	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 1 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

Network Connection Safeguards Procedure

I. SCOPE

This procedure applies to Tenet Healthcare Corporation, its consolidated subsidiaries and all hospitals and other healthcare operations owned or operated by Tenet’s consolidated subsidiaries (Tenet). This procedure applies to all Tenet information assets and information asset Administrators.

II. PURPOSE

Provide guidelines for the use of network connection safeguards to secure Tenet’s network environment. Network connection safeguards, including firewalls, de-militarized zones (DMZs), and virtual private networks (VPNs), are security tools used to protect the confidentiality, integrity, and availability of the network environment controlled by Tenet.

Where network, system, application, or facility capabilities or processes dictate a divergence from these policies, the reasons for the exception shall be documented and maintained by the controlling entity in its Information Security Control Exceptions Book.

III. PROCEDURE


Network connection safeguards will be implemented to secure Tenet’s network environment. Firewall(s) will control, at the perimeter, all traffic between trusted and un-trusted networks, allowing access controls, monitoring and other security functions to be effectively applied. DMZs will protect the trusted network from third parties that require access to an information asset, but not the entire trusted network. VPNs will protect information during transmission between Tenet and connected parties.

A. Firewall Requirements

Approved firewall(s), and/or other access control technology or processes shall be established between trusted and un-trusted networks (as defined in the Network Security Administration Procedure No. 8.3.1). This includes, but is not limited to, a firewall controlling connections between Tenet LANs and any external network (i.e. Internet, Extranet, Dialup, VPN, external computer network).

1. Internal Firewalls

Tenet facilities shall deploy approved firewalls or security devices that are on the approved list from the Tenet Corporate Information Systems Department. This includes other network security technologies (i.e. Anti-Virus, Intrusion Detection

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 2 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

Systems, and Intrusion Prevention Systems) implemented internally to their LAN environment to isolate critical or *CONFIDENTIAL* systems, applications, data and information from the rest of the network.


B. Firewall Architecture

Firewall software or appliances will run on a dedicated device or clustered devices. Firewall architectures provide various levels of security at varying costs of installation and operation. The firewall architecture shall be selected, designed, implemented, and configured with consideration as to the risks to the trusted network.

1. Firewall Device Selection

The following requirements should be followed when selecting a firewall device.

- a) Part of the firewall’s interrogation of network traffic must take into consideration the User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) protocol state of the connection. Each time a TCP connection is established in one interface and out another interface of the firewall, the information about the connection should be logged in a stateful session table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular host(s) and connection. Subsequent packets should be compared against session known states in the connection table and are permitted through the firewall only if an appropriate connection exists to validate their passage. This connection information should be temporarily stored until the connection is closed or abnormally terminated.
- b) Packet oriented firewall filtering doesn’t meet the requirements for being stateful. Firewalls should support defining security policy with specific source host, specific destination host, and specific protocol/port.
- c) High availability or cluster capabilities must be incorporated into the firewall device or by using another like device that would support automated failover of firewall functionality from the primary unit to a standby or secondary firewall device.
- d) Firewall devices must have the capability to support centralized management, preferably through an administration tool. Local device management via a web browser does not constitute centralized management. All remote access to

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 3 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

centralized management stations should be controlled through authentication and encryption.

- e) Firewall devices must have the capability to support centralized logging.
- f) Firewall devices must come with or be able to support hosting a DMZ.
- g) Proven firewall manufacturers, including those certified by the ICSA Labs are recommended.

2. Firewall Design and Implementation


The following requirements should be followed when designing and implementing a firewall device.

- a) Firewalls shall be designed so that no single point of failure would cause network services to be unavailable. A reserve firewall should be maintained to be used as a backup to the primary firewall.
- b) Firewalls shall be tested for vulnerabilities and configuration prior to moving into “production”. Firewalls shall be retested annually as part of the contingency plan testing process (see Contingency Planning Policy No. 6.0.0).
- c) All outbound connections will be translated to a registered IP Address owned or leased by Tenet. Specific applications requiring a specific Network Address Translation will be assigned on a case by case basis.

3. Firewall Configuration

Firewalls shall be configured in such a way so as to fulfill their purpose of protecting the trusted network from un-trusted sources. Accordingly, the following requirements should be followed when configuring a firewall.

