PenTest Standard magazine

Network Segmentation

The clues to switch a PCI DSS compliance's nightmare into an easy path

Although best security practices should be implemented in all systems of an organization, whether critical or not, the business needs and the limited capabilities of the organizations to maintain rigorous security controls cause that the desired balance between business objectives and security requirements is not often achieved.

This issue opens the need for a security architecture distributed in levels of criticality, where the stringent security controls are applied to critical systems and other more flexible controls are applied to less critical or sensitive systems.

In the case of PCI DSS compliance, the compliance mandates require organizations (merchants, services providers and acquirers) to initiate a detailed analysis of the scope of compliance, discovering in most cases the need to take action to isolate the affected processes and systems limiting the scope of PCI DSS compliance. Typically the reduction and limitation of the scope of PCI DSS is achieved through proper network segmentation, but before carrying out this network segmentation it is necessary to understand how to set boundaries in the area of PCI DSS compliance and which aspects will be assessed by the QSA auditor in a PCI DSS assessment. In fact, the misunderstanding of the scope of PCI DSS causes organizations to believe that compliance with PCI DSS is much easier than it actually is, and sometimes these organizations insist on taking a direct PCI DSS compliance audit without having had proper advice previously and ending in an unsatisfactory audit and higher final costs.

Addressing PCI DSS compliance

One of the common problems in addressing PCI DSS deployments is to make the customer understand that PCI DSS not only apply to systems that store, transmit or process cardholder data but usually the PCI DSS scope is much greater, including management systems, security systems and in many cases all customer processes and infrastructure.

Adequate network segmentation can help organizations to reduce the scope and cost of implementation and evaluation of PCI DSS. The aim is to limit where cardholder data is processed, stored and transmitted to limit the scope of PCI DSS, achieving:

Figure 1. *Understanding PCI DSS Scope*

- Reduce the risk, as attention focuses on those areas that require additional controls.
- Reduce time, effort and cost.
- Avoid heavy fines, financial fallout and reputational damage.
- Cost-effective strategies to manage and protect cardholder data.

The intention is to protect cardholder data from threats on other networks or environments that could potentially affect the cardholder data. It is necessary to evaluate the possible interactions between the PCI DSS environment of the organization and any other environment, such as network management of a managed service provider. A scenario that can dramatically complicate compliance efforts of an organization is when the organization hasn't analyzed in depth the contracted services of third parties, as an option that ideally would have been valid to reduce the scope by outsourcing; may in some cases act totally against, expanding PCI DSS scope beyond the boundaries of the organization. To better understand this scenario we will give an example:

- An organization in order to reduce the scope of PCI DSS contracts with Company B firewall and IDS management services and time synchronization.
- Company B offers the same services on a shared basis for various clients. Company B never manages customers' servers, or access to them at all, not even the backups.
- As the company B does not process or manage cardholder data, since no client shares the data with this company, Company B is not required to validate PCI DSS compliance as a service provider.
- Normally companies within their PCI DSS audit process include the services of Company B in the assessment, as the case of the organization A.
- Company B has in its facilities the firewall management console, another management console for the IPS, the NTP time server and a RADIUS server for authentication of users in each of the management consoles.
- Also on the same network there are other servers and devices from Company B that are not used for services provided to the organization A.
- As the company B has no obligation to validate PCI DSS on their own network, there are no guarantees that the other network components are protected with the latest security patches, antivirus, strong access control, etc...
- That means that for example a potential security compromise from the wireless access point, on which have not changed the default settings, a hacker can completely compromise company B network including the NTP server, RADIUS users used to manage firewalls of customers and of course reaching compromise on this point to PCI DSS network of the organization A.
- For this reason, in this scenario the entire network of company B would be within the scope of PCI

