Security Standards Council®

**Standard:** PCI Data Security Standard (PCI DSS)

**Date:** May 2017

**Author:** PCI Security Standards Council

# Information Supplement:

# Guidance for PCI DSS Scoping and Network Segmentation

# Document Changes

| Date | Document Version | Description | Pages |
|---|---|---|---|
| December 2016 | 1.0 | Initial release | All |
| May 2017 | 1.1 | Correction of minor typographical errors, minor clarification to wording (with added footnote) in Section 3, and correction of errors in the Scenario 1 and Scenario 2 Logical Data Flow diagrams (in the legend, and diagram and legend, respectively). | 5, 10, 11, 17, 22 |

# Table of Contents

# 1 Introduction

Many organizations struggle to understand where PCI DSS controls are required and which systems need to be protected. This document provides guidance to help organizations identify the systems that, at a minimum, need to be included in scope for PCI DSS. Additionally, the document provides guidance on how segmentation can be used to help reduce the number of systems that require PCI DSS controls.

When it comes to scoping for PCI DSS, the best practice approach is to start with the assumption that everything is in scope until verified otherwise. When properly implemented, network segmentation is *one method* that can help reduce the number of system components in scope for PCI DSS. Other methods may also be effective at reducing the number of systems to which PCI DSS controls apply and/or the size of the CDE (such as outsourcing to a third-party service provider or using a PCI-listed P2PE solution). *However, these methods are not the subject of this paper.*

Illustrative examples of some common segmentation approaches are included in Section 4. These examples highlight PCI DSS scoping impacts and considerations around shared services (such as directory services) and provide guidance for consistent scoping and protection of CHD. The examples in this document do not represent the only way that segmentation can be used to impact PCI DSS scope, and in fact may not be effective for a given system or network configuration.

Just because a system is not in scope for PCI DSS it does not mean the entity should leave that system unprotected, as it could still pose a risk to the entity's network and business. A common pattern seen in data breaches is where the attacker targets systems deemed by the entity to be out-of-scope for PCI DSS, then leverages those systems to gain access to more systems, which eventually provide a path to systems where CHD data can be found. While segmentation may help reduce the number of exposure points to the cardholder data environment (CDE), it is not a silver bullet; implementing segmentation is no replacement for a holistic approach to securing an organization's infrastructure.

## 1.1 Intended Use and Target Audience

This guidance is intended for any entity looking to understand scoping and segmentation principles when applying PCI DSS to its environment. The recommendations provided in this document can be used by both large and small entities to evaluate which system components should be covered by PCI DSS requirements. The guidance does not address PCI DSS compliance. Entities should contact their acquirer (merchant bank) or payment card brand directly, as applicable, for information about PCI DSS compliance programs.

This guidance also provides a method for facilitating effective scoping discussions between entities and is useful for:

- Merchants, acquirers, issuers, service providers—for example, issuer processors and Token Service Providers (TSPs)—and others responsible for meeting PCI DSS requirements for their enterprises
- Assessors (such as Qualified Security Assessors or Internal Security Assessors) responsible for performing PCI DSS assessments
- Acquirers evaluating merchants' or service providers' PCI DSS Reports on Compliance or Self-Assessment Questionnaires

- PCI Forensic Investigators (PFIs) responsible for determining PCI DSS scope as part of an investigation.

This guidance is intended to be used as a supplement to PCI DSS but does not supersede or replace PCI DSS requirements. It clarifies scoping principles and provides guidance that can be applied to a variety of situations.

*Ultimately each entity is responsible for making its own PCI DSS scoping decisions, designing effective segmentation (if used), and ensuring its own PCI DSS compliance and related validation requirements are met. Following this guidance does not guarantee that effective segmentation has been implemented, nor does it guarantee compliance with PCI DSS.*

## 1.2 Terminology

The following terms and acronyms are used throughout this document:

- CDE – Cardholder data environment
- CHD – Cardholder data
- SAD – Sensitive authentication data
- Account Data – Cardholder data and/or sensitive authentication data

Definitions for these terms are provided in the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.*

# 2 Understanding Scoping and Segmentation for PCI DSS

At a high level, scoping involves the identification of people, processes, and technologies that interact with or could otherwise impact the security of CHD. Segmentation involves the implementation of additional controls to separate systems with different security needs. For example, in order to reduce the number of systems in scope for PCI DSS, segmentation may be used to keep in-scope systems separated from out-of-scope systems. Segmentation can consist of logical controls, physical controls, or a combination of both. Examples of commonly used segmentation methods for purposes of reducing PCI DSS scope include firewalls and router configurations to prevent traffic passing between out-of-scope networks and the CDE, network configurations that prevent communications between different systems and/or subnets, and physical access controls.

The types of technologies used for segmentation are often also used to manage access between in-scope systems or networks. For example:

> To meet PCI DSS Requirement 1.2.1, an entity may install a network firewall between the CDE and corporate network to ensure only designated systems in the corporate network can communicate, via approved ports, to systems in the CDE. Additionally, the entity may use the same, or another, firewall to block all connections and prevent access between the CDE and an out-of-scope network. In this way, a firewall is being used to implement a PCI DSS requirement for in-scope systems and network, and is also used to segment an out-of-scope network.

Note that when technologies are used to manage access between systems and networks for purposes of meeting PCI DSS requirements, this is not considered segmentation that reduces PCI DSS scope. While still in scope for PCI DSS, these communications are potentially more secure than uncontrolled communication channels.

The principles of scoping and segmentation are outlined in the "Scope of PCI DSS Requirements" section of the PCI DSS. Some excerpts from this section are provided below with additional guidance.

***Scope of PCI DSS Requirements***

> *The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data.*[1]

An organization's CDE is only the starting point to determine the overall PCI DSS scope. Accurate PCI DSS scoping involves critically evaluating the CDE and CHD flows, as well as all connected-to and supporting system components, to determine the necessary coverage for PCI DSS requirements. Systems with connectivity or access to or from the CDE are considered "connected to" systems. These systems have a communication path to one or more system components in the CDE. Connectivity may occur over various technologies, including physical, wireless, and virtualized.

- Physical connectivity may be via a traditional network (for example, Ethernet or power-line communication) or direct system-to-system connection (for example, USB, component, etc.).