- a) Firewalls shall be configured to deny services and ports not required.
 - (i) Inbound Connectivity - Users/Systems wishing to establish a connection, from any un-trusted network (the Internet or non-core Tenet LANs), to Tenet internal networks (LANs), must use one of the Virtual Private Network (VPN) technologies offered by the Tenet Corporate Information Systems Department.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 4 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

(ii) Outbound Connectivity - Only the most common and widely utilized services will be allowed outbound without further business justification. Any other connectivity outbound should be considered an exception to the standard. Approval from Tenet Corporate must be obtained and documented before the connectivity can be implemented.

- b) Only services required to conduct Tenet business shall be allowed. See Addendum A for firewall configuration recommendations, including allowed services.
- c) Opening connectivity to and from large networks with non-restrictive access are not allowed.
- d) IP Spoofing will be guarded against with all available firewall features. Any spoofing attempt will be denied. Any attempt to traverse the firewall from a network believed to be coming from the wrong logical network area will be deemed as spoofing and denied.
- e) Firewalls shall reject probing or scanning.

C. Firewall Administration

Firewalls shall be continuously administered once installed in production.


1. Administrator Requirement

Only the firewall Administrator and backup Administrators shall be given accounts on the Tenet firewall(s). Two firewall administrators (one primary and one secondary) shall be responsible for continuous maintenance of the firewall. Firewall Administrators shall receive periodic training on firewalls and network security practices, and should preferably hold certification in these practices.

2. Administrative Access

The preferred method for administrative access is directly from an attached terminal.

- a) Physical access to the firewall terminal shall be limited to the firewall Administrator and backup Administrator.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 5 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

b) Remote access for firewall administration shall be allowed, however, it shall be limited to access from other hosts on the Tenet internal network.

3. Firewall Monitoring

All Tenet firewalls should be continuously monitored for up/down status.

4. Connectivity

Firewalls shall be regularly audited and monitored to detect intrusions or misuse or connectivity that is no longer needed.

5. Upgrading and Patching The Firewall

Firewall software upgrades and patches will be applied in a timely manner after adequate testing has been completed. To optimize the performance of the firewall, vendor recommendations for processor and memory capacities shall be followed.

6. Configuration Documentation

Appropriate firewall documentation shall be maintained on off-line storage. This includes diagrams, IP addresses and configurations.

7. Logging And Auditing


Firewall logging and auditing shall conform to the Logging and Auditing Procedure No. 8.2.2.

D. De-Militarized Zones (DMZs)

A DMZ is an area set aside to separate two networks, one trusted (internal) and one un-trusted (external). It is not part of either the internal or external network. DMZs, primarily used for web servers, consist of firewalls, routers, servers, authentication capabilities and monitoring capabilities that buffer Tenet networks from outside networks and their associated risks.

1. DMZ Architecture

A firewall should be installed between the un-trusted network, DMZ and trusted networks so that network traffic that traverses the DMZ can be controlled at a granular level.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 6 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

2. DMZ Configuration

The following recommendations should be considered when configuring the DMZ.

- a) Un-trusted to DMZ: Default to deny all. Allow only specific destination IP address and port access.
- b) Un-trusted to Trusted: Default to deny all. No access without Tenet approved exception.
- c) DMZ to Un-trusted: Default to deny all. Allow DMZ network to un-trusted via specific port access.
- d) DMZ to Trusted: Default to deny all. No access without Tenet approved exception.
- e) Trusted to Un-trusted: Default to deny all. Allow access via specific protocol/port address.
- f) Trusted to DMZ: Default to deny all. Only specific support, administrative, or trusted infrastructure traffic is permitted.


E. Virtual Private Networks (VPNs)

A VPN will protect information during transmission between Tenet and connected parties.

1. VPN Architecture

VPNs should be implemented with a site-to-site architecture. Client/server VPNs are not permitted. The VPN device can be a hardware appliance or server based. Server based VPN devices must run Linux or Solaris based operating systems. Microsoft operating systems are not an accepted base operating systems for VPN devices.

- a) The VPN device should incorporate firewall connection or stateful oriented inspection.
- b) VPNs should support defining security policy with specific source host, specific destination host, and specific protocol/port.


