



National Security Agency/Central Security Service



INFORMATION ASSURANCE DIRECTORATE

CGS Network Boundary and Interfaces Capability

Version 1.1.1

The Network Boundary and Interfaces Capability for an Enterprise is essential; it provides for an understanding of the resources' interface to other networks or Enterprises, as well as all the interdependencies involved. For this Capability, Network Boundaries and Interface components shall be defined as applications, data, and devices connected to both sides of a network boundary (the boundary can be internal (i.e., between enclaves) or external to the Enterprise; however, they may not always be physically connected (e.g., a wireless network interface controller [WNIC] would be one such component).

07/30/2012



CGS Network Boundary and Interfaces Capability



Version 1.1.1

Table of Contents

1	Revisions	2
2	Capability Definition	3
3	Capability Gold Standard Guidance.....	3
4	Environment Pre-Conditions.....	6
5	Capability Post-Conditions.....	6
6	Organizational Implementation Considerations	7
7	Capability Interrelationships.....	8
7.1	Required Interrelationships	8
7.2	Core Interrelationships	8
7.3	Supporting Interrelationships.....	9
8	Security Controls	9
9	Directives, Policies, and Standards	11
10	Cost Considerations	15
11	Guidance Statements.....	16



CGS Network Boundary and Interfaces Capability



Version 1.1.1

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1



CGS Network Boundary and Interfaces Capability



Version 1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Network Boundary and Interfaces Capability for an Enterprise is essential; it provides for an understanding of the resources' interface to other networks or Enterprises, as well as all the interdependencies involved.

A network boundary is typically the point at which the resources owned or controlled by an Enterprise stop, and a connection to resources controlled by other entities occurs. Network boundaries are key to ensuring the information assurance (IA) of an Enterprise. Anything inside the network boundary can be controlled, changed, or addressed by the Enterprise; anything outside the network boundary cannot be easily controlled, if it can be controlled at all.

Networking services and protocols that use open ports or accept incoming connections are considered interfaces. If an interface is directly accessible by systems that are external to the network, that interface is considered an external interface. Directly accessible means this device is on the edge between owned and un-owned resources. Network Boundaries and Interfaces can also be internal to an Enterprise (e.g., the Enterprise can choose to structure its architecture into a set of distinct networks with defined interfaces among them). This can limit damage and risk, although it often has a negative impact on performance and sharing. If an Enterprise chooses to build internal network boundaries into its architecture, it must be able to identify each boundary and determine what is on each side of that boundary.

For this Capability, Network Boundaries and Interface components shall be defined as applications, data, and devices connected to both sides of a network boundary (the boundary can be internal (i.e., between enclaves) or external to the Enterprise; however, they may not always be physically connected (e.g., a wireless network interface controller [WNIC] would be one such component).

3 Capability Gold Standard Guidance

The CGS for IA provides comprehensive, measurable, IA guidance for securing NSS Enterprises while enabling the mission in the face of continuous attack. CGS defines



CGS Network Boundary and Interfaces Capability



Version 1.1.1

what it means for Capabilities to be considered “gold.” That is, it characterizes the highest level of practice for IA Capabilities in accordance with policies, standards, and best practices, while considering the limitations set forth by current technologies and other constraints.

The Enterprise shall be able to identify and have accountability for all of its Network Boundaries and Interfaces. Having a complete understanding of the network boundaries includes knowing how expansive the network is, where the network’s endpoints are, what other network(s) it connects to it, and how those connections to other network(s) are established. Knowing this level of detail means that all interdependencies shall be identified and understood.

A boundary may be physical or logical. The Capability shall be able to identify the set of functional and hardware elements that exists in the Enterprise’s configuration and shall specify all of the elements within the scope of this Capability. This shall include any external hardware dependencies, clearly indicating what is inside and outside the network boundary. The logical description shall also clearly define software characteristics for the major functional units of the Enterprise (e.g., systems, subsystems, services). In addition, the Network Boundary and Interfaces Capability shall include details of how (logical/physical) devices work together to fulfill a necessary function.

