Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Network Security:
Layering a ^{3}R Solution @ the Perimeter

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c

Option 2:
Case Study in Network Security
Layering a ^{3}R Solution @ the Perimeter

Submitted by: Larry Copeland Jr.
Location: SANS Las Vegas
Submitted on: March 15, 2005

Paper Abstract:
The principle purpose of this paper is to present the challenges along with the solutions that corporations face in connecting their secure private networks to the world's most unsecured network: The Internet.

Securing an internet connected network is a challenge that all corporations face and it is becoming more difficult as technology evolves.

Corporations have been known to deploy various methods to secure their organization from harmful external traffic. The designs of these networks were generally straightforward and include an external router, firewall, and internal router. The networks of yesterday are no longer applicable. Today's network designs are more complex, involve greater attention to details, and are constructed with a basic set of principals to which Network Designers adhere. The center of these principals revolves around a ^{3}R Solution.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract....1
Foreword....2
Company Background....3
Current Security Posture....3
Description....4
Assessment....4
Proposals....6
Equipment Proposal....6
Network Solution Proposal....8
Solution Implementation....10
Device Additions....11
Device Replacements....11
Internal Application-Layer Firewall....12
Network Completion....13
Security at Work....14
Conclusion....16
References....17
Terminology....18
Tools....19
Devices....20
Appendices....21
A – Before Vulnerability Assessment....21
B – Change Control Request Form....24
C – Change Control Completion Form....25
D – Router Configurations....26
E – PIX Configuration....32
F – ISA Server Installation and Configurations....40

List of Figures

Figure 1: Original Layout....4
Figure 2: Final Network Diagram....13
Figure 3: Network Security Levels....14

List of Tables

Table 1: Feature Grid....6
Table 2: Equipment Grid....7

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

The principle purpose of this paper is to present the challenges along with the solutions that corporations face in connecting their secure private networks to the world's most unsecured network: The Internet.

Securing an internet connected network is a challenge that all corporation face and it is becoming progressively more difficult as technology evolves.

Corporations have been known to deploy various methods to secure their organization from harmful external traffic. The designs of these networks were generally straightforward and include an external router, firewall, and internal router. The networks of yesterday are no longer applicable. Today's network designs are more complex, involve greater attention to details, and are constructed with a basic set of principals to which Network Designers adhere. The center of these principals revolves around a ^3R Solution.

This writing explores the Defense-in-Depth (DID) and Principal of Least Privilege (POLP) principals along with how to modify and deploy these principals in a corporate environment. The fundamental principles that you need to understand and apply to this writing is Confidentiality, Integrity, and Availabilty.[1]

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Foreword

Information Technology has evolved over the years. The evolution of technology has machines performing at higher speeds that increase in six-month cycles. This in turn has led to the daily release of viruses, and provides hackers with sophisticated tools to compromise even the most secure networks. Networks and high-speed connections are no longer for large corporations. Consumers are subscribing to DSL services and they are also creating individual and home networks. Along with high-speed connectivity, users are requesting feature rich operating systems. To accommodate to a users requests, adds more complexity to an already misunderstood environment. The main objective of this writing is to demonstrate one company's development, practice, and practical approach of securing information systems and its network architecture at the perimeter.

This writing will focus on the U.S. based portion of an international company that spans more than 30 countries. With the events of 9/11 the company was forced to make changes that were at the time not part of its strategic plan. In recent years companies have turned their focus from just being on the cutting edge, to being on the cutting edge, securely. Network security needs are ever changing. It is a very large task to keep architecture current with these new trends.

Security Policy can be defined by the combining the following two definitions. Security was defined earlier as "Confidentiality, Integrity and Availability". The SANS Security Policy Project states, "A policy is typically a document that outlines specific requirements or rules that must be met." The security framework is the operations parameter for implementing the technical portions of the security infrastructure. That framework can be suggested by the implementer but needs approval before starting the project. That process should be quick, easy and not delay the project. The security framework can later be expanded and incorporated into the security policy. The Security Architecture provides us with a security framework. [2]

We will begin with an introduction to FTA Corporation and provide a company profile that will help the reader understand the challenges FTA Corporation faces. The second segment of our case study will look at the current security in place for FTA and how it compares with the strategic goals defined by the corporation. The strategic goals of FTA will assist in the design and building of the new security architecture. We outline the changes of our network perimeter devices and design. This writing will conclude with a final review into FTA's current perimeter network design along with its effective security posture.

© SANS Institute 2000 - 2005 Author retains full rights.

Company Background

FronTier Airborne (FTA) is a global engineering company with operations in more than 30 countries. FTA began aerospace part manufacturing in 1996 with two concepts after being awarded a contract from the U.S. Department of Defense. The business is comprised of helicopter manufacturing, a joint venture with International of Italy, and Space Services, a designer and manufacturer of various propulsion systems such as fighter ducts and turbofan cases. FTA also has a supply division which produces airframe, engine, and other components to manufacturers for assembly.

FTA along with its suppliers bring a vast background in tactical aircraft integration, carrier suitability, stealth technologies, avionics systems integration, sensors and advanced commercial aircraft manufacturing. Throughout the U.S., FTA has several locations which house a specific component of the company's global engineering. From its Tennessee facility FTA designed their program to incorporate the low-cost, rapid-prototyping, and advanced technology. The program office located in Missouri focuses on the integrated product team structure, critical stealth technologies and firsthand knowledge of cutting edge aerial products. The total systems integration and world-class, lean assembly line production takes place in the Alabama facility.

Current Security Posture

The Information Technology department consist of 22 individuals comprised mostly of contract workers with eight being foreign nationals. The foreign nationals provided the concept, design, and implementation of the perimeter network infrastructure. The Patriot Act, a federal regulation that was enacted as the result of the tragic events of 9/11 placed U.S. corporations in a frenzy and required network administrators to become knowledgeable in how the USA Patriot Act would affect their companies.[3] As a tier two manufacturer of military aircraft parts FTA received a mandate that no foreign national could be involved in network operations or see data as it pertained to aircraft parts. FTA began the process to replace the foreign national employees with American citizens. The company moved swiftly to replace these workers. It was during this transition that FTA discovered that documentation on their network, both interior and exterior, was limited or none existent.

