Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# The Firewall has been Installed, Now What? Developing a Local Firewall Security Policy

Given the responsibility of configuring firewalls for a departmental network, I discovered that a local firewall security policy had not been written. This paper details the process I used to draft a perimeter device security policy for these firewalls. The firewall policy at the end of this document completes the policy draft process. The information gathered to draft a local firewall policy also lead to the creation of a PIX Firewall Security Services and Requirements matrix. This matrix maps HIPAA and local security...

Copyright SANS Institute
Author Retains Full Rights

AD

**The Firewall has been Installed, Now What?**
**Developing a Local Firewall Security Policy**

**Richard Walker**
**March 12, 2002**

## Abstract

Given the responsibility of configuring firewalls for a departmental network, I discovered that a local firewall security policy had not been written. This paper details the process I used to draft a perimeter device security policy for these firewalls. The firewall policy at the end of this document completes the policy draft process. The information gathered to draft a local firewall policy also lead to the creation of a PIX Firewall Security Services and Requirements matrix. This matrix maps HIPAA and local security requirements to the security technology solutions provided by the PIX firewall.

## Background

Without a firewall policy in place to direct the initial firewall setup and configuration, the department firewalls had been installed without access control lists. (ACL's) Documentation outlining the security rationale for purchasing the firewalls could not be found. To move forward, the following questions had to be addressed:

- Why were the firewalls purchased and what functional security roles were the firewalls expected to perform?
- What kind of a security policy should be written to ensure that the firewalls are configured and managed by a written policy?

To answer these questions, a situational analysis was conducted. This analysis process was performed with several objectives in mind:

- Ensure that the firewall purchase decision is validated and sanctioned.
- Determine the optimal firewall configuration and feature set utilization based on a formal review of the firewall topology and feature set.
- Perform an initial traffic study to assist in rule set or access control list creation
- Develop departmental consensus on the role the firewalls would play in departmental security.

Using the information gathered from this situational review, a local firewall policy was written.

## Situational Analysis

### Examining the Firewall Purchase Decision

To determine why the firewalls were purchased, an informal survey was sent to departmental managers identified as stakeholders and potential security committee


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

members. Utilizing the Information Technology Security Evaluation Criteria published by The National Institute of Standards and Technology, survey questions were developed to query departmental stakeholders about the purchase of the firewalls and their functional role in protecting the department's internal network. With a pressing need to complete the firewall installation and configure the firewalls based on a written policy, this survey:

- Reinforced management support for the firewall purchase and further defined the role that the firewalls will play in providing departmental security
- Raised awareness about which security threats the firewalls would address and which security threats the firewall singularly cannot protect against

**Survey Findings**

Ten (10) departmental stakeholders completed the survey. Security issues with the highest composite tallies are listed below.

Question: Please rank the security threat or risk posed by:

| Respondent Totals | Security Issue |
|---|---|
| 10 | Internet access to System Resources |
| 10 | Remote Access to System Resources |
| 10 | Data Exchange - securing all communications pathways to and from system Resources |
| 7 | Minimal or weak network data accountability mechanisms that link all network activity to a user identity |
| 6 | Minimal or weak Access Control (User identification and Authentication) to System Resources (preventing non authorized users from accessing materials that they are not permitted to see) |
| 5 | Weak or Minimal audit trails - the inability to determine when and where a possible security breach has occurred |
| 4 | Email attachments to and from System Resources |
| 4 | Web Surfing and downloads to/from Resources |
| 3 | Object Reuse -the ability to secure access to any system resource that is accessed by multiple users |

Question: Which of these security threats or concerns will the firewall(s) mitigate?

| Respondent Totals | Security Issue |
|---|---|
| 15 | HIPAA requirements and concerns |
| 10 | Internet access to System Resources |
| 10 | Remote Access to System Resources |
| 8 | Data Exchange - securing all communications pathways to and from system Resources |
| 7 | Minimal or weak network data accountability mechanisms that link all network activity to a user identity |


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

| Respondent Totals | Security Issue |
|---|---|
| 6 | Minimal or weak Access Control (User identification and Authentication) to System Resources (preventing non authorized users from accessing materials that they are not permitted to see) |
| 5 | Weak or Minimal audit trails - the inability to determine when and where a possible security breach has occurred |
| 4 | Email attachments to and from System Resources |
| 4 | Web Surfing and downloads to/from Resources |

**Survey Conclusions**

Departmental security stakeholders had a general picture about what security threats the departmental network faced, but lacked implementation details and specifics about the role the firewall would play in addressing security threats. Further discussions with the stakeholders revealed that the department looked to the campus IT group to address most of their security concerns. However, the same stakeholders felt the need to institute a layered security approach that addressed Health Information Portability and Accounting Act (HIPAA) concerns. HIPAA is clearly the business case priority that the firewalls were purchased to address.

