Compliance Component

DEFINITION

Name	Firewall Rules
Description	Firewall Rules describe how security policy will be implemented by the firewall and associated security mechanisms. The rules dictate how a firewall should handle traffic such as web, email, or telnet. The rules also describe how the firewall is to be managed and updated. The contents of these rule sets determine the actual functionality of a firewall.
Rationale	The firewall itself may become a security problem if there are no rules to guide firewall implementation and administration.
Benefits	• Enforces security policies • Protects internal networks from exploitation of vulnerabilities from outside entities and vice versa • Helps the organization establish trust with external connections NOTE: • Requires continual monitoring and updating to be effective • Rules are often complex and may slow the throughput

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	• A risk analysis must be performed before firewall rules can be created. • General rules should be kept as simple as possible, so as not to accidentally introduce holes that might allow unauthorized or unwanted traffic. • The general rule for handling inbound traffic should be to block all packets and connections unless the traffic type and connections have been specifically permitted. • Exceptions to the general firewall rules should be as specific as possible with regards to the network traffic they control. • The firewall rules should block the following types of traffic: o Inbound traffic from a non-authenticated source system

    with a destination address of the firewall. (This type of packet normally represents some type of probe or attack against the firewall.)

    - Inbound traffic with a source address indicating that the packet originated on a network behind the firewall. (This type of packet likely represents some type of spoofing attempt.)
    - Inbound traffic containing Internet Control Message Protocol (ICMP) traffic. (ICMP can be used to map the networks behind certain types of firewalls.)
    - Inbound or outbound traffic from a source address that falls within the address ranges set aside in RFC 1918 for private networks. (Such traffic typically indicates a denial-of-service attack.)
    - Inbound traffic from a non-authenticated source system containing Simple Network Management Protocol (SNMP) traffic. (These packets can indicate that an intruder is probing a network.)
    - Inbound traffic containing IP Source Routing information. (Source Routing has the potential to permit an attacker to construct a network packet that bypasses firewall controls.)
    - Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 or 0.0.0.0. (Some operating systems interpret these addresses as either local host or as a broadcast address, and these packets can be used for attack purposes.)
    - Inbound or outbound traffic containing directed broadcast addresses.
    - Executable files that should be considered for blocking include the following:
      .ade .cmd .eml .ins .mdb .mst .reg .url .wsf
      .adp .com .exe .isp .mde .pcd .scr .vb .wsh
      .bas .cpl .hlp .js .msc .pif .sct .vbe
      .bat .crt .hta .jse .msi .pl .scx .vbs
      .chm .dll .inf .lnk .msp .pot .shs .wsc
- The following services and applications traffic thus should be blocked inbound by that policy, with exceptions noted.

Application	Port Numbers	Action
Login services	telnet - 23/tcp	restrict w/strong authentication
	SSH - 22/tcp	restrict to specific systems
	FTP - 21/tcp	restrict w/strong authentication
	NetBIOS - 139/tcp	always block
	R services - 512/tcp - 514/tcp	always block
RPC and NFS	portmap/rpcbind - 111/tcp/udp	always block
	NFS - 2049/tcp/udp	always block
	Locked - 4045/tcp/udp	always block
NetBIOS in Windows NT	135/tcp/udp	always block
	137/udp	always block
	138/udp	always block
	139/udp	always block
	445/tcp/udp in Windows 2000	always block
X Windows	6000/tcp - 6255/tcp	always block
Naming Services	DNS - 53/udp	restrict to external DNS servers
	DNS zone transfers - 53/tcp	block unless external secondary
	LDAP - 389/tcp/udp	always block
Mail	SMTP - 25/tcp	block unless external mail relays
	POP - 109/tcp and 110/tcp	always block
	IMAP - 143/tcp	always block
Web	HTTP - 80/tcp and SSL 443/tcp	block unless to public web servers
	may also want to block common high-order HTTP port choices – 8000/tcp, 8080/tcp, 8888/tcp, etc.	
"Small Services"	ports below 20/tcp/udp	always block
	time - 37/tcp/udp	always block
Miscellaneous	TFTP - 69/udp	always block
	finger - 79/tcp	always block
	NNTP - 119/tcp	always block
	NTP - 123/tcp	always block
	LPD - 515/tcp	always block
	syslog - 514/udp	always block
	SNMP - 161/tcp/udp, 162/tcp/udp	always block
	BGP - 179/tcp	always block
	SOCKS - 1080/tcp	always block
ICMP	block incoming echo request (ping and Windows traceroute)	
	block outgoing echo replies, time exceeded, and destination unreachable messages except "packet too big" messages (type 3, code 4). This item assumes that you are willing to forego the legitimate uses of ICMP echo request to block some known malicious uses.	

- Firewall rules should be reviewed and updated at least twice per year, or whenever there are any enterprise computing environment modifications, or after any significant security incident. Both of the following methods should be used to review the firewall rules.
    - Obtain hardcopies of the current firewall configurations and compare these against the expected configuration

	based on the rules. o Verify the configuration of a device by attempting to perform operations that should be prohibited.		
Document Source Reference #	NIST Special Publication 800-41		
Standard Organization			
Name	NIST	*Website*	www.csrc.nist.gov
Contact Information	inquiries@nist.gov		
Government Body			
Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	www.csrc.nist.gov/publications/
Contact Information	inquiries@nist.gov		
KEYWORDS			
List all Keywords	Filter, packets, Simple Network Management Protocol (SNMP), traffic, configuration, risk assessment, routing, directed broadcast		
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			