Compliance Component

DEFINITION

Name	Firewall Selection
Description	Selecting the appropriate firewall for a specific environment requires an understanding of the basic features of the various types of firewalls available. Supported feature sets, rather than firewall type, should drive the firewall selection.
Rationale	Recent advances in network infrastructure engineering and information security have resulted in a combining of the various firewall functions into hybrid products. It is not always a simple matter to decide which specific firewall product is the most suitable for a given application or enterprise infrastructure. Hybridization of firewall platforms makes the pre-purchase product evaluation phase of a firewall project important.
Benefits	• Selecting the appropriate firewall provides the security functions needed in the most efficient and cost-effective manner

ASSOCIATED ARCHITECTURE LEVELS

List the Domain Name	Security
List the Discipline Name	Technical Controls
List the Technology Area Name	Secure Gateways and Firewalls
List Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline
Component Sub-type	

COMPLIANCE DETAIL

State the Guideline, Standard or Legislation	**Supported features, rather than firewall classification, should drive firewall selection.** • For <u>speed</u>, <u>flexibility</u> and <u>simplicity</u>, select a firewall that includes: o Packet Filter Firewall, or o Stateful Inspection Firewall • For <u>high-bandwidth</u> or <u>real-time</u> applications select a firewall that includes: o Dedicated Proxy Server • For greater <u>authentication</u>, select a firewall that includes: o Application-Proxy Gateway Firewall, or o Dedicated Proxy Server • For greater <u>logging</u> capability, select a firewall that includes:

	o Application-Proxy Gateway Firewall, or o Dedicated Proxy Server • To perform specialized filtering (restrict outbound traffic to certain locations, examine all outbound email for viruses, restrict internal users from writing to the DMZ, track outgoing client ports individually, allow only established inbound connections) select a firewall that includes: o Dedicated Proxy Server, or o Stateful Inspection Firewall • To assist in foiling internally based attacks or malicious behavior, select a firewall that includes: o Dedicated Proxy Server, or o Personal Firewall • As an endpoint for a Virtual Private Network (VPN), select: o Personal Firewall NOTE: Many application-proxy gateway firewalls have implemented basic packet filter functionality in order to provide better support for UDP (User Datagram Protocol) based applications. Likewise, many packet filter or stateful inspection packet filter firewalls have also implemented basic application-proxy functionality to offset some of the weaknesses associated with their firewall platform. In most cases, packet filter or stateful inspection packet filter firewalls also implement application proxies to provide improved network traffic logging and user authentication in their firewalls.		
Document Source Reference #			
Standard Organization			
Name	NIST SP 800-41, Guideline for Firewalls and Firewall Policy	*Website*	www.csrc.nist.gov/publications/nistpubs
Contact Information			
Government Body			
Name	National Institute of Standards and Technology (NIST)	*Website*	http://csrc.nist.gov/
Contact Information			
KEYWORDS			
List all Keywords	Hybrid, packet filter, application proxy, stateful inspection, personal firewall, dedicated proxy server		
COMPONENT CLASSIFICATION			
Provide the Classification	☐ *Emerging* ☒ *Current* ☐ *Twilight* ☐ *Sunset*		
Rationale for Component Classification			
Document the Rationale for Component Classification			

Conditional Use Restrictions			
Document the Conditional Use Restrictions			
Migration Strategy			
Document the Migration Strategy			
Impact Position Statement			
Document the Position Statement on Impact			
CURRENT STATUS			
Provide the Current Status)	☐ *In Development* ☐ *Under Review* ☒ *Approved* ☐ *Rejected*		
AUDIT TRAIL			
Creation Date	05/27/2004	*Date Accepted / Rejected*	06/08/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			