The current security posture status is UNKNOWN, which translates to a unsecured security posture. The infrastructure that makes up the perimeter network lacks documentation to support a sound secure network structure with integrity and resilience. Although no known security assessment has taken place it is thought that no vulnerabilities exist. The essential security principles were not defined, documented, nor in place to defend FTA against the growing number

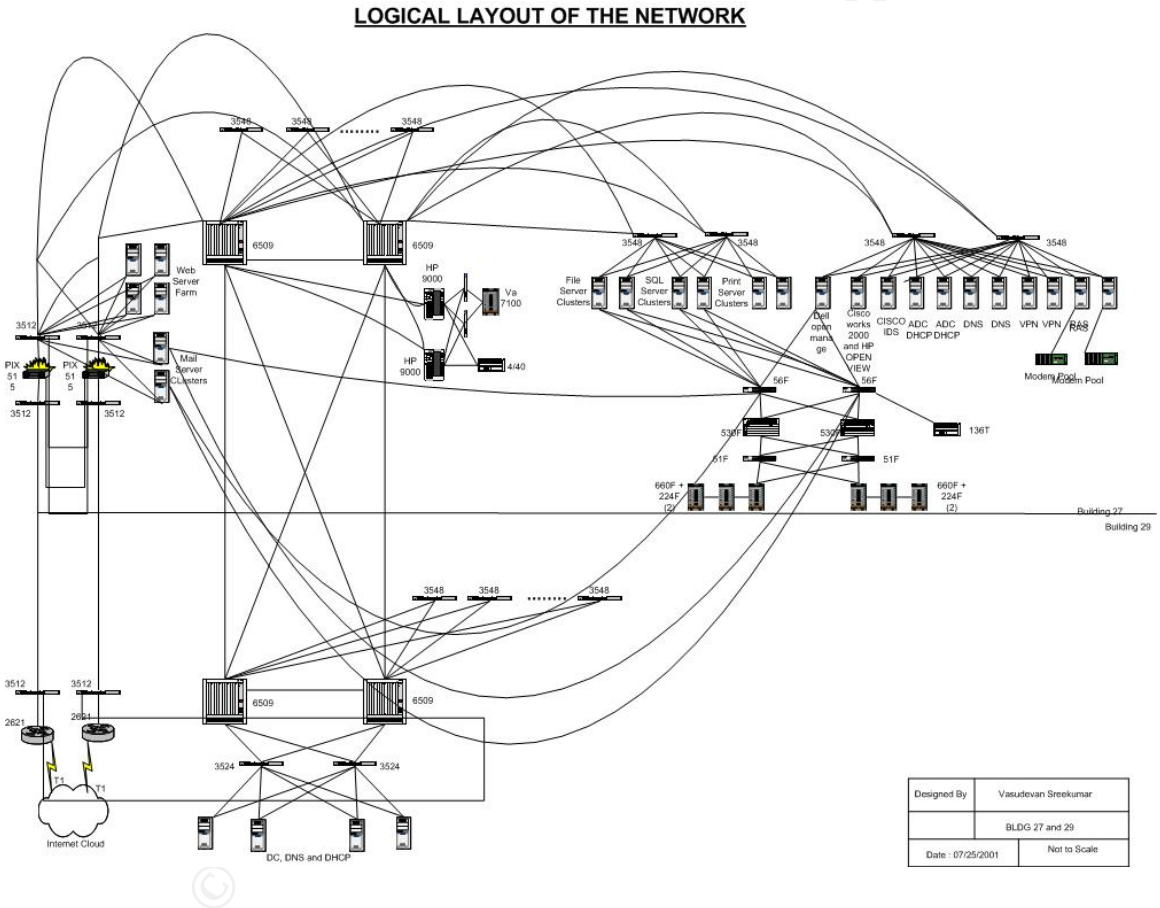
© SANS Institute 2000 - 2005 Author retains full rights.

of external threats. Network owners have pledged a commitment to learn, secure, and control their network perimeter.

Description

The main problem FTA faces is that no clear security stance has been defined. Proper documentation of the existing network does not exist beyond a very generic Visio drawing of how the network devices are interconnected. They have no details as it pertains to the network. Figure 1 shows the network drawing. No details are given with consideration of network gear, only servers and their relationships to each other are distinguished.

Figure 1: Original Layout



Assessment

The present network is in place and running in production, therefore we have to be particularly careful when trying to determine the vulnerability of the network. When we begin to establish the current vulnerabilities there is a potential of Denial of Service (DOS) attacks against the system. Since there are so many unknown factors in the environment we decide to begin at the enterprise edge and work our way towards the internal network, during the information gathering

© SANS Institute 2000 - 2005 Author retains full rights.

process. Security of the Internal Network is beyond the scope of this writing, we will focus our attention on the Enterprise Edge Architecture which FTA has built using Cisco Systems hardware at its core. The enterprise edge consisted of two 2611 Routers, four 3512 Cisco Switches, two PIX515 Firewalls, and two Microsoft ISA Servers, that function as web proxy servers along with enterprise firewall.

Physical Assessment

All equipment is FTA owned and operated, so with permission from FTA IT executives we identified the physical location of each device and connected a laptop with a console cable to every device. We were able to retrieve the "enable" prompt from all devices with the exception of the PIX515 firewalls. We were able to gain access to the enabled mode of the firewalls using the default password of "cisco".

Once access to each device was breached we copied the configuration files to the laptop. We were able to determine the IP address ranges that pertain to FTA. The address ranges are as follows:

External – 172.162.17.0/27
DMZ – 192.168.100.0/24
Internal – 10.230.0.0/22

Cisco output interrupter was used to look at every downloaded configuration file and determine if PSIRT advisories exist and suggest typical changes that could further secure the Cisco device. While this process will suggest enhancements to an IP network's first line of defense, the router, we will use the results as a base line for device assessment.

Vulnerability Scan Assessment

Using the IP address ranges obtained from the configuration files we are able to create Security Scanner Profile in GFiLANGaurds – Network Security Scanner software and proceeded to conduct three network scans:

1. Scan conducted from the audit laptop on the internal network to the outside network addresses.
2. Scan conducted from the audit laptop while using an external address in the range of the outside routers.
3. Scan conducted from the audit laptop with a dial-up connection to the internet via ISP Mindspring.

Risks that were exposed during the scan have been consolidated and are outlined in Appendix A.

© SANS Institute 2000 - 2005 Author retains full rights.

To determine where FTA considered themselves from a security stand point interviews with the IT staff at all levels from managers to hourly employees were conducted to understand their acceptable amount of risk. Along with those details we established the requirements for the new environment and matched those with the long term strategic plans of the corporation. This information revealed that the current design, regardless of the security flaws, would not allow them the scalable network growth that would assist them in their corporate goals. This information means we will not just secure FTA network. We must also build a new Perimeter Network, and utilize SANS teachings, DID, and POLP to ensure its security.

