Requirements and Testing Procedures		Guidance
Defined Approach Requirements **1.3.2** Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	**Defined Approach Testing Procedures** **1.3.2.a** Examine configuration standards for NSCs to verify that they define restricting outbound traffic from the CDE in accordance with all elements specified in this requirement. **1.3.2.b** Examine configurations of NSCs to verify that outbound traffic from the CDE is restricted in accordance with all elements specified in this requirement.	**Purpose** This requirement aims to prevent malicious individuals and compromised system components within the entity's network from communicating with an untrusted external host. **Good Practice** All traffic outbound from the CDE, regardless of the destination, should be evaluated to ensure it follows established, authorized rules. Connections should be inspected to restrict traffic 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.
Customized Approach Objective Unauthorized traffic cannot leave the CDE.		
Defined Approach Requirements **1.3.3** NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	**Defined Approach Testing Procedures** **1.3.3** Examine configuration settings and network diagrams to verify that NSCs are implemented between all wireless networks and the CDE, in accordance with all elements specified in this requirement.	**Purpose** The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and account data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If NSCs do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information.
Customized Approach Objective Unauthorized traffic cannot traverse network boundaries between any wireless networks and wired environments in the CDE.		