[1] PCI DSS v3.2, page 10

- Wireless connectivity uses different radio waves and frequencies as its transport mechanism (for example, wireless LANs, GPRS, Bluetooth, and cellular technologies). Wireless technologies are often connected to a physical network.
- Virtualized connectivity includes use of virtual networks, virtual machines, virtual firewalls, virtual switches, etc. Virtual devices typically share common resources, such as an underlying host system and/or hypervisor, which could be used to connect one logical partition to another.

Implementation of these technologies can be very complex. It is therefore critical that someone who understands the technology in use evaluates the impact of these technologies on scope.

It is important to understand the risks and impacts if connected-to system components are excluded or overlooked from PCI DSS scope. Compromises of connected-to system components often lead to compromise of the CDE and theft of CHD.

The following scoping concepts always apply:

- Systems located within the CDE are in scope, irrespective of their functionality or the reason why they are in the CDE.
- Similarly, systems that connect to a system in the CDE are in scope, irrespective of their functionality or the reason they have connectivity to the CDE.
- In a flat network, all systems are in scope if any single system stores, processes, or transmits account data.

Note that public, untrusted networks (for example, the Internet) are not in scope for PCI DSS. However, PCI DSS requirements must be implemented to protect the entity's in-scope systems and data from untrusted networks.

***Network Segmentation***

*Network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of an entity's network is not a PCI DSS requirement. However, it is strongly 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.*[2]

The intent of segmentation is to prevent out-of-scope systems from being able to communicate with systems in the CDE or impact the security of the CDE. Segmentation is typically achieved by technologies and process controls that enforce separation between the CDE and out-of-scope systems. When properly implemented, a segmented (out-of-scope) system component could not impact the security of the CDE, even if an attacker obtained administrative access on that out-of-scope system.

[2] PCI DSS v3.2, page 11

Note that connectivity or access is allowed into the CDE from systems outside of the CDE. However, all such connectivity is in scope for PCI DSS and all applicable PCI DSS requirements apply to secure that connection or access.

The existence of separate network segments alone does not automatically create PCI DSS segmentation. Segmentation is achieved via purpose-built controls that specifically create and enforce separation and to prevent compromises originating from the out-of-scope network(s) from reaching CHD.

It is important to note that there is no solution or technology that eliminates all PCI DSS requirements. Tools and technologies (such as encryption or tokenization) may help reduce risk, reduce the applicability of some PCI DSS requirements, reduce the size of the CDE, or help meet PCI DSS requirements more easily.

To help support ongoing security, such technologies must be implemented properly with specific configuration settings and processes to ensure ongoing secure management of the technology. These controls should be part of the annual verification and testing to confirm that they are operating effectively.

## 2.1 Service Providers and other Third Parties

In addition to including internal systems and networks in scope, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for PCI DSS scope. Once the in-scope connections have been identified, the applicable PCI DSS controls must then be implemented to reduce the risk of a third-party connection being used to compromise an entity's CDE.

Similarly, if an entity outsources in-scope functions or facilities to a third party, or utilizes a third-party service that impacts how it meets PCI DSS requirements, the entity will need to work with the third party to ensure the applicable aspects of the service are included in scope for PCI DSS—either for the entity or the service provider. It is also important for both parties to clearly understand which PCI DSS requirements are being provided by the service provider and which are the responsibility of the entity using the service. See PCI DSS Requirement 12.8.

Refer to *PCI SSC Information Supplement: Third-Party Security Assurance*[3] for guidance on management third-party relationships.

## 2.2 Responsibility for Confirming Scope

It's important to understand the shared nature of confirming that PCI DSS scope has been accurately defined. PCI DSS provides the following direction:

*The entity is responsible for ensuring that its scope is kept accurate on an ongoing basis.*

> *At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of its PCI DSS scope by identifying all locations and flows of cardholder data, and identify all systems that are connected to or, if compromised, could impact the CDE (for example, authentication servers) to ensure they are included in PCI DSS scope.*
>
> *The entity retains documentation that shows how PCI DSS scope was determined. The documentation is retained for assessor review and/or for reference during the next annual PCI DSS scope confirmation*

[3] Available on the PCI SSC Website: https://www.pcisecuritystandards.org/document_library

> *activity. For each PCI DSS assessment, the assessor is required to validate that the scope of the assessment is accurately defined and documented.*[4]

This means that while the assessed entity is responsible for annually determining PCI DSS scope and confirming its accuracy, the assessor performing the PCI DSS validation is responsible to confirm that the scope has been defined and documented properly. The assessor should question scoping decisions if any are not clear in the assessed entity's documentation. In such cases, the assessor should work collaboratively with the entity to understand the scoping decisions made.

> *If network segmentation is in place and being used to reduce the scope of the PCI DSS assessment, the assessor must verify that the segmentation is adequate to reduce the scope of the assessment.*[5]

All segmentation controls must also be penetration tested at least annually per PCI DSS Requirement 11.3.4[6], to ensure that controls in place continue to provide effective segmentation.

[4] PCI DSS v3.2, page 10
[5] PCI DSS v3.2, page 11
[6] Effective 1 February, 2018, service providers must perform penetration testing at least every six months to verify segmentation controls.

# 3 Scoping Definition and Categories

In the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms*, scoping is defined as: "Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review."

Accurate scoping involves critically evaluating the CDE and connected-to system components to determine the necessary coverage for PCI DSS requirements.

A typical scoping exercise may include the following:

| Activity | Description |
|---|---|
| Identify how and where the organization receives CHD. | 1. Identify all payment channels and methods for accepting CHD, from the point where the CHD is received through to the point of destruction, disposal or transfer. |
| Locate and document where account data is stored, processed, and transmitted. | 2. Document all CHD flows, and identify the people, processes, and technologies involved in storing, processing, and/or transmitting of CHD. These people, processes, and technologies are all part of the CDE[7]. |
| Identify all other system components, processes, and personnel that are in scope. | 3. Identify all processes (both business and technical), system components, and personnel with the ability to interact with or influence the CDE (as identified in 2, above). These people, processes, and technologies are all in scope, as they have connectivity to the CDE or could otherwise impact the security of CHD. |
| Implement controls to minimize scope to necessary components, processes, and personnel. | 4. Implement controls to limit connectivity between CDE and other in-scope systems to only that which is necessary.<br>5. Implement controls to segment the CDE from people, processes, and technologies that do not need to interact with or influence the CDE. |
| Implement all applicable PCI DSS requirements. | 6. Identify and implement PCI DSS requirements as applicable to the in-scope system components, processes, and personnel. |
| Maintain and monitor. | 7. Implement processes to ensure PCI DSS controls remain effective day after day.<br>8. Ensure the people, processes, and technologies included in scope are accurately identified when changes are made. |

[7] While people who participate in storing, processing, or transmitting cardholder data are part of the CDE, when implementing segmentation for PCI DSS scoping, these people do not have to be segmented or isolated from people who are outside of the CDE. This is because the processes and technologies put in place to implement and maintain the segmentation also ensure that people in the CDE are the only ones with the requisite access.

