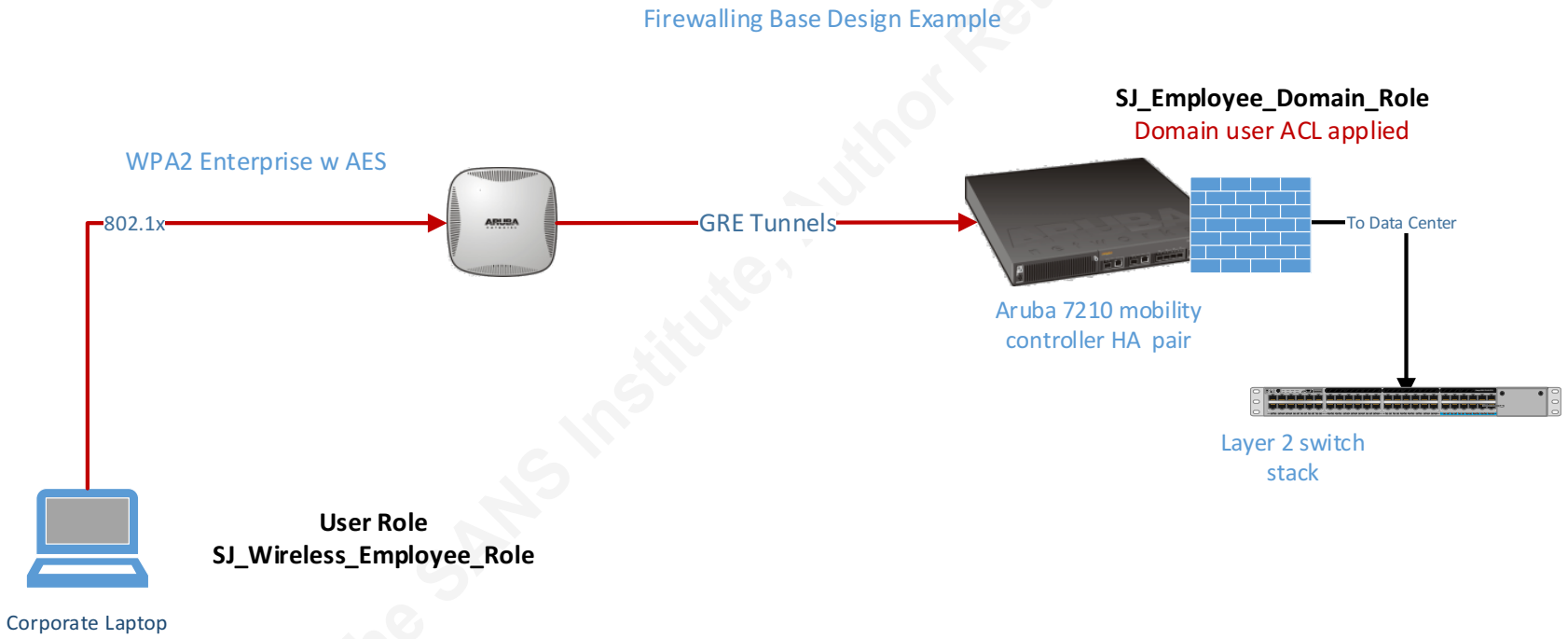
Appendix A

Network Diagrams


HIPAA Compliant WLAN Design – Base Overview
Layer 3 – data center
Aruba 7210 mobility controller HA pair
Layer 2 switch stack
PA-3020 Firewall – HA pair
Corporate Laptop
Active Directory
PKI
Domain Controllers
Employee BYOD Devices
Contractor and Guest Devices
Aruba ClearPass Policy Manager
TACACS/RADIUS
SSH
Contractor/Employee Captive Portal
Guest Captive Portal
Management access

