Requirements and Testing Procedures		Guidance
1.2 Network security controls (NSCs) are configured and maintained.		
Defined Approach Requirements **1.2.1** Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained. **Customized Approach Objective** The way that NSCs are configured and operate are defined and consistently applied.	**Defined Approach Testing Procedures** **1.2.1.a** Examine the configuration standards for NSC rulesets to verify the standards are in accordance with all elements specified in this requirement. **1.2.1.b** Examine configuration settings for NSC rulesets to verify that rulesets are implemented according to the configuration standards.	**Purpose** The implementation of these configuration standards results in the NSC being configured and managed to properly perform their security function (often referred to as the ruleset). **Good Practice** These standards often define the requirements for acceptable protocols, ports that are permitted to be used, and specific configuration requirements that are acceptable. Configuration standards may also outline what the entity considers not acceptable or not permitted within its network. **Definitions** NSCs are key components of a network architecture. Most commonly, NSCs are used at the boundaries of the CDE to control network traffic flowing inbound and outbound from the CDE. Configuration standards outline an entity's minimum requirements for the configuration of its NSCs **Examples** Examples of NSCs covered by these configuration standards include, but are not limited to, firewalls, routers configured with access control lists, and cloud virtual networks.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Good Practice** Changes should be approved by individuals with the appropriate authority and knowledge to understand the impact of the change. Verification should provide reasonable assurance that the change did not adversely impact the security of the network and that the change performs as expected. To avoid having to address security issues introduced by a change, all changes should be approved prior to being implemented and verified after the change is implemented. Once approved and verified, network documentation should be updated to include the changes to prevent inconsistencies between network documentation and the actual configuration.
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	**1.2.2.a** Examine documented procedures to verify that changes to network connections and configurations of NSCs are included in the formal change control process in accordance with Requirement 6.5.1.	
	1.2.2.b Examine network configuration settings to identify changes made to network connections. Interview responsible personnel and examine change control records to verify that identified changes to network connections were approved and managed in accordance with Requirement 6.5.1.	
Customized Approach Objective	**1.2.2.c** Examine network configuration settings to identify changes made to configurations of NSCs. Interview responsible personnel and examine change control records to verify that identified changes to configurations of NSCs were approved and managed in accordance with Requirement 6.5.1.	
Changes to network connections and NSCs cannot result in misconfiguration, implementation of insecure services, or unauthorized network connections.		
Applicability Notes		
Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **1.2.3** An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks. **Customized Approach Objective** A representation of the boundaries between the CDE, all trusted networks, and all untrusted networks, is maintained and available. **Applicability Notes** A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.	**Defined Approach Testing Procedures** **1.2.3.a** Examine diagram(s) and network configurations to verify that an accurate network diagram(s) exists in accordance with all elements specified in this requirement. **1.2.3.b** Examine documentation and interview responsible personnel to verify that the network diagram(s) is accurate and updated when there are changes to the environment.	**Purpose** Maintaining an accurate and up-to-date network diagram(s) prevents network connections and devices from being overlooked and unknowingly left unsecured and vulnerable to compromise. A properly maintained network diagram(s) helps an organization verify its PCI DSS scope by identifying systems connecting to and from the CDE. **Good Practice** All connections to and from the CDE should be identified, including systems providing security, management, or maintenance services to CDE system components. Entities should consider including the following in their network diagrams: • All locations, including retail locations, data centers, corporate locations, cloud providers, etc. • Clear labeling of all network segments. • All security controls providing segmentation, including unique identifiers for each control (for example, name of control, make, model, and version). • All in-scope system components, including NSCs, web app firewalls, anti-malware solutions, change management solutions, IDS/IPS, log aggregation systems, payment terminals, payment applications, HSMs, etc. • Clear labeling of any out-of-scope areas on the diagram via a shaded box or other mechanism. • Date of last update, and names of people that made and approved the updates. • A legend or key to explain the diagram. Diagrams should be updated by authorized personnel to ensure diagrams continue to provide an accurate description of the network.

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **1.2.4** An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment. **Customized Approach Objective** A representation of all transmissions of account data between system components and across network segments is maintained and available. **Applicability Notes** A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.	**Defined Approach Testing Procedures** **1.2.4.a** Examine data-flow diagram(s) and interview personnel to verify the diagram(s) show all account data flows in accordance with all elements specified in this requirement. **1.2.4.b** Examine documentation and interview responsible personnel to verify that the data-flow diagram(s) is accurate and updated when there are changes to the environment.	**Purpose** An up-to-date, readily available data-flow diagram helps an organization understand and keep track of the scope of its environment by showing how account data flows across networks and between individual systems and devices. Maintaining an up-to-date data-flow diagram(s) prevents account data from being overlooked and unknowingly left unsecured. **Good Practice** The data-flow diagram should include all connection points where account data is received into and sent out of the network, including connections to open, public networks, application processing flows, storage, transmissions between systems and networks, and file backups. The data-flow diagram is meant to be in addition to the network diagram and should reconcile with and augment the network diagram. As a best practice, entities can consider including the following in their data-flow diagrams: • All processing flows of account data, including authorization, capture, settlement, chargeback, and refunds. • All distinct acceptance channels, including card-present, card-not-present, and e-commerce. • All types of data receipt or transmission, including any involving hard copy/paper media. • The flow of account data from the point where it enters the environment, to its final disposition. • Where account data is transmitted and processed, where it is stored, and whether storage is short term or long term. *(continued on next page)*