Proposals

Equipment Proposal

Frontier Airborne Corporation re-evaluated its goals for the company and the position that it wanted to take regarding the network and security posture. It was decided that they would focus their attention on intra-site collaboration and secured partner access. They realized better business to business (B2B) interaction would lead to increased profits and the internet would be the facilitator. Though separated geographically, team members will collaborate in a virtual workspace. The created systems will allow shared web content, databases along with common audio, video, and computer systems. Additional features both required and optional are outlined in table 1.

Table 1: Feature Grid

Feature	Required	Optional
3DES Encryption	X	
Dial-back		X
Dial-in Remote Access	X	
DMZ	X	
Extranet		X
FTP Services	X	
IPSEC	X	
Public Web Services	X	
Redundancy	X	
Resilient	X	
Robust	X	
Secured Web Services	X	
SMTP mail Services	X	
Streaming Multi-Media		X
Video Conferencing	X	
VOIP		X
VPN	X	

© SANS Institute 2000 - 2005 Author retains full rights.

Web mail Services	X	
Quality of Services Routing		X
Intrusion Detection Systems		X
Intrusion Prevention Systems		X

The current equipment was audited to determine if the required features for the new environment could be achieved with existing equipment. Since the previous network perimeter equipment consisted of devices that would not work in the new environment, replacement of these devices were required. The new devices are identified and a plan of how the devices are going to be introduced into the existing environment via the change control procedures was created. Replacement devices and current perimeter devices are outlined in table 2.

Table 2: Equipment Grid

Current Equipment		Proposed Replacement
Cisco 2611		**Cisco 3725**
32MB		*128MB*
8MB Flash		*30MB Flash*
Features		*Features*
IP		*IP*
		Firewall
		VPN (DES, AES, 3DES
Cisco PIX515-UR		**Cisco PIX525E-UR**
64MB		*256MB*
DES		*3DES*
		VPN Accelerator Card
Cisco PIX515-FO		**Cisco PIX525E-FO**
Failover License Only		*Failover License Only*
Cisco 3512		**Cisco 3512**
ISA 2000 Enterprise		**ISA 2004 Enterprise**
DELL Power edge 2500		*DELL Power edge 2650*
Windows 2000		*Windows 2003*

© SANS Institute 2000 - 2005 Author retains full rights.

Network Solution Proposal

The solutions that we are proposing are bound by Rule 3R, DID, and POLP. See the solutions:

1. Internet Service Provider

Existing

FTA has had problems in the past with its current ISP, Valuenet. At times connectivity has been a problem, but the biggest concern to FTA is the black listing of its IP addresses. Valuenet became associated with known spammers, and providers of Open Relay services.

Proposal

An interruption in service could mean the potential loss of income for FTA so we needed to incorporate ^{3}R in the perimeter. This is accomplished by changing ISP's to Sprint and adding two additional lines for a total of four lines. Two lines terminate in Kansas with the other two having a POP in Dallas.

2. Internet Router

Existing

Two Cisco 2611 routers with one serial connection each going to Valuenet and the FastEthernet0/0 connections connected to the Cisco 3512 Switch.

Proposal

Replace the 2611 routers with 3725 routers, each 3725 router has two serial connections and two Fast Ethernet (should this be one word) connections. Router A's Serial connections are connected to the Kansas Internet POP while Router B's serial connections are connected to the Dallas Internet POP.

Enable HSRP on the FastEthernet0/0 Interfaces.

Add an additional 3512 Switch and connect each FastEthernet0/0 port from the router to individual switches. Router A's FastEthernet0/0 is connected to Switch A's FastEthernet0/1 port. Router B's FastEthernet0/0 is connected to Switch B's FastEthernet0/1 port.

Enable logging to syslog server Local.

Create ACL for Layer 3 protection against internet access, enabled logging for ACL matches.

© SANS Institute 2000 - 2005 Author retains full rights.

3. Net Switches

Existing

One Cisco 3512 Switch, that connects each 2611-Router to public LAN

Proposal

Add an additional 3512 Switch and connect each FastEthernet0/0 port from the router to individual 3512 switches. Router A's FastEthernet0/0 is connected to Switch A's FastEthernet0/1 port. Router B's FastEthernet0/0 is connected to Switch B's FastEthernet0/1 port.

4. Business Partner Switch/Router addition

Existing

No pre-existing conditions.

Proposal

The requirement for this connection came as a result of the strategic business plan expansion.

Add a 3512 Switch, create a BPN VLAN and connect Router A's FastEthernet0/1 port to the BPN Switch Port FastEthernet0/1 and connect Router B's FastEthernet0/1 port to the BPN Switch Port FastEthernet0/2.

FastEthernet0/12 on the BPN Switch has the Ethernet connection that connects to the Fiber Media Converter. This connection servers a direct Fiber link to a local business partner.

Enable HSRP on the FastEthernet0/1 Interfaces.

5. Cisco PIX525E-UR w/Failover unit

Existing

Two Cisco PIX515 Firewalls are in place and working. The license is Un-Restricted allowing the use of most features. No 3DES license exists**,** but is being required in order to communicate securely with customers and business partners. The 515 model does not contain the VPN accelerator card to allow hundreds of multiple concurrent connections. No DMZ network for publicly accessible servers.

© SANS Institute 2000 - 2005 Author retains full rights.

Proposal

Change the PIX515 Firewalls to the PIX525E-UR Firewall. Upgrade the license on the firewall from DES to 3DES. The 3DES license will be required in order to communicate securely with customers and business partners. Add the VPN Accelerator card to offload the VPN processing from the CPU. Enable Failover to Standby unit and configure both active MAC failover and HTTP failover.

6. ISA – Server

Existing

Microsoft's ISA Server 2000 is installed on a DELL 2550 server and working in both a Firewall and Web Proxy configuration. All traffic is allowed to go out from the private network to the Internet with no filters.

Proposal

Install Microsoft's ISA Server 2004 onto a DELL 2650 server configure ISA to function as both a Web Proxy and Firewall. Route all private network traffic through this server. Traffic destined for the internet is filtered and compared against internet rules before access is allowed. Allow only this machine to connect to the PIX for internet access.

To ensure that traffic leaving the internal network is legitimate a default rule is set to allow only HTTP, HTTPS, FTP request from the internal network out.

Solution Implementation

Although there are several methods available to implement our proposed solutions, we decide to use a phase approach that will allow configuring, replacing, and securing devices by layers. Several tools will be used during implementation to ensure that configurations among similar devices are uniform. All tools and their functions are listed in the Tools section.

All device replacements required the submission, acceptance, and approval of a Change Control Request (CCR). An example of the CCR form can be seen in Appendix B. Once Change Control Requests are submitted and approved, installation occurs during the allotted change control hours which are defined in the CCR Policy.

Installation of the new Sprint T1's are completed within the projected 30 day time frame. Since we will change ISP's completely all routers will run concurrent with each other, which allows us the ability to fine tune our configuration without any impact to production or internet services.

