Compliance Component

DEFINITION	
Name	Application-Proxy Gateway Firewalls
Description	Application-Proxy Gateway Firewalls combine OSI Layer 7 (Application Layer) functionality with lower layer access control. The application-proxy gateway firewall software performs the routing between the inside and outside interfaces of the firewall.
Rationale	Application-Proxy Gateway Firewalls add to defense in depth when used with other types of firewalls. They strengthen enforcement of security policies and provide user authentication capability.
Benefits	• In the event the application-proxy gateway software ceases to function, the firewall system will not pass network packets through the firewall system. • Application-Proxy Gateway Firewalls usually have more extensive logging capabilities than packet filter or stateful inspection because they examine the entire network packet rather than just the network addresses and ports. • Application-Proxy Gateway Firewalls provide superior authentication than packet filter or stateful inspection packet filter firewalls where network layer addresses can be easily spoofed. • Application-Proxy Gateway Firewalls are less vulnerable to address spoofing attacks than packet filter and stateful inspection firewalls. NOTE: • Application-Proxy Gateway Firewalls are not generally well suited to high-bandwidth or real-time applications. To reduce the load on the firewall, a Dedicated Proxy Server can be used to secure less time-sensitive services such as email and most web traffic. • Application-Proxy Gateway Firewalls tend to be limited in terms of support for new network applications and protocols. A separate, application-specific proxy agent is required for each type of network traffic that needs to transit a firewall.

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	• Each individual application-proxy, also referred to as a proxy agent, shall interface directly with the firewall access control rule set to determine whether a given piece of network traffic should be permitted to transit the firewall. • Each individual application-proxy shall have the ability to require authentication of each individual network user. This user authentication shall take two or more of the following forms: o User ID and Password Authentication o Hardware or Software Token Authentication o Source Address Authentication (on dedicated circuits only) o Biometric Authentication • Proxy applications should be used for inbound/outbound HTTP connections and for inbound/outbound email that are capable of the following operations: o Blocking Java applets and applications o ActiveX and JavaScript filtering o Blocking specific MIME extensions o Scanning for viruses Note: This is not a recommendation to enable blocking of active web content, but to 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 firewall proxies 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	Dedicated Proxy Server, proxy agent, block, packets, deny, ports, protocols, logging, attacks, Layer 7, application layer, OSI, HTTP, ActiveX, Java, MIME, authentication, spoof		
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			