**Firewalls and The Health Information Portability and Accounting Act (HIPAA)**

HIPAA does not state or require specific security technology solutions. The key is to choose new or existing technology solutions that will establish and maintain the security of information that HIPAA was created to protect. The purchase of the firewalls is an important first step in addressing technical security mechanisms requirements listed under Title II Administrative Simplification of HIPAA. This portion of the HIPAA regulations is organized under the broad HIPAA subject area of Security and Privacy. (See URL: http://www.ready4hipaa.com/tools/HIPAAQuickReferenceCard.pdf for a quick overview). Under the security subject area, it is the Technical Security Services and Technical Security Mechanism provisions that speak to the use of access controls, authorization, and data authentication for ensuring patient privacy and medical information security on our departmental network. Further, HIPAA requires that Patient Health Information, or PHI, be kept private and secure. The firewall features that establish and maintain the privacy and security of PHI information should be identified and implemented as soon as possible. The firewall's ability to perform extensive logging will develop an audit trail to document the flow of PHI through the department's network. This audit capability will help address HIPAA administrative procedures concerned with record keeping and auditing capabilities. The HIPAA Security Subject area also addresses the use of physical safeguards, such as physical access controls, media controls, and security awareness training.

**Firewall Topology Review**

A formal review of the firewall topology and feature set is required to verify that, at a minimum, the firewall hardware was installed correctly and in a secure location. The


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

topology must allow the firewalls to function as a perimeter security device, effectively positioned to control access to the internal network. The topology review involved a look at firewall physical security, firewall hardware configuration, and an analysis of the firewall's network connectivity.

**Firewall Physical Security**

As previously mentioned, The HIPAA Security subject area describes the use of physical safeguards, such as physical access controls, and media controls, and security awareness training. The firewalls were installed in an access-controlled area that requires card key access for entry. Further, the firewall's console has been configured with a privileged password to restrict access to the firewall through the console port. While this is not optimal, it does provide enough initial physical security to proceed with developing a firewall policy that will put additional administrative access controls in place.