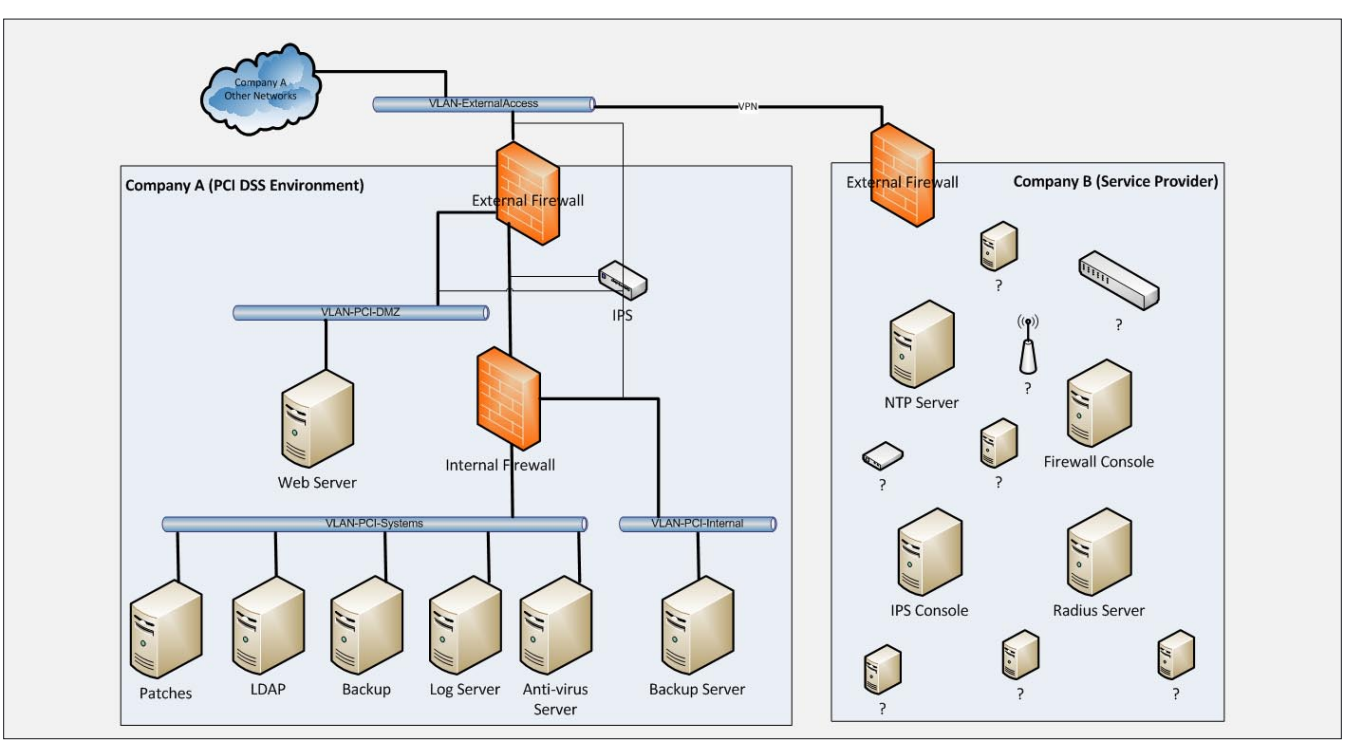

Figure 2. *Company B network within PCI DSS scope*

DSS in organization A, making compliance with the standard of something unapproachable.

This does not mean that companies should not outsource services in the PCI DSS environment, quite the opposite as this reduces the scope of PCI DSS but it is essential to ensure that outsourcing is not going to be a security risk and therefore an extension of the PCI DSS scope. In fact, the same scenario wouldn't pose the security problems detailed above if Company B has had network segmentation for services affected by PCI DSS for those who are not.

PCI DSS Scope

To determine how PCI DSS affects the organization, it is necessary to conduct an evaluation to see how the cardholder data flows through the organization and to analyze where it is critical the storage, processing or treatment of this information, eliminating those that are not critical flows. It is necessary that the evaluation of each of the flows where cardholder data appears is considered the starting point (what, when and how data is obtained by the organization), the intermediate states (all treatments and locations where cardholder data flows) and the end point (if any, how cardholder data leaves the organization). This analysis should be conducted in all areas of the organization, since it is common that a specified area of the organization ignores that other areas also interact with cardholder data. Here are some examples of flows or services where may appear cardholder data at some point:

- Processing, storage or transmission of payment transactions.
- Service Providers (any service offered on which cardholder data could be transmitted, stored or processed by the service provider or the customer):
  - Web hosting, dedicated servers, housing, datacenter
  - Network services, administration and systems management
  - Application Development
  - …
- Billing / Payment for services with credit card by Internet, telephone, mobile, etc...
- Customer Services, for example:
  - Call-centers (recorded conversations).
  - Incidents received on paper, for example FAX.
  - Incidents received electronically (email, applications, etc.).
- Loyalty Programs.
- Fraud Management.
- Booking Management.
- ...

