

Unisys Stealth Solution for Network

Supporting PCI Compliance

UNISYS

Page 1

Many security breaches—especially those that make the nightly news—involve credit card data.

A consortium of the major credit card companies—VISA, Master Card, American Express, JCB, and Discover Financial Services—joined forces to create the Payment Card Industry Security Standards Council. The PCI SSC then drafted a security standard aimed at protecting payment cardholder data. This standard is called the Payment Card Industry Data Security Standard or PCI DSS. The PCI SSC controls both the PCI standard and the assessment process.

Three types of organizations must comply with the PCI standard: merchants, processors, and service providers, merchants are further classified by the number of credit card transactions they process each year.

As part of the PCI assessment process, each merchant, processor, or service provider must have a pass/fail annual audit performed by a PCI SSC approved Qualified Security Assessor (QSA). (Fail twice in a row and you are subject to fines and potentially the loss of your ability to process credit card transactions.) There are audit companies that perform these audits, and other companies (including Unisys) that assist in achieving or regaining compliance post-audit, or in running a pre-audit. No single company is allowed to provide both the auditing and compliance services for the same customer.

As the Stealth Solution is an infrastructure product, it is not compliant on its own. However, the Stealth Solution does assist organizations with their compliance. One of the biggest selling points of the Stealth Solution for PCI compliance is its FIPS 140-2 certification. This presentation further provides an overview of how the Stealth Solution for Network helps to address several of the PCI DSS requirements, specifically to ensure the security of the following credit card data items:

PAN or the Principle account number (the 16-digit number)

PIN or the Personal ID number

CCV or the Card validation number (the 3- or 4-digit number on the back of most cards)

PCI DSS: 12 Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

The PCI DSS consists of 12 requirements, described in detail in the standard document. The Stealth Solution assists in addressing several of these requirements. Those requirements are highlighted in red.

PCI DSS: 12 Requirements

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

And here are the remaining six requirements of the PCI DSS. Again, the requirements addressed by the Stealth Solution are in red. We'll go into those in more detail now.

The Unisys Stealth Solution for Network Assists with Some Requirement 1 Controls

Install and maintain a firewall configuration to protect cardholder data

- 1.1.4: Description of groups, roles, and responsibilities for logical management of network components
- 1.2: Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment
- 1.3: Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks

PCI DSS Requirement 1 addresses firewall configuration to protect cardholder data. First, it requires that the logical management of network components be defined. Next, the firewall must be configured to deny all “untrusted” traffic. And third, the firewall must protect the cardholder data from public servers or wireless networks.

How the Unisys Stealth Solution for Network Assists with Requirement 1

Stealth:

- A Stealth network device will only communicate with other devices that are also Stealth enabled and where both devices share the same community of interest
- This strengthens the overall network security well beyond what a Firewall, IDS, and VPN combination alone can accomplish

UNISYS

Page 5

The Stealth Solution for Network addresses PCI Requirement 1 through its key management. This allows multiple communities of interest to share the same network without fear of unauthorized access. Any unauthorized network traffic—meaning anything that doesn't have the appropriate workgroup key—is simply ignored.

In essence, the Stealth Solution further fortifies the strength of existing security solutions—including firewalls, IDS, and VPNs.

The Unisys Stealth Solution for Network Assists with Some Requirement 4 Controls

Encrypt transmission of cardholder data across open, public networks

- 4.1: Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

The next PCI DSS requirement that Stealth addresses is Requirement 4. This requirement addresses the need for encryption to protect data during transmission over open, public networks.

How the Unisys Stealth Solution for Network Assists with Requirement 4

Stealth:

- In addition to strong encryption (AES 256), Stealth splits the encrypted data into multiple packets at the bit level, such that no packet contains the information necessary to rebuild even one byte of the original transmission, even if the interceptor has the encryption and split session keys
- Stealth works across wired and wireless networks, LAN, WAN both inside and outside the enterprise
- While in a Stealth network, a device cannot send any data to a non-Stealth device, nor even to a Stealth device that does not share the same community of interest

UNISYS

Page 7

There are three ways in which the Stealth Solution for Network addresses PCI DSS Requirement 4.

First, the Stealth Solution offers AES 256 encryption. But even more powerful—and unique—is Stealth’s ability to further encrypt data by randomly splitting it into multiple packets at the bit level. This protects the data because no single packet contains the full data—just an encrypted “slice” of it. Without the appropriate keys to reassemble the data slices and unlock the encryption, individual slices are worthless to hackers.

Second, the Stealth Solution works on a variety of networks—wired, wireless, LAN, and WAN, as required by the PCI standard.

And third, devices are cloaked from any user that does not share the same community of interest. You can’t even ping them. That also works the other direction: a Stealth device cannot talk to any device that is not running Stealth and is part of the same community of interest.

The Unisys Stealth Solution for Network Assists with Some Requirement 7 Controls

Restrict access to cardholder data by business need-to-know

- 7.1: Limit access to computing resources and cardholder information only to those individuals whose job requires such access
- 7.2: Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed

PCI Requirement 7 addresses the ability of IT systems to limit data access to only those who need to know.

How the Unisys Stealth Solution for Network assists with Requirement 7

Stealth:

- While in a Stealth network, a device cannot send any data to a non-Stealth device, nor even to a Stealth device that does not share the same community of interest
- For workstations, the community of interest is established based on the identity of the user, potentially along with the specific device's location, type, etc.
 - A user cannot access an unauthorized community of interest even if the user is physically at an authorized workstation
 - Changing a user's role is a matter of changing the user's communities of interest in the organization's identity management system, not in modifying the network infrastructure configuration

UNISYS

Page 9

The Stealth Solution for Network addresses PCI Requirement 7 through its use of communities of interest, which define people both inside and outside the organization who need to share the same data while restricting access to that data by others not in the same community.

With Stealth, device and data access are strictly defined. First, a Stealth device cannot send any data to a non-Stealth device or even to a Stealth device assigned to a different community of interest. However, for shared devices such as shared workstations, the community of interest is defined by the user's logon, not the physical workstation. This way, a workstation can be securely shared by members of different communities of interest because each defined community of interest limits each user's data access to only that community's data and devices, not another community's.

When roles and responsibilities change within the organization, the communities of interest change, not the network infrastructure configuration.

The Unisys Stealth Solution for Network Assists with Some Requirement 10 Controls

Track and monitor all access to network resources and cardholder data

- 10.2: Implement automated audit trails for all system components to reconstruct the following events:
 - 10.2.1 All individual user accesses to cardholder data
 - 10.2.3 Access to all audit trails
 - 10.2.4 Invalid logical access attempts

Requirement 10 addresses the ability of the network administrator to track and monitor all access to the network and its cardholder data—be it authorized or not.

How the Unisys Stealth Solution for Network Assists with Requirement 10

Stealth:

- Stealth logs all session open and close events at a Stealth appliance
- Since a Stealth device can only communicate with another Stealth device that shares a community of interest, a user logged in to a Stealth device can not have any unlogged sessions
- Stealth appliances are normally in a secured IT environment with high physical security

The Stealth Solution for Network assists with addressing PCI Requirement 10 by simplifying forensics. Stealth automatically logs all session open and close events at a Stealth appliance. These logs are standard Windows logs and can be accessed by an administrator with the appropriate admin key. Since each session, the communication between two Stealth end points that share a workgroup key, have their own set of session encryption and splitting keys, their traffic is unusable by any other device. You know nothing is gaining any information by sniffing on that traffic, and that those message cannot be rerouted to a different device with any loss of data.

Conclusion

- Adding the Unisys Stealth Solution for Networks takes PCI compliance to a new level while also offering the possibility of long term cost savings
 - Improve network security by segmenting systems and users preventing non-PCI related systems or users from accessing systems containing cardholder data and ensuring that transmissions are encrypted in a way that goes beyond the requirements of the PCI/DSS
 - Achieve long term cost savings by reducing the overhead involved in running VLAN or other network segmentation schemes, and eliminating the need for additional hardware to support multiple networks

The Stealth Solution for Network greatly assists organizations in meeting the PCI standard requirements to keep cardholder data safe, while simultaneously providing long-term value. First and foremost, the Stealth Solution leapfrogs existing network security solutions, offering provable security of cardholder data that goes well beyond the requirements of PCI.

Additionally, long-term costs savings are achieved by reducing VLAN overhead requirements as well as my eliminating the need for additional hardware and resources to maintain multiple networks.

The Unisys Stealth Solution

Security Unleashed

Questions?
UnisysStealthSolution.com

UNISYS
Imagine it. done.

UNISYS

Page 13

With Unisys as your partner, security doesn't hold you back. It empowers your operations. The Unisys Stealth Solution—security unleashed to create Secure Network Operations.

For more information, including a White Paper with a lot more detail on how Stealth works, visit the Unisys eCommunity. It's free and full of information about Unisys products and services, including:

- one stop destination for information
- browser based access to live Webcasts
- direct line to people who can help
- answers by Unisys experts to your questions, and
- collaboration with others who have shared interests

You simply need to register, and will have the option to opt-in to receive email updates in areas of your interest.