AVAYA
The Power of We™

Leveraging Stealth Networking to Facilitate HIPAA-compliance

Table of Contents

Delivering and maintaining a converged HIPAA-compliant network can be dramatically simplified by leveraging the Avaya VENA Fabric Connect technology to create stealthy networking services.

Introduction

As communication technologies continue to evolve, many previously independent systems are now networked and operate in highly regulated environments. A prime example is health care environments, where the protection of personal medical records and data is government mandated. In the United States, the Health Insurance Portability and Accountability Act (HIPAA) places specific obligations on businesses operating in such environments.

HIPAA applies to Protected Health Information (PHI). PHI and ePHI, protected information that is transmitted electronically[1], is health information that relates to a specific individual, such as the individual's name, email address, phone number, medical record number, photo, driver's license number, and similar identifying information.

HIPAA compliance applies to entities that handle PHI, which include:

1. **Health plans**: With certain exceptions, an individual or group plan that provides or pays the cost of medical care.

2. **Health care clearinghouses**: An entity that either processes or facilitates the processing of health information from various organizations such as those who reformat or process the data into standard formats.

3. **Health care providers**: Individuals that provide care, services, or supplies related to the health of an individual, including preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual that affects the structure or function of the body; and sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Protecting the confidentiality, integrity, and availability of ePHI is the essence of the HIPAA Security Rule.

The HIPAA language uses the terms 'required' and 'addressable'. Required (R) means that the given standard is mandatory for compliance. Addressable (A) means that the given standards must be implemented by the organization unless assessments and in depth risk analysis conclude that implementation is not reasonable and appropriate specific to a given business setting. Addressable does not mean optional.

The United States Department of Health and Human Services (HHS) provides guidance around the implementation required (R) and addressable (A) standards in the specifications below:

Unique User Identification (R) – Assignment of a unique user ID to each employee that allows organizations to track user activity while the user is logged into an information system.

Automatic Logoff (A) – Automatic logoff, after a certain period of inactivity, should be implemented on every workstation that has access to ePHI.

Encryption and Decryption (A) – This is not required, but recommended as a safeguard to be implemented if deemed reasonable and appropriate for the covered entity.

Audit Controls (R) – This refers to implementing a system that logs and monitors activity on information systems with ePHI.

Authentication (R) – In terms of person or entity authentication, proof of identity should include a password or pin, smart card, token, key and/or biometrics.

Transmission Security (A) – The primary method to protect ePHI is through the use of network communications protocols, although other methods include data or message authentication codes. Encryption is another option to consider.

Protecting the confidentiality, integrity, and availability of ePHI is the essence of the HIPAA Security Rule. Since data centers are typically used to store, transmit, or process ePHI, they must comply with the HITECH standards and citations to meet HIPAA compliance.

First and foremost is the need to secure the data path. By providing strict control of forwarding path behavior, the Avaya VENA Fabric Connect technology contributes to meeting HIPAA requirements.

The fast and nimble private networking circuit-based capabilities of Avaya Fabric Connect are unparalleled in the industry and do not require complex mixes of protocols or design practices.

Avaya VENA Fabric Connect Technology

Fabric Connect is Avaya's extended implementation of the IEEE 802.1aq Shortest Path Bridging standard. It offers a series of 'circuit-based' services that can be provisioned as either Layer 2 or Layer 3. These circuits are constructs known as I-SID's (or I-Component Service Identifiers). When deployed in a specific manner, they can yield stealthy networking services including networking constructs that are enclosed, are self-contained with strictly controlled external accessibility (in or out), have little or no observable attack profile, and are mutable in both services and coverage characteristics. The comparable terms in conventional networking are MPLS IP-VPN, Routed Black Hole Networks, and IP VPN Lite.

Fabric Connect's fast and nimble private networking circuit-based capabilities are unparalleled in the industry and do not require a complex mix of protocols or design practices. These private, stealth networks are provided as standalone services within the Fabric Connect cloud and are available as:

Layer 2: non-IP Virtual Service Network

Layer 3: IP Virtual Service Network

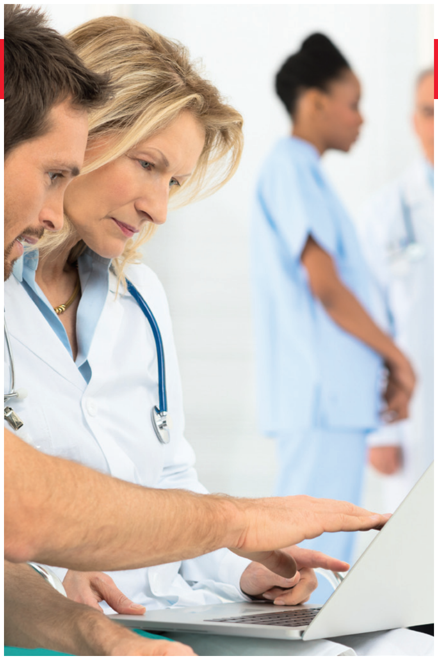
Stealth networks basically fall into two category types. The first includes networks that require security and isolation such as HIPAA compliance. The second is comprised of networks that require services separation such as Multicast, Bonjour and SCADA-based applications. Stealth networks effectively provide for both requirements categories.

Service and Path Separation and Control

In the context of ePHI, the major focus for Fabric Connect is service and path separation and control, which is enabled by its next generation-network segmentation capabilities.

Using network segmentation to reduce the scope of compliance to the segment of a network where the particular applicable data resides helps organizations reduce resources, costs and time needed for the audit process.

Network segmentation can also help limit data exfiltration. Many high-profile breaches today involve the failure to strictly control access to protected data. Using network segmentation, application servers and data can be designated in different segments based on their risk factors and security classifications, with access to them tightly controlled. This not only limits user access to sensitive ePHI, but if a breach does occur, exfiltration is restricted to a particular segment.



Simplifying the Delivery of Network Segmentation

The Avaya Fabric Connect technology can be deployed in concert with an access control broker element known as Avaya Identity Engines (IDEs). When deployed together with Fabric Connect, Identity Engines becomes a very powerful enforcement tool that can address the topic of network segmentation.

Fabric Connect and IDEs can be used to provide an enforcement paradigm for the ePHI network service paths that help in the protection of ePHI data as it is stored and transported across the network. Considerations include restricting access to only those with unique, valid, and auditable credentials, and enforcing the compliance of devices with current anti-virus and anti-spyware software. Additionally, it can compliment and simplify audit requirements.

There is another concept known as 'composite identities'. This basic concept relates to elemental constructs of device/user combinations, but can become unclear when the concept extends to applications or services. Alternatively, it can extend to elements such as the location or system users log into. All are elements of a composite instance of a user and are contained within a space/time context. As an example, 'User A' may be allowed to access 'Application A' from 'Location A' with 'Device A'. But any other location, device or even time combination may provide a totally different authentication, and trigger an access authorization response, up to and including complete denial of service.

The composite approach is particularly powerful when combined with the strong path control capabilities of Fabric Connect. This combination enables IT to determine network placement, both expected and within profile, but more importantly for those that don't match the normal user's profile. These instances may require additional challenges and authentications.

Many businesses operating in the heath care field also have a parallel requirement to deliver ubiquitous network segmentation to support payment card services. Traditionally, payment for medical services involved a small number of terminals restricted to set locations, and this has been ably supported by a dedicated point-of-sale infrastructure, usually supplied by the principle financial services clearing house.

However, the situation has evolved. Organizations increasingly need to support a widespread card payment infrastructure, which is typically driven by the need to process payment for non-medical bedside services such as Pay TV, Internet access, concierge services, etc.

This scenario mandates multiple card terminals spread throughout the environment. It is driving businesses that want reliable and secure network segmentation toward converging card payment services onto the unified multi-service network. This acts as further justification for deploying a feature-rich network virtualization technology that can easily support multiple mission-specific service networks.

The composite approach is particularly powerful when combined with the strong path control capabilities of Fabric Connect.

Think of this concept as a series of gates. The first gate identifies a particular user/device combination. Network access is provided according to a policy, and users are limited to the paths that provide access to a normal profile. As a user attempts to access a secure application, the network responds with another challenge, which could be an additional password or secure token and biometric signature to reassure identity for an added degree of trust. This is normal, 'steady-state' behavior. However in this scenario, access is provided at the systems level, which increases the possibility to conceal a user's identity.

In this approach, the network placement profile of the user changes. In other words, in the previous network profile, the system that provides the secure application is not available by any viable network path. Access (versus connectivity) is granted by meeting additional challenges and authentication tiers. At the user edge, entire logical topology changes occur, which place the user into a fabric-based, stealth virtual private network environment where secure, segregated access to the sensitive application can be ensured.

