Compliance Component

DEFINITION	
Name	Packet Filter Firewalls
Description	Packet Filter Firewalls are the most basic, fundamental type of firewall. Packet filter firewalls are essentially routing devices that include access control functionality for system addresses and communication sessions. The access control functionality of a packet filter firewall is governed by a set of directives collectively referred to as a rule set. In the basic form, packet filters operate at Layer 3 (Network) of the Open Systems Interconnect (OSI) model. This provides network access control based upon information contained in the packet.
Rationale	Packet Filter Firewalls allow for speed and flexibility, as well as the capability to block denial-of-service and related attacks. This makes them ideal for placement at the outermost boundary with an untrusted network. The packet filter firewall, commonly placed on a boundary router, can block certain attacks, filter unwanted protocols and perform simple access control. Packet filter firewalls are very suitable for high-speed environments where logging and user authentication with network resources are not important.

Benefits	• Packet Filter Firewalls provide:
	  • Speed
	  • Flexibility
	  • Simplicity
	NOTE:
	• Packet Filter Firewalls are only an initial layer of defense and should be used in conjunction with other types of firewalls
	• Packet Filter Firewalls cannot prevent attacks that employ application-specific vulnerabilities or functions
	• Most packet filter firewalls do not support advanced user authentication
	• Limited logging functionality

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	• Packet Filter 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. • Packet Filter Firewalls shall be able to filter both outbound as well as inbound traffic. • 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	Block, packets, deny, ports, protocols, rule set, logging, attacks, black hole, layer 3, OSI, boundary router		
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			