



How to Dramatically Reduce the Cost and Complexity of PCI Compliance

Using Network Segmentation and Policy-Based Control Over Applications, Users And Content to Protect Cardholder Data

December 2008

Palo Alto Networks
232 E. Java Dr,
Sunnyvale, CA 94089
Sales 866.207.0077
www.paloaltonetworks.com

Table of Contents

Executive Summary.....	3
PCI Compliance is Not Optional.....	4
Network Segmentation Reduces the Cost and Complexity of PCI Compliance	4
Key Network Segmentation Requirements.....	5
Network Segmentation Challenges With Existing Technology.....	6
Network Segmentation with Palo Alto Networks	6
Controlling Application Access	6
User-based Access Control With Active Directory	7
Monitoring and Inspecting the Content	7
Zone-based Protection Without Performance Degradation.....	8
Proof of Controls for Auditing Purposes	8
Role-based Administration Simplifies Auditor Access	9
Palo Alto Networks Policy Example	9
Summary	10
Appendix 1: Palo Alto Networks and PCI Security Requirements	11

Copyright 2008, Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks, the Palo Alto Networks Logo, PAN-OS, App-ID and Panorama are trademarks of Palo Alto Networks, Inc. in the United States. All specifications are subject to change without notice. Palo Alto Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is a broad effort to protect cardholder data that is stored, processed or transmitted by merchants and processors. Most importantly, anyone who accepts cardholders must become PCI compliant.

PCI compliance is not a one-time occurrence, it is an ongoing process of using best practices and technology to protect the cardholder data. The process encompasses many groups, not just the IT group, is ongoing and cannot be achieved by adding technology. Auditing the network for compliance means that wherever the cardholder data goes on the network is within the scope of an audit. In short, the scope of PCI compliance for any organization is significant both in terms of effort and costs. One way in which companies can reduce the cost and complexity of PCI compliance is by segmenting the network and isolating the cardholder data into a secure segment.

Network segmentation is considered to be a network security best practice because it enables the IT department to isolate critical data behind a set of security policies and in so doing, more effectively protect that data. For those companies that are required to become PCI compliant, network segmentation can be used to isolate cardholder data and in so doing, help reduce the scope of the audit process.

From the October 2008 update to the PCI DSS documentation:

Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- *The scope of the PCI DSS assessment*
- *The cost of the PCI DSS assessment*
- *The cost and difficulty of implementing and maintaining PCI DSS controls*
- *The risk to an organization (reduced by consolidating cardholder data into fewer, more controlled locations)*

Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment.

Many networking devices, including firewalls, are capable of implementing some rudimentary network segmentation based on either IP address, logical zone or combination thereof. The problem with all of these devices, including firewalls, is that their control mechanisms are based on ports, protocols, and IP addresses. None of the existing networking devices are able to identify and control access to segments based on application identity, nor are they able to tie policies directly to user and group information from Active Directory. Because of this technology limitation, they are ineffective at protecting cardholder data from innovative attackers and threats that can easily bypass these offerings.

Palo Alto Networks' next-generation firewall can isolate and protect cardholder data through security policies that are based on the user or group identity from within Active Directory. The user and group identity is then tied directly to a specific application and the application can then be inspected for threats and unauthorized data transfer. This level of granular control is unmatched by any firewall solution on the market.

PCI Compliance is Not Optional

Anyone who accepts cardholders needs to be PCI compliant—it is not optional. Companies that do not comply face financial pressure from the cardholder companies. And as economies rely more and more on cardholder transactions, the risks of lost cardholder data will only increase, making any effort to protect the data critical (compliance related or otherwise). Regardless of whether or not a company is PCI compliant, a data breach can be very costly. According to Forrester, the estimated PER RECORD cost of a breach (fines, clean up, lost opportunities, etc) ranges from \$90 (low profile, non-regulated company) to \$305 (high profile, highly regulated company). So losing 10,000 records could be as costly as \$3 Million in fines while the cost to the company reputation is immeasurable.

Compliance with PCI is a combination of documented best practices and technology that, in the long run, will prove to be beneficial to any company in their desire to protect not just cardholder data but the company assets. In the short run however, the costs can be significant in terms of manpower, hardware and consulting.