Within the anatomy of circuit-based services, a Layer 2 stealth network is an I-SID associated with a specific VLAN; in this case the VLAN is not configured with an IP Address. As such, a standalone Layer 2 network is created where no traffic can enter or exit, which is extremely useful to secure and extend Layer 2 environments. Additionally, IP can operate inside this network, but it is a self-contained IP subnet and not one routed to the outside world so it appears, in essence, invisible. As a result it can be leveraged for secure Data Center usage under circumstances where it's undesirable to enable IP accessibility. In comparison, the equivalent service in MPLS, known as Layer 2 VPLS, requires approximately 30 to 40 unique lines of configuration versus a Fabric Connect Layer 2 stealth network, which is typically created with a single command.

The anatomy of Layer 2 stealth networking is simply an I-SID, essentially an SPB 'circuit', associated with a Virtual Routing and Forwarding (VRF) instance. The VLANs attached to the VRF are assigned IP Addresses, however none of the IP subnets are reachable outside of the IP VPN environment. As a result, a standalone Layer 3 IP network is created that is essentially invisible to the outside world. This scenario is useful for a variety of secure Layer 3 environments, such as in HIPAA networks, but is also valuable in providing service separation in possible conflicting protocol environments such as the case of multiple multicast domains.

Employing Network Stealth to Secure the Data Path

Fabric-based services can be used in combination to yield genuinely closed and segregated network topologies. A L3 VSN might extend to the Data Center security demarcation point where there is a single secure port at the perimeter's Firewall/IDS boundary. On the other side of the demarcation, L2 VSNs provide for secure connectivity to Data Center services. The complete end-to-end design creates a closed network systems environment that is totally isolated from the outside world; there is simply no way in or out.

Avaya takes the concept of IP Virtual Private Networks to a new level with Fabric Connect. The combination of segmentation and mutability enables Fabric Connect to deliver highly effective stealth networking services.

This model delivers something significant. Users are assigned to 'communities of interest' where only certain traffic pattern profiles are expected. As a result, IPS/IDS alerts, generated as a result of new anomalies, are something more than white noise; they become discrete events set against a backdrop of the expected monitoring profile. Anomalies outside of that profile will produce a 'positive' alert. This enables 'Day Zero' threat systems to work far more efficiently by identifying patterns outside of the expected behaviors normally seen in the network.

Fabric Connect's role is keeping communities strictly separated and isolated. With a smaller isolated community it is far easier to use such systems accurately, defining a discrete and easily manageable virtualized security perimeter. It should be noted that any end-point is logically on the 'outer' network. Even though different VSNs traverse a common network footprint, they never see one another or have the opportunity to inter-communicate unless specifically configured as an exception, through formal monitored gateways.

Firewalls are notoriously complex when they are used for community separation or multi-tenant applications because the separation capability is dependent on the security policy database (SPD) and how well it covers all given applications and port calls. If a new application is introduced and needs to be isolated, the SPD must be modified. If this evolution is overlooked, or the settings are not correct, the application will not be isolated and the network's entire security posture may be compromised. This is the major flaw in the logic of explicit administration.

Fabric Connect's network virtualization helps control user's paths and keeps communities separate. The firewall's security policy database can be 'white listed' with a 'black list' policy that denies all. As new applications get installed, and unless they are specifically added to the white list, they will, by default, be isolated to the community in which they reside. This results in far less manipulation of individual security databases, in addition to significantly reducing the risk of an attack surface developing in the security perimeter simply due to a missed policy statement.

The stealth networking capability of Fabric Connect is particularly useful for networks that require full privacy to comply with HIPAA and a L3 Virtual Service network meets those requirements perfectly. An example is a HIPAA environment in which all subsystems are within a totally closed L3 VSN virtual private network. Ingress and egress is only available via well-defined virtual security perimeters that allow for the full monitoring of any and all allowed traffic. This combination provides an environment that, when properly designed, should meet HIPAA compliance. In addition, these networks are not only private, but invisible to external, would-be attackers. The attack surface is mitigated to the virtual security parameter only, which is practically non-existent.

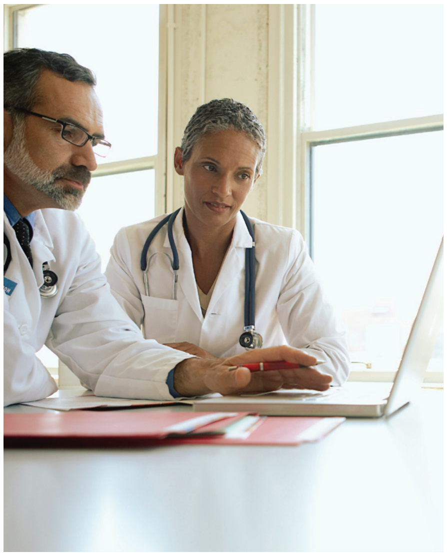
The stealth networking capability of Fabric Connect is particularly useful for networks that require full privacy to comply with HIPAA and a L3 Virtual Service network meets those requirements perfectly.