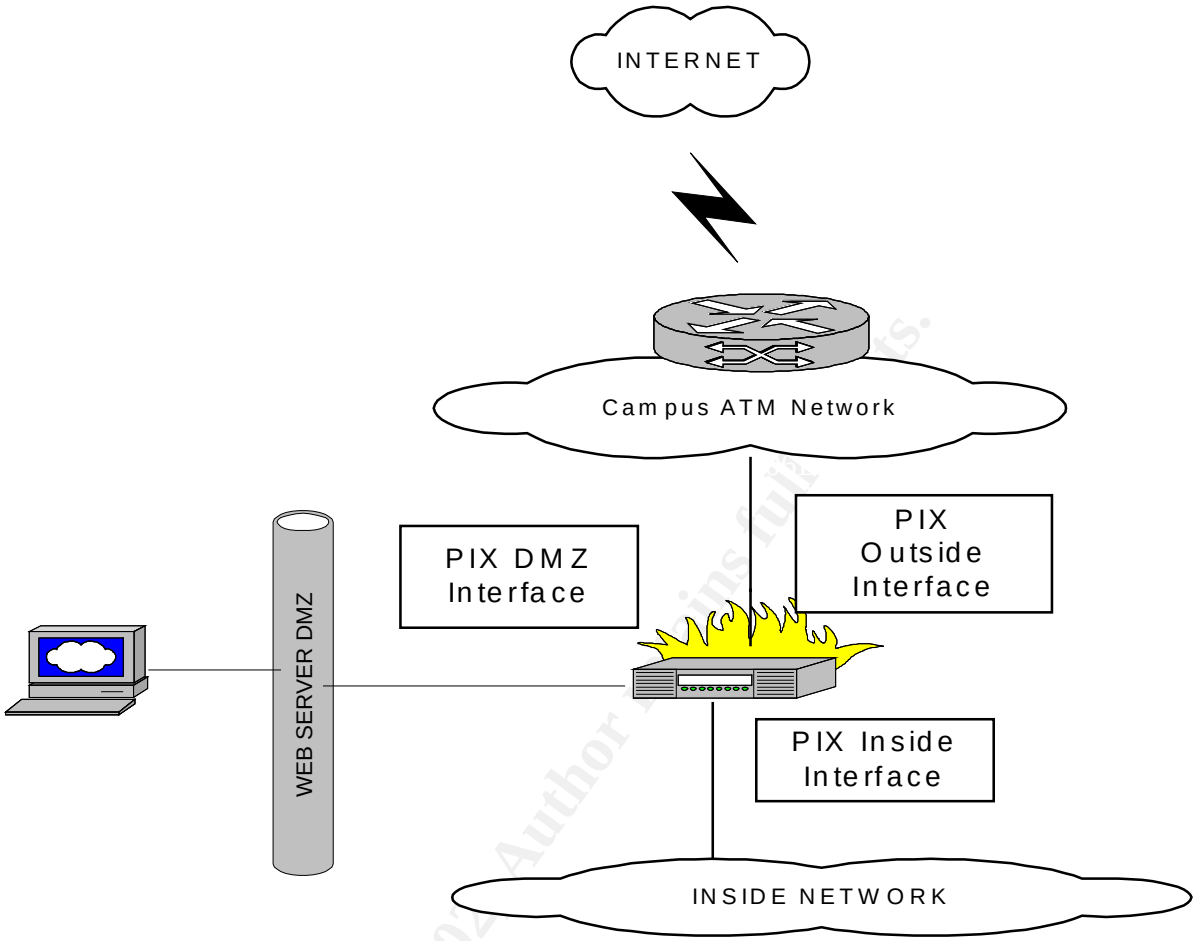
**PIX Firewall Hardware Configuration**

With 256 megabytes of ram and a Pentium III 600 MHZ processor, the PIX hardware is robust enough to implement access control and support IPSEC VPN connectivity without performance throughput degradation. In addition, the PIX firewall was installed with a redundant unit to provide a fail over capability. Once configured, the PIX firewall will have an active fail over capability allowing the fail over to occur without human intervention. This architecture removes the firewall as a single point of failure, enhancing the reliability of the department network.

**PIX Network Topology**

The firewall physical topology review verified that the physical installation of the firewall(s) would permit the establishment an effective security perimeter for the department's network. The drawing below shows a summary view of the network topology.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.




This drawing illustrates that a Cisco Private Internet Exchange (PIX) firewall has been successfully installed as a perimeter device, and the firewall is properly positioned at a choke point. A single Gigabit Ethernet connection from the firewall outside interface connects the department to the campus backbone and provides Internet access. The firewall also segments the inside network from the web server HTTP traffic, because the web server has been correctly housed in a separate demilitarized zone. (DMZ).
No other physical access points are provisioned for these core network segments. This configuration will allow the firewall to act as the primary access control point for network traffic to and from the internal network.

Another key finding: None of the core internal departmental network devices are running any routing protocols, such as Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP) to broadcast network information to external networks. Whether by accident or design, the use of static routing in this configuration enhances the security or the internal network. The use of static routes limits the amount of information advertised to backbone switches and routers about the department's internal network. With only a single link to the backbone, the campus network personnel better trained to manage the network infrastructure absorb the administrative downside of using static routes.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

**PIX Firewall Feature Set Review**

Once the firewall topology review was complete, an examination of the PIX firewall feature set was completed. Taken together, this information lead to the creation of PIX Firewall Security Services and Requirements matrix in Appendix B. This matrix is a pivotal outcome of this situational analysis; the matrix effectively maps HIPAA and departmental security requirements to the security technology solutions provided by the PIX firewall.

**Initial Traffic Study**

A combination of administrative and diagnostic techniques was used to develop an initial traffic map. These techniques included:

- A protocol analyzer monitoring traffic from a mirrored or spanned switch port. Cisco Catalyst switches permit traffic to be monitored from another port with out service interruption. Data flows where monitored on a per VLAN (Virtual LANs) basis.
- Static route statements and host file entries found in mission critical hosts. This information provided insight about production related data flows and network connectivity requirements.
- Interviews with system administrators to determine what database and interface engines processes were being used.
- Information from the monitoring tools used by system administrators in the department. Such tools included Sitescope, Ciscoworks, What's Up Gold, among others.