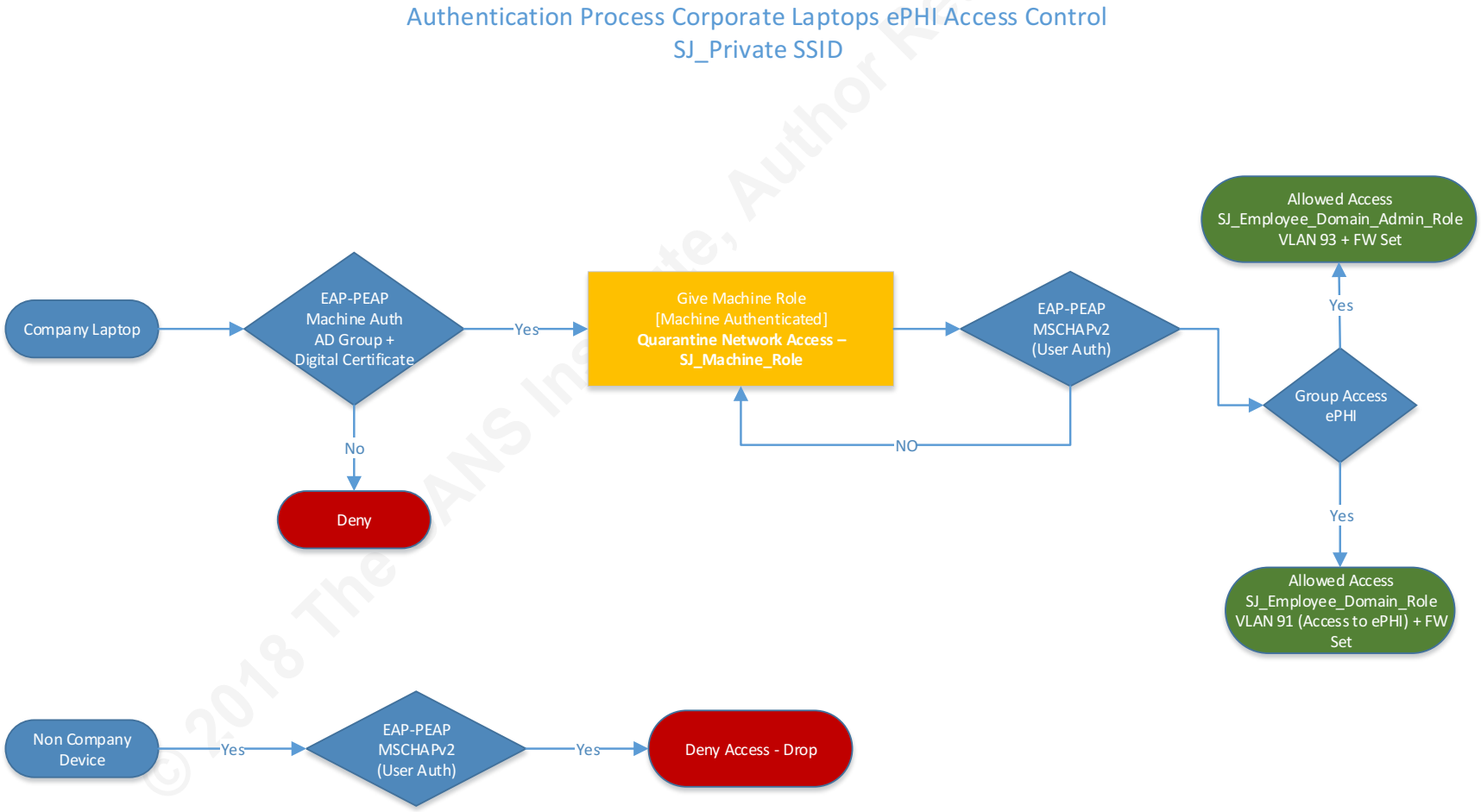


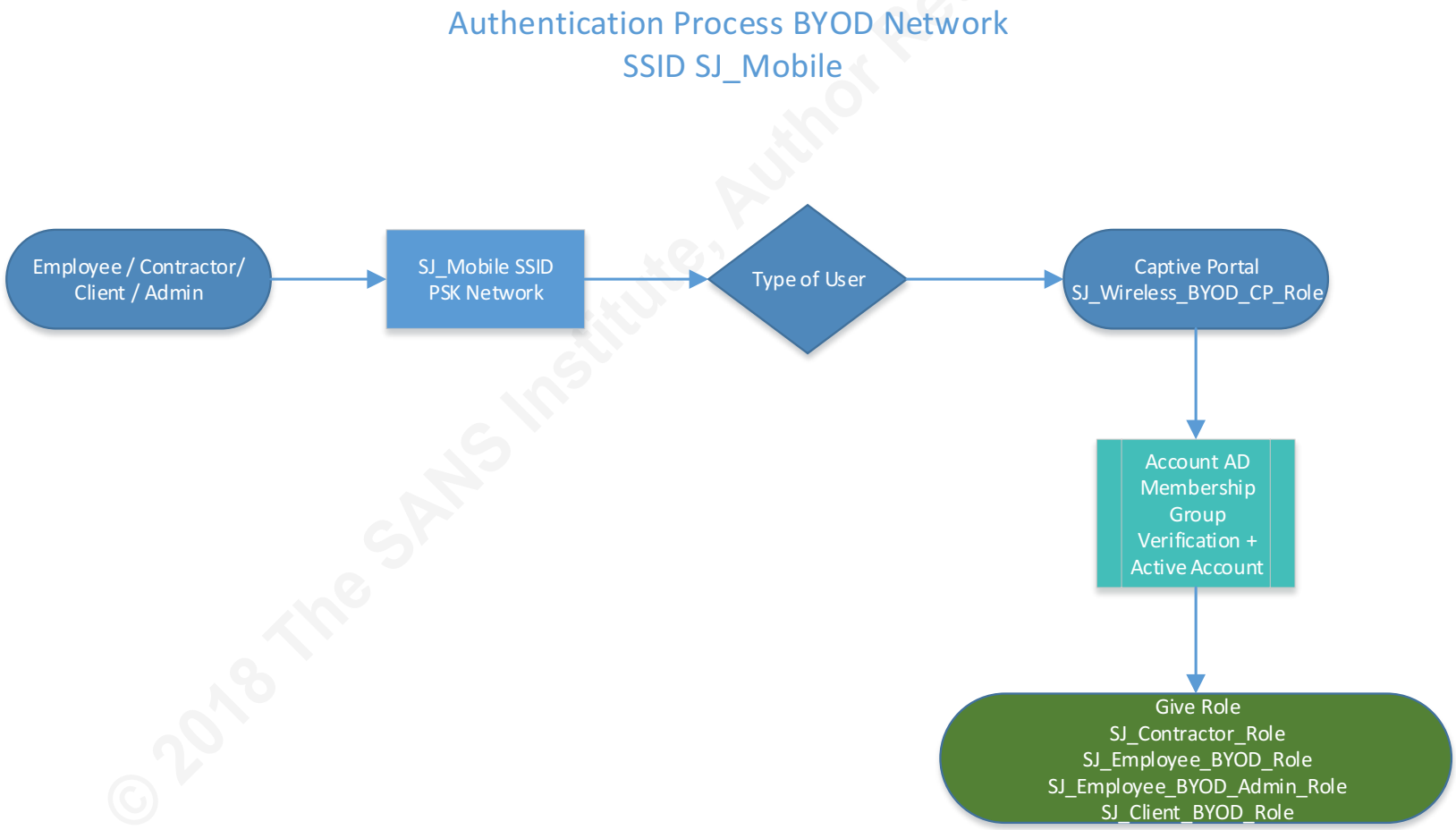

HIPAA Compliant WLAN Design – Encryption Design
Data Center
WPA2 Enterprise w AES
802.1x
GRE Tunnels
To Data Center
To Data Center
WPA2 personal w AES
Aruba 7210 mobility controller HA pair
IPSec
Captive Portal
Layer 2 switch stack
Corporate Laptop
PA-3020 Firewall – HA pair
Employee BYOD Devices
Aruba ClearPass Policy Manager
Internet Public interface
Contractor and Guest Devices
Red – encrypted traffic
Black – data center traffic
Blue – not encrypted by WLAN