	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 7 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

- c) High availability or cluster capabilities must be incorporated into the VPN authentication process.
- d) VPN devices must have the capability to support centralized management, preferably through an administration tool. Local device management via a web browser does not constitute centralized management. All remote access to centralized management stations should be controlled through authentication and encryption.
- e) VPN devices must have the capability to support centralized logging.
- f) VPN devices must come with or be able to support hosting a de-militarized zone (DMZ).
- g) VPN devices should support pre-shared key authentication. It is recommended that the VPN support the 3DES, AES128 and AES256 encryption algorithms and MD5 and SHA1 data integrity algorithms.
- h) Proven VPN manufacturers, including those certified by the ICSA Labs are recommended.
- i) VPNs shall be designed so that no single point of failure would cause network services to be unavailable. A means of providing backup connections shall be maintained to return service in the event of an internet outage or denial of service.

2. VPN Configuration

The following recommendations should be considered when configuring the VPN.

- a) Establishment of VPNs over the internet requires written approval of facility management and the Corporate Information Systems Department.
- b) Adding networks to an existing VPN shall follow the same process as required by an original connection.
- c) For internal connections, Tenet firewalls shall operate in the Trusted Link mode, encrypting VPN traffic but not requiring the use of firewall proxies for VPN traffic.

	Information Security Policies and Procedures	No. COMP-Sec 8.3.4
	Title: NETWORK CONNECTION SAFEGUARDS PROCEDURE	Page: 8 of 12
		Revised Date: 12/22/04
		Original Date: 12/22/04

- d) For external connections, Tenet firewalls shall operate in the Private Link mode, encrypting VPN traffic and requiring the use of firewall proxies limiting the services available to remote VPN hosts.

IV. RELATED DOCUMENTS AND REFERENCES

This document is directly related to the following documents:

- Corporate Information Security Policy No. 1.0.0.
- Technical Security Management Policy No. 8.0.0.
- Change Control Procedure No. 8.2.1.
- Logging and Auditing Procedure No. 8.2.2.
- Network Security Administration Standard No. 8.3.0.
- Network Security Administration Procedure No. 8.3.1.
- Network Access Controls Administration Procedure No. 8.3.2.
- Network Connections Procedure No. 8.3.3.
- Transmission Security Procedure No. 8.3.6.

ADDENDUM A

FIREWALL CONFIGURATION RECOMMENDATIONS

STANDARD PROTOCOLS AND PORTS

The following standard protocols/ports may be allowed from the internal trusted network to the internet (or DMZ where appropriate):

- DNS udp/53 (DNS servers only)
- DNS tcp/53 (DNS servers only)
- HTTP tcp/80
- HTTP tcp/81 (common HTTP server redirect)
- HTTP tcp/8080 (common HTTP server redirect)
- HTTPS tcp/443 (SSL)
- ICMP (echo request)
- SMTP tcp/25 (SMTP relays only)

The following standard protocols/ports may be allowed from the internet to the internal trusted network (or DMZ where appropriate):

- DNS udp/53 (DNS servers only)
- DNS tcp/53 (DNS servers only)
- HTTP tcp/80 (web servers only)
- HTTPS tcp/443 (web servers only)
- ICMP (echo reply)
- ICMP (destination unreachable)
- SMTP tcp/25 (SMTP relays only)

CONSIDERATION FOR SPECIFIC SERVICES

The following information provides an overview of current known risks and vulnerabilities that need to be addressed to provide a standard level of information security controls for information assets. Information asset Administrators shall follow these recommendations where appropriate and/or document their alternative approach.

- **ActiveX And Java** - Unless otherwise specified, ActiveX and Java shall be disabled in all Tenet systems. If these services are required, the appropriate security software shall be employed.
- **DNS (Domain Names Service)** - DNS does zone transfers and contains names of hosts and information about hosts that could be helpful to attackers. This service can be spoofed. (Port 53)
- **Finger And WHOIS** - Finger and WHOIS shall be disabled at the firewall.
- **FTP** - The following configuration statements apply to FTP (ports 20, 21):

