Securing Distributed Enterprise Networks for PCI DSS 3.0 Compliance

Accelerating Compliance and Simplifying Complex Networks

Introduction

Distributed Enterprise networks have grown in complexity over the last decade as they expand network access and add more security technologies to protect their networks. The adoption of standards such as the Payment Card Industry Data Security Standard (PCI DSS) has also improved the overall security of data in distributed enterprise networks like retail and food service by requiring specific practices.

However, in light of many well-publicized data breaches, it is clear that distributed enterprise networks are still vulnerable to being compromised. This paper will discuss some of the common challenges Distributed Enterprise networks face in securing their remote or branch locations. It will also provide several specific ways Fortinet’s comprehensive product portfolio can help secure and simplify Distributed Enterprise networks to accelerate compliance with PCI DSS 3.0.

Most attacks are focused at cardholder data:
According to the 2014 PCI Verizon Business Report, 74% of attacks on retail, accommodation, and food services companies target payment card information.¹

The Evolving Network in Distributed Enterprise Environments

Distributed Enterprise networks have grown in complexity over the last several years with the addition of numerous networking technologies to meet changing business requirements.

Network Challenges

A typical Distributed Enterprise network may include the following:

- "Store-within-a-Store" operation by retail partners
- Wireless LAN access for employees and guests
- Kiosks and Point of Sale (POS) terminals
- LTE to support Quality of Service (QoS) requirements
- Power over Ethernet (PoE) powered-systems like VoIP phones or IP video surveillance systems
- WAN access technologies such as 4G or satellite for primary or secondary access
- Switches to expand capacity to connect all of these devices to the network
- Support for ‘Store of the Future’ initiatives such as wireless inventory management, customer analytics, customer web portals, social marketing, smart digital signage, and other omni-channel marketing technologies

Security Challenges

What started out as an initial Firewall deployment in a store or office may have grown to include a range of technologies from several vendors:

- Application Control
- Web Filtering
- Intrusion Prevention (IPS)
- WAN Optimization
- Data Leak Prevention (DLP)
- Wireless Access Points
- End-Point Protection

¹ Data from Verizon Data Breach Investigations Reports (DBIRs), 2011, 2012 and 2013.
Verizon 2014 PCI Compliance Report
www.verizonenterprise.com/pcrireport/2014
These stand-alone technologies can create gaps in policy enforcement caused by separate devices with separate rule sets that lack central management. They can also overwhelm small IT teams and drive up CapEx and OpEx costs, especially when duplicated over dozens, hundreds or even thousands of locations.

**PCI DSS 3.0 Compliance and Distributed Enterprise Networks**

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard for data security of cardholder data that affects a very broad group of businesses. It applies to all entities involved in processing of payment cards, such as merchants, card issuers, processors, and service providers, as well as those that process, transmit, or store cardholder data. There are 12 requirements within six control objectives:

<table>
<thead>
<tr>
<th>PCI DSS CONTROL OBJECTIVES</th>
<th>REQUIREMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network and Systems</strong></td>
<td>Install and maintain a firewall configuration to protect cardholder data&lt;br&gt;Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
<td>Protect stored cardholder data&lt;br&gt;Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td><strong>Maintain a Vulnerability Management Program</strong></td>
<td>Protect all systems against malware and regularly update anti-virus software or programs&lt;br&gt;Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td><strong>Implement Strong Access Control Measures</strong></td>
<td>Restrict access to cardholder data by business need-to-know&lt;br&gt;Identify and authenticate access to system components&lt;br&gt;Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Regularly Monitor and Test Networks</strong></td>
<td>Track and monitor all access to network resources and cardholder data&lt;br&gt;Regularly test security systems and processes</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
<td>Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>

PCI DSS version 3.0, the current version of the standard, includes many updates from the previous version of the requirements to reflect the evolving networking and threat landscapes. The intent of version 3.0 is to reduce confusion, misinterpretation, and reinforce best practices, and the majority of the updates are “Clarifications” or “Additional Guidance” to existing requirements. The goal is to make PCI DSS compliance “Business As Usual” and to be incorporated in everyday business practices instead of being a periodic focus.