Network Segmentation Reduces the Cost and Complexity of PCI Compliance

As stated in the PCI documentation, network segmentation can be used to reduce the scope of a PCI audit. The premise is relatively simple. Reduce the sheer size (scope) of the audit, then the costs and complexity can be reduced as well. By proving that the cardholder data is isolated in a secure segment, then only that segment need be audited.

The value of segmentation in this case cannot be overstated. Here are just a few of the elements that can be reduced if the network is segmented:

- Number of servers is reduced.** This will vary by customer but imagine a flat network with 100 servers and only four of them actually contain the cardholder data. Because the network is flat, and any server or user can conceivably touch the cardholder data, the entire network is within scope. Now imagine taking the four servers that hold the data and isolating those servers in a secure segment, then only the servers and the traffic to and from that segment is within scope. In this scenario, the scope of the audit is reduced by 96%.

	Flat network	Segmented network
Cardholder servers	4	4
Total servers	100	100
Open to audit scope	100	4
Reduction of audit scope	0%	96%

Table 1: Theoretical example of reduction in audit scope

- Cost of audit is reduced.** Simple math says that if the number of servers is lowered, then the time and materials charges for an audit can similarly be lower.
- Effort to protect the segment is lessened.** Less effort will be required to develop and apply security policies to protect the segment than it would be to apply the same policies to an entire network.

- **Network re-architecting is minimized.** Without segmentation, some companies may need to move servers and conceivably re-architect the network in order to effectively isolate the cardholder data. Segmentation may be a means by which the amount of changes to the network are minimized.
- **Forensic effort is lowered.** In the event that a security incident occurs, investigating traffic in and out of a network segment will be achieved more quickly and with far less effort than it would across an entire network.

Network segmentation is not a new concept nor is it one that is overly complex. It is used in most any network (subnets) and it can be implemented using a variety of networking equipment such as switches, routers and firewalls. As networks changed, users became mobile and application access less controlled, network segmentation became a security best practice as a means of isolating risk and protecting resources.

Key Network Segmentation Requirements

Many different technologies can be used to segment the network, but when looking at segmentation as a way to isolate the cardholder data for PCI compliance, several key requirements need to be taken into account.

- **Flexibility.** To segment the network for security purposes may sometimes require the modification of the network architecture, a task that most companies will avoid if at all possible. This means that the ability to segment the network for security should be able to do so using IP address ranges, VLANs, physical interfaces or a combination thereof.
- **Policy-based Security.** Segmentation for the sake of dividing the network does little good if specific security policies cannot be applied to the segment. For PCI compliance a firewall should be used to protect the segment and policies must be based on identity of users and the applications – not just IP addresses, ports and protocols. Without knowing and controlling exactly who (users) and what (applications and content) has access to the cardholder data within the segment, the data may be exposed to applications and users that can easily bypass controls based on IP addresses, ports and protocols.
- **Proof of policy controls.** Compliance means showing the auditors the policies that have been put in place and giving them access to the network data to see what has been done to protect the card data. Auditors need to see the security policies and who has made edits. They need to be able to sift through the logs, looking for traffic patterns and potential risk areas.
- **Performance is critical.** Segmentation for purposes of PCI compliance means applying in depth security policies in a network location that is typically business critical, high volume traffic. This means that the solution delivering the secure segment must operate at multi-Gbps speeds with very high session ramp rates and minimal amounts of latency.

The concept of segmentation is easy to grasp and the benefits derived in terms of achieving and maintaining PCI compliance are significant.

Network Segmentation Challenges With Existing Technology

Many existing technologies can be used to segment the network, however these same technologies are ineffective at establishing **secure** segments for purposes of PCI compliance.