Each tool provided clues about the traffic flows the department used to do its work. Taken as a whole, this information was incorporated into a network data flow map upon which firewall rule sets can be created. Some of the services discovered in the traffic flow for the department network were:

- HTTP (Web surfing)
- HTTPS (secure HTTP)
- FTP (file transfers)
- SMTP (e-mail)
- ICMP (reporting services; ping)
- Telnet (bi-directional communication sessions)
- X Windows

Network traffic flows are controlled by firewall rule sets, also known as access control lists (ACL's). If properly configured, the rule sets or ACL's will specify what services will pass through your firewall, and which services are kept out. These ACL's also define the parameters against which each connection is compared, resulting in a decision (permit or deny) to take for each connection.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Ultimately, the department must determine what traffic it will permit or trust, and what traffic it will deny or not trust. The department is not on the perimeter of the campus network, so an appropriate trust model that fits legitimate network traffic flow must be devised. Examples of trust models are:

- Trust everyone all of the time. Without a security policy and firewall rule sets in place, this is the default trust policy in effect at this time.
- Trust no one at any time. This position affords the most secure posture, but the department lacks the manpower or resources to implement or enforce this as a trust policy.
- Trust some people some of the time. This trust posture realistically supports the department's operational environment. Access is granted or revoked as needed. This security posture fits the profile of the PIX firewall. As a basic principle of operation, the PIX firewall denies all inbound traffic unless explicitly permitted, while permitting inside traffic out.

By adapting a trust policy of trusting some of the people some of the time, the department will be able to focus on closing the "front door", -traffic entering and leaving the firewall's external interface. This trust model stratagem will also allow firewall configuration work to begin as a security consensus on implementing internal security controls is being forged.

**Firewall Role Limitations and Firewall Policy Creation**

The positioning of our firewalls allows the department to exercise access control between internal and external networks. A closer look at this architecture shows that the department firewall cannot protect data from internal compromise. While the departmental stakeholders are rightfully concerned about data leaking out of its network from an external source, the fact remains that data could just as easily be moved out of the network in more mundane ways. Someone could copy data to a floppy or remove a magnetic tape. Data could be transferred via modem lines.

In short, the firewall cannot protect against internal information flows that do not pass through the firewall, nor can firewalls always detect or protect against hacks using application ports to tunnel into a network and/or use Trojan house techniques via unsecured network hosts or clients.

**Developing a Consensus and Organizing Support for a Local Firewall Policy**

Proper dissemination of the survey and matrix results demanded a unique forum where the firewall(s) would be the sole focus of discussion. A debut departmental security meeting was held. At the conclusion of this meeting, the following consensus points were reached:


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- The PIX firewalls were sanctioned as a departmental security asset. As the department's primary perimeter device, it will enforce access to and from our department network.
- The firewalls cannot be viewed or relied upon as the sole provider of departmental security, as there are many internal security issues that the firewalls cannot address.
- A departmental firewall policy will be drafted as the first step to completing a departmental security policy. The departmental policy must be subordinate to any existing enterprise wide security policies, regulations, and guidelines.
- Prioritize the use of the firewall's feature set to address HIPAA requirements first. Devise firewall rule sets to implement departmental security measures. Implement these security measures once the departmental security committee has approved them.
- Given that data flows have not been documented, the firewall will permit all outbound traffic, allowing the rule set creation to focus on determining what information flows from the outside interface should be allowed in and what should be blocked.

To address these internal security vulnerabilities, the department will need to draft a local departmental security policy. The firewall policy, as an issue specific policy will be an important component or module within the department's local security policy. In turn, the department's local security policy must be written in a way that augments and supports higher-level division or campus security policies, rules, regulations and federal law.

**Firewall Policy Definition –What kind of firewall Policy should be created?**

Out of the situational review findings, key facts emerged to shape the firewall policy draft:

- The firewall is a perimeter device between the department and the campus backbone.
- The department manages the firewall so the firewall policy will be written as a local, issue specific security policy.
- A department security policy must be written.
- The firewall policy should be considered as just one module or component of an overall departmental security policy
- The firewall policy, as a part of the department security policy, must be written as an extension of any existing local, state, federal laws and campus directives.

**Situational Analysis Summary**

The situational analysis performed the information gathering and analysis needed to begin a security policy draft. Out of this review, it is clear that a local issue specific security policy must be written in order to provide order and guidance to the firewall rule set creation process. With a perimeter security policy in place, the firewall's role as the technical implementer of the department's perimeter security policy will be firmly entrenched and effective access control policy can be deployed.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Conclusion

This paper outlines the systematic approach taken to draft an issue specific, local firewall policy. A copy of the firewall policy draft submitted to the security committee was included in the appendix of this document. This local firewall policy, also known as a perimeter security device policy, was written in a modular fashion to allow it to be incorporated into the department's overall security policy draft. In fact, the groundwork done for the firewall policy created the momentum needed to move the department to draft a comprehensive local departmental security policy

Ultimately, a security policy reflects the department's consensus or voice on how security concerns and issues will be addressed. In this sense, a security policy is not an edict that prevents people from doing their work. Making this point clear helps to remove fears that a security policy will be very difficult to follow and even harder to implement.