An interface is the specific point of interconnection for the communication layer being described. The Capability shall ensure that there are no boundary connections in place that subvert Network Boundary devices as defined within the Network Boundary Protection Capability.

Internal and external boundaries are dealt with differently. External boundaries apply to environments that may be out of the Enterprise’s control. Internal boundaries are between enclaves within an Enterprise and can be mechanisms to segregate information. Internal network segmentation is central to internal network control, because if intruders succeed in getting inside a network, they will more than likely attempt to target the most sensitive machines.

An Enterprise shall identify each of its internal and external network boundaries. This full and thorough identification shall include a description of the following:

1. Internal resources that connect to the external environment via that boundary.
2. External resources that can connect to the Enterprise system via that boundary.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

3. The risk(s) that the Enterprise incurs by operating such a boundary.

The description shall include type of devices, unique identifiers (e.g., Internet Protocol [IP]/Media Access Control [MAC] address), software/firmware version, and function. In addition, out-of-band (OOB) management systems for the boundary devices shall be known and documented. To identify each boundary device, the Network Boundary and Interfaces Capability exchanges information with the Network Mapping Capability in a central repository. The Network Boundary Protection Capability defines the protections for ensuring the control of the flow of traffic through network borders and to police its content to and from external networks.

Inside an Enterprise, the Enterprise controls the internal network segmentation, which changes in level of control and monitoring. That control, however, ends at the external network boundaries. Once an Enterprise understands the characteristics of both sides of a network boundary, that Enterprise will know where its control responsibilities lie, and how to gauge its control. Understanding that both sides of the network boundary have different characteristics and therefore behave differently is key to knowing where the internal boundary's control changes and who is in control. The Enterprise shall understand that it does not control the external network.

An Enterprise that wants to understand its risk status shall be able to identify all of its external network boundaries and identify what is on the other side of each boundary, where possible. However, Enterprises shall treat information about external network entities with skepticism and not depend on the accuracy of such information for the Enterprise's protection. If an Enterprise's architecture contains internal network boundaries, the Enterprise shall identify each of these boundaries and maintain a database of the same information stored for external boundaries.

Areas such as Demilitarized Zones (DMZ) also need to be accounted for within the Network Boundary and Interfaces Capability. In addition to devices beyond the boundaries, the Enterprise shall be aware of virtual private network (VPN) devices, which enable remote users to connect to the network. It is necessary to account for the devices connecting via VPN or other remote connections to have a full understanding of all boundaries and interfaces.

Once the Enterprise has identified all of its external and internal network boundaries, it works with other Community Gold Standard Capabilities to provide additional security



CGS Network Boundary and Interfaces Capability



Version 1.1.1

services (e.g., Network Boundary Protection, Network Access Control, Network Enterprise Monitoring, and Network/Host Intrusion Prevention/Detection).

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The Enterprise understands its internal system architecture, can identify each internal boundary point, and explain why it exists and what it protects.
2. The Enterprise understands its connections to external networks and can identify the risks incurred in the connection through that boundary.
3. Network boundaries use different network boundary devices, depending on the connection type and connection requirements.
4. Network boundary devices that are not discoverable by automated means are documented and can be provided as input to the Capability.
5. If network boundary devices are discoverable, the Capability can import device information.
6. Procedures for determining what device is appropriate at boundary and interface points accrediting those devices are established and employed.
7. Aggregation of boundary and interface data for the environment occurs at the same or high classification level using the appropriate protections or OOB networks, depending on Enterprise policy.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Enterprise will be able to identify external boundary points and identify (to the extent possible) what is on the outside of that boundary.
2. Network boundary device descriptions will be exportable to the Network Mapping Capability.
3. A boundary consists of an entire suite of IA functions, which may reside on multiple devices.
4. The Enterprise directly controls only what is on the internal side of the network boundary.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

An Organization will continuously monitor its Network Boundaries and Interfaces. This monitoring is conducted by other Community Gold Standard Capabilities (see Capability Interrelationships section). Usually, internal network protections are not set up to defend against an internal attacker. Setting up even a basic level of security segmentation across the network and protecting each segment with a proxy and a firewall will greatly reduce the internal attacker's access to the other parts of the network (see Network Boundary Protection Capability).