- **Legacy firewalls are blind to applications and users.** Legacy firewalls are incapable of identifying and controlling access to the cardholder data based on who (user identity) and what (applications and content). Today's firewalls can only apply rudimentary segmentation with policies that are based solely on ports, protocols and IP addresses.
- **Firewall "helpers" are of little or no help in controlling access based on users.** Firewall helpers such as NAC deliver the marginal benefit of user control that NAC which is negated by the fact that it is yet another appliance (with associated user agents) that needs to be managed. And because of the multi-appliance aspect, the burden of proof becomes more difficult because the auditor sees different devices, log formats, and management interfaces. Adding an IPS does little to help in controlling who and what has access to the data because IPS offerings are designed to allow all traffic, blocking only specific threats, so their ability to control users and applications is limited. Note that an IPS can help address the threat prevention requirement for PCI.

Network Segmentation with Palo Alto Networks

Palo Alto Networks next generation firewalls bring a unique combination of hardware and software related segmentation capabilities to customers who are required to be PCI compliant. From a flexibility perspective, every Palo Alto Networks firewall supports security zones, which, for purposes of the PCI discussion are equivalent to network segments. A security zone is a logical container for physical interface(s), VLANs, a range of IP addresses or a combination thereof. Using security zones as a means to isolate the cardholder data can not only help protect the data, it may also reduce the amount of physical network re-architecting required.

To protect the cardholder data, the key differentiator that Palo Alto Networks can provide, over and above any other firewall on the market, is the ability to control the applications, users and content that can traverse each security zone. Once the network has been divided into distinct zones, security policies can be applied that control, at a very granular level, which applications, users and content are allowed in and out of the zone that contain the cardholder data servers.

From a hardware platform and performance perspective, the combination of 10 Gbps firewall performance and high interface density (up to (24) 1 Gbps interfaces) means that a single firewall can be used to physically separate the network into distinct zones and secure them without creating a performance bottleneck.

Controlling Application Access

Palo Alto Networks is the only firewall on the market that uses a patent-pending technology called App-ID™ to identify and control more than 750 applications, irrespective of port, protocol, SSL encryption or evasive tactic employed. The determination of the application identity by App-ID is done inline (not proxied) using four different techniques (decoders, decryption, signatures and heuristics) to determine the application identity which is then used as the basis for all policy decisions including appropriate usage, content inspection, logging and reporting.

From a PCI compliance perspective, knowing the exact identity of the application means that instead of trying to protect the zone that isolates the cardholder data using broad-based terms such as IP address range, along with port and protocol, a PCI project leader can define a policy that enables a specific application (e.g., Oracle) to access the zone containing the cardholder data. So any other application that might hop ports or tunnel another application will be blocked from accessing the zone and that activity is logged for forensics and auditing purposes.

User-based Access Control With Active Directory

The next step in isolating the cardholder data within a zone for PCI compliance is to associate the application identity with specific user name information from Active Directory. Palo Alto Networks delivers this capability with User-ID, a technology that seamlessly integrates with Active Directory, enabling user- and group-based policy control, without requiring an agent on every desktop.

With User-ID, the PCI project leader can create a policy that marries the application (e.g., Oracle) with the user and group identity (e.g., Finance users) stored within Active Directory. The policy can be created to allow only inbound traffic from the users and in so doing, limit the cardholder data exposure. Alternatively a policy can be created that says do not allow any other users or groups to access the cardholder data within the zone.

User-ID helps address the challenges presented to IT by an increasingly mobile enterprise, where employees access the network from virtually anywhere around the world, internal wireless networks re-assign IP addresses as users move from zone to zone, and network users are not always company employees.

Monitoring and Inspecting the Content

Controlling the applications and users that can access cardholder solves only part of the visibility and control challenge that IT departments face when trying to achieve and maintain PCI compliance. With the understanding that cardholder data represents a significant corporate asset, the process of monitoring and inspecting the application traffic traversing each zone becomes the next significant challenge and one that is addressed by Content-ID, a real-time content inspection engine.

Content-ID blocks a wide range of threats (viruses, vulnerability exploits, bots, Trojans) and controls unauthorized transfer of files and data. Content-ID enables PCI project managers to implement policies that achieve two significant goals relative to protecting cardholder data:

- Inspects the inbound traffic for all manner of threats, particularly those that may be focused on finding and stealing data (bots, Trojans, worms).
- Monitoring outbound traffic for unauthorized transfer of cardholder data (files or data patterns) and either blocking the transfer altogether or sending an alert.

