



DEPARTMENT OF HUMAN RESOURCES FIREWALL GUIDELINES

Inbound and Outbound Access

References:

1. ISO 17799 Information Technology – Code of practice for information security management
2. National Institute of Standards and Technology (NIST) Publication 800-41, Guidelines on Firewalls and Firewall Policy

DHR Guidelines for firewall Inbound and Outbound Access are:

All inbound and outbound network traffic through DHR firewalls must be blocked unless it is explicitly permitted. Only DHR mission-related applications and services that are approved by the designated Information Security Manager, Manager of Information Systems or appointed network manager are allowed to pass through DHR firewalls.

The following types of network traffic originating from outside the DHR network must always be blocked:

- Inbound traffic from a non-authenticated source address with a destination address of the firewall system itself
- Inbound traffic with a source address indicating that the packet originated on a network behind the firewall
- Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks
 - 10.0.0.0 to 10.255.255.255 (Class A, or “/8” in CIDR notation)
 - 172.16.0.0 to 172.31.255.255 (Class B, or “/12” in CIDR notation)
 - 192.168.0.0 to 192.168.255.255 (Class C, or “/16” in CIDR notation)
- Inbound traffic containing IP Source Routing information. This type of traffic potentially permits an attacker to construct a network packet that bypasses firewall controls
- Inbound or Outbound traffic containing a source or destination address of 127.0.0.1 (localhost/loopback) or 0.0.0.0, whether originating internally or externally of the DHR network. Such traffic is usually indication of attack against the firewall itself
- Examples of inbound traffic to be blocked or restricted can be found in table 1.0 below.



DEPARTMENT OF HUMAN RESOURCES FIREWALL GUIDELINES

Examples of Inbound Services and Applications Traffic Originating Externally of the DHR network to be Blocked or Restricted

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
	lockd - 4045/tcp/udp	always block
NetBIOS in Windows NT	135/tcp/udp	always block
	137/udp	always block
	138/udp	always block
	139/tcp	always block
	445/tcp/udp in Windows 2000	always block

Table 1.0

At a minimum, firewall rule sets must contain the following fields:

- The source address of the packet, i.e., the Layer 3 address of the computer system or device the network packet originated from
- The destination address of the packet, in other words., the Layer 3 address of the computer system or device the network packet is trying reach
- The type of traffic, in other words, the specific network protocol being used to communicate between the source and destination systems or devices – often Ethernet at Layer 2 and IP at Layer 3
- *Characteristics of the Layer 4 communications sessions* – the protocol, such as TCP, and the source and destination ports of the sessions (e.g., TCP:80 for the destination port belonging to the web server and TCP:1320 for the source port belonging to the personal computer accessing the server)
- An action, such as Deny, Permit or Drop the packet.

Examples of fields in the firewall rule sets can be found in table 2.0 below.



DEPARTMENT OF HUMAN RESOURCES FIREWALL GUIDELINES

Sample Firewall Rule Set

	Source Address	Source Port	Destination Address	Destination Port	Action	Description
1	192.168.1.1	Any	Any	Any	Deny	Prevent Firewall system itself from directly connecting to anything
2	Any	Any	192.168.1.2	SMTP	Allow	Allow External Users to send email to proxy
3	Any	Any	192.168.1.2	HTTP	Allow	Send inbound HTTP to proxy
4	Any	Any	Any	Any	Deny	"Catch-All" Rule - Everything not previously allowed is explicitly denied

Table 2.0