© SANS Institute 2002, Author retains full rights.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## References


NCHICA Data Security Work Group. "Policy Matrix for HIPAA Draft Security Regulations." November 2001. URL: http://www.nchica.org/HIPAA/Samples/matrix.pdf (28 February 2002)

Fraserm B. "RFC Site Security Handbook" Request for Comments: 2196. September 1997. URL: http://www.ietf.org/rfc/rfc2196.txt (18 December 2001)

Wenstrom, Micheal. Managing Cisco Network Security. Indianapolis: Cisco Press. 2001. 228-230.

Geul, Michele. "A Short Primer for Developing Security Policies- The SANS Policy Primer." 2001. URL: http://www.sans.org/newlook/resources/policies/Policy_Primer.pdf (6 February 2002)

"Data Sheet Cisco PIX 525 Firewall." 27 February 2002.
URL: http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/prodlit/pix2_ds.htm
(1 March 2002)

"Common sense HIPAA advice for the IT professional" 2001.
URL: http://www.ready4hipaa.com/concern.cfm (15 January 2002)

CERT Coordination Center. "Configure firewall logging and alert mechanisms. A practice from the CERT® Security Improvement Modules" May 1 2001.
URL: http://www.cert.org/security-improvement/practices/p059.html (March 1 2002)

NIST. "Information Technology Security Evaluation Criteria (ITSEC)" London, June 1991. http://csrc.nist.gov/publications/secpubs/itsec.txt (14 February 2002)



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Appendix A

# Firewall Policy Draft

### Firewall Policy Scope and Compliance Requirements

The department's security policy *is subordinate to any governing* campus or Health Insurance Portability And Accountability Act Of 1996 (HIPPA) regulations relevant to the security policy issues or concerns in this document. These guidelines are intended to supplement, not replace all existing laws, regulations, agreements, and contracts that currently apply to departmental computing and networking services. In accordance with HIPPA and NIH security guidelines, this policy will not address specific technical and security implementation methodologies, unless otherwise noted in the security policy subject areas included in this document. Persons given access to the department's technology and information assets must sign a statement that they have read, understood, and agree to abide by this policy.

### Firewall Policy Enforcement

Security policy enforcement will emphasize the use of security technology mechanisms to mitigate security risks wherever possible. When actual prevention is not enforceable with security tools, sanctions will be used.

### Minimum Firewall Platform and Feature-set Implementation Requirements

- Meet ICSA firewall and IPSEC certification 1.0a or later
- Meet Common Criteria Firewall and IPSEC Certification EAL4 or higher
- Utilize a Hardened kernel - rewritten specifically to be secure and not running SMTPd, FTPd, telnetd, or any other vulnerable daemons or services
- Perform Packet Filtering (IPFW) and State full Packet Inspection
- Ability to use RFC 1918 non-publicly routed addresses for servers
- Security script identifies any services/ports being probed
- Default deny device - tight control of traffic allowed to pass through
- Protects itself and servers from ICMP attack (thwarts ping attacks)
- Can reap idle connections (thwarts Denial of Service attacks)
- Can perform source route tracing (thwarts IP spoofing)
- Perform Unacknowledged SYN without ACK buffers (thwarts SYN floods)
- Thwarts teardrop and land attacks
- Map well-known ports to any ports (Port mapping)
- Perform Network Address Translation (NAT)


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

**Terms and Definitions**

The following terms are used throughout this document:

| | |
|---|---|
| Authorized Users | Department users with a valid, pre-authorized account, or approved system access. Department users consent to use only those departmental computer resources that they are specifically authorized for. |
| Trusted Network | Internal departmental networks which are placed behind the Firewall internal interface |
| Untrusted Network(s) | Networks outside the Firewall(s) external interface |

**Perimeter Security Maintenance**

Perimeter security for this department will be maintained by a PIX firewall. This firewall has a redundant fail over unit to provide service continuity should the primary firewall unit fail. The PIX firewall(s) will inspects packets and sessions to determine if they should be transmitted or dropped. In effect, the firewalls will act a single point of network access where traffic can be analyzed and controlled. The PIX will provide forward authentication requests to a radius server. Access to the department's internal network will be based on parameters such as (but not limited to)

- Application use.
- User authentication, authorization, and accounting, for both incoming traffic from remote users and outgoing traffic to the Internet.
- IP Address and Port.