Version 3.0 includes several examples of best practices:
- Monitoring of security controls such as firewalls to ensure effective operation
- Detecting and responding to any security control failures
- Reviewing changes to the environment (such as new configurations or systems) in the context of PCI DSS scope before completing the change, and updating security controls appropriately
- Reviewing deployed hardware and software technologies to confirm that they are still being supported by the vendor and they meet the entity’s security requirements

---

1 Payment Card Industry Data Security Standard “Requirements and Security Assessment Procedures version 3.0”
New Requirements

There are several new requirements that will affect distributed environments in particular, due to their large number of locations, wide range of hardware and software systems deployed in those environments and use of managed services. Some examples include:

New Requirement 2.4: Maintain an Inventory of System Components that are in Scope for PCI DSS

Organization are now required to maintain a list of all system components (both hardware and software) including a description of each component’s function, and interviewing personnel to verify that the inventory is current.

New Requirement 5.1.2: For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.

This requirement expands the requirement to include all systems that could be affected by malware, which includes open source and custom software, not just the critical systems previously identified.

Requirement 8.5.1: Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.

This requires service providers to use unique authentication credentials for each customer, such as two-factor authentication. The intent is to prevent multiple customers from being compromised by a single set of credentials.

Limitations of Legacy Security Systems

The PCI core requirements cover controlled network isolation, inbound/outbound traffic flows and DMZ implementation related to defining and protecting the Cardholder Data Environment (CDE). Specific functions include:

- Real-time perimeter anti-malware/anti-virus
- IPSec/VPN tunneling support
- Intrusion Detection/Prevention (IDS/IPS)
- Use of strong cryptography (SSL/IPSec)
- Default “deny-all” settings
- Support of digital certificates and two-factor user authentication
- Event monitoring
- Federated device management and reporting
- Network vulnerability analysis support

A legacy firewall cannot provide these services due to the lack of required functions and/or the lack of performance, whether it is at remote location like a store or distribution center, in a central location like headquarters, or in a datacenter. Organizations need the ability to deploy a single operating system with a range of firewall personalities, both physical and virtual. In addition to simplifying deployment and standardizing IT staff training, a single flexible OS also enables the delivery of the appropriate security and networking functions for a particular use case:

- At the remote location, a single all-in-one device to consolidate all of the security functions and eliminate the cost and complexity of deploying multiple devices
- At the headquarters or regional office, a high performance next generation firewall to provide the core network security features
- At the data center, a high performance firewall to deliver core firewall functions with extremely high throughput and ultra-low latency

Fortinet Network Security Solution

Fortinet’s FortiGate® line of high performance network security devices can help organizations address the wide range of requirements of PCI while minimizing implementation and operational costs.

FortiGate devices provide seamless integration of networking and security in a single appliance with the most comprehensive feature set of any consolidated network security device, including Anti-Malware/Anti-Virus, Intrusion Prevention, Application Control, SSL and IPsec VPN, Web filtering, support for two-factor authentication, and asset discovery/vulnerability management. Customers can deploy as much or as little technology as they want, based on their specific requirements.

PCI DSS 3.0 states “Network segmentation of, or isolating (segmenting) the CDE from the remainder of an entity’s network, is not a PCI DSS requirement.”

As a best practice, however, network segmentation reduces the scope and cost of the PCI DSS assessment, reduces the complexity of maintaining controls, and reduces risk to an organization.

Every FortiGate supports physical and virtual segmentation of data with switched ports and the ability to create virtual domains to isolate the CDE and significantly reduce the number of systems in scope.
Figure 2 - Comprehensive security and networking feature set with every FortiGate physical and virtual appliance

The FortiGate family of appliances includes physical and virtual appliances that range in form factor from compact desktop models to chassis-based systems delivering over 500 Gbps firewall throughput.