Zone-based Protection Without Performance Degradation

Palo Alto Networks next-generation firewalls are purpose-built platforms, designed specifically to handle enterprise traffic loads while identifying and controlling applications, users and content (at speeds of up to 10 Gbps). The two elements that are used to achieve this goal are the hardware platform architecture and the single pass architecture—which governs how traffic is handled.

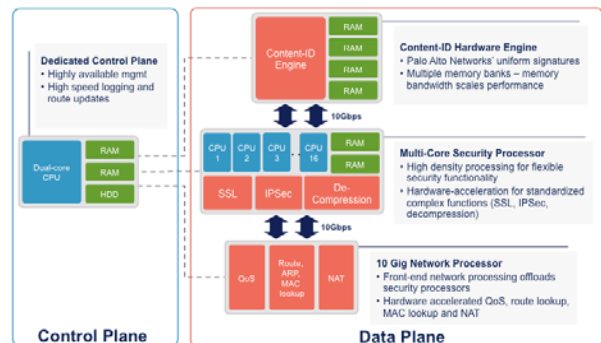


Image 1: Palo Alto Networks PA-4000 Series hardware architecture

The hardware architecture uses dedicated, function-specific processors and memory for networking, security, management and content inspection. The physical separation of data and control planes means that heavy utilization of one doesn't negatively impact the other.

In legacy network security infrastructure, traffic flows through several security devices, each with its own networking engine, classification engine, pattern matching engine, and policy engine. This duplication of effort is not only inefficient, but also slow. This poor performance is the key reason why enterprises are loath to put yet another device in the traffic flow.

Palo Alto Networks next-generation firewalls utilize a single pass architecture, with traffic flowing through a single networking component, a single application classification engine, a user classification capability, and a single content/pattern matching engine – resulting in the ability to see and enforce policy control across applications, users, and content (including confidential data and threats) – without slowing traffic.

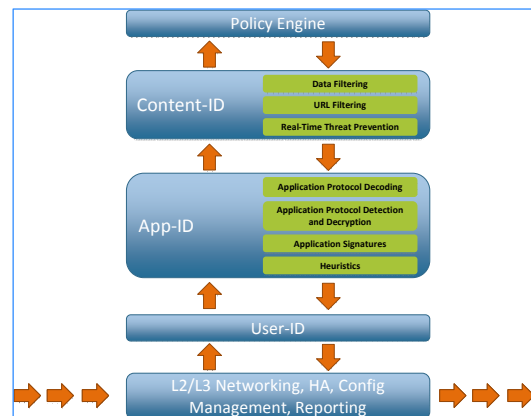


Image 2: Palo Alto Networks Single pass architecture

Proof of Controls for Auditing Purposes

PCI compliance is only achieved when an auditor comes on-site and evaluates the controls that are put in place to protect cardholder data. To do this, auditors require access to many pieces of data, including the firewall logs and reports. Auditors will not only want to see proof of the security policy, but they will be interested in reviewing the traffic logs to determine who has access to the zone and what may have changed, if anything.

With Palo Alto Networks, PCI auditors can be given fingertip access to reporting and logging tools that can be used to help address the audit proof requirements. Reporting and the log viewer both leverage the integration with Active Directory to provide visibility into user behavior that complements the views into application and threat activity for a more complete picture of the zone traffic. For additional 3rd party analysis and event correlation all logs can easily be forwarded to a syslog server.

- Reporting: More than 30 pre-defined reports can be used as is or they can be customized, combining elements of other reports and saved for future use. Fully customized reports can be created from scratch, using any of the information sources on the firewall. Report generation can be automated to run on a scheduled basis and the results can be emailed or exported to PDF or Excel.
- The log viewer provides a view into application and threat activity with flexible filtering capabilities. Clicking on a cell value immediately creates a filter that can be narrowed down further by combining multiple criteria using an expression builder and additional log fields, even if they are not visible in the log viewer. Log filters can be saved for future use and an export button allows results matching the current filter to be exported to a CSV file for offline archival or further analysis. Alternatively, all log files can be sent to a syslog server.

