Extreme™
Customer-Driven Networking

Solution Brief

Leveraging Stealth Networking to Facilitate PCI-Compliance

In recent decades communication technologies have realized significant advancement and these technologies now touch almost every part of our lives, sometimes in ways that are not immediately apparent. As this evolution continues, many systems that have previously been treated as discrete are now networked. Examples of these systems are power grids, metro transit systems, water authorities, and many other public services. Other examples are networks that operate in environments subject to the compliance and regulatory requirements of the Health Insurance Portability and Accountability Act and the Payment Card Industry Security Standards Council.

While this evolution has brought on a very large benefit to both those managing and using the services, there is the rising specter of security concerns and the precedent of documented attacks on these systems. This has brought about strong concerns about this convergence and what it portends for the future.

The requirements for total Payment Card Industry Data Security Standard (PCI DSS) compliance are numerous and complex, and as such no technology or solution can claim as automatically compliant to the regulation.

Ultimately, scanning or auditing of the actual implementation by qualified staff is required, however a lot can be done to prepare for site-specific validation. First and foremost is the need to secure the data path; Extreme's Fabric Connect technology contributes to these requirements by providing strict control of forwarding path behavior.

Fabric Connect Technology

The effort to deliver and maintain a unified network that supports PCI compliance can be dramatically simplified by leveraging the Fabric Connect technology from Extreme Networks to create and deliver stealthy networking services.

Fabric Connect is Extreme's extended implementation of the IEEE 802.1aq Shortest Path Bridging standard. Fabric Connect offers a series of 'circuit-based' services that can be provisioned as either Layer 2 or Layer 3, depending on requirements. These circuits are constructs known as I-SID's (or I-Component Service Identifiers). If these services are deployed in a specific manner they can yield stealthy networking services; networking constructs that are enclosed, self-contained with strictly controlled external reachability (in or out), and with little or no observable attack profile. It is also highly desirable that these constructs be 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.

Extreme's Fabric Connect provides for fast and nimble private networking circuit based capabilities that are unparalleled in the industry and do not require complex mixes of protocols or design practices. Hence, stealth networks are private ('dark') networks that are provided as standalone services within the Fabric Connect cloud. They come in two different forms:

- Layer 2 non-IP Virtual Service Network
- Layer 3 IP Virtual Service Network

There are many uses for stealth networks, but they basically fall into two category types. The first being for networks that require security and isolation, and examples are PCI & Health Insurance Portability and Accountability Act (HIPAA) compliance, financial and trading applications, video surveillance and process flow control environments such as those facilitated by SCADA (Supervisory Control And Data Acquisition) type protocols. The second category is networks that require services separation such as Multicast, Bonjour, and again for SCADA-based applications.

Stealth networks help provide for both requirements categories. While this document is focused on PCI DSS, these services can also be applied to other closed, service-separated networking requirements such as those for HIPAA and CIP/NERC (Energy Regulatory).

Payment Card Industry Standards

It is valid to first define the PCI standards of PCI DSS and PA-DSS. PA-DSS, the 'Payment Application – Data Security Standard', is the security standard that specifically addresses the application, as such it is a subset of PCI DSS, the 'Payment Card Industry Data Security Standard'. An important aspect of PA DSS is that it defines what a 'compliant' application must, by design, support. Areas of concern are the handling of magnetic stripe data, card verification codes and personal identification numbers (PINs). If a point of sale application is sold 'off the shelf' it must comply with this certification. Where developed in-house, it is the responsibility of the merchant or service provider to properly design and certify the application.

In contrast, PCI DSS deals with the broad end-to-end implementation as deployed. As such, the end-to-end system must be 'scanned' by properly trained and certified consultants to gain compliance. This is an important consideration because if the deployment is not properly thought-out, compliance can become a moving target where any changes to the deployment can put compliance a risk. Fortunately, there is an approach referred to as 'sampling' and the use of deployment templates that can dramatically ease both the attainment and on-going maintenance of compliance. Fabric Connect and the use of secure circuit-based services can drastically ease the burden of developing and enforcing a template PCI DSS design.

In the context of PCI, the major focus for Fabric Connect is in the areas of service and path separation and control; this is enabled by its next generationnetwork segmentation abilities. According to PCI DSS, while network segmentation is not explicitly required for compliance, its use is strongly recommended. Network segmentation can provide an effective foundation for sampling and templates. As such, its use can reduce the scope of the initial assessment and as a result its overall cost. Additionally, it can provide for significant reduction in the cost of ongoing maintenance of the environment. But this is only if the network segmentation is properly designed, implemented, and secure.

Proper design can lead to modularity and the ability to maintain consistency between modules. The end result is the ability to streamline compliance by the use of these templates and sampling.