**PIX Firewall Logon Access**

Enable or privileged logon access to the firewall will be restricted to a Primary firewall administrator and one designee. Enable password construction will be consistent with the strong password creation practices utilized in the department.

**Firewall Operational Maintenance and Responsibility**

Day-to-Day operation and maintenance will be the responsibility of the department's Network and Security Engineer. Firewall support duties for the Network and Security Engineer include:


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Act as the departmental technical lead for departmental security policy and procedure implementation, has the primary responsibility for ensuring operational continuity for the department's security policy.
- Perform firewall rule set changes, adds and deletions as approved by the departmental security committee.
- Perform firewall software maintenance and hardware upgrades to the firewall; implement feature set on PIX firewalls as approved by the security committee.
- Monitor firewall logs, and departmental intrusion detection system. Initiate the department's response to any possible security incident. Act as the departmental liaison for incident reporting to the campus network security division.
- Perform security risk management by initiating a cycle of securing, monitoring, and testing security mechanisms and procedures. Review findings will be used to update security policy, procedures, and security mechanisms on a continual basis.
- Launch bi-annual review of the departmental firewall security policy to ensure the firewall policy is current with actual firewall rule set practices.

**PIX Firewall Log Configuration and Maintenance**

The pix firewall will be configured to use system logging (syslog) to export its log messages to the System Log Server (syslog) server(s). The PIX firewall's logs will be base lined thirty (30) days to determine how best to fine-tune message traffic information. At a minimum, the firewall log will be configured to detect:

- Emergencies, such as system unusable messages
- Alerts, critical conditions, and Error message
- VPN sessions,
- Failed/unsuccessful login attempts
- Logon Access and configuration attempts made to the firewall

The PIX firewall logs will be backed up daily and archived on a weekly basis, in accordance with current practices implemented on the syslog server. In addition, the firewall will be configured to send Simple Network Management Protocol (SNMP) Traps to the network management server. Construction of SNMP access lists and community strings will be consistent with established security practices.

**PIX Firewall Networking Role**

The department's Firewall(s) will not act perform routing, or act as a router for Internet services. PIX firewall routing protocol support (such as Routing information Protocol-RIP) shall be disabled and static IP mappings shall be configured. The firewall will forward all packets intended for the Internet to the campus backbone. Firewall rules to prevent IP spoofing will be supplemented by similar rules on XXX perimeter firewalls/routers and department core switches, in order to reject packets containing the source route option.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

**PIX Firewall(s) Security Services**

At a minimum, the departmental firewall(s) will perform the following security services:

- Access control between the internal network and un-trusted networks.
- Block unwanted traffic, as determined by firewall rule sets designed to implement the department's Security Policy while providing security that does not place an undue burden on authorized users.
- Hide system names, network topology, network device types, and internal user ID's from the Internet.
- Provide more robust authentication (RADIUS/TACACS+) than standard applications.
- IPSEC VPN Connectivity.
- Log interesting traffic to and from the department's internal network.

**Firewall Rule Set Management and Change Control Process**

The departmental security committee must approve all rule set (ACL's) changes.
The departmental security committee must approve all IOS changes and upgrades. At a minimum, the following information will be included in any firewall change request.

- Requesters Name and POC information
- Requested Due Date (when change will be applied)
- Change impact statement. Include any supporting documentation necessary to determine why the change is necessary. The change request will be delayed until change requirement has been established and approved.
- Rule Change Notification requirements (who need to be alerted about the change because of potential operational impact).
- Change Priority Level
  1 –emergency change needs to go in ASAP because of possible security breach
  2- Change will be applied as scheduled, upon security committee approval

Firewall rule sets (ACL's) will work to achieve a "best practices" approach in an effort to balance security risk and operational access requirements. Recommended practices include:

- Anything from inside the network is allowed out.
- All access to the firewall itself is blocked from the Internet.
- Restricted internal access to the firewall. Firewall administrators must be validated by two-factor authentication, such as SECURID.
- Allow SMTP e-mail support.
- ICMP services turned off
- Block FTP and Telnet access to all internal servers from the Internet.
- Remote access services for authorized users via VPN and/or campus approved secure authentication system.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

**PIX Virtual Private Networks (VPN) Policy**

Virtual Private Networks allow a trusted network to communicate with another trusted network over untrusted networks such as the Internet. The firewall will provide IPSEC VPN capability. Any authorized VPN connections between firewalls and/or VPN clients over public networks shall use encrypted VPN tunnels to ensure the privacy and integrity of the data passing over the public network. Authorized VPN connections shall use 3DES encryption, unless the security committee approves an exception.

