[redacted]

[redacted] Network Architecture & Security: DMZ, Firewalls, and Intrusion Detection

Version <3.5>

Issued by:

[redacted]	NUMBER [redacted]
TITLE: [redacted] NETWORK ARCHITECTURE & SECURITY: DMZ, FIREWALLS, AND INTRUSION DETECTION	Page 1 of 20
SUBJECT: High-level discussion of the network architecture and security that includes DMZ, firewalls, and intrusion detection.	EFFECTIVE August 5, 2005
ISSUING AUTHORITY: [redacted] Chief, Network Operations Division	SUPERSEDES None

Revision History

Date	Version	Description	Author
March 2005	0.1	First Draft	[redacted] and Melodie Hawkins
June 2005	0.9	Revised to reflect current architecture	[redacted] & Melodie Hawkins
August 2005	1.0	Added procedure number block and issued FINAL	Melodie Hawkins
August 2006	2.0	Updated	[redacted] elodie Hawkins
September 2006	2.0	Final Issued	Melodie Hawkins
February 2008	2.0	Issuing Authority changed from Jacki Burns to Stephanne Petree	Melodie Hawkins
April 2008	2.0	Procedure number mis-numbered	Melodie Hawkins
February 2009	2.0	Updated header/footer formats and added Acronym list	Melodie Hawkins
December 2009	3.0	Updated to using Verizon cloud	[redacted]e Melodie Hawkins
May 2010	3.5	Updated to include T3 between ARL & LAK (lifted sections of the Contingency Plan as needed)	Melodie Hawkins
November 2010	3.5	Updated footer	Melodie Hawkins

Table of Contents

1. Introduction

This procedure contains [redacted] official technical standards for building, re-building, and configuring the WAN (*Wide Area Network*) and LANs (*Local Area Networks*) for MSHA. Because network security is an integral part of the architecture itself, we discuss it here in that context as the DMZ (*Demilitarized Zone*), firewalls, and intrusion detection. MSHA just migrated its WAN service and management to Sprint so the Agency now only manages the internal routers and LANs.

1.1 Scope

[redacted] WAN and LAN engineers that must build or maintain the [redacted] WAN and LAN network shall adhere to the scope and practice of these procedures.

1.2 Audience

The intended audience for these procedures is all [redacted] WAN and LAN engineers and network administrators in all locations.

Note:
If you need more detail than what is provided here, please contact the **WAN engineers, the [redacted] Information Security Office, or the Chief of System Operations & Communications Division**. More detail is available; however, because of its sensitive nature access is extremely limited.

2. Architecture

[redacted] WAN consists of approximately 100 remote sites physically located all over the continental US. Of those 102 remote sites, most of the Field offices are in relatively remote locations and may have very few staff, primarily mine inspectors. Some of the larger Field offices may have a dedicated IT Specialist on staff to manage computer hardware and software issues; however, typically only the five District offices have dedicated IT staff and resources: [redacted] Of these five locations, [redacted] form the core of the WAN architecture protecting all locations behind their DMZ architectures, firewall structures, and security implementations. These two locations provide IT resources for the entire Agency.

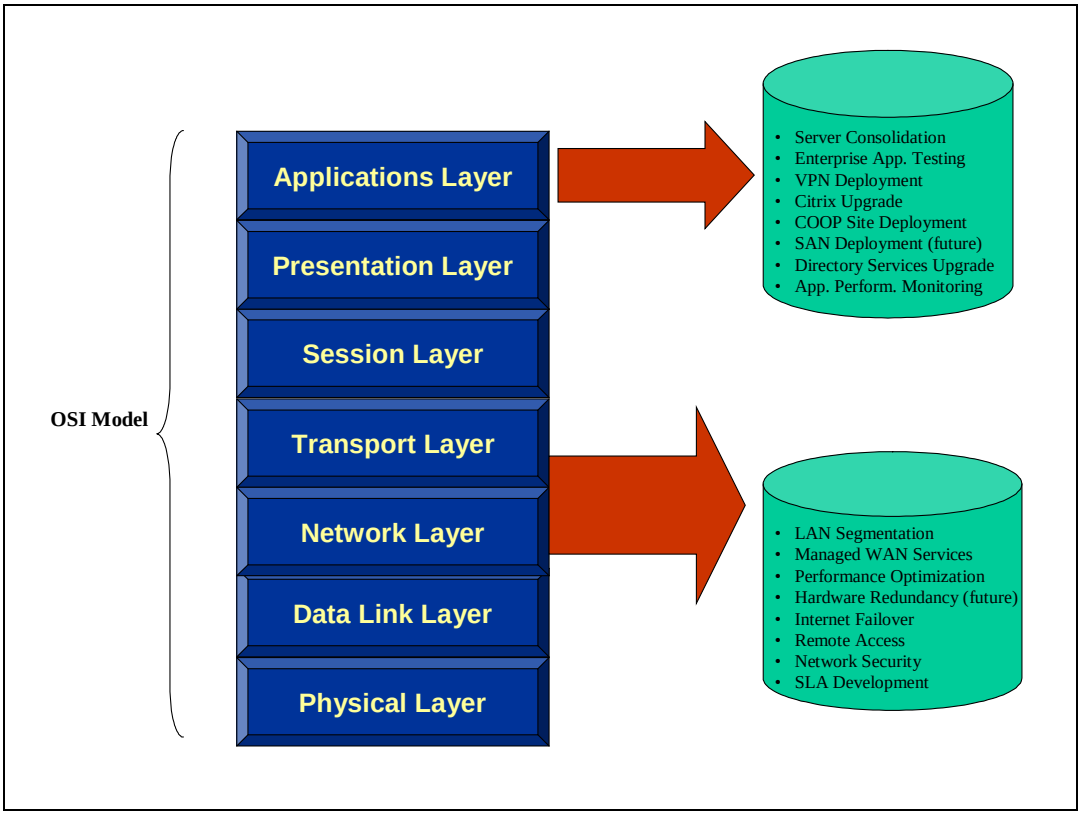
2.1 Security: Integration with Architecture