Deployment Considerations

From the Avaya Fabric Connect perspective, it's all about services separation and path control; or 'network segmentation'. No other networking technology provides a more comprehensive set of services, and with so little complexity. When creating a HIPAA compliance checklist, IT should consider:

- Terminating L3 VSNs as close to the edge as possible
  - Avoid using shared broadcast domains or VLAN extensions via tagged trunks, and if VLAN extensions are required, use L2 VSNs to maintain total separation.
- Limiting port memberships into the security demarcation only to those required.
  - Ideally this should be a single port membership to prevent unauthorized system access to the DMZ.
- Limit porting memberships to HIPAA end-points only
  - Identity Engines can greatly ease the enforcement of these access policies.
- Validating the security demarcation module and creating a defined security policy database
  - Test the demarcation to be sure that the policy database is enforced.
- Avoiding the use of the public Internet or wireless services within the end-to-end design
  - When this avoidance is impractical, use encryption to protect transit data; MACsec encryption can be used to protect exposed Ethernet trunks, and full VPN encryption (using either IPSec or SSL) can be used to provide endpoint or site connectivity. Be sure to have the VPN Gateways attached directly to the stealth network topology to ensure that no unencrypted data paths are exposed.

Private IP VPN environments have been around for many years, yet they are typically clumsy and complex to provision. This is particularly true for environments where quick dynamic changes are required. As an example, the typical MPLS IP VPN provisioning activity requires approximately 200 to 250 lines of configuration, depending on the vendor and the topology. Ironically, much of this error-prone configuration activity is not directly related to provisioning the VPN, but in provisioning underlying protocols such as gateway routing protocols. This complexity only provides the primary service path. Redundant service paths need further manual configuration. By comparison, the Avaya Fabric Connect technology provides the same service type with as few as a dozen commands, and there is no requirement to engineer and provision resilient service paths as this is provided for by the SPB's native intelligence.



Fabric Connect-based VPNs can be provisioned in minutes, and dynamically moved or extended to satisfy a variety of business requirements.

As a result, Fabric Connect-based VPNs can be provisioned in minutes, and dynamically moved or extended to satisfy a variety of business requirements. The evolution of emergency telephony services (E911) is an example of how a L3 VSN IP VPN can morph over the duration of a short-term emergency, with different agencies and individuals coming into and out of the VPN environment on a dynamic basis due to their identity, role, and group associations.

Furthermore, using SPB's IS-IS Fabric Connect-enabled nodes are themselves mutable; meaning that they may be liable to and easily capable of change. An active Fabric Connect node can be detached from the topology, relocated, and reconnected at any point and the underlying protocol will immediately re-establish full topology connectivity, with provisioned services again available. The Fabric Connect network will extend all services to the node, delivering complete portability to that node and its resident services and users.

In addition, Fabric Connect can provide separation for non-IP data environments. Using L2 VSNs, mission-specific applications can enjoy an isolated, non-IP environment where there is simply no viable path into the environment for would-be hackers.

Conclusion: Stealth Networking – Fast, Nimble and Invisible

Avaya takes the concept of IP Virtual Private Networks to a new level with Fabric Connect. The combination of segmentation and mutability enables Fabric Connect to deliver highly effective stealth networking services. Virtually undetectable, these networking constructs cannot be seen and therefore they cannot be attacked. Other IP VPN technologies would find it difficult to make these claims, if indeed they can make them at all, and certainly not with operational simplicity unique to Fabric Connect.

The Avaya VENA Fabric Connect technology, based on the IEEE 802.1aq Shortest Path Bridging technology, sets the foundation for genuine private cloud networking, allowing for the versatile creation and deployment of stealth networking services, which facilitates HIPAA compliance.

[1] U.S. Dept. of Health and Human Services, HIPAA Security Series: Basics of Risk Analysis and Risk Management

About Avaya

Avaya is a global provider of business collaboration and communications solutions, providing unified communications, contact centers, networking and related services to companies of all sizes around the world. For more information please visit **www.avaya.com**.

Provide FEEDBACK for this document