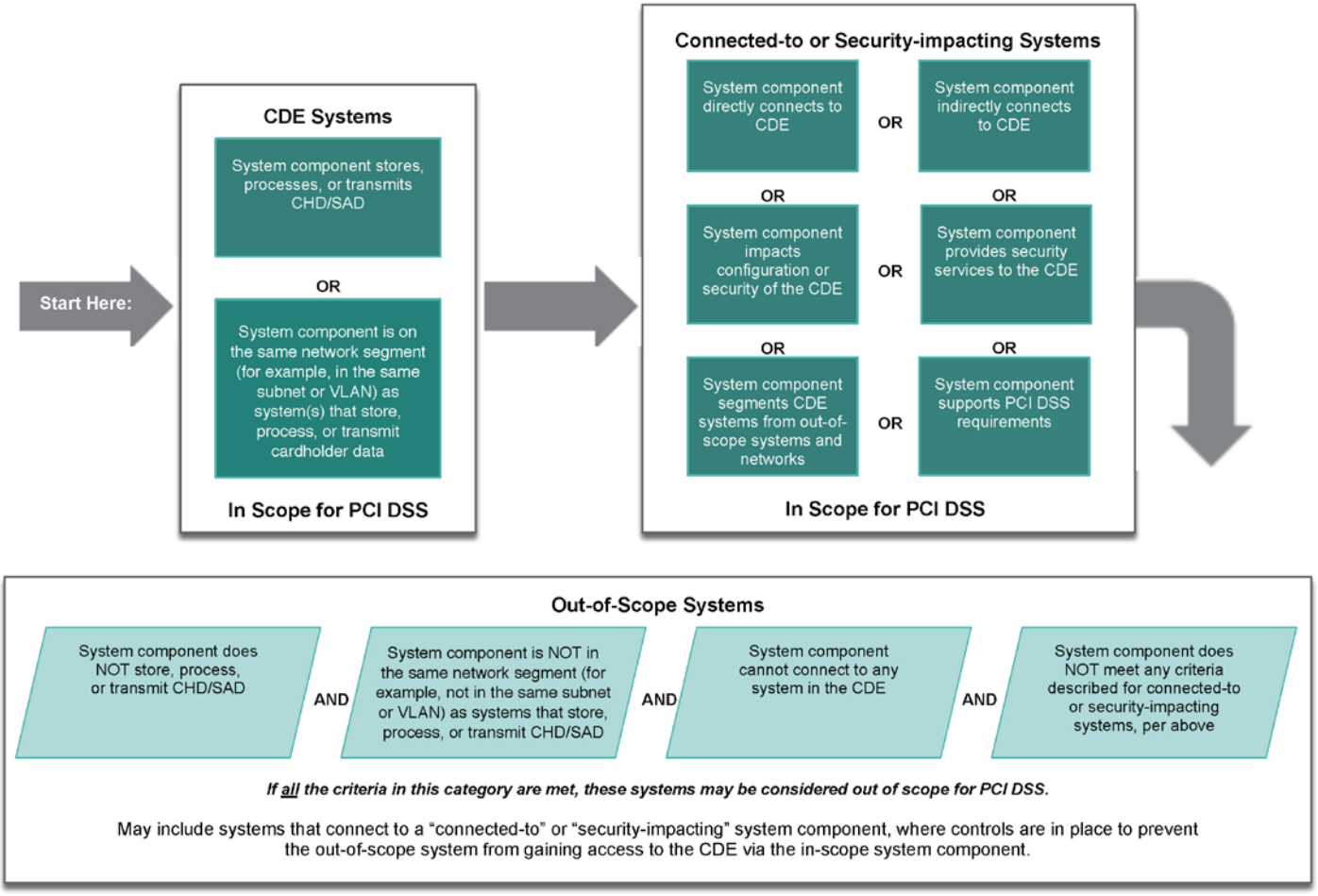
Note that being in scope does not mean that all PCI DSS requirements apply to a given system component; the applicable PCI DSS requirements[8] depend on the function and/or location of the system component.

The diagram and table in this section illustrate how system components can be categorized using several factors:

- Whether account data (CHD/SAD) is being stored, processed, or transmitted.
- The connectivity between the system component and the CDE.
- Whether a system component impacts the security of the CDE.

*The categories provided here are examples only, and illustrate one way to consider different components and the impact on PCI DSS scope. Entities can follow this approach or use another evaluation process, at their discretion. Use of these categories is not required.*

**FIGURE 1 – PCI DSS Scoping Categories**




In this approach, system components can be categorized into *only one* of these categories. These categories

[8] SAQ-eligible entities meeting all criteria for a particular SAQ may consider the applicable requirements to be those identified within that SAQ.

are hierarchical, with CDE Systems as the highest category that should be considered first; if a system meets any criteria in CDE Systems, it is a CDE system regardless of whether it also meets a description for a lower category. The next category includes connected-to and security-impacting systems; this category takes priority over and is evaluated before the out-of-scope systems category is considered. To be considered out of scope, a system must meet ALL the criteria of the out-of-scope category and NONE of the criteria of a higher category.