- o Incoming FTP data connections shall be directed to a high TCP port (>1024)
 - o All incoming FTP connections shall be blocked or restricted to specific systems.
 - o Passive FTP shall be used.
 - o All outgoing FTP connections are allowed.
 - o Trivial FTP (TFTP) is used for booting diskless workstations, terminal servers and routers. TFTP can also be used to read any file on the system if set up incorrectly. (Port 69)
- **Gopher (HTTP for Mosaic)** - Gopher information servers and client programs for gopher and WWW clients, shall be restricted to an application gateway that contains proxy services. (Ports 70, 80)
 - **High Port Numbers** - All services on high port numbers that listen for TCP connections shall be blocked. These include, but are not limited to:
 - o X-windows (port 6000+)
 - o OpenWindows (port 2000+)
 - o NFS (port 2049) (usually runs over UDP, but can be run over TCP)
 - **ICMP Redirects** - All outgoing ICMP echo-reply and destination-unreachable messages shall be blocked. This is to hide the internal network and prevent its unauthorized use.
 - o Before deciding to completely block ICMP, the Administrator shall be aware of how the TCP protocol does "Path MTU Discovery", to make certain connectivity to other sites is not broken. If it cannot be safely blocked everywhere, consider allowing selected types of ICMP to selected routing devices. If ICMP is not blocked, the Administrator shall ensure that routers and hosts don't respond to broadcast ping packets.
 - **Low Port Connections** - All connections to low port numbers shall be blocked, with the exception of SMTP and DNS connections.
 - **NFS** - NFS shall not be allowed through a firewall.
 - **NNTP** - NNTP (Network News Transfer Protocol) is used for accessing and reading network news. NNTP servers shall not be run on the firewall, but standard proxy services are available to pass NNTP. (Port 119)
 - **RIP (Routing Information Protocol)** - RIP can be spoofed to redirect packet routing, (port 520)
 - **RPC (Remote Procedure Calls)** - RPC services, which include NIS and NFS, can be used to read and write to files and to steal system information such as passwords. (Port 111) There is

a problem with a number of RPC services. They are difficult to filter effectively because the associated servers listen at ports that are assigned randomly at system startup.

- o If the router cannot be told which ports the services reside at, it is not possible to block completely these services unless one blocks all UDP packets (RPC services mostly use UDP).
 - o Blocking all UDP would block potentially necessary services such as DNS.
- **SMTP And DNS (Incoming)** - All incoming SMTP and DNS shall be routed to the external mail server (alt - the mail server). (Port 25)
- **TELNET** - The telnet service shall be restricted to specific systems. (Port 23)
- **UDP (User Datagram Protocol) Traffic** - UDP is a connectionless protocol. UDP is to be disabled (dropped) at the firewall. While this action may reduce some functionality, it protects Tenet from:
 - o NFS attacks caused by improper configuration
 - o NFS attacks caused by bugs
 - o TFTP sniffing attacks
 - o DNS attacks on machines inside the network
 - o FSP traffic (FTP-like program, popular with software piracy addicts)
 - o Routing Protocol (RIP) spoofing attacks
 - o Attacks upon some common-but-insecure RPC based services.
- **Unix R Commands** - BSD "r" commands, such as rsh, rlogin, rexec, rcp, etc., are designed to allow UNIX system Users to execute commands on remote systems. If these services are improperly configured, they can permit unauthorized access to accounts and commands. Most implementations do not support authentication or encryption and are very dangerous to use over the Internet. The "r" commands shall be disabled at the firewall. (Ports 512, 513, 514)
- **Unix Remote Printing Protocols** - In general, lp and lpr shall be disabled at the firewall unless vendor supplied proxies are available.
 - o The UNIX remote printing protocols lp and lpr allow remote hosts to print using printers attached to other hosts. Lpr is a store and forward protocol, while lp uses the rsh function to provide remote printing capabilities.
- **Unix UUCP (Unix To Unix Copy)** - UUCP if improperly configured can be used for unauthorized access. (Port 540)

- **Web Server Restrictions** - Web server hosts shall have all traffic except HTTP blocked. This shall reduce the number of services available to attack to one.
- **X11, X Windows Or OpenWindows** - X11, X Windows and OpenWindows can leak information from X Window displays including all keystrokes. These services shall be blocked. (Ports 6000+, port 2000)
 - o The X Windows System is a very useful system, but unfortunately has some major security flaws. Remote systems that can gain or spoof access to a workstation's X display can monitor keystrokes that a User enters, download copies of the contents of their windows, or perform other unauthorized activities.
 - o While attempts have been made to overcome them (i.e. MIT "Magic Cookie"), it is still entirely too easy for an attacker to interfere with a User's X display. Most firewalls block all X traffic. Some permit X traffic through application proxies such as the DEC CRL X proxy (FTP crl.dec.com). The firewall toolkit includes a proxy for X, called x-gw, which a User can invoke via the Telnet proxy, to create a virtual X server on the firewall.
 - o When requests are made for an X connection on the virtual X server, the User is presented with a pop-up asking them if it is OK to allow the connection. While this is a little unaesthetic, it is entirely in keeping with the rest of X.