Once all cardholder data flows are identified, it is important to look for areas where cardholder data can be consolidated or removed to reduce the scope. With this

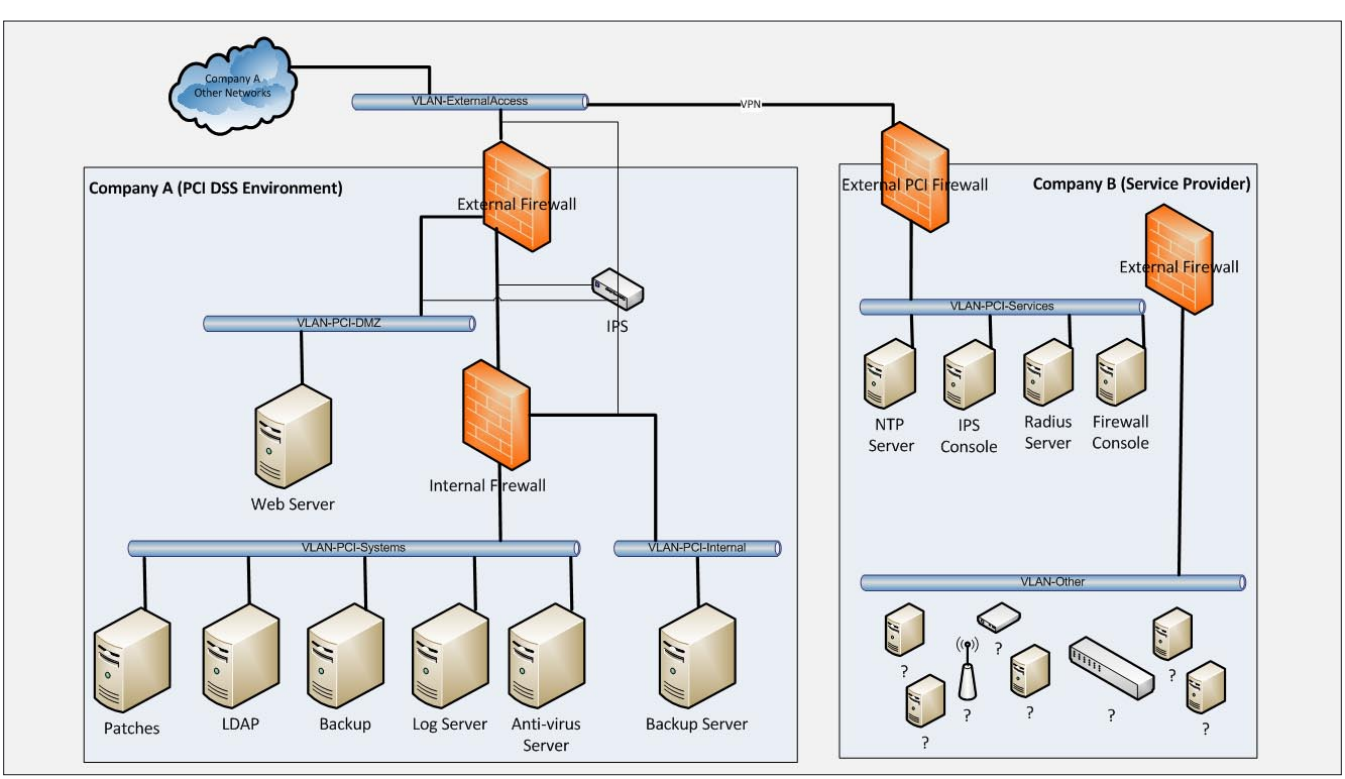

Figure 3. *Small segment of Company B network included within PCI DSS scope*

information obtained, it can be determined the scope of PCI DSS. Considering that any other system that is in the same network area of the system components identified in the previous flows is also within the scope of PCI DSS (even if are not part of the systems that process, store or transmit cardholder data).