Simplifying the Delivery of Network Segmentation

Extreme's Fabric Connect technology, based on an extended implementation of the IEEE's 802.1aq Shortest Path Bridging standard, can be deployed in concert with an access control broker integrated into Extreme Management Center. When used in tandem with Fabric Connect, this becomes a very powerful PCI enforcement tool that can address the topic of network segmentation as it is addressed in 'Appendix D' for PCI DSS compliance. A high level overview of the twelve requirements is provided as follows:

Build and Maintain a Secure Network

1. Install and maintain firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect cardholder stored data
4. Encrypt transmission of cardholder data accross open, public network

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software system or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know
8. Assign a unqiue ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and carholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

Fabric Connect and ExtremeControl, within the Extreme Management Center suite, can be used to provide an enforcement paradigm for the PCI DSS network service paths for a number of these requirements; namely 3, 5, 7, 8, and 10. The solutions use also compliments and simplifies PCI audit requirements.

There is a concept known as 'composite identities' and, in cyber-space all identities are essential thus. This basic concept is rather obvious when it speaks to elemental constructs of device/user combinations, but it gets smeared and somewhat fuzzy when the concept extends to applications or services. Alternatively it can extend to elements such as location or systems that a user is logged into. All are elements of a composite instance of a user and they are contained within a space/time context. As an example, we may allow 'User A' for 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 consequent access authorization response, up to and including complete denial of service.

This composite approach is very powerful, and particularly so when combined with the rather strong path control capabilities of Fabric Connect. This combination yields an ability to determine network placement, both expected and within profile, but more importantly for those that are unusual and out of the normal users profile.

These instances may require additional challenges and consequent authentications. This concept can be visualized as a series of gates. The first gate provides identification of a particular user/device combination. From this elemental composite, network access is provided according to a policy, and users are limited to the particular paths that provide access to a normal profile. As a user attempts to access a secure application the network responds with an additional challenge. This may be an additional password or perhaps a certain secure token and biometric signature to reassure identity for the added degree of trust. This is all normal, 'steady-state' behavior. However in this scenario, access is provided at the systems level, thereby increasing the 'smear' of the user's identity.

A critical distinction for the approach under discussion is that 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 even available by any viable network path. It is by the renewal of challenge and additional tiers of authentication that connectivity is finally granted. It should be noted that we are discussing access as opposed to connectivity. Systems access controls would of course remain, but, by and large, these would be the final gates involved. At the user edge, entire logical topology changes occur that place the user into a Fabric-based, stealth virtual private network environment where more secure, segregated access to the sensitive application can then be obtained.

Taking a moment to discuss the anatomy of circuit-based services, a Layer 2 stealth network is simplicity itself, being 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, and these are extremely useful to help secure and extend Layer 2 environments (such as those delivering SCADA services). Layer 2 stealth networks allow for a pain-free and more secure distribution of such environments. Additionally, IP can operate inside this style of network, but it is a self-contained IP subnet and not one routed to the outside world; it is, in essence, invisible. As a result they can be leveraged for more secure Data Center usage where it may be undesirable to enable IP reachability.

As a comparison, the equivalent service in MPLS, known as Layer 2 VPLS, requires approximately thirty to forty unique lines of configuration whereas a Fabric Connect Layer 2 stealth network is typically created with a single command.

The anatomy of a Layer stealth networking is correspondingly simple. It is nothing more than 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 such, a standalone Layer 3 IP network is created where nothing can enter or exit. It is, in essence, invisible to the outside world. This scenario is useful for a variety of Layer 3 environments with enhanced security, such as PCI DSS networks, but is also useful in providing service separation in possible conflicting protocol environments such as the case of multiple multicast domains.

Securing the Data Path

Fabric-based services can be used in combination to yield genuinely closed and segregated network topologies. A Layer 3 VSN can be used to extend network PCI compliance support to distant point-of-sale applications. These PA-DSS application end-systems will gain access to the network via authentication provided by ExtremeControl technology. The L3 VSN might then extend to the Data Center security demarcation point where there is a single 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 yields a closed network systems environment that is isolated from the outside world.

This model delivers something significant. Users are now 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 correctly flag as a 'positive' alert that should be investigated. This enables 'Day Zero' threat systems to work far more efficiently, complementing the very logic of their theory of operation, that being to look for patterns outside of the expected behaviors that are normally seen in the network. Fabric Connect's role is in keeping communities strictly separated. 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 are 'ships in the night'; 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. The reason for this is that 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 to reflect it.

