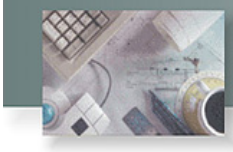

Compliance Component

DEFINITION	
Name	Dedicated Proxy Servers
Description	A Dedicated Proxy Server performs filtering or logging operations on inbound traffic and then forwards it to internal systems. A Dedicated Proxy Server could also accept outbound traffic directly from internal systems, filter or log the traffic, and then pass it to the firewall for outbound delivery. Dedicated Proxy Servers differ from Application-Proxy Gateway Firewalls in that they retain proxy control of traffic but they do not provide firewall capability.
Rationale	Dedicated Proxy Servers add to defense in depth when used with a firewall.
Benefits	• Decrease the work load on the firewall. • Perform specialized filtering. An organization can restrict outbound traffic to certain locations, examine all outbound email for viruses, or restrict internal users from writing to the DMZ. • Allow an organization to enforce user authentication requirements. • Perform specialized logging. • Assist in foiling internally based attacks or malicious behavior.

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	• Dedicated Proxy Servers shall be deployed behind traditional firewall platforms.
	  o A traditional firewall shall hand off the inbound traffic to the appropriate proxy server.
	  o A proxy server may be set up to accept outbound traffic directly from internal systems and pass it to the firewall for outbound delivery.
	• The proxy server shall be capable of performing filtering operations on all traffic before forwarding it.

	• The proxy server shall be capable of performing logging operations on all traffic. • The proxy server shall have the ability to require authentication of each individual network user. This user authentication may take one or more of the following forms, depending on data or information sensitivity: o User ID and Password Authentication o Hardware or Software Token Authentication o Biometric Authentication • Dedicated Proxy Servers should perform web and email content scanning, including but not limited to the following: o Java applet or application filtering (signed versus unsigned or universal) o ActiveX control filtering (signed versus unsigned or universal) o JavaScript filtering o Blocking specific Multipurpose Internet Multimedia Extensions (MIME) types o Virus scanning and removal o Macro virus scanning, filtering, and removal o Application-specific commands, for example, blocking the HTTP delete command o User-specific controls, including blocking certain content types for certain users Note: This is not a recommendation to enable blocking of active web content, but the proxy server should be capable of blocking it if necessary. The decision to block active content, excluding viruses, should be weighed carefully, as blocking active content will render many websites unusable or difficult to use. Organizations should not rely solely on the proxy server to remove the above content.
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	Application-Proxy Firewall, proxy agent, block, packets, deny, ports, protocols, logging, attacks, application layer, OSI, HTTP, ActiveX, Java, MIME, authentication, email, filtering, gateway		
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	06/08/2004	*Date Accepted / Rejected*	06/08/2004
Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			