An Organization will be able to identify all of its external network boundaries and identify, to the extent possible, what is on the other side of each boundary. The vulnerabilities that lie on the external network pose risk to data and applications.

An Enterprise will structure its internal systems into logically or physically separate networks, with internal network boundaries between them. For example, this could be done to segregate systems handling information of different security classifications or information associated with different projects.

The Organization will use a standard reporting format for sharing Network Boundary and Interfaces information with the Network Mapping Capability tool, to produce reports on points of interest on a network, which is paramount to fully identifying the Network Boundaries and Interfaces.

Implementation of network boundary devices may also leverage other Community Gold Standard protection Capabilities such as Network Access Control, Network Boundary Protection, and Network Intrusion Detection. Most boundary interfaces connected to external networks will include other protection Capabilities; however, internal enclave boundaries may not include additional protections.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping—The Network Boundary and Interfaces Capability relies on the Network Mapping Capability to provide a picture that captures the network layout to determine the boundaries and interfaces (e.g., internal, external, physical, logical) of the Enterprise architecture.
- Understand Mission Flows—The Network Boundary and Interfaces Capability relies on the Understand Mission Flows Capability to provide mission context of information flowing across network boundaries and connections to other networks.
- Understand Data Flows—The Network Boundary and Interfaces Capability relies on the Understand Data Flows Capability to provide context of data flowing across network boundaries.
- Configuration Management—The Network Boundary and Interfaces Capability relies on the Configuration Management Capability to ensure that all network boundary devices, entry points, and exits are compliant with configurations as outlined in the Configuration Management Plan.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management—The Network Boundary and Interfaces Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards—The Network Boundary and Interfaces Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable U.S. laws, Executive Orders, regulations, directives, policies, procedures, and standards.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

- IA Awareness–The Network Boundary and Interfaces Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA. The IA Awareness Capability uses information provided by the Network Boundary and Interfaces Capability when constructing awareness messages.
- IA Training–The Network Boundary and Interfaces Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Network Boundary and Interfaces Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Security Evaluations–The Network Boundary and Interfaces Capability relies on the Network Security Evaluations Capability to provide information that is used to fill any gaps that may have been overlooked when enumerating boundaries and interfaces.
- Host Intrusion Detection–The Network Boundary and Interfaces Capability relies on the Host Intrusion Detection Capability to detect malicious activity affecting hosts that operate on the Enterprise’s network borders.
- Risk Mitigation–The Network Boundary and Interfaces Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, <i>Recommended Security Controls for Federal Information Systems and Organizations</i>	
AC-20 USE OF EXTERNAL	Control: The Organization establishes terms and conditions, consistent with any trust relationships established with other



CGS Network Boundary and Interfaces Capability



Version 1.1.1

<p>INFORMATION SYSTEMS</p>	<p>Organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:</p> <ul style="list-style-type: none"> a. Access the information system from the external information systems; and b. Process, store, and/or transmit Organization-controlled information using the external information systems. <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The Organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit Organization-controlled information only when the Organization: <ul style="list-style-type: none"> (a) Can verify the implementation of required security controls on the external system as specified in the Organization's information security policy and security plan; or (b) Has approved information system connection or processing agreements with the Organizational entity hosting the external information system. (2) The Organization limits the use of Organization-controlled portable storage media by authorized individuals on external information systems.
<p>CA-3 INFORMATION SYSTEM CONNECTIONS</p>	<p>Control: The Organization:</p> <ul style="list-style-type: none"> a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements; <p>Enhancement/s:</p> <ul style="list-style-type: none"> (1) The Organization prohibits the direct connection of an unclassified, national security system to an external network. <p>Enhancement</p> <ul style="list-style-type: none"> (2) The Organization prohibits the direct connection of a classified, national security system to an external network.
<p>SA-9 EXTERNAL INFORMATION SYSTEM SERVICES</p>	<p>Control: The Organization:</p> <ul style="list-style-type: none"> b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services <p>Enhancement/s: None Applicable</p>



