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.