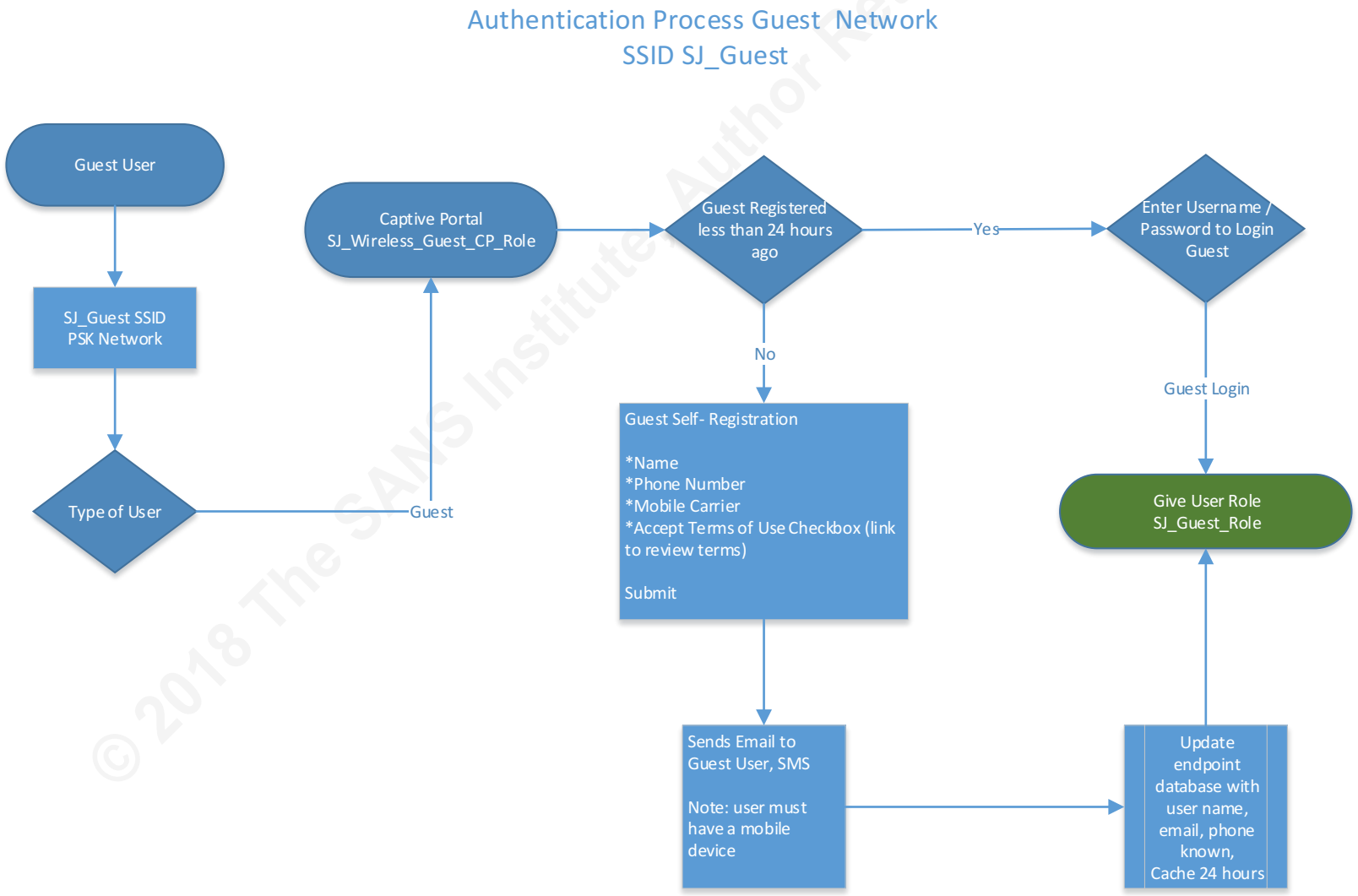


Appendix B

Authentication and Authorization Decision Diagrams



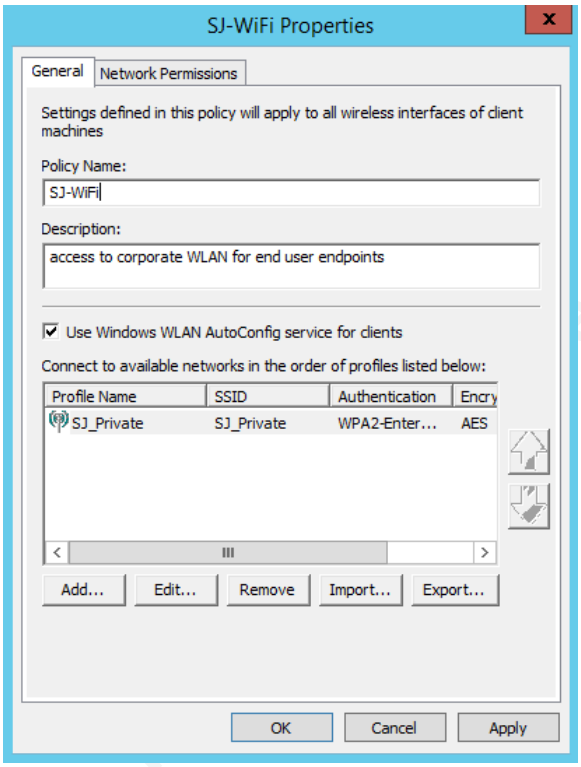




Appendix C

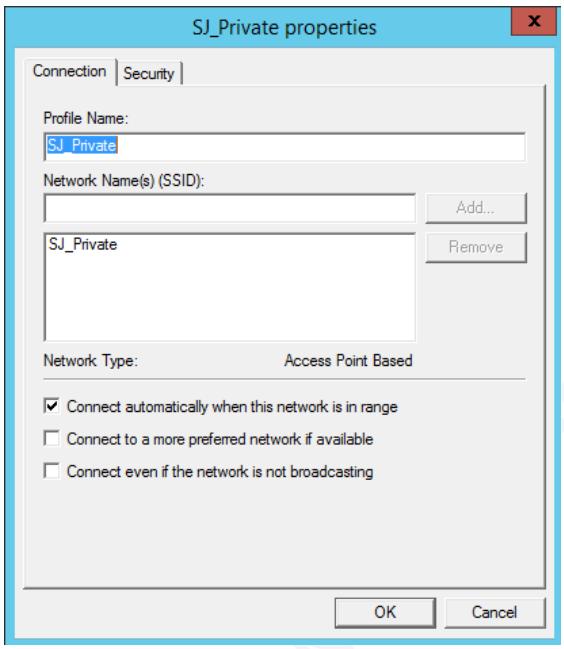
Active Directory Wireless Policy

The group policy is applied at the organizational unit level where corporate laptops are placed in Microsoft Active Directory