© SANS Institute 2000 - 2005 Author retains full rights.

Device Additions

- Save router 2611-A configuration
- Install Router 3725-A rack along side 2611-A
- Restore 2611-A CiscoConfig to Router 3725-A
- Change Router 3725-A configuration from commands in the 2611-A CiscoConfig that are not compatible
- Attach Router 3725-A serial connections to the Sprint T1's terminating into the Dallas-POP
- Save Router 3725-A's configuration, reboot, and test
    - Testing of Router 3725-A is a success

- Save router 2611-B configuration
- Install Router 3725-B in rack along side 2611-B
- Restore 2611-B CiscoConfig to Router 3725-B
- Change Router 3725-B configuration from commands in the 2611-B CiscoConfig that are not compatible.
- Attach Router 3725-B's serial connections to Sprint T1's terminating into the Kansas-POP
- Save Router 3725-B's configuration, reboot, and test
    - Testing of Router 3725-B is a success

Additional switches are added to meet the *3R* requirement outline in the Network proposal. Where there was only one switch that routers use for LAN connectivity 3 switches will be in use in the current environment.

- Assign new device name to existing switch NetSwitch-01
- Add new 3512 for Internet switching assign name NetSwitch-02
- Add new 3512 for BPN direct connection assign name BPNSwitch

Device Replacements

Given that the Firewalls are the go between for the public internet traffic and the private network traffic, the timing of their replacement is critical. There are already two Cisco PIX Firewalls installed with one working in a failover function, we will use the following procedure to ensure a successful upgrade.

- Disable Failover on PIX515-A
- Save PIX515-A Configuration
- Remove Failover unit PIX515-FO
- Install PIX525-A in rack next to PIX515A
- With no network connections, apply PIX515-A's save configuration to PIX525-A

© SANS Institute 2000 - 2005 Author retains full rights.

- Change PIX525-A's configuration from commands in the PIX515-A CiscoConfig that are not compatible
- Set PIX515-A to standby enabled
- Connect network connections
- Set PIX525-A enabled and active
  - Test network connectivity
    - Network connectivity test, successful
- Remove PIX515-A
- Install PIX525-FO
- Install Failover Cable
- From the Primary unit PIX525-A save the configuration to the standby unit
  - Power off primary unit, test network connectivity
    - Network connectivity test, successful

In our design proposal we included a DMZ configuration and the addition of an internal firewall that filters outbound traffic. The DMZ will be located between the PIX525 firewall and the new ISA 2004 Firewall. The internal firewall will also server as a Web Proxy server to ensure only authorized users are allowed internet access. The Installation details of the ISA Server have been adapted from (Shinder M.D., Thomas W "Installing ISA Server 2000 on Windows Server 2003." Jul 23, 2004)$_5$ detailed in Appendix F while the information below provides how we included ISA during implementation.

Internal Application-Layer Firewall

- Install the ISA 2004 Server software on the DELL 2650 server.
- Joined the ISA 2004 server to the Enterprise ISA chain
- Promote the ISA 2004 server to Primary ISA site server which demotes the current ISA 2000 server to backup ISA server
- Backup the ISA 2000 server
- Restore the ISA 2000 server backup file to new DELL 2650 Server
- Upgrade the ISA 2000 server installation to ISA 2004.
  - Test ISA installation
    - Successful testing.

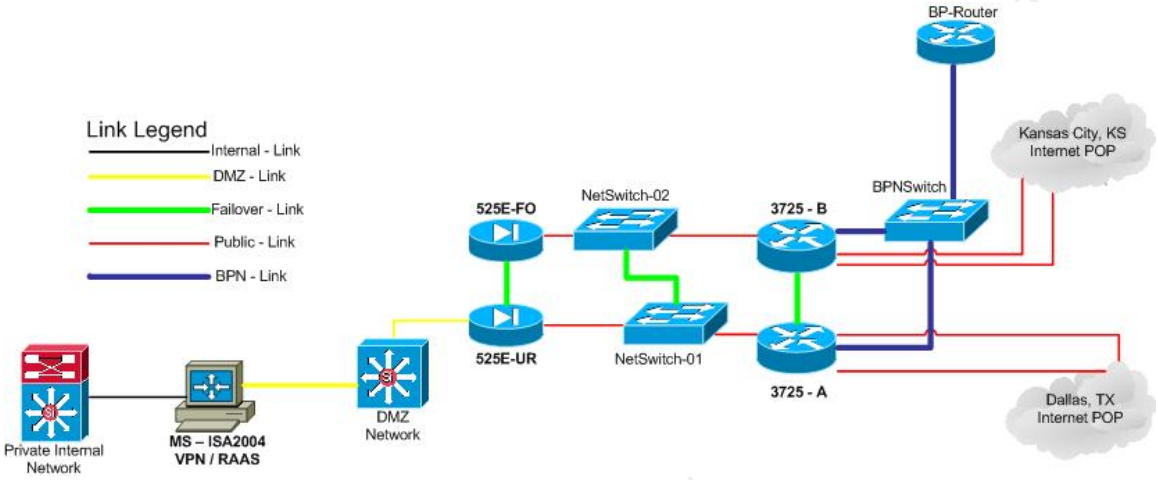
- Deploy the new 2004 ISA secured NAT client to all workstation via SMS deployment script.
  - Test Client installation
    - Successful testing.

© SANS Institute 2000 - 2005 Author retains full rights.

Network Completion

Refer to figure 2: final network diagram, to see a successfully implemented network design.

Figure 2: Final Network Diagram



The perimeter network is clearly defined and meets the requirements for Layering of a ^{3}R Solution @ the Perimeter.

The initial request was to secure an existing network perimeter and ensure that it maintained its security. During the course of our discovery, it was determined from FTA's corporate that for a variety of technical reasons, the current network from a design and equipment standpoint, would no longer serve its needs. FTA would soon be taking its business in a more global direction and looks to the vast opportunities the World Wide Web offers to make that happen.

Our main design goal is to provide ^{3}R Solution:

Robust Networking – Strong hardware, software, secure, design
Redundant Networking – Multiple paths eliminate Single Points of Failure
Resilient Networking – Self-healing devices that recover from failure

The challenge of providing the items listed in Table 1: Feature Grid was accepted without hesitation. Not only was the challenge met, it was exceeded. We were able to provide all required technologies along with our 3R Solution. The optional items are merely a key-stroke away, without changing the underlying architecture.