Best industry practices dictate taking security into consideration from the first designs of the architecture. All networking basics include elements of security, such as protecting the internal network from untrusted (Internet) traffic, as well as protecting the network from its own users that may unknowingly (or knowingly) compromise the network. As part of the overall security of the network, this document contains a separate section discussing *Security*, including *security zones*, the DMZs, firewalls, controlling traffic, intrusion detection, and VPN (*Virtual Private Network*) remote access, because all of these security areas are considered during WAN and LAN design.

2.2 Overview

The network architecture addresses [redacted] primary business and technical requirements and ensures that [redacted] LAN and WAN networks are fully able to support its mission-critical business processes, enterprise applications, local applications, and end-user workstations. The architecture is based on industry standards and best practices for LAN / WANs and security. Its modular design enables

supporting future business and technical requirements. The figure below illustrates the key components the architecture addresses at various layers of the OSI (*Open System Interconnection*) model.



MSHA uses several protocols to communicate over its WAN/LAN, however, TCP/IP is the predominant protocol; most [redacted] enterprise applications use TCP/IP for end-to-end communications. [redacted] uses EIGRP (*Enhanced Interior Gateway Routing Protocol*) as the routing protocol over both its LAN and WAN. EIGRP is a Cisco proprietary routing protocol that combines the advantages of both link-state and distance-vector protocols. Routes are dynamically chosen based on the optimum metric calculation between the source and the destination.

The majority of [redacted] network is configured with private network addresses that are not routable over the Internet. To circumvent this, and to add an additional level of security, [redacted] uses NAT (*Network Address Translation*) technology. NAT is a mechanism for reducing the need for globally unique IP addresses to connect to the Internet. It translates private IP addresses into globally routable addresses before sending packets over the Internet. It also provides security by shielding the internal network addresses from public communities/domains such as the Internet.

Both the D[redacted] and Atlanta COOP site are now nodes on the Verizon PIP network for accessing department enterprise applications.

Best industry practices dictate taking security into consideration from the first designs of the architecture. All networking basics include elements of security, such as protecting the internal network from untrusted (Internet) traffic, as well as protecting the network from its own users that may unknowingly (or knowingly) compromise the network. As part of the overall security of the network, this document contains a separate section discussing *Security*, including *security zones*, the DMZs, firewalls, controlling traffic, intrusion detection, and VPN (*Virtual Private Network*) remote access,

because all of these security areas are considered during WAN and LAN design.

2.3 Approach

The network architecture for [redacted] has been designed using the seven-layer OSI model. The four lowest layers (physical, data link, network, and transport) provide network-specific functions such as routing, addressing, protocol support, and flow control. The enterprise network supports several diverse user communities, including management, inspectors, auditors, educators, technical support; therefore, it is designed for robustness, reliability, and scalability.

Additionally, the architecture incorporates several layers of security to ensure confidentiality and data integrity. Redundancy is built into several areas and will continue to be built in as resources permit. TCP / IP is the primary transport-layer protocol used over the enterprise network because it provides a reliable data transportation.

In February 2005, the WAN design was migrated from a hub-and-spoke topology to a *mesh* topology, with all traffic encrypted using static and dynamic IP-Sec VPN tunnels. Now, each Field office is equipped with a full DS-1 (T-1) line to accommodate security and application patches as they are sent from Arlington and Lakewood. Arlington and Lakewood are both equipped with full DS-3 (T-3) lines. WAN management was transferred to DOLnet / Verizon in 2008/9.

The [redacted] WAN consists of roughly 100 geographically dispersed sites interconnected by a fully meshed IP MPLS backbone with IP-Sec tunnels provided by Verizon through a managed services contract provided by ESO.