As mentioned above, PCI DSS requirements apply to all system components. System components are defined as any network component, server or application that includes or is connected to the cardholder data environment. The *cardholder data environment* (CDE) is the area of the network cardholder data or sensitive authentication data, including:

- Firewalls, switches, routers, wireless access points and other network and security devices.
- Servers, for example: web, application, database, authentication, mail, Proxy, NTP, DNS, etc.
- Applications, licensed, bespoke, whether internal or external (Internet).
- All user computers, laptops, etc...

Importance of Network Segmentation

Flat networks (or simple) significantly increase the potential exposure of a single violation of data without adequate network protection.

- A violation of cardholder data can occur at any shop, office or site that accepts payment cards.
- A flat network leaves all vulnerable systems to the weakest point. Once achieved access at any point through the weakest point, an attacker can reach other critical systems in other locations.

On the other hand, we must bear in mind that network segmentation is not a mandatory requirement of PCI DSS; but a flat network or erroneous or incomplete network segmentation can lead:

- Increased risk for the organization (increased number of cardholder data, more data locations so more locations to control).
- Increased cost and difficulty of deploying and maintaining PCI DSS controls.
- Requirement to perform network and application penetration test of all system components in the network, whether or not they have anything to do with cardholder data.
- Vulnerability scan requirements for all internal and external system components on the network, whether or not they have anything to do with cardholder data.
- Implement strict audit logs for system all components on the network, whether or not they have anything to do with cardholder data.
- Configure all system components securely on the network, whether or not they have anything to do with cardholder data.
- Code Reviews and Application Firewalls need for applications that have nothing to do with cardholder data.
- User management and strict account policies for all system components in the network, whether or not they have anything to do with cardholder data.
- ….

The idea or concept to keep in mind at all times is *How does other environments or networks security could affect*

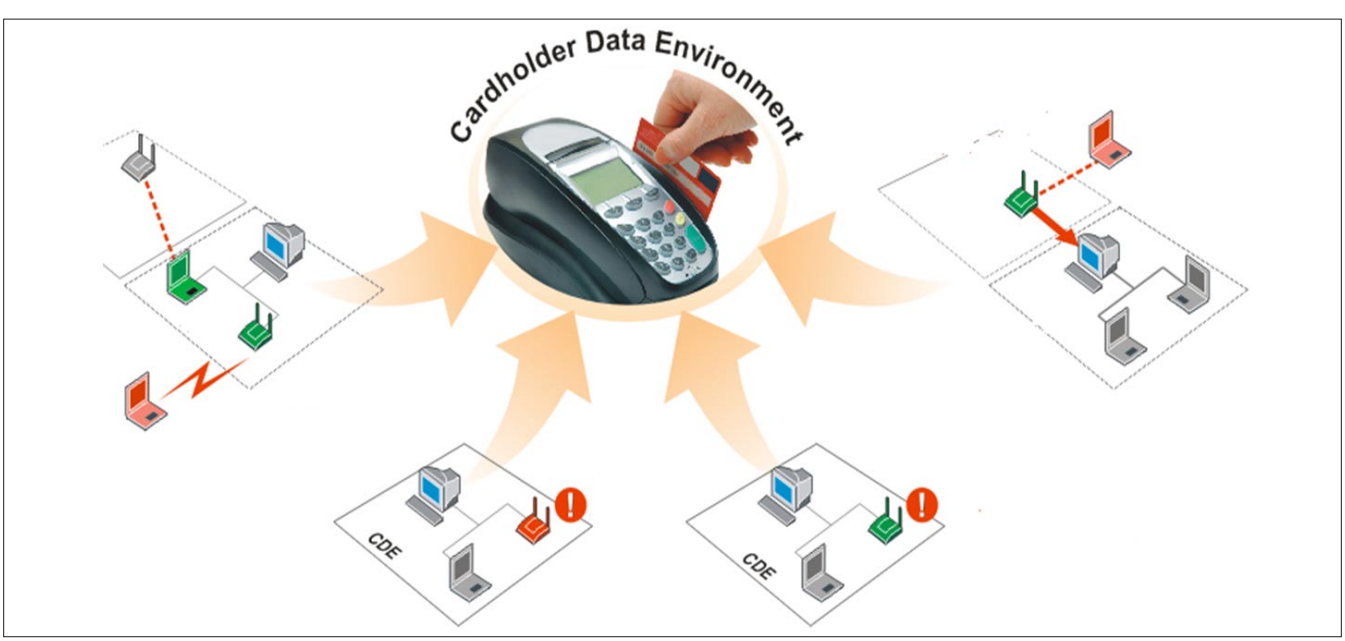

Figure 4. *PCI DSS Scope Analysis*

the security of the existing cardholder data environment (CDE)?. That is, a security problem on the connected network of my *managed service provider* (MSP), could affect the security of our PCI DSS environment?