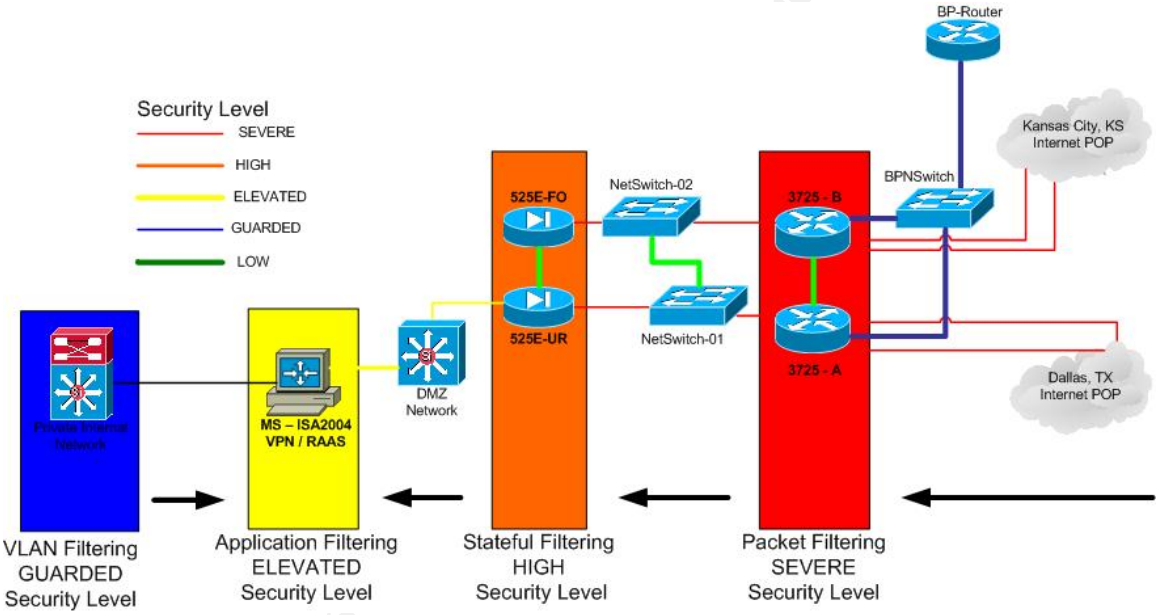
© SANS Institute 2000 - 2005 Author retains full rights.

Security at Work

The Nation requires a Homeland Security Advisory System (HSAS) to provide a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people.[6]

Our security zones are based on the HSAS key and our network uses a similar security model for the filtering of devices within our infrastructure. The Layering of a ^{3}R Solution @ the Perimeter creates a working four tier model that applies security at all tier layers. Figure 3, outlines the security filtering by levels along with there security severity.

Figure 3: Network Security Levels



SEVERE – Enterprise Edge defenses. External Routers are the early problem detection and prevention for our network. At the edge of our network we use packet filtering technology which is fast, but not as secure as some of the other filtering we use in the Layering of a ^{3}R Solution. Since routers already transfer at Layer 3 packets are compared against both Standard and Extended Access Control List's - (ACL). Detail Router Configurations are included in Appendix D. Below is a list of the basic controls that block illegal traffic:

© SANS Institute 2000 - 2005 Author retains full rights.

```
access-list 110 deny   ip 10.0 0.255.255.255 any log
access-list 110 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny   ip 224.0.0.0 31.255.255.255 any log
```

HIGH – DMZ defenses Our Firewall solution resides in front of the DMZ defenses and is the technology responsible for our HIGH security level. This tier layer in the security model uses stateful filtering technology which is slower than the previous layer, but more secure. It is like a packet filtering system, but maintains the state of active connections. Firewalls are the main measure of prevention and by applying intelligent traffic management in this layer, companies can not only minimize the effects of attacks that get through the perimeter; they can also intelligently manage surges of legitimate traffic and surges from problematic applications such as instant messaging and peer-to-peer file-sharing.

ELEVATED – Campus Edge defenses. Our slowest but most secure defenses protects both traffic leaving the internal network going to the outside and traffic returning to the internal network from outside. Security at this layer focuses on the contents of traffic reaching applications. Web application gateways, e-mail spam filters, XML security systems and Secure Sockets Layer virtual private networks help ensure that application traffic is clean, efficient and secure.

A fundamental phase of the Security Implementation is the Lifecycle outline. The Lifecycle outline will ensure that security continues to work as outlined. Security Reviews and Audits are important and they will help FTA maintain its current security posture along with the management of its security process, technologies and compliance with FTA policies and the industry best practices.

The results of these Reviews can be used to immediately correct deficiencies, to pre-empt potential attacks or abuse and to assist in future security planning. While the Security Review looks to current physical and logical security requirements, the Policy Compliance Review verifies compliance with existing security policies in the course of independent hands-on assessment and inspection of on-premises computer facilities and documentation.

© SANS Institute 2000 - 2005 Author retains full rights.

Conclusion

Security administration is not about achieving some unobtainable goal of absolute security. Instead, it's about managing risk. There will never be "absolute" security when it comes to computing environments, but there are ways to effectively minimize risk levels through reducing the number of vulnerabilities. [7]

This writing details Layering a ^{3}R Solution @ the Network Perimeter. The goal of having a Robust, Redundant, and Resilient network is one that was achieved through network device replacement, addition, and configuration fine tuning. The approach taken to perimeter network security, by the Network design architect comes as a result of recent consultant projects as a security practitioner and network design engineer.

The case study covers FronTier Airborne network architecture issues such as positioning and configuration of firewalls, routers, and other network devices. We study the effectiveness of firewall and router access control and fine tune the Web proxy set of authorized users so that we can be good net citizens. The website intek.net says: ”Infosecurity is about mitigating risk. Of course, there are many ways to define and evaluate risk, and many subtle and substantial differences in the application of risk-related terms.”

The most effective way we've found to define risk is with this simple equation:

Risk = Threat x Vulnerability x Cost

Although there is Risk associated with all aspects of network and information security. We mitigate the risk, by Layering a ^{3}R Solution @ the Network Perimeter.

There is also a broader perspective on network requirements. It's a holistic view that encompasses security as well as availability, bandwidth and control. We call it network integrity. This is the real goal behind securing a network. When the network is functioning properly, providing applications with the bandwidth and availability they need, then the network has integrity, and security is doing its job, even when the network is under attack.[8] Technological advancements will continue to evolve, we must keep corporations and individuals alike, prepared and protected.

© SANS Institute 2000 - 2005 Author retains full rights.

References

1. Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials Version 2.3 Volume 3 Sans Press, 2004.

2. Johnston, John David. Architecting, Designing and Building a Secure Information Technology Infrastructure, a case study. 24 August 2003 SANS Reading Room

3. The Impact of the USA Patriot Act on Network Security Practice"
   By Bill Reilly
   Posted: Apr 24 2002
   http://www.onlinesecurity.com/Community_Forum/Community_Forum_detail22.php

4. HSAS – Homeland Security Advisory System Director, Federal Bureau of Investigation,
   http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html

5. Shinder M.D., Thomas W "Installing ISA Server 2000 on Windows Server 2003." Jul 23, 2004
   http://www.isaserver.org/tutorials/installon2003.html

6. Building a Roadmap for Securing Your Enterprise
   By Greg Shipley.
   Date: Nov 16, 2001.
   http://www.informit.com/articles/article.asp?p=24089&seqNum=3&rl=1

7. Using a layered security approach to achieve network integrity
   Opinion by Eric Ogren, The Yankee Group
   FEBRUARY 12, 2004
   http://www.computerworld.com/securitytopics/security/story/0,10801,89861,00.html?SKC=security-89861

8. The Risk Equation
   Intek.net
   http://www.intek.net/Secure/risk_equation.htm

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Terminology

^{3}R Solution

Robust – Physically strong
Redundant – the preservation of data integrity
Resilient – recovering readily from adversity, returning to original state

ACL – Access Control List

BPN – Business Partner Network

DID – Defense-in-Depth

Foreign Nationals – Any person who is not a citizen or national of the United States.

POLP – Principle of Least Privilege Let people have the minimal access needed to do a job.

PSIRT – Product Security incident Response Team advisories, security issues that directly impact Cisco products and actions necessary to repair the Cisco product.

SANS – is the most trusted and by far the largest source for information security training and certification in the world.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Tools

Visio – The Microsoft Office business and technical diagramming program.
http://www.microsoft.com/office/visio/prodinfo/default.mspx

Cisco Output Interpreter
https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl

Kiwi Syslog - Syslog Daemon for Windows. It receives, filters, logs, displays and forwards Syslog messages and SNMP traps from hosts such as routers, switches, Unix hosts and any other syslog enabled device.
http://www.kiwisyslog.com/whats_new_syslog.htm

Kiwi Cat - Kiwi Cat Tools is a application that provides automated device configuration management on routers, switches and firewalls.
http://www.kiwisyslog.com/cattools2.htm

GFiLANguard – Network Security Scanner - checks your network for all potential methods that a hacker might use to attack it
http://www.gfi.com/lannetscan/

CISCO Router / Security Device Manger
Cisco SDM offers smart wizards and advanced configuration support for LAN and WAN interfaces, Network Address Translation (NAT), stateful firewall policy, IPS, IPSec VPN, and QoS policy features. Cisco SDM also offers a 1-click router lockdown and an innovative security auditing capability to check and recommend changes to router configuration based on ICSA Labs and Cisco TAC recommendations.
http://www.cisco.com/en/US/products/sw/secursw/ps5318/index.html

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Devices

Cisco 3725 – Multiservice Access Router
http://www.cisco.com/en/US/partner/products/hw/routers/ps282/ps283/index.html

- Two Integrated 10/100 LAN ports
- Two Integrated Advanced Integration Modules (AIM) slots
- Three Integrated WAN Interface Card (WIC) slots
- Two (Cisco 3725) or four (Cisco 3745) Network Module (NM) slots
- One (Cisco 3725) or two (Cisco 3745) High Density Service Module (HDSM)-capable slots
- 32MB Compact Flash (default); 128MB maximum
- 128MB DRAM (default, single 128MB DIMM); 256MB DRAM maximum
- Support for all major WAN protocols and media: LL, FR, ISDN, X.25, ATM, fractional T1/E1, T1/E1, xDSL, T3/E3, HSSI
- Support for selected NMs, WICs and AIMs from the Cisco 1700, 2600 and 3600 Series 2 RU (Cisco 3725) or 3 RU (Cisco 3745) Rack-mountable chassis

Cisco PIX 525 – Security Appliance is a reliable, purpose-built security appliance for medium to large enterprise networks.
http://www.cisco.com/en/US/partner/products/hw/vpndevc/ps2030/ps2118/index.html

> The Cisco PIX 525 modular two-rack-unit design supports up to eight 10/100 Fast Ethernet interfaces or three Gigabit Ethernet interfaces, making it an ideal appliance for businesses that need a resilient, high-performance, Gigabit Ethernet-ready solution that provides solid investment protection. It delivers more than 330 Mbps of firewall throughput with the capability to handle more than 280,000 simultaneous sessions. VPN acceleration that delivers up to 155 Mbps of Triple Data Encryption Standard (3DES) VPN throughput and 170 Mbps of Advanced Encryption Standard-256 (AES) VPN throughput.

ISA Server 2004 – Protect your network, enforce Internet usage policies, and securely enable remote access
http://www.microsoft.com/isaserver/

> Microsoft Internet Security and Acceleration (ISA) Server 2004 is the advanced application-layer firewall, virtual private network (VPN), and Web cache solution that enables customers to easily maximize existing IT investments by improving network security and performance.

© SANS Institute 2000 - 2005 Author retains full rights.

Appendices

A – Before Vulnerability Assessment

Scanning range:**(Valuenet-FTA) P.U.B.1-P.U.B.64**[**17** computer's found]

Computer	Details	Hostname	Username	Operating System
P.U.B.3				undetermined
P.U.B.4	Time to live (TTL) : 245 (255) - 10 hop(s) away Open Ports (1) 80 [Http => World Wide Web, HTTP] HTTP/1.1 400 Bad Request Date: Wed, 13 Aug 2003 20:43:21 GMT Server: cisco-IOS Accept-Ranges: none			probably Unix
P.U.B.6	Time to live (TTL) : 245 (255) - 10 hop(s) away Open Ports (1) 80 [Http => World Wide Web, HTTP] HTTP/1.1 400 Bad Request Date: Wed, 13 Aug 2003 20:43:32 GMT Server: cisco-IOS Accept-Ranges: none			probably Unix
P.U.B.8	Time to live (TTL) : 247 (255) - 8 hop(s) away Open Ports (3) 23 [Telnet => Remote Login Protocol] User Access Verification Password: 79 [Finger] 80 [Http => World Wide Web, HTTP] HTTP/1.0 501 Not Implemented Date: Mon, 10 May 1993 22:29:07 central Content-type: text/html Expires: Thu, 16 Feb 1989 00:00:00 GMT Alerts (1) (Legend :- High-Medium-			probably Unix

© SANS Institute 2000 - 2005 Author retains full rights.