The following table contains more details about each category:

| System Type | Description | Scope and Applicability |
|---|---|---|
| **CDE Systems** | • System component stores, processes, or transmits CHD/SAD.<br>OR<br>• System component is on the same network segment—for example, in the same subnet or VLAN as system(s) that store, process, or transmit CHD/SAD. | **These systems:**<br>• Are in scope for PCI DSS.<br>• Must be evaluated to determine the applicability of each PCI DSS[9] requirement. |
| **Connected-to and/or Security-Impacting Systems** | • System component is on a different network (or subnet or VLAN), but can connect to or access the CDE (e.g., via internal network connectivity).<br>OR<br>• System component can connect to or access the CDE via another system—for example, via connection to a jump server that provides access to the CDE).<br>OR<br>• System component can impact configuration or security of the CDE, or how CHD/SAD is handled—for example, a web redirection server or name resolution server.<br>OR<br>• System component provides security services to the CDE—for example, network traffic filtering, patch distribution, or authentication management.<br>OR<br>• System component supports PCI DSS requirements, such as time servers and audit log storage servers.<br>OR<br>▪ System component provides segmentation of the CDE from out-of-scope systems and networks—for example, firewalls configured to block traffic from untrusted networks. | **These systems:**<br>• Are in scope for PCI DSS. Even where a connection is limited to specific ports or services on specific systems, those systems are included in scope to verify that the applicable security controls are in place.<br>• Must be evaluated to determine the applicability of each PCI DSS[9] requirement.<br>• Must not provide an access path between CDE systems and out-of-scope systems. |

[9] SAQ-eligible entities meeting all criteria for a particular SAQ may consider the applicable requirements to be those identified within that SAQ.

| System Type | Description | Scope and Applicability |
|---|---|---|
| **Out-of-scope Systems** | • System component does NOT store, process, or transmit CHD/SAD.<br>AND<br>• System component is NOT on the same network segment or in the same subnet or VLAN as systems that store, process, or transmit CHD.<br>AND<br>• System component cannot connect to or access any system in the CDE.<br>AND<br>• System component cannot gain access to the CDE nor impact a security control for CDE via an in-scope system.<br>AND<br>• System component does not meet any criteria described for connected-to or security-impacting systems, per above.<br>***Note:*** *These systems are not in scope for PCI DSS but could still represent a risk to the CDE if not secured. It is strongly recommended that security best practices be implemented for all out-of-scope systems/networks.* | **Out-of-Scope Systems:**<br>• Are not in scope for PCI DSS; therefore PCI DSS controls are not required.<br>• Have no access to any CDE system; if there is any access, then system is in scope.<br>• Are considered untrusted (or "public")—there is no assurance they have been properly secured.<br>• If on the same network (or subnet or VLAN) as, or otherwise has connectivity to, a connected-to or security impacting system, controls must be in place to prevent the out-of-scope system from gaining access to the CDE via the in-scope systems. These controls must be validated at least annually. |

## 3.1 Verifying segmentation of out-of-scope systems

To be considered out of scope, a system component must not have access to any system in the CDE. It is possible for an out-of-scope system to be on the same network segment or subnet as a connected-to or security-impacting system, as long as the out-of-scope system cannot access the CDE, either via the in-scope system or via any other method.

In order for a system to be considered out of scope, controls must be in place to provide reasonable assurance that the out-of-scope system cannot be used to compromise an in-scope system component, as the in-scope system could then be used to gain access to the CDE or impact security of the CDE. Examples of controls that could be applied to prevent out-of-scope systems from compromising a connected-to or security-impacting system include:

- Host-based firewall and/or intrusion detection and prevention system (IDS/IPS) on in-scope systems that block connection attempts from out-of-scope systems.
- Physical access controls that allow only designated users to access in-scope systems.
- Logical access controls that permit only designated users to login to in-scope systems.
- Multi-factor authentication on in-scope systems.
- Restricting administrative access privileges to designated users and systems/networks.
- Actively monitoring for suspicious network or system behavior that could indicate an out-of-scope system attempting to gain access to an in-scope system component or the CDE.

These examples are not all-inclusive nor would they all be applicable to every scenario. The intent of such controls is to provide reasonable assurance that an out-of-scope system cannot leverage an in-scope system component to gain access to the CDE or impact security of the CDE. The controls used to provide this assurance are part of the overall segmentation verification. Once all the segmentation controls are verified, the systems may be considered out of scope for PCI DSS.

***Security of Out-of-Scope Systems and Networks***

While it is not required to implement PCI DSS controls on out-of-scope systems, it is strongly recommended as a best practice to prevent out-of-scope systems from being used for malicious purposes. Examples of controls that can help reduce this risk include minimizing access between out-of-scope systems and public networks to only that which is necessary, keeping systems up to date with security patches and anti-virus software, using change-detection mechanisms (for example, file-integrity monitoring software), and implementing access controls based on strong authentication and least privilege.

***Note:*** *Securing out-of-scope systems/networks does not bring them into scope for PCI DSS requirements. However, if those controls also prevent the out-of-scope systems from accessing the CDE, the controls should be included in the segmentation verification.*

# 4 Example Segmentation Implementations: Shared Services

The examples in this section illustrate only two types of scenarios; there are many other implementation and configuration options that could be applied to segment the CDE from out-of-scope systems. A given implementation does not have to meet the criteria as stated in these examples—an implementation may need more or fewer controls depending on the specific environment. Because all environments and organizations are different, these examples are simplified to provide clarity around the issue of scope boundaries.

The following examples do not address the risk of an attacker compromising or gaining access to an administrator account in the out-of-scope network, and then using that account to gain access to the CDE. To mitigate the risk of such attacks, the ability to use administrator and user accounts should be limited to the system(s) and/or network segment(s) for which the administrator personnel has a specific, assigned administrative role. In this way, an account compromised in an out-of-scope network cannot be leveraged to gain access to other systems, networks or the CDE.

For segmentation of out-of-scope systems to be effective, rigorous controls must be in place to monitor and enforce the separation. Diligent logging and event monitoring are essential to detect and respond to failures in segmentation controls that could result in unauthorized access to the CDE from the out-of-scope network.

The following principles apply to both Example 1 (outlined in Section 5.1) and Example 2 (Section 5.2):

- Three distinct network zones are defined:
  - Corporate LAN
  - Shared Services
  - CDE
- Firewall and router rules ensure that:
  - The only connections permitted into and out of the CDE are to Shared Services, via specifically designated ports and systems, and only where there is a documented business need.
  - All connection attempts between the Corporate LAN and the CDE are actively blocked (no traffic that originated in the Corporate LAN is allowed into the CDE).
  - Communications between Shared Services and the Corporate LAN:
    - Are permitted only between designated systems, ports, services etc., and all other connection attempts are blocked.
    - Are limited by business need—for example, connectivity between workstations and a Directory Server is limited to only network authentication traffic.
- CHD is not stored, processed, or transmitted outside the CDE except via secured network connections to the acquiring bank/processor (not shown in the diagrams).
- All applicable PCI DSS requirements are applied:
  - To the CDE and Shared Services networks and system components
  - To manage and secure connectivity between the CDE and Shared Services, including firewalls, ACLs, IDS/IPS, anti-malware and other threat defense tools and techniques
  - To manage and secure inbound/outbound traffic between Shared Services and the Corporate LAN.

