COMPLIANCE COMPONENT

DEFINITION	
Name	Firewall Environments
Description	Firewall Environment is a term used to describe a set of systems and access controls between or within networks.
Rationale	The Firewall Environment provides protection for the organization's networks while minimizing complexity and management.
Benefits	• One part of a defense-in-depth security strategy • May integrate with other security solutions • Restricts connectivity between or within networks • Provides network segmentation • Provides remote access security

ASSOCIATED ARCHITECTURE LEVELS	
Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Secure Gateways and Firewalls
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE	
Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL	
State the Guideline, Standard or Legislation	**Firewall Environments may consist of:** • Firewall(s) • Demilitarized Zones (DMZs) • Virtual Private Networks Concentrators (VPNs) • Intranets • Extranets • Routers, hubs and switches • Intrusion Detection Systems (IDS/IPS) • Dynamic Host Configuration Protocol (DHCP) • Domain Name Server (DNS) A simple firewall environment may perform only packet filtering. In a more complex and secure environment, it may consist of packet filtering, proxies, IPS, VPN, and specific technologies supporting network security. **Building Firewall Environments** • A firewall shall be used between any agency-controlled equipment and equipment not controlled by the agency such as that owned by other agencies, contractors, business partners or public service providers.

	• The deployment should be as simplified as possible. Simplified firewall deployment will result in a more secure and manageable system. Complexity in deployment can lead to errors in configuration. • Equipment not intended to be Firewalls should not be configured as firewalls. For example, network equipment used as firewalls are not hardened systems and can lead to vulnerabilities. • A router should not be used as a firewall unless special firewall software is installed on it. • Internal firewalls should be used to minimize the threat landscape. **DMZs** • A DMZ is created to provide network segmentation and access control between environments with different security requirements. • Agencies should provide DMZ redundancy to minimize service degradation during denial of service attacks. • DMZs shall serve as connection points for systems that require or support external connectivity, or between internal systems with different levels of access control. • Agencies should place remote access servers, publically available assets and external VPN endpoints within DMZs. **VPNs** • External VPN connections shall be terminated on the firewall, ensuring that traffic passed through the VPN tunnel is encrypted between firewalls. **Intranets** • A computer network, which is not public, in contrast to the internet. • An intranet should be behind the firewall. • An internal firewall should be used to separate intranets. **Extranets** • An extranet is two or more networks that are joined via the Internet
Document Source Reference #	NIST SP 800-41, Guideline for Firewalls and Firewall Policy

Compliance Sources			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/Intpubs
Contact Information	inquiries@nist.gov		
Name	National Institute of Standards and Technology (NIST)	*Website*	http://csrc.nist.gov/
Contact Information			

KEYWORDS	
List Keywords	Threat landscape, DMZ, VPN, DNS, extranet, intranet, IDS, IPS, packet filter, defense-in-depth, access control, contractors, business partners, firewall

COMPONENT CLASSIFICATION				
Provide the Classification	☐ *Emerging*	☐ *Current*	☐ *Twilight*	☐ *Sunset*

Sunset Date			
CURRENT STATUS			
Provide the Current Status	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	6-8-2004	*Date Approved / Rejected*	3-29-2017
Reason for Rejection			
Last Date Reviewed	3-29-2017	*Last Date Updated*	3-29-2017
Reason for Update			