<table>
<tr><th colspan="2">Requirements and Testing Procedures</th><th>Guidance</th></tr>
<tr><td colspan="2"></td><td>• The source of all account data received (for example, customers, third party, etc.), and any entities with which account data is shared.
• Date of last update, and names of people that made and approved the updates.</td></tr>
<tr><td>Defined Approach Requirements</td><td>Defined Approach Testing Procedures</td><td rowspan="3">Purpose
Compromises often happen due to unused or insecure services (for example, telnet and FTP), protocols, and ports, since these can lead to unnecessary points of access being opened into the CDE. Additionally, services, protocols, and ports that are enabled but not in use are often overlooked and left unsecured and unpatched. By identifying the services, protocols, and ports necessary for business, entities can ensure that all other services, protocols, and ports are disabled or removed.
Good Practice
The security risk associated with each service, protocol, and port allowed should be understood. Approvals should be granted by personnel independent of those managing the configuration. Approving personnel should possess knowledge and accountability appropriate for making approval decisions.</td></tr>
<tr><td>1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.</td><td>1.2.5.a Examine documentation to verify that a list exists of all allowed services, protocols, and ports, including business justification and approval for each.</td></tr>
<tr><td>Customized Approach Objective
Unauthorized network traffic (services, protocols, or packets destined for specific ports) cannot enter or leave the network.</td><td>1.2.5.b Examine configuration settings for NSCs to verify that only approved services, protocols, and ports are in use.</td></tr>
</table>

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Compromises take advantage of insecure network configurations. **Good Practice** If insecure services, protocols, or ports are necessary for business, the risk posed by these services, protocols, and ports should be clearly understood and accepted by the organization, the use of the service, protocol, or port should be justified, and the security features that mitigate the risk of using these services, protocols, and ports should be defined and implemented by the entity. **Further Information** For guidance on services, protocols, or ports considered to be insecure, refer to industry standards and guidance (for example, from NIST, ENISA, OWASP).
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	**1.2.6.a** Examine documentation that identifies all insecure services, protocols, and ports in use to verify that for each, security features are defined to mitigate the risk.	
	1.2.6.b Examine configuration settings for NSCs to verify that the defined security features are implemented for each identified insecure service, protocol, and port.	
Customized Approach Objective		
The specific risks associated with the use of insecure services, protocols, and ports are understood, assessed, and appropriately mitigated.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** Such a review gives the organization an opportunity to clean up any unneeded, outdated, or incorrect rules and configurations which could be utilized by an unauthorized person. Furthermore, it ensures that all rules and configurations allow only authorized services, protocols, and ports that match the documented business justifications. **Good Practice** This review, which can be implemented using manual, automated, or system-based methods, is intended to confirm that the settings that manage traffic rules, what is allowed in and out of the network, match the approved configurations. The review should provide confirmation that all permitted access has a justified business reason. Any discrepancies or uncertainties about a rule or configuration should be escalated for resolution. While this requirement specifies that this review occur at least once every six months, organizations with a high volume of changes to their network configurations may wish to consider performing reviews more frequently to ensure that the configurations continue to meet the needs of the business.
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	**1.2.7.a** Examine documentation to verify procedures are defined for reviewing configurations of NSCs at least once every six months.	
	1.2.7.b Examine documentation of reviews of configurations for NSCs and interview responsible personnel to verify that reviews occur at least once every six months.	
Customized Approach Objective	**1.2.7.c** Examine configurations for NSCs to verify that configurations identified as no longer being supported by a business justification are removed or updated.	
NSC configurations that allow or restrict access to trusted networks are verified periodically to ensure that only authorized connections with a current business justification are permitted.		

Requirements and Testing Procedures		Guidance
Defined Approach Requirements **1.2.8** Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations. **Customized Approach Objective** NSCs cannot be defined or modified using untrusted configuration objects (including files). **Applicability Notes** Any file or setting used to configure or synchronize NSCs is considered to be a "configuration file." This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.	**Defined Approach Testing Procedures** **1.2.8** Examine configuration files for NSCs to verify they are in accordance with all elements specified in this requirement.	**Purpose** To prevent unauthorized configurations from being applied to the network, stored files with configurations for network controls need to be kept up to date and secured against unauthorized changes. Keeping configuration information current and secure ensures that the correct settings for NSCs are applied whenever the configuration is run. **Examples** If the secure configuration for a router is stored in non-volatile memory, when that router is restarted or rebooted, these controls should ensure that its secure configuration is reinstated.