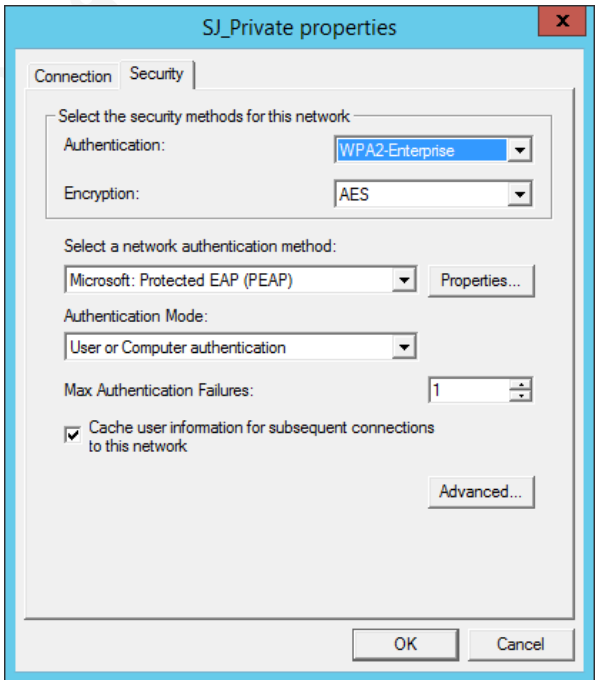
Properties for the SSID

Connect automatically when this network is in range is used to connect the device without user intervention. Note: users may disconnect from the network and connect to a different SSID.



Security Specification – WPA2-Enterprise with AES encryption

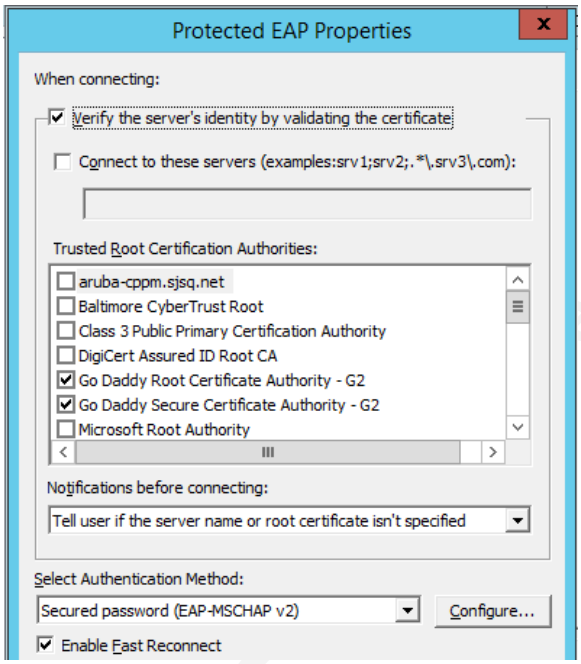
Authentication Method – Microsoft Protected EAP (PEAP) – Authentication Mode: User or Computer authentication



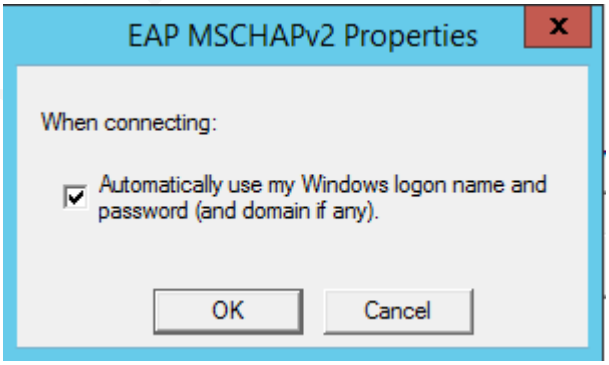
Network Authentication Method Properties

Mutual authentication is forced by the "Verify the server's identity by validating the certificate" setting.

The authentication method for users is Secured password (EAP-MSCHAP v2)



For user authentication the users' Windows password is used



Network permissions