CGS Network Boundary and Interfaces Capability



Version 1.1.1

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Network Boundary and Interfaces Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
ICD 503 IC Information Technology Systems Security Risk Management, Certification and Accreditation, Effective 15 September 2008, Unclassified	Summary: This directive addresses interconnection of accredited information technology (IT) systems and the standards for interconnections.
ODNI/CIO-2009-031 Connections of US and Commonwealth Secure Telephone Systems, 12 February 2009, Classified	Summary: This memorandum is classified and available for review.
DOD-IC Enterprise Email-multiple documents	Summary: This document identifies ... Enterprise email and identity management requirements to and across the network boundary.
See CGS Classified Annex for additional directives, policies and standards	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	



CGS Network Boundary and Interfaces Capability



Version 1.1.1

<p>DoDD 4630.05 Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), Certified Current as of 23 April 2007, Unclassified</p>	<p>Summary: This directive establishes DoD policy: It is DoD policy that: 4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate. The Department of Defense shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.</p>
<p>DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Unclassified</p>	<p>Summary: This Instruction implements DoD policy: It is DoD policy that: 4.1. IT and NSS employed by U.S. Forces shall, where required (based on capability context), interoperate with existing and planned, systems and equipment, of joint, combined and coalition forces and with other U.S. Government Departments and Agencies, as appropriate. The Department of Defense shall achieve and maintain decision superiority for the warfighter and decision-maker by developing, acquiring, procuring, maintaining, and leveraging interoperable and supportable IT and NSS.</p>
<p>DoDI 8110.1 Multinational Information Sharing Networks Implementation, 6 February 2004, Unclassified</p>	<p>Summary: This instruction identifies a purpose: "Assigns responsibilities and provides procedures to standardize the means for connecting the DoD components electronically to foreign nations on an Enterprise basis. It sets policy: "This Instruction implements policy established in reference to (a) multinational information sharing networks (MNIS) using the GIG." In addition, it establishes responsibilities for many elements including Associate Secretary of Defense for Networks and Information Integration (ASD(NII)) to: 5.1.5. Develop and promulgate additional guidance consistent with this Instruction regarding MNIS CENTRIXS networks to address such topics as: 5.1.5.1. Network standards, procedures, and management., and for the MINS Program Manager to: 5.8.5. Provide for the type-security test and certification of</p>



CGS Network Boundary and Interfaces Capability



Version 1.1.1

	MNIS CENTRIXS networks, their interfaces to each other, and their interfaces to U.S. networks, as appropriate, in accordance with...
CJCSI 6212.01E Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008, Unclassified	Summary: This instruction applies to: b. All IT and National Security Systems (NSS) (systems or services) acquired, procured, or operated by any component of the Department of Defense (DoD), including: (5) All DoD IT and NSS external information exchange interfaces with other U.S. government departments and agencies, combined and coalition partners, and multinational alliances (e.g., North Atlantic Treaty Organization).
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: Instruction addresses the needed authorities and processes for interconnections of Intelligence Community (IC) systems and DoD systems and involvement of agreed upon requirements of the DoD Chief Information Office (CIO) and the Associate Director of National Intelligence (ADNI)/CIO principal accrediting authorities.
Committee for National Security Systems (CNSS)	
NTISSI 1000 National Information Assurance Certification and Accreditation Process (NIACAP), April 2000, Unclassified	Summary: This Instruction addresses certification and accreditation and in that context also identifies network connection to other systems and networks.
CNSS Instruction No. 1253 Security Categorization and Control Selection for National Security Systems, October 2009, Unclassified	Summary: This instruction provides all Federal Government departments, agencies, bureaus, and offices with a process for security categorization of NSS that collect, generate, process, store, display, transmit, or receive National Security Information. This instruction also defines the National Institute of Standards and Technology (NIST) 800-53 controls for NSS.
Other Federal (OMB, NIST, ...)	
Nothing found	