Every FortiGate system offers complete yet flexible network services and threat protection that meets and exceeds the compliance requirement:

1. **Firewall** – Enables network segmentation using virtual domains, VLANs and switched ports for traffic segmentation/isolation. Prevents unauthorized access to critical resources
2. **Intrusion Prevention System (IPS)** – Detects and blocks network intrusion and other hacks by cybercriminals
3. **Application Control** – Identifies and stops malicious application activities while allowing only authorized applications
4. **Web Filtering** – Blocks visits to or content from malicious sites
5. **VPN** – Encrypts and protects data transmitted across untrusted networks
6. **Advance Threat Protection** – Anti-Malware engine and Sandbox integration prevents malicious code exploitation, detects targeted and advance persistent threats
7. **Data Leak Prevention (DLP)** – Discovers and prevents unauthorized transmission of sensitive data
8. **Vulnerability Management** – Automatically and routinely scans to ensure that systems and applications are at appropriate patch levels and vulnerabilities have been addressed
9. **Visibility & Monitoring** – Provides monitoring, logging and notification of incidents or suspicious activity that may indicate an incident allowing organizations to quickly respond
10. **Switched Ports and High Port Density** – Every FortiGate device includes switched Ethernet ports for network segmentation and data isolation. High port density consolidates connectivity, networking and security into a single device

Figure 3 - FortiGate devices consolidate security, networking, and connectivity into a single device

**Wireless Security Solution**

In addition, every FortiGate device has an integrated Wireless Controller, enabling organizations to consolidate wired and wireless traffic and enforce policies consistently. Administrators can plug in wireless access points directly into a FortiGate device, which allows the FortiGate to eliminate the need for a separate stand-alone wireless network and the need to try to duplicate policies on separate network and wireless security systems.

- All of the FortiGate desktop models (FortiGate-20C through the FortiGate-90D) offer FortiWiFi versions, which incorporate a Wireless fat client.
- Many FortiGate devices for remote locations and offices support Power Over Ethernet (PoE) which eliminates the need to supply power to wireless access points, VoIP handsets, IP security cameras or other IP-based devices.

**Wireless Access Points**

*Requirement 11: Regularly test security systems and processes.*

Requirement 11 contains several components related to Wireless Access and the need to inventory Wireless Access Points and detect Rogue Access Points.

FortiAP Thin Wireless Access Points enable simple, cost-effective, and secure Wireless Network Access. FortiAPs are an ideal solution for extending FortiGate protection to the wireless network. The integrated Wireless Controller within every FortiGate device eliminates the majority of the cost of deploying a wireless network.
With models designed for small Branch Offices, Distributed Enterprise locations, as well as high-density Headquarters, FortiAPs allow consistent enforcement of security policies across both wired and wireless networks.

The FortiGate Rogue AP detection engine, including the ‘on-wire’ detection feature, automates the scanning process and continuously monitors for unknown APs and determines if any unknown APs are on the network.

High-Performance ASICs

Fortinet provides high-performance network security with custom ASIC (Application Specific Integrated Circuits)-based silicon processing hardware. Custom content and network processors are able to offload compute-intensive security processing from the general purpose CPU, reducing the load on the CPU.

Traditional Security Appliances that use multi-purpose CPU based architectures becomes an infrastructure bottleneck. The only way for a Network Security Appliance to scale is via purpose built ASICs to accelerate specific parts of the packet processing and content scanning function. Optimum path processing (OPP) is used to optimize the different resources available in packet flow.

- **Content Processor ASIC** – Accelerates content security, such as application control and intrusion prevention
- **Network Processor** – Accelerates network security tasks such as Firewall, VPN and IPv6 translation
- **System-On-A-Chip Processor (Hybrid ASIC)** – Integrates all ASICs including CPU into a single process for best price/performance

This off-loading of traffic enables Fortinet appliances to deliver unmatched performance and low latency, as well as support a wide range of security services. These levels of performance are critical as networks are upgraded to take advantage of increasingly faster LAN and WAN standards, such as 40-Gigabit Ethernet and beyond.
• Easy deployment of database activity monitoring/audit across hundreds of databases via centralized policy management
• Provides Privilege change data for User Access management and integration
• Out-of-the-box reports help meet security and PCI DSS compliance requirements

Centralized Management

Centralized Security Management, Logging, and Reporting – FortiManager™ & FortiAnalyzer™

FortiManager Security Management appliances allow you to centrally manage any number of Fortinet Network Security devices, from several to thousands, including FortiGate, FortiWiFi, and FortiCarrier™. Network administrators can better control their network by logically grouping devices into administrative domains (ADOMs), efficiently applying policies and distributing content security/firmware updates. FortiManager is one of several versatile Network Security Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