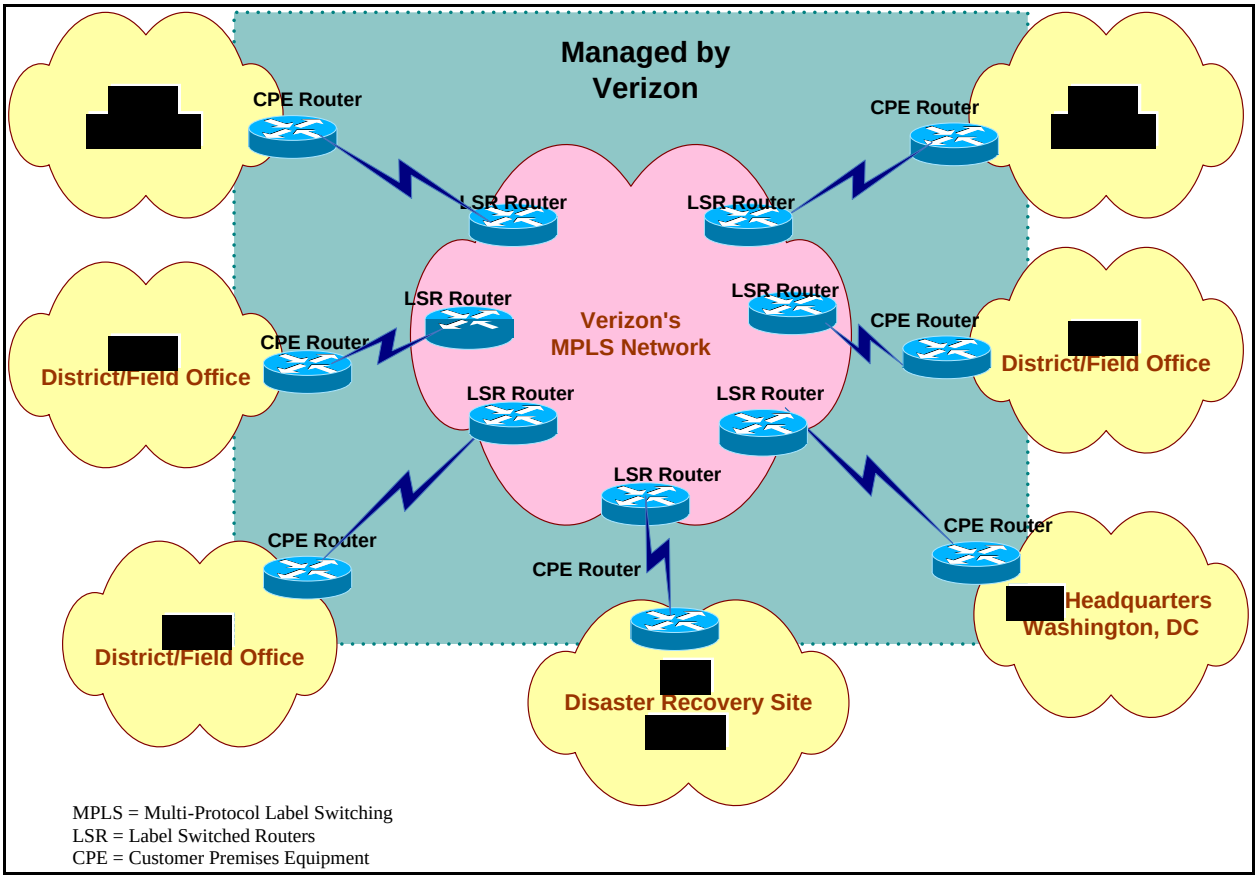
2.4.WAN: Mesh Topology

Strictly defined, a *mesh topology* is a design where there are at least two nodes (location, workstation, or other device) with two or more paths between them. A *mesh network* is a WAN (or LAN) that employs either a full- or partial-mesh topology. In the full-mesh topology, each node is connected directly to each of the other nodes. In the partial-mesh topology, some nodes are connected directly to all the others, but some are connected only to those with which they exchange the most data. MSHA has implemented a full mesh topology.

MPLS *(Multiprotocol Label Switching)* defines a mechanism for packet forwarding in network routers. It was originally developed to provide faster packet forwarding than traditional IP routing; however, its flexibility has led it to become the default way for modern networks to achieve QOS (*Quality of Service*), next generation VPN (*Virtual Private Network*) services, and optical signaling.

The mesh WAN architecture is non-hierarchical and ensures any-to-any connectivity using state-of-the-art IP / MPLS technology. MPLS is one of the central elements of next-generation networks. It provides very high-speed data forwarding and works alongside existing technologies. It provides an IP-compatible, Quality-of-Service-capable infrastructure that enables the convergence of voice, video, and data onto the same backbone network.

This design provides reliability and redundancy so that if one node cannot operate the other nodes can still communicate directly with each other or indirectly through one or more intermediate nodes. In this configuration, the network itself becomes more stable because the connections become more redundant. Therefore, if one node goes down the impact is much less, than it would have been with the old hub-and-spoke topology. Our current structure is full mesh using EIGRP (*Enhanced Interior Gateway Routing Protocol*) for the dynamic routing protocol. EIGRP uses distance and delay to calculate routes.



