Requirements and Testing Procedures		Guidance
1.3 Network access to and from the cardholder data environment is restricted.		
Defined Approach Requirements	**Defined Approach Testing Procedures**	**Purpose** This requirement aims to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner. **Good Practice** All traffic inbound to the CDE, regardless of where it originates, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to ensure traffic is restricted to only authorized communications—for example, by restricting source/destination addresses and ports, and blocking of content. **Examples** Implementing a rule that denies all inbound and outbound traffic that is not specifically needed—for example, by using an explicit "deny all" or implicit deny after allow statement—helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic.
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**1.3.1.a** Examine configuration standards for NSCs to verify that they define restricting inbound traffic to the CDE is in accordance with all elements specified in this requirement.	
	1.3.1.b Examine configurations of NSCs to verify that inbound traffic to the CDE is restricted in accordance with all elements specified in this requirement.	
Customized Approach Objective		
Unauthorized traffic cannot enter the CDE.		