FortiAnalyzer Network Security Logging, Analysis, and Reporting Appliances securely aggregate log data from Fortinet Security Appliances. A comprehensive suite of easily customizable reports allows you to quickly analyze and visualize network threats, inefficiencies and usage. FortiAnalyzer is one of several versatile Fortinet Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

Protecting Web Applications

Because web applications are exposed to the Internet by definition, the PCI DSS standard addresses them in detail in requirement 6.6. Web Application Firewalls (WAFs) provide an important layer of protection against vulnerable code, configuration errors, and advanced threats.

The FortiWeb™ WAF provides specialized, layered application threat protection for enterprises, application service providers, and SaaS providers. Using advanced techniques to provide bidirectional protection against malicious sources, network and application layer DoS attacks and sophisticated threats like SQL injection and XSS, FortiWeb platforms help prevent identity theft, financial fraud and denial of service.

Centralized Authentication

Integrated, centralized authentication with single sign-on and policy enforcement is critical to providing secure access to the appropriate systems that compose a distributed enterprise environment.

In addition to Requirement 8.5.1 described above, Requirement 8.3 in PCI DSS 3.0 specifies that two-factor authentication applies to users, administrators, and all third parties, including vendor access for support or maintenance.

FortiAuthenticator™ User Identity Management Appliances provide two-factor authentication, RADIUS, LDAP and 802.1X wireless authentication, certificate management and Fortinet single sign-on. It is compatible with and complements the FortiToken™ range of Two-Factor Authentication Tokens for secure remote access enabling authentication with multiple FortiGate appliances and third party devices.

Figure 6 - Fortinet's comprehensive approach to accelerating PCI DSS compliance in Distributed Enterprise environments
<table>
<thead>
<tr>
<th>PCI DSS CONTROL OBJECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL OBJECTIVE</td>
</tr>
<tr>
<td>1. Build and Maintain a Secure Network and Systems</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2. Protect Cardholder Data</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>3. Maintain a Vulnerability Management Program</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>4. Implement Strong Access Control Measures</td>
</tr>
<tr>
<td>5. Regularly Monitor and Test Networks</td>
</tr>
<tr>
<td>6. Maintain an Information Security Policy</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Securing Distributed Enterprise Networks for PCI DSS 3.0 Compliance

FortiGuard Labs: Delivering Constant Threat Protection

The FortiGuard Global Threat Research Team continually updates Fortinet products to address the latest threats. Fortinet deploys a variety of security filters for a variety of products including traffic anomaly filters, vulnerability-based filters, IP reputation, and signatures.

Given the speed with which new attacks are released to the wild, it is imperative that organizations have protection in place to guard against the latest attacks. FortiGuard Labs, utilizing data centers around the world located in secure, high availability locations, automatically deliver updates to the Fortinet security platforms. With the FortiGuard Subscription Services enabled, customers can rest assured that their Fortinet security platforms are performing optimally and protecting their corporate assets with the latest security technology.

Increased Bandwidth and Lower Costs

As Distributed Enterprises move to support “Store of the Future” opportunities they are consuming more bandwidth. Unfortunately, existing MPLS deployments cannot support the need for bigger pipes due to caps on bandwidth.

An alternative is to move to sending traffic over IPsec via the integrated VPN functionality within the FortiGate device. This transition can result in a 6X to 8X performance increase while lowering costs by 50% or more.

Conclusion

Today’s distributed environments are faced with the daunting task of having to add new technology to their networks in order to remain competitive while keeping sensitive data flowing through those networks secure. PCI DSS is the foundation of security in these networks, and requires a wide variety of mitigating controls be in place to protect cardholder data.

Fortinet’s consolidated approach to network security enables the FortiGate product family to provide unmatched protection by delivering high performance and consolidated security, for both wired and wireless networks in each remote location or branch, as well as at the enterprise edge and in the data center. Specialized technologies, including FortiMail, FortiWeb, and FortiDB, protect mail, web applications, and databases respectively at the data center or headquarters locations. Together, these technologies provide a comprehensive solution to secure distributed enterprises and accelerate PCI compliance.