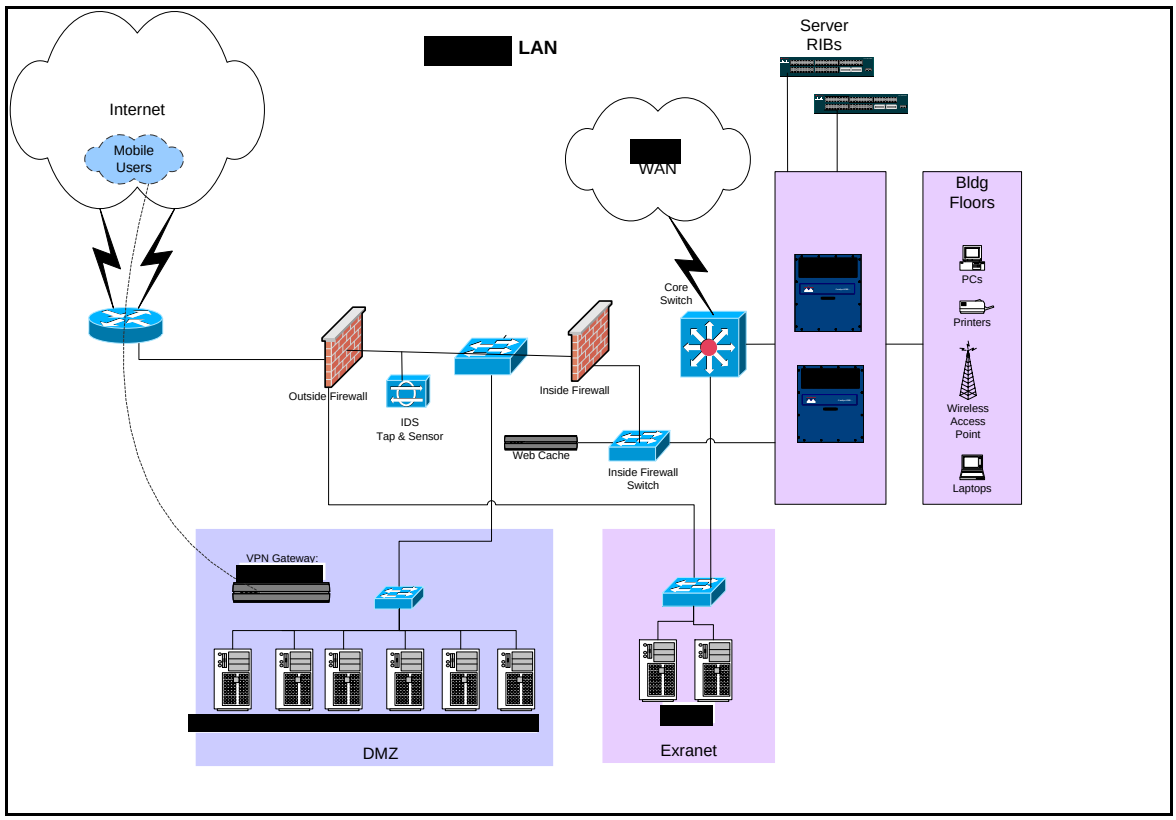
2.5. LANs

The [redacted] and [redacted] LANs are each protected by two firewalls. The LAN architecture for these two main locations is client / server. MSHA has also implemented VLANs (*Virtual LANs*) in the Beckley, WV site.

VLANs improve the performance, scalability, manageability, and security of LANs at primary sites and large district offices. They create separate logical groups that do not depend on the physical location of the hosts.

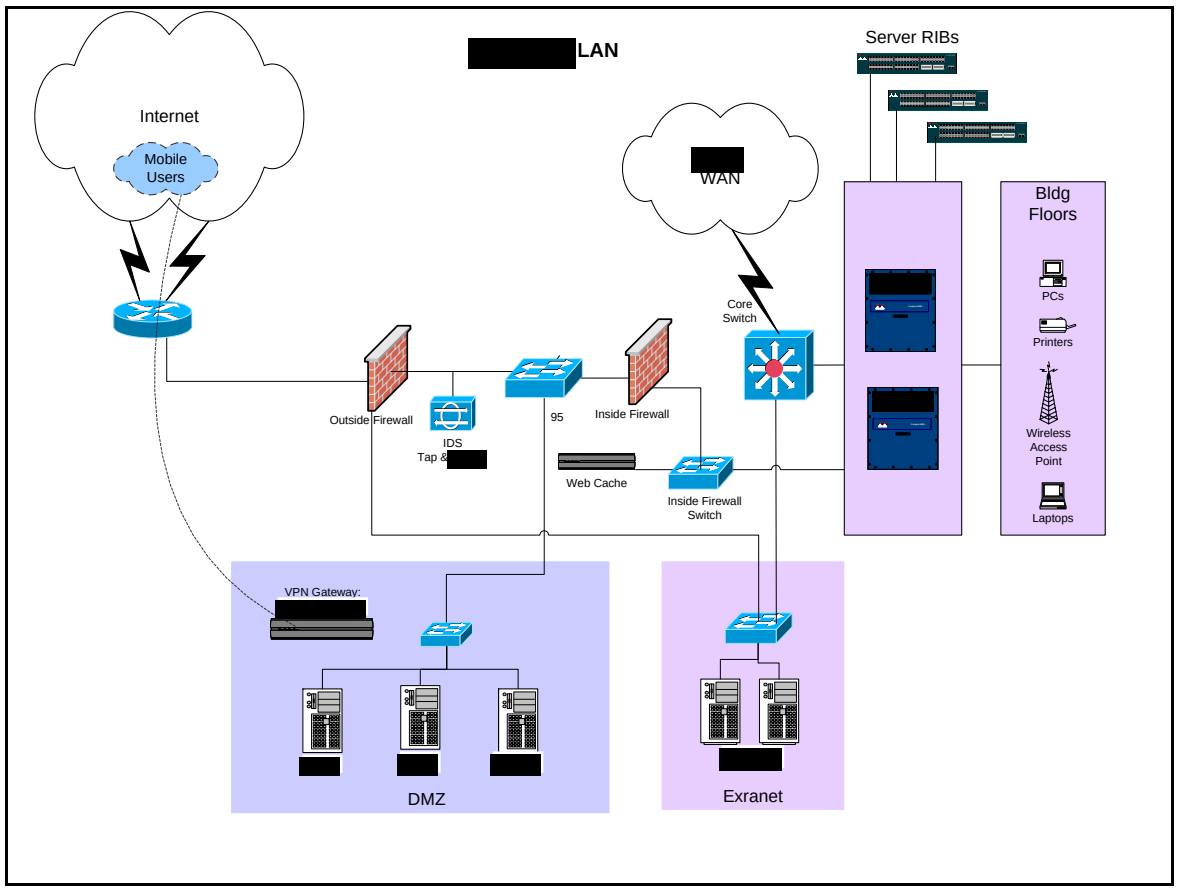
[redacted]