Role-based Administration Simplifies Auditor Access

One of the keys to a smooth and successful audit process is providing adequate access to the data that an auditor needs to review. Palo Alto Networks simplifies the data access challenge through the most granular role-based administration on the market.

An auditor can be granted full access to any of the reporting and logging features while access to device, and security policies can be limited to read-only, thereby maintaining appropriate controls, yet supporting the required audit process.

Palo Alto Networks Policy Example

Using a greatly simplified network diagram helps emphasize how Palo Alto Networks next generation firewall can reduce the cost and complexity of PCI compliance. The diagram on the left is flat and as such, the entire network falls within the scope of a PCI audit. The diagram on the right shows the cardholder data isolated in a security zone and it shows the finance users as the only group who can access the data.

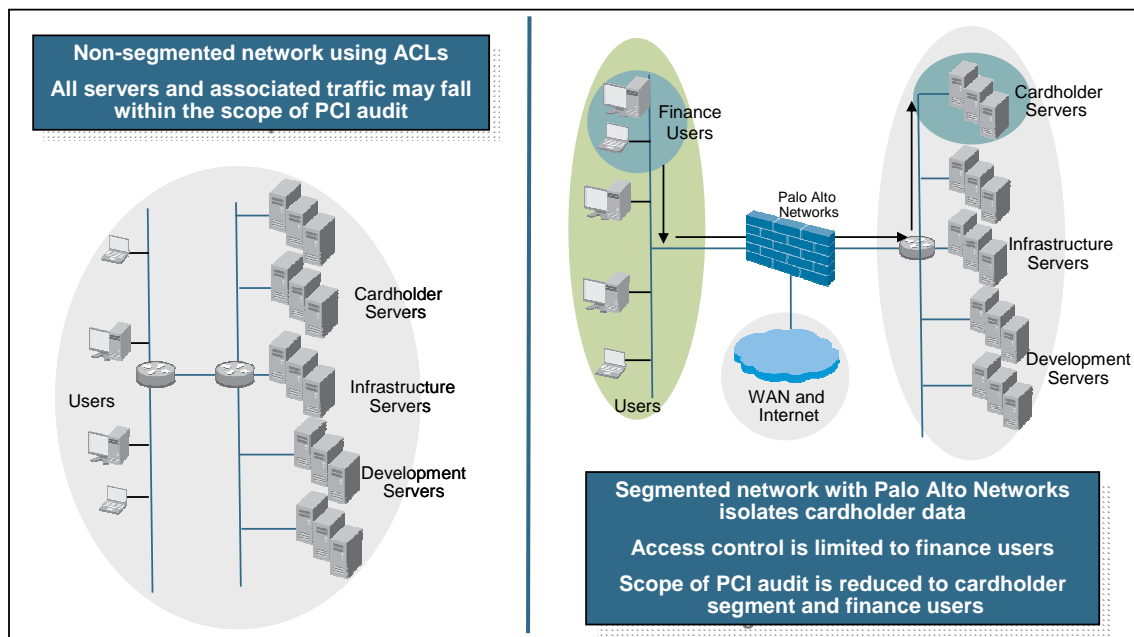
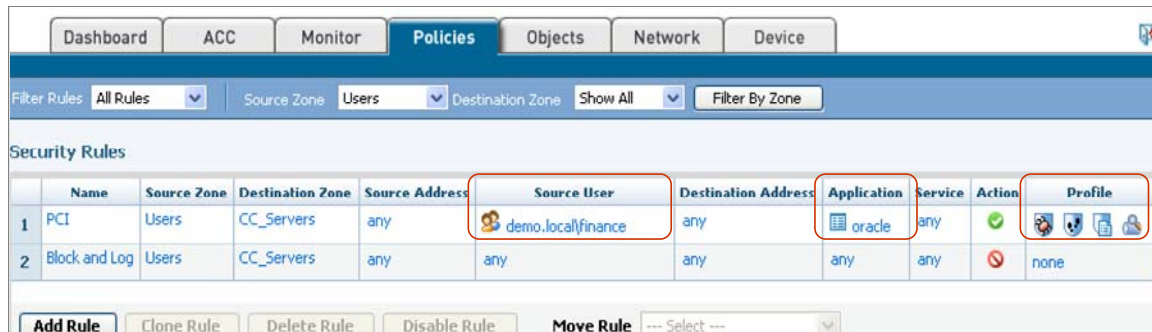


Image 3: Comparison of flat vs segmented network.

Looking at a policy example demonstrates the simple, yet straightforward manner in which Palo Alto Networks can divide the network into security zones and then apply policies to control who (users) and what can traverse the zone. First, security zones are established for cardholder servers, users (internal) and WAN/internet traffic using any one of a number of different techniques (VLAN, IP address range, physical interface, etc).

The next step entails the creation of the policy to control who (users and groups) and what (applications and content) has access to the cardholder zone (CC_servers).



	Name	Source Zone	Destination Zone	Source Address	Source User	Destination Address	Application	Service	Action	Profile
1	PCI	Users	CC_Servers	any	demo.local/finance	any	oracle	any	✓	Threat Prevention
2	Block and Log	Users	CC_Servers	any	any	any	any	any	⊘	none

Image 4: Policy example that isolates and protects cardholder data.

Specifically, the simple 2 rule policy example executes the following protection mechanisms.

- Rule 1 (PCI) enforces the following conditions:
 - Only allow traffic from the user zone (source) to the CC_servers zone (destination) for the finance users Oracle.
 - The Profile scans traffic going to the CC_servers zone for threats (viruses, vulnerability exploits) and monitors outbound traffic for cardholder data such as card numbers in either file or text format..
- Rule 2 (Block and Log) enforces the following conditions
 - Deny all user and application traffic from any zone (source) to CC_servers zone (destination) and log any activity that is denied for use in forensic analysis or proof of audit purposes.

While many firewalls support zone-based policy enforcement, no other firewall, or single solution can implement policies to specifically control application access based on user and group information from within Active Directory.

Summary

The value of using network segmentation as a means of reducing the scope of PCI compliance is significant, regardless of company size. While there are many ways to segment and secure the network to protect the cardholder data, only Palo Alto Networks provides the unique combination of flexible network segmentation and policy control over who (users) and what (applications and content) can access the cardholder data.

Appendix 1: Palo Alto Networks and PCI Security Requirements

PCI Compliance is only achieved via a combination of best practices and technology--there is no such thing as a "PCI compliance product or solution".

The Palo Alto Networks next generation firewall enables policy-based visibility and control over applications, users and content traversing the network. In PCI environments, Palo Alto Networks can help address the requirements within several of the security related sections. Access control policies (applications, users from Active Directory) can be applied to each distinct security zone (aka segment) while inspection policies can be applied to detect and block threats. Rich reporting and logging allow PCI project leaders to demonstrate the proof for purposes of the audit.

The table below summarizes the areas in which the Palo Alto Networks next generation firewall can help companies in the quest for PCI compliance. Actual capabilities should be evaluated within each PCI environment.

PCI DSS Requirement	Palo Alto Networks Can Help
Build and Maintain a Secure Network	
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	Yes--Via policy-based access control over users and applications
Requirement 2: Do not use vendor supplied defaults for system passwords and other security parameters.	---
Protect Cardholder Data	
Requirement 3: Protect stored cardholder data	
Requirement 4: Encrypt transmission of cardholder data across open, public networks	---
Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update anti-virus software or programs	Yes--Network-based threat prevention
Requirement 6: Develop and maintain secure systems and applications	A very small percentage of the threat prevention aspects
Implement Strong Access Control Measures	
Requirement 7: Restrict access to cardholder data by business need-to-know.	Yes--Via policy-based control over users and applications
Requirement 8: Assign a unique ID to each person with computer access	---
Requirement 9: Restrict physical access to cardholder data	---
Regularly Monitor and Test Networks	
Requirement 10: Track and monitor all access to network resources and cardholder data	Yes--Via policy-based control over users and applications
Requirement 11: Regularly test security systems and processes	---
Maintain an Information Security Policy	
Requirement 12: Maintain a policy that addresses information security for employees and contractors	---