Benefits of Reducing the Scope of PCI Compliance

Network segmentation of the cardholder environment can significantly reduce the scope of PCI DSS. Here are some of the benefits to be gained if the network is properly segmented:

- *Reduce the scope*. From a situation where anyone can access the corporate network, to a situation where specifically authorized users with a business need access to the cardholder data environment.
- *Number of systems (servers, applications, devices)*. Up to each organization, such as a flat network containing 100 servers but only 4 processing cardholder data and its security. In a flat network architecture or improperly segmented, all system components are within the scope. However, isolating the four servers in a secure segment, only these servers and traffic to/from this segment should be within the scope (in addition to other infrastructure required by PCI DSS).
- *Less effort*. Less effort is necessary to develop and implement security policies to protect the segment of what would be needed for an entire network.
- *Lower cost*. A smaller number of system components means lower cost regarding security audits, vulnerability analysis, penetration test, etc...
- *Less forensic effort*. In the event that a security incident occurs, the forensic investigation in a limited network segment is much faster and more effectively.

Without adequate network segmentation, compliance with PCI DSS requirements impact any system and employee with access to the network and may require:

- 2-factor authentication for remote network access.
- Systems hardening, change control management, audit logs management and analysis, anti-virus systems.
- Increase of processes and procedures for all changes and IT tasks.
- Inclusion of all applications, even those not dealing with cardholder data, in future assessments. The requirement 6.6 requires that all web applications are protected by a firewall application or perform a code review.

Graphical Example

The following diagram shows a very simple and short example of network segmentation, which will show the involvement of PCI DSS on each segment.

On network segment labeled as *VLAN 2* there is not any stored, processed, or transmitted cardholder data by any system component. In addition, any system component of the segment *VLAN 2* cannot access the segment *VLAN 1*, where the firewall implements a secure access control to ensure strict and proper network segmentation. As a result, the network segment *VLAN 2* is out the scope of PCI DSS.