The diagram below shows a high-level overview of the [redacted] LAN. More detailed diagrams (that include IP addresses, cable placement, and so forth) are available if needed. If you need more detail, please contact the WAN engineers, the [redacted] Information Security Office, or the Chief of the Network Operations Division.



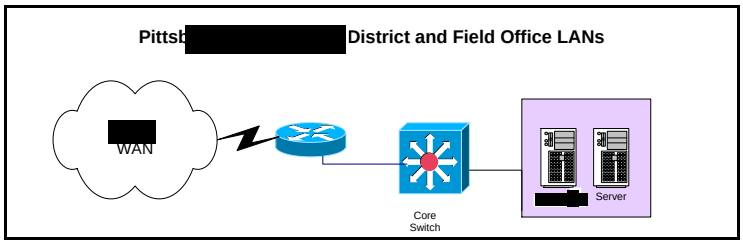
2.5.2. [redacted]

The diagram below shows a high-level overview of the [redacted] LAN. More detailed diagrams (that include IP addresses, cable placement, and so forth) are available if needed. If you need more detail, please contact the WAN engineers, the [redacted] Information Security Office, or the Chief of the Network Operations Division.



2.5.3. Bec[redacted]; District and Field Offices

The diagram below shows a high-level overview of the [redacted] District, and Field office LANs. Be aware that a VLAN for [redacted] is currently in the design and early test stages. More detailed diagrams (that include IP addresses, cable placement, and so forth) are available if needed. If you need more detail, please contact the WAN engineers, the [redacted] Information Security Office, or the Chief of network Operations Division.



3. Security

Security concerns are integral to the architecture of the network. [redacted] architecture is designed around the defense-in-depth principle that provides multiple layers of protection for external and internal resources. The following sections elaborate on some key elements of this principle:

- Security Zones;
- DMZ;
- Active and Passive Traffic Monitoring; and
- Controlling Traffic Flow.

3.1 Security Zones

The network security architecture includes multiple security zones with predefined rule-sets in both the [redacted] locations. Each location has included in its design:

- A DMZ
  Demilitarized Zone protecting trusted domains from untrusted domains.
- An Extranet zone
  This area contains a(an) application server(s) for access through the VPN.
- An Internal Zone
  That contains our internal applications and database servers.

The discussion that follows concerning the DMZ also discusses the relevant components that define the additional areas of the Extranet zone and the Internal zone.

3.2 DMZ

The DMZ is an integral part of the architectural design. It includes several components, such as gateway computers, proxy computers, firewalls, intrusion detection devices, and so forth. Often, the firewall unit serves as all three of these. The configuration of each individual server in the LAN depends on whether it will be deployed inside the DMZ or behind the DMZ.

DMZs create a buffer or transition zone between networks with different trust levels, such as the Internet and the internal computing resources. You can see the DMZ in both the Arlington and Lakewood LAN diagrams, where a number of Web servers (E-GOV, Web, FTP, SMTP, LIB, and so forth) are located in the DMZ. The NetScreen server (the VPN server itself) is also located in the DMZ for both locations.

MSHA uses a double-firewall design for both Arlington and Lakewood, wherein the DMZ is located between the two firewalls and all internal computing is located behind the inside firewall. The DMZ also contains the IDS (*Intrusion Detection System*).

The DMZ design results in several enhancements to security, and internal policies separating business and data centers also function effectively as DMZ's in their own right. Each of these is discussed below.

Enhanced Security is Derived from Design
Enhanced security results in part from the design providing additional protection for the involved Web servers, which are notorious weak points in any design. This protection stems from both the additional intervening firewall and the proxy server, which essentially acts as a new front-end to the application environment. The proxy server not only enforces user authentication prior to allowing sessions to reach the Web servers, but also eliminates many network-layer attacks and affords the opportunity to apply even further filtering by virtue of it terminating the original connection, providing an opportunity for detailed inspection, and then rebuilding the packets and connection with its own IP stack.

Improved Economics and Flexibility
Fewer total servers are required because the proxy server more readily supports a one-to-many relationship with the application environment. Additionally, this arrangement supports access to the same applications by both external and internal parties without having to install separate instances of the application or having to resort to cumbersome and potentially insecure configurations (such as routing internal users backwards through the DMZ or routing them "out" to the Internet and then back in through the customer/partner-facing DMZ infrastructure).