- Physical access to the CDE and Shared Services network is restricted to specifically designated personnel, as defined by business need.
- All controls that establish segmentation are included in each PCI DSS assessment to validate their effectiveness, including those that limit connections to specific ports or services on specific systems.
- Traffic and activity between Shared Services and the CDE, and within the CDE, is actively monitored and inspected to detect anomalies and reduce the risk of a Shared Services compromise leading to a compromise of the CDE.

## 4.1 Example 1: "Connected-to" Shared Services

***Note:*** *This example and the related diagrams are for illustration purposes only. Each network is different, and segmentation techniques that work well in one network may not work in another network. Thus, any segmentation method used must be thoroughly tested per PCI DSS requirements to confirm it works as expected and continues to provide effective segmentation in that environment. Similarly, controls noted herein are in addition to PCI DSS and may not be required or necessary for every environment.*

"Shared services" are common system components that provide services, such as authentication or management support, to system components across an organization's enterprise, including to both CDE systems and out-of-scope systems.

Common shared services include, but are not limited to:

- Directory and authentication (e.g., Active Directory, LDAP/ AAA)
- NTP – Network Time Protocol
- DNS – Domain Name Service
- SMTP – Simple Mail Transfer Protocol
- Monitoring and scanning tools
- Backup tools
- Anti-virus and patch deployment servers

For this example, the Shared Services are located outside of a segmented CDE but provide services to the CDE. The Shared Services also provide authentication and/or other operational support functions to other corporate systems that are deemed to be out-of-scope. Since these Shared Services are connecting to and providing services into the CDE, they are in scope for PCI DSS.

The question in this scenario is how to implement segmentation such that systems on the Corporate LAN can connect to the Shared Services but be effectively segmented from the CDE such that they cannot access the CDE. In other words, how to establish Shared Services that support both the CDE and the Corporate LAN, while keeping systems in the Corporate LAN out of scope for PCI DSS.

The following principles apply in addition to those defined above. See Figures 2 and 3.

- Administrative access to Shared Services systems is permitted only from within the Shared Services network, and all such access is logged and monitored.
- Administrative access to CDE systems is permitted only from systems within the CDE or from designated systems in the Shared Services network.

- Multi-factor authentication is used for all administrative access from Shared Services systems to the CDE. All administrative access to CDE is logged and monitored.
- Accounts used to access Shared Services from the Corporate LAN do not have any access to the CDE.
- All access controls are established and managed at the firewalls in the Shared Services and CDE zones.

