Compliance Component

DEFINITION

Name	Stateful Inspection Firewalls
Description	Stateful Inspection Firewalls are packet filter firewalls that incorporate added awareness of the data at the OSI model Layer 4 (Transport Layer). The first line of the packet filter rule set allows any inbound connection if the destination port is between 1023 and 16384. Opening this many ports creates an immense risk of intrusion. Stateful inspection firewalls reduce this risk by creating a state table of outbound TCP connections, along with each session's corresponding port greater than 1023, which is then used to validate any inbound traffic.
Rationale	Stateful Inspection Firewalls add to defense in depth when used with other types of firewalls. They strengthen enforcement of security policies and add transport layer filtering.
Benefits	• Speed • Flexibility • Simplicity • Greater security than packet filter firewall because the Stateful Inspection Firewall tracks outgoing client ports individually and allows only established inbound connections.

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	• Stateful Inspection Firewalls shall create a state table of outbound TCP connections greater than 1023, along with each session's corresponding inbound port. This table shall be used to validate inbound and outbound traffic. • According to TCP specifications, the client source port shall be some number greater than 1023. According to convention, the destination port on the remote host will likely be less than 1024. • Stateful Inspection Firewalls shall accept a packet and examine its source address, destination address, port, and protocol. The firewall shall apply the rule set and perform one of the following: o Accept: Pass the packet through the firewall as requested. o Deny: Drop the packet and return an error message to the

	source system. o Discard: Drop the packet, but do not return an error message to the source system. This particular action does not reveal the firewall's presence ("black hole methodology") to an outsider. ● Outbound filtering should be employed on IP addresses, ports, protocols and application traffic to block unauthorized users, internal and external, from connecting to sensitive systems.		
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			
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	04/22/2004	*Date Accepted / Rejected*	06/08/2004

Reason for Rejection			
Last Date Reviewed		*Last Date Updated*	
Reason for Update			