Extending the Perimeter: Achieving Internal Isolation
Reality demands support for mobile users. The varied and many connections required by these users complicate the traditional perimeter-focused security designs. Furthermore, it is also necessary to account for *internal* users who are a significant threat in their own right, regardless of whether they are intentionally being malicious or not.

The result is the need to extend conventional network security controls inward. Specifically, internal "perimeters" have been implemented to provide containment and isolation services that are more localized to critical resources on the internal network. The intent is to supplement the Internet DMZ with internal business-unit and data center DMZ constructs, such as we have done at [redacted], isolating finance, HR, [redacted] and so forth.

- **Business-Unit Barriers**
  MSHA has implemented a recognized approach in the creation of security boundaries between different business units, not only in the implementation of ACLs and permissions, but also in the form of antivirus engines. An advantage of this approach is that it enables each business unit to make its own decisions regarding how much security it requires. For example, the finance department implements tighter security requirements than other departments to guard its financial information, as does the ITC around its servers. This approach also provides relatively good containment of threats, such as worms.

- **Data Center DMZ**
  Because we do not have sufficient, distributed security skills and resources, we simply isolate centralized applications and resources from the general user population as an effective data-center DMZ. This approach provides greater protection for our most critical assets.

Strengthening the Perimeter
There are two main areas where we improve effectiveness: greater application-layer control and attack-protection capabilities. The simultaneous augmentation of these core services with even more extensive security functions, such as antivirus, VPNs, intrusion detection, vulnerability scanning, and so forth moves us toward the goal of creating an all-in-one network security gateway. [redacted] has in place *McAffee* antivirus and its *e-Policy Orchestrator* agent so that the most current virus files are pushed-out to the users computers. We also have in place the *NetScreen VPN* so that mobile users enter through a secure tunnel.

- **Application-Layer Awareness and Control**
  Historically, the predominant network security product has been the firewall, which makes access control decisions based on network-layer information.

- **The SSL VPN**
  Previously, the predominant mechanism for achieving secure remote access has been IPSec VPN technology. Yet IPSec has been hindered by the burden of having to deploy, manage, and maintain a software component on each node that needs to communicate. It has also been impacted by the inability to effectively provide access that is more granular than to an entire network. As a result, most organizations (including [redacted] constrained their usage of IPSec remote access solutions to a relatively small portion of their user population.

  In contrast, SSL VPNs take advantage of ubiquitous browsers and dynamically downloaded modules to achieve the client-end of an encrypted session. This introduces a great deal of flexibility, relieving the limitation of users being restricted to only those computers with pre-installed client software. Even Internet kiosks can now be leveraged to provide secure communications. MSHA's *NetScreen* VPN takes advantage of the SSL VPN model.

  The focal point of the SSL-enabled gateway is that it is typically located within the DMZ, as is our *NetScreen* device. (The *NetScreen* device actually has one part in the DMZ and the other behind the DMZ.) Other elements of the architecture include the client (i.e., a browser), a management application that addresses both policy configuration and system monitoring, and a separate policy store.

3.2.1 Gateways

Domain Name Server
The DNS (*Domain Name Server*) resides in the DMZ, as shown on the LAN diagrams above. The DNS translates IP addresses and domain names, directing traffic coming in from the Internet to the correct server (E-GOV, Web, FTP, and so forth). The [redacted] site handles all Internet as well as Intranet traffic for MSHA.

Proxy Servers
The proxy server is used to access Web pages by the other computers. When another computer requests a Web page, the proxy server retrieves then sends it to the requesting computer. The net effect of this action is that the remote computer hosting the Web page never comes into direct contact with anything on the network other than the proxy server.

Proxy servers increase the efficiency of Internet access through caching pages. [redacted] has two proxy servers, one at [redacted] and one at [redacted] The proxy server is labeled "Web Cache" on the LAN diagrams above and is located behind the inside firewall.

3.2.2 Firewalls

Firewalls are the first layer of defense for protecting the WAN and LANs against external attacks. They ensure that only authenticated, permitted inbound connections on explicitly approved ports are allowed to establish connections to the Web servers in the DMZ. Firewalls function as gateway and proxy servers as well as firewalls because they have first contact with any outside network traffic and they decide whether that traffic can pass on to the inner, protected network or whether the traffic is rejected. MSHA's PIX Firewalls also provide NAT (*Network Address Translation*) so that NIC-registered IP addresses are visible outside the firewall, while others are not.

The rules for the firewalls are setup so that the firewalls *deny* inbound traffic that:

- Originates from an unidentified source with a destination address of the firewall system itself;
- Contains a source address indicating the packet originated on the [redacted] network behind the firewall;
- Originates from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks;
- Originates from a unidentified source containing SNMP traffic;
- Contains IP-source routing information;
- Contains a source or destination address of the local host (inbound our outbound);
- Contains a source address of 0.0.0.0 (inbound or outbound); or
- Contains directed broadcast addresses (inbound or outbound).

MSHA has deployed its firewalls in-line, not in fail-over mode so that if an unwelcome visitor were able to bypass the first firewall, the inside firewall would still provide some protection.

Firewalls use several methods to control traffic flow throughout the network:

- **Packet Filtering**
  Packets are analyzed against the rule set, and those passing the filters are sent to the requesting system.
- **Proxy Service**
  The firewall retrieves information from the Internet and then sends it to the requesting system and vice versa.
- **Stateful Inspection**
  A newer method that does not examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information. Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

CiscoSecure PIX Firewall 525 Installation and Configuration
The Cisco Secure PIX Firewall 525 arrives ready to power on and configure. The configuration in the Flash memory allows the PIX Firewall start up but does not permit traffic to pass through the network until it is configured to do so.

Installation consists of unpacking the unit, placing it in a safe place, installing any optional hardware or mounting it in an equipment rack, connecting the network cables, and powering on the unit.

Configuration consists of following the **Firewall Setup Wizard.** Accept the default values for most screens in the **Firewall Setup Wizard.**

For more detail on the configuration of the firewalls, including rule sets and load balancing, contact the WAN engineers, the MSHA Information Security Office, or the Chief of Network Operations Division.

3.2.3 Active and Passive Traffic Monitoring: IDS and Log Monitoring

Monitoring network traffic is the second layer of defense against malicious activities and network break-ins. Only through constant traffic monitoring one can detect intrusion attempts and take action against it. Therefore, IDS' are required to continuously monitor network traffic and generate alerts when suspicious activity is detected. This activity may be a successful or unsuccessful break-in attempt, as well as network discovery, mapping, and vulnerability probing that typically precedes a break-in attempt. The information contained in the IDS alerts and logs allows network administrators to stop imminent or ongoing attacks by adjusting firewall policies.

[redacted] network security architecture uses these mechanisms to monitor network traffic.

- **Network-Based IDS**
  All critical network segments are constantly monitored.

- **Host-Based IDS Agents**
  HIDS agents are installed on all key servers and workstations to monitor activities.

- **System Log Monitoring**
  Currently, logs from various network, security, and application devices are manually monitored. Best practices dictate sending logs to a SYSLOG server that alerts administrator(s) when an anomaly is detected.

3.2.3.1 Network-Based IDS

The network-based IDS consists of a *Shomiti* tap that allows monitoring network traffic in real-time via a *RealSecure* Sensor. The *Shomiti* tap makes a copy of the Ethernet signal without impacting the original traffic even if it looses power.

3.2.3.2 Host-Based IDS Agents

MSHA has at least two of these systems. Contact the MSHA Information Security Office, or the Chief of Network Division for more detail.

3.2.3.3 System Log Monitoring

Currently, the network administrators monitor the system logs manually on a daily basis.

3.2.4 Controlling Traffic Flow

The ACS server (*CiscoSecure Access Control Server*) controls traffic flow for all network devices requiring Authentication, Authorization, and Accounting services. [redacted] has two of these servers, one in [redacted] and one in [redacted] The server in [redacted] is the master server, replicating its database out to the [redacted] site nightly. The ACS allows network administrators to control:

- Who logs on to the network;
- The privileges granted;
- Security audit or account billing information; and
- Access and command controls enabled for each configuration's administrator.

For more details on the *CiscoSecure Access Control Server*, see the separate [redacted] server build procedure.

3.2.5 Remote Access: VPN

Both [redacted] and [redacted] have a *NetScreen* VPN for secure, remote access to the network. Each unit consists of the dedicated *NetScreen* server located in the DMZ and its software that restricts access according to the assigned permissions for each user. Network administrators and selected users requiring access to even more secure realms have key-fobs to use. The key-fobs receive an encryption code for their password that is changed in certain intervals. For more details, see the separate *NetScreen* procedures.

Appendix 1: WAN Outage Procedures

Initial WAN Outage Procedures as described in the [redacted] Helpdesk manual follows. Use this procedure if either *InterMapper*® or a user reports a connection down.

WAN Troubleshooting Steps	
1.	Identify the remote office *Serial Interface IP Address.* Use the attached list of WAN IP Addresses.
2.	Ping the IP address. From the command line (Start →: Run →), enter < Ping X.X.X.X>. Replace the Xs with the IP address. If there is no reply, perform the next step; if there is a reply, skip the next step and continue.
3.	If there is NO Ping. Re-PING the IP address again a few minutes later. Occasionally, a connection may temporarily bounce, slow down, and not reply to pings.
	Still No Ping: Call Sprint technical support at XXX.XXX.XXXX. Sprint will ask for the circuit ID (see the attached *Circuit ID* list), your name, and call back number. Please record the ticket number Sprint supplies because it will be necessary later.
4.	Ping REPLY If the PING is returned, the circuit is up and the problem lies elsewhere, possibly the LAN.
5.	Ping the LAN IP address, using the attached *LAN IP Addresses* list. From the command line (Start →: Run →), enter < Ping X.X.X.X>. Replace the Xs with the LAN IP address of the remote office. If there is no reply, THE LAN is DOWN. Contact the office and have someone troubleshoot the LAN with you. Make sure the switch and wireless access point (if it is a wireless office), have POWER. Once power is confirmed and the LAN is still not replying, contact Sprint as listed in Step 3.
6.	Create a ticket in Support Magic, in the Client ID Field enter "WAN OUTAGE." In the Subject field select *WAN* then WAN Impairment. In the incident Description field enter in the description of the outage. For Example : "The Bartow, FL T-1 is down. We have opened a ticket with Sprint on this issue." Save the ticket per normal and the WAN outage notification will be sent out to the correct personnel.
7.	Call the office to verify power.
8.	Contact [redacted] to verify they have opened a ticket and are working on it. [redacted]
9.	When the circuit is restored, contact the office to verify it has connectivity and close the [redacted] ticket.

Appendix 2: Network Addressing

The locations below are arranged alphabetically by location name.

WAN / Serial	Location	ST		LAN Subnet:
[redacted]	Albany	NY		[redacted]
	Albany	OR		
	Albuquerque	NM		
	Anchorage	AK		
[redacted]	Atlanta	DOL		[redacted]
	Aztec	NM		
[redacted]	Barbourville	KY		[redacted]
	Bartow	FL		
	Beaver Dam	KY		
	Beckley	WV		
	Bellevue / Kent	WA		
	Benton	IL		
	Bessemer	AL		
	Birmingham	AL		
	Boise	ID		
	Boulder City	NV		
	Bridgeport	WV		
	Bryan	TX		
[redacted]	Carlsbad	NM		[redacted]
	Charlottesville / Staunton	WV		
	Clearfield	PA		
	Columbia	SC		
	Craig	CO		
[redacted]	Dallas	TX		[redacted]
	Delta	CO		
	Denham Springs	LA		
	Duluth	MN		
[redacted]	Elkhorn City / Belcher	KY		[redacted]
	Elko	NV		
[redacted]	Franklin	TN		[redacted]
	Ft. Dodge	IA		
[redacted]	Geneva	NY		[redacted]
	Gillette	WY		
	Green River	WY		
	Harlan	KY		
	Hazard	KY		

WAN / Serial	Location	ST		LAN Subnet:
[redacted]	Helena	MT		[redacted]
	Hibbing	MN		
	Hillsboro	IL		
	Hindman	KY		
	Hunker / Hempfield	PA		
[redacted]	Indiana	PA		[redacted]
[redacted]	Jacksboro	TN		[redacted]
	Johnstown	PA		
[redacted]	Kittanning	PA		[redacted]
	Knoxville	TN		
[redacted]	Lansing	MI		[redacted]
	Lexington	KY		
	Little Rock	AR		
	Logan/ Mt Gay	WV		
	Longview	TX		
[redacted]	Macon	GA		[redacted]
	Madisonville	KY		
	Manchester	NH		
	Marquette	MI		
	Martin	KY		
	McAlester	OK		
	McHenry	MD		
	Mesa	AZ		
	Morganfield	KY		
	Morgantown	WV		
	Mt. carbon	WV		
	Mt. hope	WV		
[redacted]	Newark / Hebron	OH		[redacted]
	Norman	OK		
	Norton / Wise	VA		
[redacted]	Peru	IL		[redacted]
	Phelps	KY		
	Pikeville	KY		
	Pineville	WV		
	Pittsburgh	PA		
	Pottsville	PA		
	Price	UT		
	Princeton	WV		
	Prosperity / Ruff Creek	PA		

WAN / Serial	Location	ST		LAN Subnet:
[redacted]	Rapid City	SD		[redacted]
[redacted]	Redlands / San Bernardino	CA		[redacted]
[redacted]	Rolla	MO		[redacted]
[redacted]	Salt Lake	UT		[redacted]
[redacted]	San Antonio	TX		[redacted]
[redacted]	San Juan	PR		[redacted]
[redacted]	Sanford	NV		[redacted]
[redacted]	Shamokin	PA		[redacted]
[redacted]	St. Clairsville	OH		[redacted]
[redacted]	Summersville	WV		[redacted]
[redacted]	Topeka	KS		[redacted]
[redacted]	Triadelphia	WV		[redacted]
[redacted]	Uneeda / Madison	WV		[redacted]
[redacted]	Vacaville	CA		[redacted]
[redacted]	Vansant / Oakwood	VA		[redacted]
[redacted]	Vincennes	IN		[redacted]
[redacted]	Vincennes FO			[redacted]
[redacted]	Warrendale / Cranberry	PA		[redacted]
[redacted] [redacted]	WASH DC	DOL		[redacted]
[redacted]	Whitesburg	KY		[redacted]
[redacted]	Wilkes-Barre	PA		[redacted]
[redacted]	Wyomissing	PA		[redacted]

Appendix 3: Acronyms

The official [redacted] Acronym Web page is located here:

[redacted]

EIGRP	Enhanced Interior Gateway Routing Protocol
[redacted]	[redacted]
DMZ	Demilitarized Zone
DNS	Domain Name Server
IP	Internet Protocol
ISO	Information Security Office
ITC	Information Technology Center
LAN	Local Area Network
[redacted]	[redacted]
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
NOD	Network Operations Division
OEM	Original Equipment Manufacturer
OSI	Open System Interconnection
QOS	Quality of Service
SSL	Secure Socket Layer
TCP / IP	Transmission Control Protocol / Internet Protocol
VPN	Virtual Private Network
VLAN	Virtual LAN
WAN	Wide Area Network