If this evolution gets overlooked or the settings are not correct, the application is not isolated and the network's entire security posture may be compromised. This is the major flaw in the logic of explicit administration. Again Fabric Connect's network virtualization helps in controlling user's paths and keeping communities separate. Now the Firewall's security policy database can be 'white listed' with a 'black list' policy that then denies all. Now as new applications get installed, and unless they are specifically added to the white list, they will, by default, be isolated to the community that they reside in. This results in far less manipulation of individual security databases in addition to a significantly reducing the risk of an attack surface developing in the security perimeter simply as the result of a missed policy statement.

Networks that require full privacy in order to support PCI compliance are those where Fabric Connect's stealth networking capability is particularly useful; L3 Virtual Service Networks are perfect for these solution requirements. A ready example might be that of a PCI 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 yields an environment that, when properly designed, should pass PCI compliancy scanning and analysis. In addition, these networks not only are private, but they are invisible to external, would-be attackers. The attack surface is mitigated to the virtual security parameter only, and as such it is practically non-existent.

As previously noted, the use of sampling can greatly reduce the cost and complexity of attaining and maintaining compliance. The practice does however require discipline in both the modularity and consistency of the design and implementation. Modules can be based upon well-defined templates and subsequently re-produced, but this must be done exactly as defined within the approved template. Variations will result in the need for re-scanning and caution must be exercised, as small, seemingly inconsequential divergence from the templates can result in the need to scan. For example, where a new operating system is used in a remote point-of-sale location, or in a Data Center where a particular data repository is migrated to a different Storage Area Network (SAN) technology.

However, where properly implemented, sampling and templates can drastically reduce the overall compliance and on-going maintenance costs.

As defined in 'Appendix D' of the PCI DSS documentation, if the requirements for network segmentation are both realized and validated then the entire process moves on to the sampling of business facilities, system components, and practices. Extreme's Fabric Connect technology can address all network segmentation requirements without the need for undue complexity such as that observed with technologies such as MPLS.

Dictating module demarcation points and implementing modules exactly as defined within the templates enables compliancy to be streamlined. As an example, for remote point-of-sale locations, a series of templates can be created, such as small, medium and large, and these templates could cover typical hardware, network topologies and configurations. Adhering to these templates means that during compliance scanning only one representative of each type needs to be validated, being equivalent for all like templates. Therefore, an organization dealing with a large number of point-of-sales locations can significantly reduce the overall cost and difficulty of attaining and maintaining compliance.

Deployment Considerations

From Extreme's Fabric Connect perspective it's all about services separation and path control; or 'network segmentation' in PCI DSS parlance. No other networking technology provides a more comprehensive set of services, and with so little complexity. The PCI DSS compliance checklist will run along the lines of:

- Be sure to terminate 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
- Limit 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 port memberships to PA-DSS end-points only
  - Extreme Management Center can greatly ease the enforcement of these access policies.
- Avoid mixing any non PA-DSS applications in the PCI DSS stealth network topology even if they do not access anything on the outside
  - Such mixing can result in the violation of templates and hence require full site scanning
- Validate the security demarcation module and create a defined security policy database and network topology template
  - Be sure to do testing of the demarcation to be sure that the policy database is enforced
- Avoid 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 help ensure that no unencrypted data paths are exposed.

Private IP VPN environments have been around for many years, yet they typically remain clumsy and complex to provision, and this is particularly true for environments where quick dynamic changes are required. As an example, the typical MPLS IP VPN provisioning activity will require 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. And remember that this is just to provide the primary service path, with redundant service paths needing further manual configuration. By comparison, Extreme's 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 natively provided for by SPB's intelligence.

As a result, Fabric Connect-based VPNs can be provisioned in minutes, and dynamically moved or extended to satisfy a variety of business requirements. For example, the evolution of emergency telephony services (E911) speaks to how an 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, Fabric Connect-enabled nodes are themselves mutable; meaning that they may be liable to and easily capable of change; SPB's IS-IS delivers this capability. An active Fabric Connect node can be detached from the topology, relocated, and reconnect 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, thereby delivering complete portability to that node and its resident services and users.

In addition, Fabric Connect can provide separation for non-IP data environments where mission-specific applications can enjoy an isolated, non-IP environment by the use of L2 VSNs and further, they can be isolated to mitigate any risk of would-be hackers gaining a viable path into the environment.

Conclusion

It's the combination of segmentation and mutability that enables Fabric Connect to deliver highly effective stealth networking services. Presenting virtually no observability these networking constructs cannot be seen and therefore they mitigate the risk of attack, lacking the 'profile' for such an endeavor. They are agile in the way they can morph through the use of services extensions. Other IP VPN technologies would be very hard pressed to make such claims, if indeed they can make them at all, and certainly not with operational simplicity unique to Fabric Connect.

The Fabric Connect technology from Extreme Networks, based as it is 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, and as such facilitates the acquisition and retention of PCI DSS compliance.