The Security Committee must approve all VPN connections. The Network Security Engineer will implement Van's using the VPN feature set on the department's PIX firewall. The Network Security Engineer, upon approval by the Security Committee distributes VPN encryption keys.

**Virtual Private Networks (VPN) Session Length Timeouts**

VPN sessions will have an absolute session timeout length set at 3 hours. An inactivity timeout will be set for 30 minutes. At the end of these timeout periods, users will be required to re-authenticate to continue or reestablish their VPN connection.

**Network Connection Policy**

The Security Committee must approve all connections from the department network to any external networks. Only network connections that have been found to have acceptable security controls and procedures will be allowed to connect to the departmental network. Every attempt will be made to ensure that all external connections will pass through firewalls that meet the guidelines established by this policy.

All connections and accounts related to external network connections shall be validated on an annual basis. When a network connection is no longer needed all accounts and system processes related to the connection should be deleted within one workweek.

**Trusted Networks Policy**

Network Trust Relationships Overview

Approved and authorized network connections are considered trusted networks. Trusted networks share the similar security policy or implement security controls and procedures. Un-trusted networks do not implement common security controls, or where the level of security is unknown or unpredictable. Network segments external to the department are under the control of different organizational entities, and will be considered as unknown and possibly compromised


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

The following networks are considered trusted networks and permitted **controlled access** by the department firewall(s). These networks are provided data services by the department's network:

The xxx **Backbone Network** (xxx.xxx.xxx)
This network contains the XXX firewall that separates XXX from the Internet and also interconnects all of the Institute networks together through xxx switches and routers Medical researchers from multiple locations traverse the backbone to retrieve patient data. This data is captured via xxx running on Windows and Unix hosts.

The xxxxx **LAN** (xxx.xxx.xxx.)
This network hosts the xxx, xxx and xxx. The xxx network also provides remote access connectivity via the xxx network. The xxx network interconnects doctors, transcriptionists, and other authorized users using analog, cable modems, and DSL media.

**Non-trusted Networks Policy**

All networks not specifically listed as a trusted network are non-trusted networks. Access to the department's network will be denied by the firewall(s). If complete access control cannot be managed by the firewall(s), other security technologies will be used in tandem to the department's firewalls to mitigate the security threat. Modem connections with business partners and/or remote sites are also considered untrusted networks connections.

The Network and Security Engineer may terminate unauthorized connections to departmental network without notice. An active network port or connection does not imply authorization for connectivity. To support this policy, unused and/or unknown network connections (switch ports, analog lines, etc) will be disabled until they are properly identified, documented, and placed in or out of service.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Appendix B
## Firewall Security Feature Set and Requirements Summary Matrix[1]

(Note: N/A* indicates that the PIX technology feature is not a specified HIPAA technology requirement)

| Firewall Feature Set | Addresses HIPAA Requirements? | Addresses Department Security Concerns? | Feature Set Implemented with Initial rule set? | Comments |
|---|---|---|---|---|
| IPSEC support for 168-bit Triple DES algorithms. | Yes | Yes | Yes | Support for VPN IPSEC to web server and internal network<br>Secures Internet access to System Resources<br>Secures Remote Access to System Resources |
| Provide perimeter security by maintaining state full control of all connections | Yes | Yes | Yes | Pix tracks the source and destination address, Transmission Control Protocol (TCP) sequence numbers, port numbers, and additional TCP flags of each packet<br>Addresses Data Exchange - securing all communications pathways to and from System Resources<br>Addresses Weak or Minimal audit trails - the inability to determine when and where a possible security breach has occurred |
| Access is permitted through the Cisco PIX Firewall only if an authorized connection exists | Yes | Yes | Yes | Addresses HIPAA and Departmental access control requirements. Provides transparent access for internal and authorized external users, while protecting internal networks from unauthorized access |
| Real-Time, Embedded System | No | Yes | Yes | Eliminates the risks associated with a general-purpose operating system firewall |
| URL Filtering | No | Yes | No | Campus IT group manages web site access, will enable feature if this becomes a departmental responsibility |
| Cut-Through Proxy | N/A* | Yes | Yes | Improve RADIUS authentication performance |
| Network Address Translation (NAT) | N/A* | Yes | Yes | Addresses network security; obscures IP addresses from the outside world |
| State full Fail over/Hot Standby | No | Yes | Yes | Provides high availability and firewall redundancy |
| Unacknowledged SYN without ACK buffers (thwarts SYN floods) | N/A* | Yes | Yes | DOS Attack Prevention Protects the firewall and the servers/clients behind it from hacks |