**FIGURE 2 – Example Segmentation Illustration: "Connected-to" Shared Services**

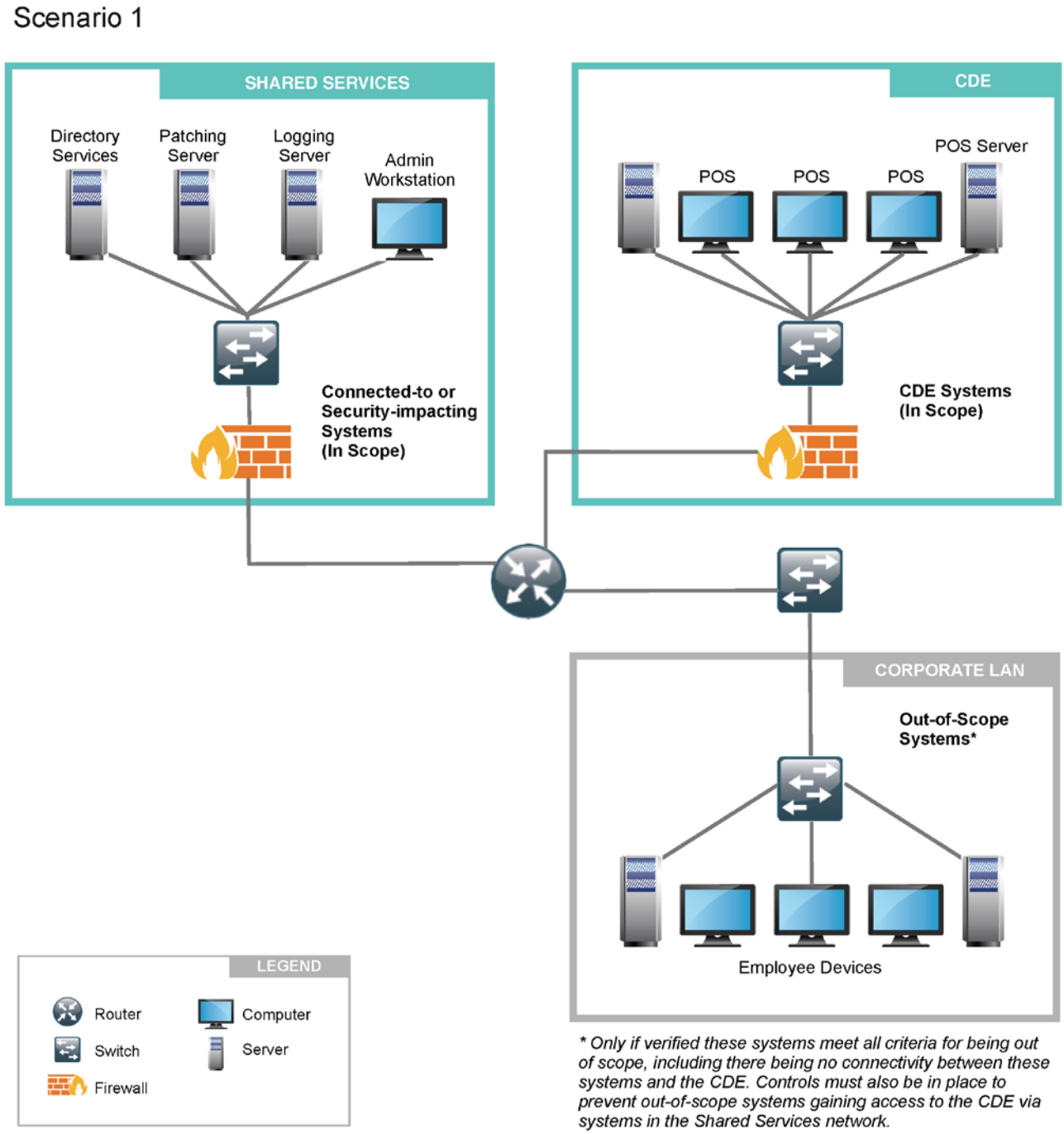
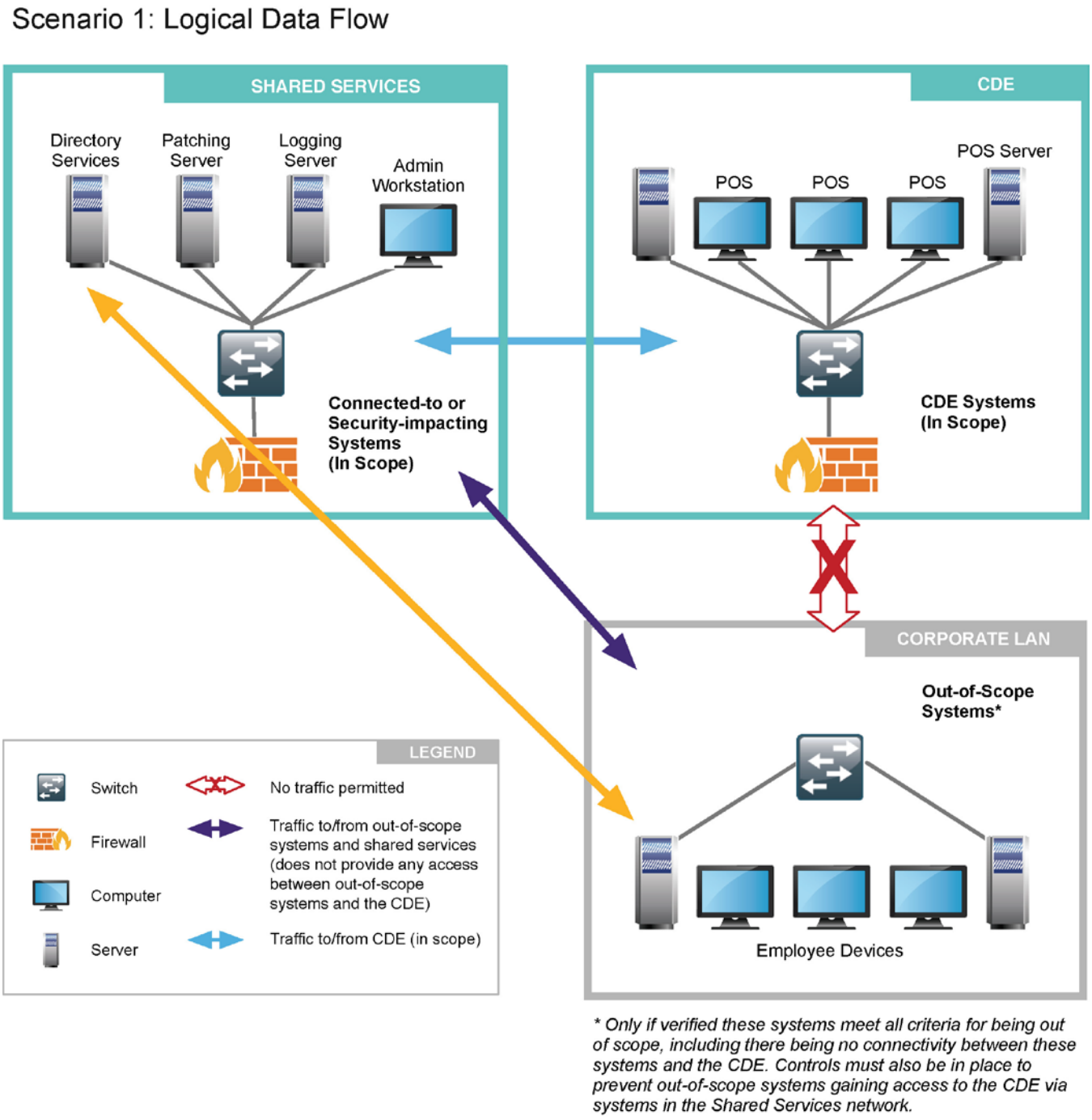


**FIGURE 3 – Logical Data Flow for "Connected-to" Shared Services**




** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

The following table summarizes the network zones illustrated in Figures 2 and 3 above, and the potential impact on PCI DSS scope.

| Network Zones | Category | Impact on PCI DSS Scope |
|---|---|---|
| CDE | CDE Systems | Fully in scope for all applicable PCI DSS requirements |
| Shared Services | Connected-to and/or Security-Impacting Systems | Fully in scope for all applicable PCI DSS requirements |
| Corporate LAN | Out-of-Scope Systems | Not in scope<br>*Segmentation controls must be fully tested and verified before the Corporate LAN systems can be determined to be out of scope. Systems and personnel in the Corporate LAN accessing Shared Services must not be able to gain access the CDE via the Shared Services. Segmentation controls need to be verified at least annually.* |

## 4.2 Example 2: CDE Administration Workstation outside of the CDE

***Note:*** *This example and the related diagrams are for illustration purposes only. Each network is different, and segmentation techniques that work well in one network may not work in another network. Thus, any segmentation method used must be thoroughly tested per PCI DSS requirements to confirm it works as expected and continues to provide effective segmentation in that environment. Similarly, controls noted herein are in addition to PCI DSS and may not be required or necessary for every environment.*

A system administrator often has responsibilities for systems across the enterprise, which may include CDE systems, connected-to and security-impacting systems, as well as out-of-scope systems. Administrator accounts are privileged accounts that need to be managed and monitored carefully since individuals with these higher privileges may grant elevated privileges to other users, and can access, add, delete, and change many (if not all) system and configuration files and settings, change or delete audit log data, and access CHD.

For this example, a system administrator is responsible for CDE Systems as well as systems in Shared Services and for out-of-scope systems in the Corporate LAN. The administrator's workstation is located in the Corporate LAN, and outside of the CDE. Therefore, system administration of the CDE originates from outside of, but requires connectivity to the devices within, the CDE.

This example builds on the Shared Services network from the previous example, with the addition of:

1) An administrator's workstation in the Corporate LAN and
2) A jumpbox within the Shared Services network to manage and control administrative access into the CDE.

The key question for this example is how to implement segmentation that allows for secure administration of CDE systems from a security-impacting system located in the Corporate LAN, and that also keeps the rest of the Corporate LAN systems out of scope.

The approach taken in this example is similar to that of a remote access scenario, where an administrator connects remotely to the CDE from their home network:

- The Corporate LAN is an untrusted network in a similar way as a home network would be.
- The Shared Services network zone acts like a DMZ, providing services both to untrusted computers as well as a trusted user with access to CDE.
- The Admin workstation is protected in the same way that a remote computer needs to be, with personal firewall software, multi-factor authentication, and all other applicable PCI DSS requirements in place.
- Access to the CDE from untrusted networks is managed and controlled by dedicated systems in the Shared Services network.

All the controls that apply to Example 1 also apply to this example, with the exception that administrative access to the CDE is permitted from a designated administrative workstation in the Corporate LAN. In addition to the controls defined above, the following segmentation principles are applicable to this example. (See Figures 4 and 5.)

- A "jumpbox" (Bastion host[10]) is installed in the Shared Services network.
- Firewall and router rules ensure that
  - Connections to the jump host from the Corporate LAN are restricted to only designated personnel from the Admin workstation, and all other connection attempts are blocked.
  - The Admin workstation is unable to access the CDE directly and must go through the Jump Box for all access to the CDE.
- Active monitoring and data loss prevention tools (DLP) are in place to ensure account data cannot be transferred from the CDE to the jumpbox.
- Administration of the jumpbox itself is via local console only, and there is no remote management of this device.
- The Admin workstation does not itself store, process, or transmit CHD.
- The Admin workstation is fully in scope for PCI DSS and all applicable PCI DSS requirements are applied.
- The Admin workstation (which is essentially located in an untrusted network) is protected from the Internet via personal firewall functionality as defined in PCI DSS Requirement 1.4.
- Use of the Admin Workstation is restricted to designated administrative personnel.
- Access to the jumpbox from the Admin workstation is via a different user account than that used to administer the CDE. The account used to access the jumpbox does not have elevated privileges on the Jump Box.

[10] A computer specifically designed and configured to withstand attacks. (Source: wikipedia.org)

- Access to the jumpbox from the Admin workstation requires multi-factor authentication for individuals. At least one of the multi-factor authentication methods is independent of the Admin workstation and is "in hand" of the designated administrator personnel (e.g. a physical smart card or token is used as "something you have" authentication).
- All applicable PCI DSS requirements are in place to manage and secure connectivity between the Admin workstation and jumpbox, including firewalls, IDS/IPS, anti-malware and other threat defense tools and techniques.
- All applicable PCI DSS requirements are in place to manage and secure connectivity between the jumpbox and CDE, including firewalls, IDS/IPS, anti-malware and other threat defense tools and techniques.

**FIGURE 4 – Example Segmentation Illustration: Administration of CDE Systems from a Security-Impacting System in the Corporate LAN**

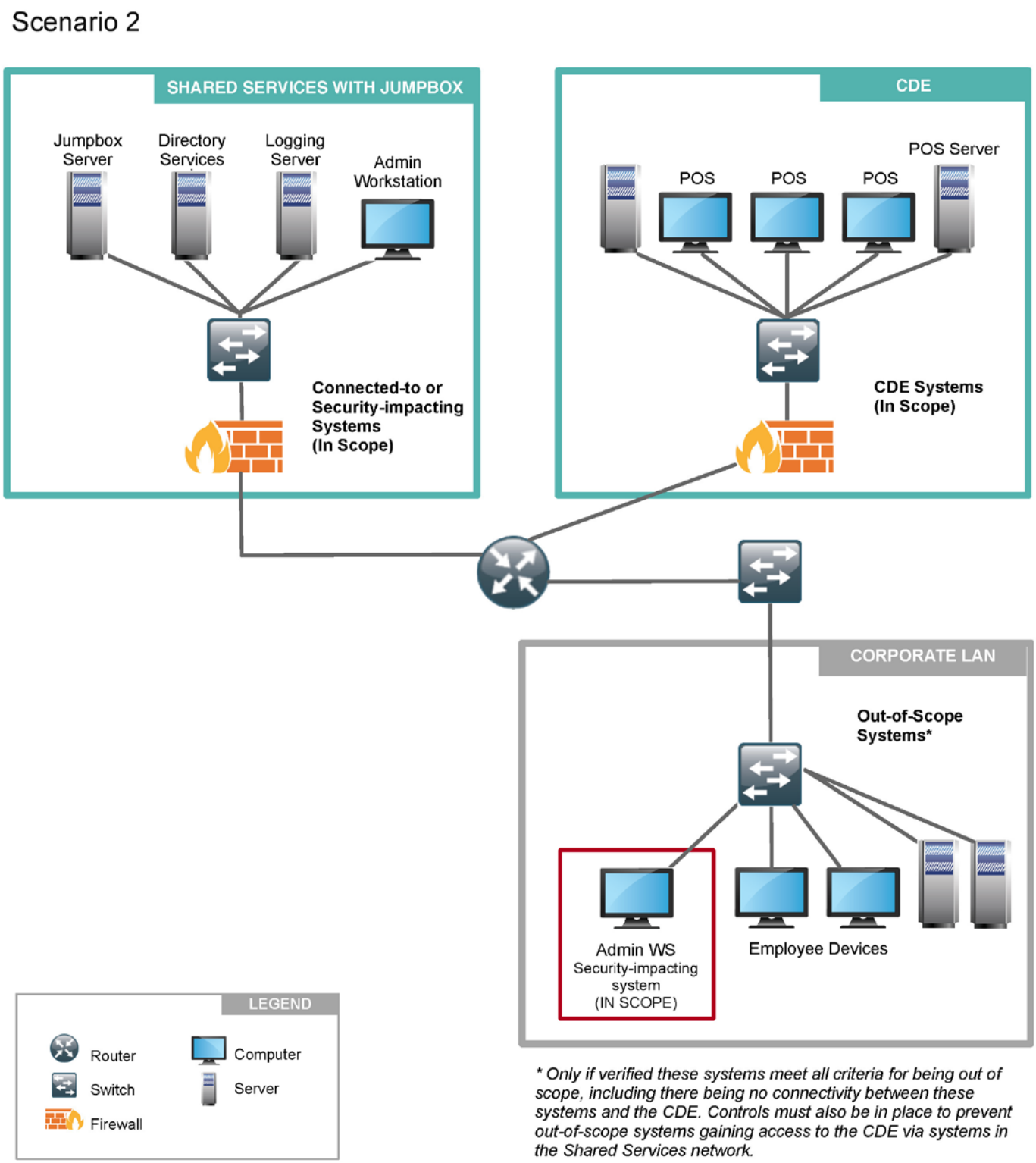
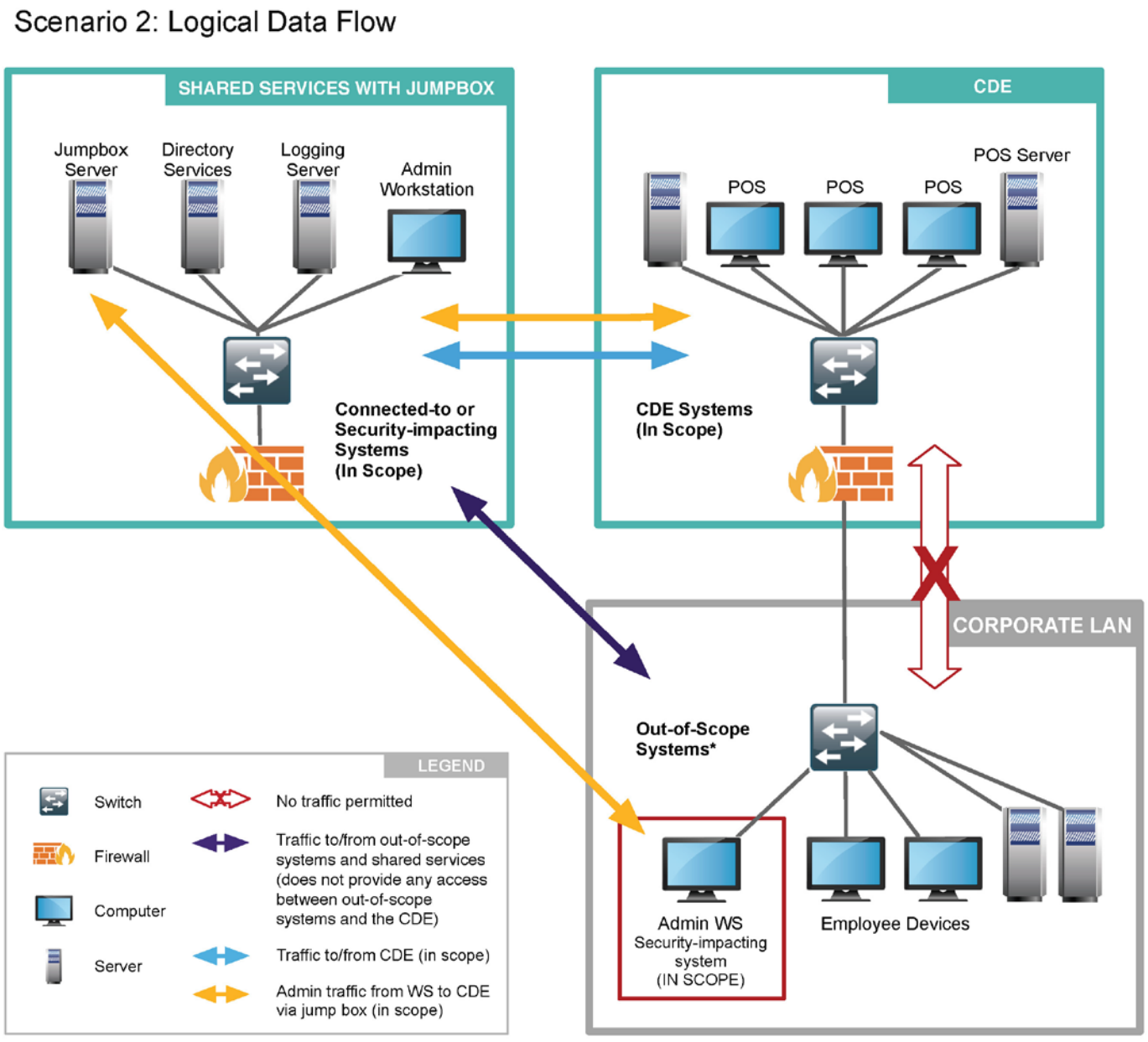


**FIGURE 5 – Logical Data Flow: Administration of CDE Systems from a Security-Impacting System in the Corporate LAN**




** Only if verified these systems meet all criteria for being out of scope, including there being no connectivity between these systems and the CDE. Controls must also be in place to prevent out-of-scope systems gaining access to the CDE via systems in the Shared Services network.*

The following table summarizes the network zones illustrated in Figures 4 and 5 above, and the potential impact on PCI DSS scope.

| Network Zones/Systems | Category | Impact on PCI DSS Scope |
|---|---|---|
| CDE | CDE Systems | Fully in scope for all applicable PCI DSS requirements |
| Shared Services (including Jump Box) | Connected-to and/or Security-Impacting System | Fully in scope for all applicable PCI DSS requirements |
| Admin Workstation in Corporate LAN | Security-Impacting System | Fully in scope for all applicable PCI DSS requirements |
| Other systems in Corporate LAN | Out-of-Scope Systems | Not in scope<br>*Segmentation controls must be fully tested and verified before other systems in the Corporate LAN can be determined to be out of scope. Systems and personnel in the Corporate LAN accessing Shared Services must not be able to gain access the CDE via the Shared Services. Segmentation controls need to be verified at least annually.* |

# 5 Conclusion

When scoping an environment for PCI DSS, it is important to always start with the assumption that everything is in scope until it is verified that all necessary controls are in place and are actually providing effective segmentation. Effective segmentation can greatly reduce the risk of CDE systems being impacted by security weaknesses or compromises originating from out-of-scope systems.

Remember that improper scoping (deciding something is out of scope without proper verification) can put a business at risk. To be effective, scoping and segmentation require careful planning, design, implementation, and monitoring. Many compromises have occurred via systems and networks incorrectly determined to be out of scope, where the breached entity placed false reliance on segmentation, only to find out after the breach that those controls were not effectively protecting its networks. It is therefore critical that entities focus on the security of their entire environment rather than solely on what is required by PCI DSS in order to minimize the risks to their organizations.

# About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and other standards that increase payment data security. Created in 2006 by the founding payment card brands American Express, Discover Financial Services, JCB International, Mastercard, and Visa Inc., the Council has more than 650 Participating Organizations representing merchants, banks, processors, and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.