CGS Network Boundary and Interfaces Capability



Version 1.1.1

Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	

Network Boundary and Interface Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
IC Standard ICS 503-1, Interconnection Security Agreements, 28 January 2009, Classified	Summary: This document identifies the standard for Interconnection Security Agreements.... The NIST SP 800-47 "Security Guide for Interconnecting Information Technology Systems," dated August 2002 is identified within this standard.
Draft ICS 2009-503.x Access by Commonwealth Partners to Information Technology Systems Processing U.S. National Intelligence Information, Draft 26 February 2009, Classified	Summary: This IC standard provides the requirements for access by Commonwealth ... users to U.S.-owned, Commonwealth-owned, and jointly owned IT systems processing U.S. national intelligence information.
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, ...)	
NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy,	Summary: This publication provides guidance related to "Boundary, or perimeter, of an untrusted network to block.., packet filters... "



CGS Network Boundary and Interfaces Capability



Version 1.1.1

September 2009, Unclassified	
NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, August 2002, Unclassified	Summary: This publication provides guidance for planning, establishing, maintaining, and terminating interconnections between IT systems owned and operated by different Organizations.
Executive Branch (EO, PD, NSD, HSPD, ...)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, ...)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Solution used for implementation—Factors that can affect this Capability include the size, weight, and power requirements.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

2. Storage requirements—The Enterprise will have to provide a facility to store and retrieve boundary information.
3. Impact/dependency on existing services—Some equipment requires an existing function to provide adequate cooling so it does not overheat.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Network Mapping Capability.

- The Enterprise shall identify and account for all of its network boundaries and interfaces, which include knowing how expansive the network is, where the network's end points are, what other networks it connects to, and how those connections to other networks are established.
- The Enterprise shall identify the set of functional and hardware elements that exists in the Enterprise's configuration for physical and logical boundaries. This shall include any external hardware dependencies, clearly indicating what is inside and outside the network boundary.
- The description for a logical boundary shall clearly define software characteristics for the major functional units of the Enterprise (e.g., systems, subsystems, services).
- Details of how (logical/physical) devices work together to fulfill a necessary function shall be defined.
- The Enterprise shall ensure there are no boundary connections in place that subvert network boundary devices.
- The Enterprise shall identify each of its internal and external network boundaries.
- If an Enterprise's architecture contains internal network boundaries, the Enterprise shall maintain a database of the same information stored for external boundaries.
- When identifying internal and external network boundaries, the Enterprise shall include a description of the internal resources that connect to the external environment via that boundary.
- When identifying internal and external network boundaries, the Enterprise shall include a description of the external resources that can connect to the Enterprise system via that boundary.



CGS Network Boundary and Interfaces Capability



Version 1.1.1

- When identifying internal and external network boundaries, the Enterprise shall include a description of the risks that the Enterprise incurs by operating such a boundary.
- The description for network boundaries shall include the type of device, unique identifiers (e.g., IP/MAC address), software/firmware version, and function.
- OOB management systems for the boundary devices shall be known and documented.
- The Enterprise shall identify what is on the other side of each external boundary, where possible.
- The Enterprise shall account for all demilitarized zones (DMZs).
- The Enterprise shall account for all VPN devices or other remote connections.
- The Enterprise shall account for all devices connecting via VPN or other remote connections.