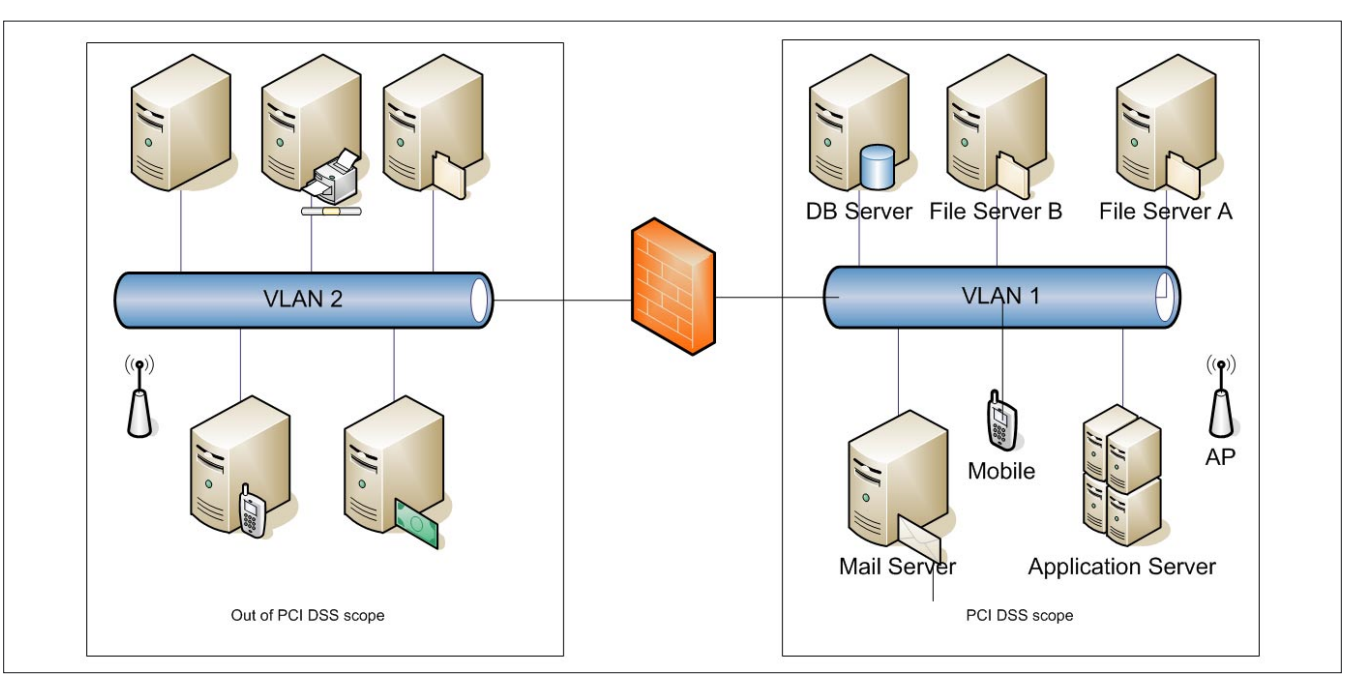

Figure 5. *Graphical Example*

On the other hand, in the network segment *VLAN 1* cardholder data is transmitted and stored. The following describes the functionality of the components shown in the diagram:

- *DB Server*: Stores the PAN, cardholder name and card expiration date in the database.
- *File Server B*: file server for employees, never stores cardholder data.
- *File Server A*: Contains dump files of the database; it can sometimes contain cardholder data.
- *E-Mail Server*: Sometimes incidents are received by email containing the full PAN.
- *AP (Access Point)*: wireless access point connected to the network segment, so cardholder data may be transmitted through this channel.
- *Mobile*: Blackberry Terminal for some employees to access e-mail.

The result is that all system components are within the scope of PCI DSS because they are part of the same network segment with those which process cardholder data:

- *File Server B*: Even having anything to do with cardholder data is within the scope for being in the same network segment.
- *Mobile*: By accessing email employees can access cardholder data so is also within the scope.
- *Rest*: The rest deal directly with cardholder data so that their involvement is direct.

The conclusion is that PCI DSS Requirements (e.g. penetration test, vulnerability scans, monitoring, etc..) must be applied to all system components, including the *File Server B* and *Mobile* leading to more efforts and cost to achieve and maintain PCI DSS compliance.

Considerations to take into account

Some considerations to keep in mind for proper network segmentation:

- Proper user authentication to access the secure network segment (cardholder data environment – CDE).
- Access Lists (ACLs) properly configured.
- Access audit logs.
- Anything that oversteps the secure network segment should be checked, either:
  - Devices.
  - Packets.
  - Protocols.
  - Applications.
  - Users.
- In addition, checks should be implemented on incoming traffic and outgoing traffic.
- Do not allow the exit of cardholder data to another network segment outside of PCI DSS scope.
- Security policies based on user identity or application, to identify who has access to what data, not based solely on IP addresses, ports and protocols.

Examples of bad practices

- *Mail server out of the secure network segment, but sometimes emails are sent with the PAN encrypted.* Although data is encrypted is still cardholder data so both the mail server and any server, computer or network component that is within the same network segment are considered within the scope of PCI DSS.
- *An application within the scope of PCI DSS allows data extraction to files so that the user can manipulate them.* These files are stored on the computer of the employee or a file server outside of the PCI DSS scope. If these data dumps contain the full PAN, even encrypted, the file server, employee workstation and any other system component within that network segment is within the scope of PCI DSS.

MARC SEGARRA LÓPEZ

Senior Security Consultant and Project Manager

msegarra@isecauditors.com

INTERNET SECURITY AUDITORS

As a Security Consultant working in many industries for over ten years, Marc Segarra is accustomed to advising clients on all aspects of Information Assurance. Specialized in the payment card industry and security best practices, he offers an expert insight into security principles for both clients and security professionals. Currently works for Internet Security Auditors as a Senior Security Consultant and Project Manager and holds CISA, CISSP, ISO27001 LA, PCI QSA, PA-QSA security certifications and accreditations.

Public Profile: http://es.linkedin.com/in/marcsegarralopez

Company Website: http://www.isecauditors.com