
	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 1	

Firewall

	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 2	

1. Introduction

Firewalls are systems designed to prevent unauthorised access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both and are frequently used to prevent unauthorised Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.


Network firewalls and Intrusion Detection Systems (IDS) are the most common types of security products that work at the network layer.

2. Objective(s)

- 2.1 To define a set of baseline firewall security controls applicable to hardware/software firewalls within the organization.
- 2.2 Limit inbound and outbound services among internal computer networks and between the Internets to only those services required for authorized MTD business functions.
- 2.3 Ensure the integrity of MTD's information systems data.
- 2.4 Safeguard information assets from exposure to external threats from disruption, interference, unauthorized access, misuse, theft, denial of service, or other potentially destructive activity.

3. Scope

- 3.1 Controls specified in this document apply to all firewall systems.
- 3.2 All of the organization's networked systems will be subject to the policies specified within this firewall security standard. The policies will be applied to new and existing installations.

	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 3	

- 3.3 The scope of this policy includes all connections among internal networks and between any publicly accessible computer networks, and includes all other connections between MTD computer system networks and external public or private organizations.

4. Definitions

Extranet

An extranet is a virtual network created by connecting two intranets. An organization that connects remote locations with a VPN creates an extranet by linking its intranets together to form one virtual network.

Firewall Rule set

A firewall rule set is a table of instructions that the firewall uses for determining how packets should be routed between its interfaces.

IDS

Intrusion Detection System, a software application that can be implemented on host operating systems or as network devices to monitor for signs of intruder activity and attacks.

Intranet


An intranet is a network internal to an organization but that runs the same protocols as the network external to the organization. Every organizational network that runs the TCP/IP protocol suite is an intranet.

SSL

Secure Sockets Layer, based on public key cryptography, used to generate a cryptographic session that is private to a web server and a client browser.

VPN

Virtual Private Network is used to securely connect two networks or a network and a client system, over an insecure network such as the Internet. A VPN typically employs encryption to secure the connection.

	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 4	

Inbound traffic

Data that travels from an untrusted source (Internet or public network) to a trusted network (Internal network), the reverse is applicable to outbound traffic.

RFC 1918

IP Address allocation for private network with IP range:-

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

5. Firewall Policy


- 5.1 Configure firewalls with outgoing access to the Internet, but strictly limit incoming access to MTD data and systems by Internet users.
- 5.2 No MTD computer or subnet that has connections to the Internet can house private or sensitive information without the use of firewalls or some other means to protect the information.
- 5.3 Firewall accounts are given to only those absolutely necessary, such as the system administrator.
- 5.4 Allow only required protocols on the firewall for inbound traffic.
- 5.5 Disable any features of the firewall that is not needed, including other network access.
- 5.6 Turn on full logging at the firewall and analyze the logs periodically.















6. Firewall Management


- 6.1 The management console for the firewall must adhere to the following criteria:











6.1.1 Management console should be accessible by system administrator.

6.1.2 Full authentication and an encrypted link is required for remote administration (this option should be disabled unless absolute necessary).


	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 5	





Name	Port	Inbound	Outbound	Description	Comments
DNS	53/udp			Domain Name Service translates domain names into IP addresses	Restrict incoming traffic to external DNS server
DNS Zone Transfers	53/tcp			The synchronization of authoritative DNS data between DNS servers.	Block unless external secondary
FTP	21/tcp			File Transfer Protocol allows sending and receiving files between machines	Restrict incoming traffic with string authenticati
HTTP	80/tcp/udp			Hypertext Transfer Protocol is the underlying protocol used by the World Wide Web (WWW)	Servers publishing web services (eg. WEBPOS which are behind the firewall should use the mapped interface (MIP
HTTPS	443/tcp			Hypertext Transfer Protocol with SSL (Secure Socket Layer) is a protocol for transmitting private documents via the Internet	
IMAP	143/tcp			Internet Message Access Protocol is a protocol used for retrieving email messages	
LDAP	389 (tcp,udp)			Lightweight Directory Access Protocol is a set of protocols used to access information directories	


	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 6	

Name	Port	Inbound	Outbound	Description	Comments
NFS	2049/tcp/ udp			Network File System allows network users to access shared files stored on computers of different types	
NNTP	119/tcp			Network News Transport Protocol is a protocol used to post, distribute, and retrieve USENET messages	
NTP	123/tcp			Network Time Protocol	
PING	ICMP			Packet Internet Groper is a utility to determine whether a specific host is accessible by its IP address	
POP3	109/tcp 110/tcp			Post Office Protocol is a protocol used for retrieving email	Restrict unless users are allowed to access remotely


RIJALUDDIN SALLEH
 Senior General Manager, Head
 Group Compliance & General Services Division

	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 7	

Name	Port	Inbound	Outbound	Description	Comments
SSH	22/tcp			Secure Shell is a program to log into another computer over a network through strong authentication and secure communications on an unsecure channel	Restrict to specific systems
TRACEROUTE	ICMP			Trace Route is a utility to indicate the path to access a specific host	

	MTD GROUP	DOC NO. 15	ISSUE: 3
		REV. DATE: 12 Feb 2020	REV. NO. 2
TITLE:	FIREWALL	PAGE: 8	

7. Firewall Monitoring and Reporting

7.1 Events to be monitored

7.1.1 Administrative events

7.1.1.1 Changes to the firewall policy

7.1.1.2 Changes of the administrative accounts

7.1.2 Network connection logs

7.1.2.1 Syslog messages should be logged on a daily basis and monitored regularly for irregularities in traffic patterns.

7.1.3 Firewall monitors

Firewalls should be monitored for the following possible network attacks. It also forms part of a passive Intrusion Detection System.

- Ping of death
- Tear drop attack
- Win nuke attack
- Filter IP source route attack
- Port scans
- Address sweep attack
- IP spoofing
- ICMP flooding
- UDP flooding
- ICMP fragment
- Large ICMP packet
- IP fragment packet