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

| Firewall Feature Set | Addresses HIPAA Requirements? | Addresses Department Security Concerns? | Feature Set Implemented with Initial rule set? | Comments |
|---|---|---|---|---|
| TACACS+ and RADIUS Support | Yes | Yes | Yes | Radius Authentication is being used to validate user access to the web server. |
| Thwarts teardrop and land attacks, perform source route tracing | N/A* | Yes | Yes | DOS Attack Prevention Protects the firewall and the servers/clients behind it from hacks |
| Security script identifies any services/ports being probed | Yes | Yes | Yes | Important Intrusion Detection and Audit trail capability |
| Default deny device - tight control of traffic allowed to pass through | Yes | Yes | Yes | Implicit Denial of traffic, unless explicitly permitted |
| Protects itself and servers from ICMP attack (thwarts ping attacks) | N/A* | Yes | Yes | DOS Attack Prevention Protects the firewall and the servers/clients behind it from hacks |
| Reap idle connections (thwarts Denial of Service attacks) | N/A* | Yes | Yes | DOS Attack Prevention Protects the firewall and the servers/clients behind it from hacks |
| Perform source route tracing (thwarts IP spoofing) | N/A* | Yes | Yes | DOS Attack Prevention, Protects the firewall and the servers/clients behind it from hacks |

[1]Pix feature set information source: "Data Sheet Cisco PIX 525 Firewall." 27 February 2002.

**PIX Firewall Logging Facilities**

In addition to providing status information about the operational status of the firewall, logging options can be configured to control the amount of detailed information presented for viewing or archiving for later analysis. PIX logs also allow you to examine how well your packet filters and access rule sets (ACL's) are controlling inbound an outbound network access. These same logs can be used to monitor attempts to hack into your firewall and network, -intrusion detection events.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Malaysia @ MCMC 2013 | Cyberjaya, MY | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| SANS Pen Test Berlin 2013 | Berlin, DE | Jun 03, 2013 - Jun 08, 2013 | Live Event |
| Industial Control Systems Security Training - Houston | Houston, TXUS | Jun 10, 2013 - Jun 15, 2013 | Live Event |
| Security Impact of IPv6 Summit 2013 | Washington, DCUS | Jun 14, 2013 - Jun 16, 2013 | Live Event |
| SANSFIRE 2013 | Washington, DCUS | Jun 14, 2013 - Jun 22, 2013 | Live Event |
| SANS Canberra 2013 | Canberra, AU | Jul 01, 2013 - Jul 13, 2013 | Live Event |
| Digital Forensics & Incident Response Summit 2013 | Austin, TXUS | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS London Summer 2013 | London, GB | Jul 09, 2013 - Jul 16, 2013 | Live Event |
| SANS Rocky Mountain 2013 | Denver, COUS | Jul 14, 2013 - Jul 20, 2013 | Live Event |
| SANS Mumbai 2013 | Mumbai, IN | Jul 22, 2013 - Jul 27, 2013 | Live Event |
| SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification | Washington, DCUS | Jul 22, 2013 - Jul 26, 2013 | Live Event |
| SANS San Francisco 2013 | San Francisco, CAUS | Jul 29, 2013 - Aug 03, 2013 | Live Event |
| SANS SEC 560: Network Penetration Testing @ Bangalore 2013 | Bangalore, IN | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| SANS Boston 2013 | Boston, MAUS | Aug 05, 2013 - Aug 10, 2013 | Live Event |
| Critical Security Controls Summit | Washington, DCUS | Aug 12, 2013 - Aug 18, 2013 | Live Event |
| Industrial Control Systems Security Training - DC | Washington, DCUS | Aug 12, 2013 - Aug 16, 2013 | Live Event |
| SANS Thailand 2013 | Bangkok, TH | Aug 19, 2013 - Aug 31, 2013 | Live Event |
| SANS Virginia Beach 2013 | Virginia Beach, VAUS | Aug 19, 2013 - Aug 30, 2013 | Live Event |
| Mobile Device Security Summit 2013 | OnlineCAUS | May 30, 2013 - Jun 06, 2013 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |