Requirements and Testing Procedures		Guidance
1.4 Network connections between trusted and untrusted networks are controlled.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Implementing NSCs at every connection coming into and out of trusted networks allows the entity to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection. **Examples** An entity could implement a DMZ, which is a part of the network that manages connections between an untrusted network (for examples of untrusted networks refer to the Requirement 1 Overview) and services that an organization needs to have available to the public, such as a web server. Please note that if an entity's DMZ processes or transmits account data (for example, e-commerce website), it is also considered a CDE.
1.4.1 NSCs are implemented between trusted and untrusted networks.	**1.4.1.a** Examine configuration standards and network diagrams to verify that NSCs are defined between trusted and untrusted networks.	
	1.4.1.b Examine network configurations to verify that NSCs are in place between trusted and untrusted networks, in accordance with the documented configuration standards and network diagrams.	
Customized Approach Objective		
Unauthorized traffic cannot traverse network boundaries between trusted and untrusted networks.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **1.4.2** Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied. **Customized Approach Objective** Only traffic that is authorized or that is a response to a system component in the trusted network can enter a trusted network from an untrusted network. **Applicability Notes** The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.	**Defined Approach Testing Procedures** **1.4.2** Examine vendor documentation and configurations of NSCs to verify that inbound traffic from untrusted networks to trusted networks is restricted in accordance with all elements specified in this requirement.	**Purpose** Ensuring that public access to a system component is specifically authorized reduces the risk of system components being unnecessarily exposed to untrusted networks. **Good Practice** System components that provide publicly accessible services, such as email, web, and DNS servers, are the most vulnerable to threats originating from untrusted networks. Ideally, such systems are placed within a dedicated trusted network that is public facing (for example, a DMZ) but that is separated via NSCs from more sensitive internal systems, which helps protect the rest of the network in the event these externally accessible systems are compromised. This functionality is intended to prevent malicious actors from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner. Where this functionality is provided as a built-in feature of an NSC, the entity should ensure that its configurations do not result in the functionality being disabled or bypassed. **Definitions** Maintaining the "state" (or status) for each connection into a network means the NSC “knows” whether an apparent response to a previous connection is a valid, authorized response (since the NSC retains each connection’s status) or whether it is malicious traffic trying to fool the NSC into allowing the connection.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Filtering packets coming into the trusted network helps to, among other things, ensure packets are not “spoofed” to appear as if they are coming from an organization’s own internal network. For example, anti-spoofing measures prevent internal addresses originating from the Internet from passing into the DMZ. **Good Practice** Products usually come with anti-spoofing set as a default and may not be configurable. Entities should consult the vendor's documentation for more information. **Examples** Normally, a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet originated. Malicious individuals will often try to spoof (or imitate) the sending IP address to fool the target system into believing the packet is from a trusted source.
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	**1.4.3** Examine vendor documentation and configurations for NSCs to verify that anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	
Customized Approach Objective		
Packets with forged IP source addresses cannot enter a trusted network.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose**
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	**1.4.4.a** Examine the data-flow diagram and network diagram to verify that it is documented that system components storing cardholder data are not directly accessible from the untrusted networks.	Cardholder data that is directly accessible from an untrusted network, for example, because it is stored on a system within the DMZ or in a cloud database service, is easier for an external attacker to access because there are fewer defensive layers to penetrate. Using NSCs to ensure that system components that store cardholder data (such as a database or a file) can only be directly accessed from trusted networks can prevent unauthorized network traffic from reaching the system component.
	1.4.4.b Examine configurations of NSCs to verify that controls are implemented such that system components storing cardholder data are not directly accessible from untrusted networks.	
Customized Approach Objective		
Stored cardholder data cannot be accessed from untrusted networks.		
Applicability Notes		
This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Restricting the disclosure of internal, private, and local IP addresses is useful to prevent a hacker from obtaining knowledge of these IP addresses and using that information to access the network. **Good Practice** Methods used to meet the intent of this requirement may vary, depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks. **Examples** Methods to obscure IP addressing may include, but are not limited to: • IPv4 Network Address Translation (NAT). • Placing system components behind proxy servers/NSCs. • Removal or filtering of route advertisements for internal networks that use registered addressing. • Internal use of RFC 1918 (IPv4) or use IPv6 privacy extension (RFC 4941) when initiating outgoing sessions to the internet.
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	**1.4.5.a** Examine configurations of NSCs to verify that the disclosure of internal IP addresses and routing information is limited to only authorized parties.	
	1.4.5.b Interview personnel and examine documentation to verify that controls are implemented such that any disclosure of internal IP addresses and routing information is limited to only authorized parties.	
Customized Approach Objective		
Internal network information is protected from unauthorized disclosure.		