	Low- Information) Misc_Alerts (1) cfingerd util-c buffer overflow Description : The cfingerd package versions 1.4.3 and earlier is vulnerable to a buffer overflow in the util.c file Bugtraq ID/URL : http://xforce.iss.net/static/6744.php			
P.U.B.9	Time to live (TTL) : 244 (255) - 11 hop(s) away			probably Unix
P.U.B.10	Time to live (TTL) : 244 (255) - 11 hop(s) away			probably Unix
P.U.B.11	Time to live (TTL) : 117 (128) - 11 hop(s) away			Windows
P.U.B.12	Time to live (TTL) : 53 (64) - 11 hop(s) away Open Ports (2) 80 [Http => World Wide Web, HTTP] HTTP/1.1 400 Bad Request Content-Length: 20 Content-Type: text/html Date: Wed, 13 Aug 2003 19:44:04 GMT Connection: close 3389 [Terminal Services] Alerts (1)(Legend :-High-Medium-Low-Information) Info_Alerts (1) Terminal Services Description : Terminal Services are installed on this computer			Windows
P.U.B.13	Time to live (TTL) : 19 (32) - 13 hop(s) away			probably Unix
P.U.B.14	Time to live (TTL) : 19 (32) - 13 hop(s) away			probably Unix
P.U.B.15	Time to live (TTL) : 117 (128) - 11 hop(s) away			Windows
P.U.B.16	Time to live (TTL) : 117 (128) - 11 hop(s) away			Windows
P.U.B.17	Time to live (TTL) : 117 (128) - 11 hop(s) away Open Ports (2) 80 [Http => World Wide Web, HTTP]			Windows 2000

© SANS Institute 2000 - 2005 Author retains full rights.

	HTTP/1.1 400 Bad Request Server: Microsoft-IIS/5.0 Date: Wed, 13 Aug 2003 19:44:39 GMT Content-Type: text/html Content-Length: 87 443 [HttpS => Secure HTTP]			
P.U.B.21	Time to live (TTL) : 117 (128) - 11 hop(s) away			Windows
P.U.B.22	Time to live (TTL) : 117 (128) - 11 hop(s) away			Windows
P.U.B.23	Time to live (TTL) : 117 (128) - 11 hop(s) away Open Ports (2) 80 [Http => World Wide Web, HTTP] HTTP/1.0 302 Moved Temporarily Date: Wed, 13 Aug 2003 19:47:20 GMT Location: /index.html Server: WebLogic WebLogic Temporary patch 2 for PeopleSoft 04/30/2002 09:54:21 Content-Type: text/plain Connection: Close 443 [HttpS => Secure HTTP]			Windows
P.U.B.26	Time to live (TTL) : 117 (128) - 11 hop(s) away Open Ports (3) 21 [Ftp => File Transfer Protocol] 220 www-stl-06 Microsoft FTP Service (Version 5.0). 80 [Http => World Wide Web, HTTP] HTTP/1.1 400 Bad Request Server: Microsoft-IIS/5.0 Date: Wed, 13 Aug 2003 19:49:29 GMT Content-Type: text/html Content-Length: 87 443 [HttpS => Secure HTTP]			Windows 2000

Generated by **LANguard Network Scanner v(2.0)**
Copyright © 2001 GFI Software Ltd.
www.languard.com

© SANS Institute 2000 - 2005 Author retains full rights.

B – Change Control Request Form

Change Request Form					
Systems Owner or delegate to complete				Job ID – Date Raised	DD/MM/YY
Raised By	Name				
	Title				
	Department				
	Email			Phone	
Systems Affected: E.g. Network, Email, Web					
Change Request Description Attach more information if required					
Business Priority[1]	Low	Standard	Urgent	Critical	
Required by:	/ /				
Approved by:	Name				
	Title				
	Department				
	Email			Phone	

1 Business Priority

- **Low** – When resources and time permits.
- **Standard**– Is performed at the next scheduled maintenance period.
- **Urgent –** Requires coordinated downtime at earliest opportunity.
- **Critical** – Requires immediate attention and possible disruption of service.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

C – Change Control Completion Form

Change Control Form				
Systems Services to Complete		Job ID/Date	Received:	/ /
Assigned to				ITHD #
Authorized				/ /
IT Priority	Low	Standard	Urgent	Critical
Estimated Start	/ /		Estimated Finish	/ /
Actual Start	/ /		Actual Finish	/ /
Description of Work Performed Attach more information if required				
Peer Reviews				
Team/Peers				
				/ /
	Other members as required			
Database Admin				/ /
Desktop				/ /
IT Security				/ /
MIS				/ /
Networks				/ /
Windows				/ /
Operations				/ /
Systems Owner				/ /
UNIX Admin				/ /
				/ /
Release Approval				
Manager – Application Services				/ /
Manager – Systems Services				/ /
Manager – Information Services				/ /
Manager – Customer Services				/ /
Director – IT Services				/ /
Job Closed				
Completed By:				/ /

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

D – Router Configurations

!This is the running config of the router: 3725-A

```
!-------------------------------------------------------------------------
!version 12.3
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname 3725-A
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging count
logging buffered 52000 debugging
logging console critical
no logging monitor
enable secret 5 $1$rMWd$iC5lqZmlx16n
enable password 7 010017115A0F0A0A
!
username SYSADMIN privilege 15 password 7 110A1615121E0A02000A2
username INFOSYS privilege 15 password 7 110D16070E1C182C0321
memory-size iomem 15
clock timezone CST -6
clock summer-time CDT recurring
aaa new-model
!
aaa authentication banner ^CCUnauthorized use is prohibited.^C
aaa authentication password-prompt "Enter your password now:"
aaa authentication login default local
aaa authentication enable default enable
aaa session-id common
ip subnet-zero
no ip source-route
!
ip cef
no ip domain lookup
ip domain name fta.com
!
no ip bootp server
ip audit po max-events 100
no ftp-server write-enable
!
```

SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
interface Null0
 no ip unreachables
!
interface FastEthernet0/0
ip address P.U.B.4 255.255.255.192
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip route-cache flow
 no ip route-cache cef
 no ip mroute-cache
 speed 100
 full-duplex
 arp timeout 900
 no cdp enable
 standby 5 ip P.U.B.5
 standby 5 priority 110
 standby 5 preempt
!
interface Serial0/0
 no ip address
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip route-cache flow
 no ip route-cache cef
 no ip mroute-cache
 clockrate 2000000
 no cdp enable
!
interface FastEthernet0/1
ip address B.P.R.59 255.255.255.248
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip route-cache flow
 no ip route-cache cef
 duplex auto
 speed auto
 no cdp enable
 standby 10 ip B.P.R.58
 standby 10 priority 110
 standby 10 preempt
!
interface Serial0/1
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
ip address S.P.R.76 255.255.255.0
 ip access-group 110 in
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip load-sharing per-packet
 ip route-cache flow
 no ip route-cache cef
 no ip mroute-cache
 no cdp enable
!
interface Serial0/2
ip address S.P.R.86 255.255.255.0
 ip access-group 110 in
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip load-sharing per-packet
 ip route-cache flow
 no ip route-cache cef
 no ip mroute-cache
 no cdp enable
!
interface Serial0/3
no ip address
 ip verify unicast reverse-path
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip accounting access-violations
 ip route-cache flow
 no ip route-cache cef
 no ip mroute-cache
 no cdp enable
!
router rip
 version 2
 redistribute static metric 1 route-map redistribute
 network P.R.V.0
 no auto-summary
!
ip http server
ip http authentication local
no ip http secure-server
no ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/2
ip route 0.0.0.0 0.0.0.0 Serial0/1
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
ip route P.R.S.0 255.255.224.0 B.P.R.57
ip route P.R.S.34 255.255.255.255 B.P.R.57
ip route P.R.S.0 255.255.0.0 B.P.R.57
ip route P.R.S.124 255.255.255.252 P.U.B.5
ip route P.R.S.0 255.255.255.0 B.P.R.57
!
logging history debugging
logging trap debugging
logging source-interface FastEthernet0/0
logging P.U.B.7
access-list 10 permit P.U.B.7 log
access-list 10 permit P.U.B.0 0.0.0.64
access-list 101 remark VTY Access-class list
access-list 101 remark SDM_ACL Category=1
access-list 101 permit ip P.U.B.1 0.0.0.63 any log
access-list 101 deny   ip any any log
access-list 110 remark Anti-Spoofing Access-Class
access-list 110 remark SDM_ACL Category=1
access-list 110 remark rem-adm-net
access-list 110 permit ip host A.D.M.213 any
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.43
access-list 110 permit udp host N.T.P.43 eq ntp host N.T.P.66 eq ntp
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.43
access-list 110 permit udp host N.T.P.43 eq ntp host N.T.P.26 eq ntp
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.3
access-list 110 permit udp host N.T.P.3 eq ntp host N.T.P.66 eq ntp
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.3
access-list 110 permit udp host N.T.P.3 eq ntp host N.T.P.26 eq ntp
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.163
access-list 110 permit udp host N.T.P.163 eq ntp host N.T.P.66 eq ntp
access-list 110 remark Auto generated by SDM for NTP (123) N.T.P.163
access-list 110 permit udp host N.T.P.163 eq ntp host N.T.P.26 eq ntp
access-list 110 deny   ip 10.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 127.0.0.0 0.255.255.255 any log
access-list 110 deny   ip 172.16.0.0 0.15.255.255 any log
access-list 110 deny   ip 192.168.0.0 0.0.255.255 any log
access-list 110 deny   ip 224.0.0.0 31.255.255.255 any log
access-list 110 deny   ip any host P.U.B.6 log
access-list 110 deny   ip any host P.U.B.6 log
access-list 110 deny   ip any host P.U.B.7 log
access-list 110 deny   ip any host P.U.B.8 log
access-list 110 deny   ip any host P.U.B.9 log
access-list 110 deny   ip any host P.U.B.10 log
access-list 110 deny   ip any host P.U.B.12 log
access-list 110 deny   ip any host P.U.B.19 log
access-list 110 deny   udp any eq snmp any log
access-list 110 deny   udp any any eq snmp log
access-list 110 deny   icmp any any redirect log
access-list 110 permit ip any any
no cdp run
!
```


© SANS Institute 2000 - 2005 Author retains full rights.

```
route-map redistribute permit 5
match ip address 5
!
route-map redistribute permit 10
match ip address 10
!
snmp-server enable traps tty
snmp-server enable traps syslog
!
banner login ^C
---------------------------------------------------------------------
!!!!!  WARNING !!!!!

This system is only for the conduct of company business or other specifically authorized
use.  This site may contain:

Classified Data, Department of State International Traffic in Arms Regulations (ITAR)
22CFR 120-130
Regulated Technical Data, Department of Commerce Export Administration Regulations
(EAR) 15CFR 700-799 Regulated

Technical Data, and/or FTA Proprietary Data.

Unauthorized transfer of this data is prohibited.  Diversion contrary to U.S. Law and
regulations is prohibited.

All information and communications on this system are subject to review monitoring and
recording at any time without notice or permission.

Unauthorized access/use of this system may be subject to civil and/or criminal penalties.
In the course of monitoring individuals improperly using this system, or in the course of
system maintenance, the activities of authorized users are subject be monitored.

Anyone using this system expressly consents to such monitoring and is advised that if
such monitoring reveals possible evidence of criminal activity, system personnel may
provide the evidence of such monitoring to law enforcement officials.

For more information about FTA Security, see policy ITD-PU-004.

---------------------------------------------------------------------
^C
!
line con 0
 transport preferred all
 transport output telnet
line aux 0
 transport preferred all
 transport output telnet
 line vty 0 3
 session-timeout 3
 access-class 101 in
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
 privilege level 15
 session-limit 1
 login authentication local
 transport preferred all
 transport input telnet ssh
 transport output all
 line vty 4
 session-timeout 3
 access-class 101 in
 privilege level 15
 session-limit 1
 login authentication local
 transport preferred all
 transport input telnet ssh
 transport output all
!
scheduler allocate 4000 1000
ntp clock-period 17180508
ntp server N.T.P.163 source Serial0/1
ntp server N.T.P.43 source Serial0/1
ntp server N.T.P.3 source Serial0/1 prefer
end
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

E – PIX Configuration

```
Building configuration...
: Saved
:
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 100full
interface ethernet3 100full
interface ethernet4 100full
interface ethernet5 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 FTA-net-dmz security25
nameif ethernet3 FTA_tn-net security95
nameif ethernet4 FTA.com-dmz security90
nameif ethernet5 dmz security50
enable password 3kvKyBSBUhK encrypted
passwd 4Gr7hS5l6ny encrypted
hostname 525E-UR
domain-name FTA
clock timezone CST -6
clock summer-time CDT recurring
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol ftp 32
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
no names
object-group service WebServices tcp
  description Allowed Web Services
  port-object eq www
  port-object eq https
  port-object eq 8443
object-group service FTPServices tcp
  description Allowed FTP Services
  port-object eq ftp-data
  port-object eq ftp
object-group service MailServices tcp
  description Allowed Mail Services
  port-object eq smtp
object-group service VCUDPServices udp
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
 description Allowed UDP Video Conf Services
 port-object eq 1719
 port-object eq 1718
 port-object range 2326 2375
object-group service VCTCPServices tcp
 description Allowed TCP Video Conf Services
 port-object eq h323
 port-object range 5555 5560
object-group service CitisServices tcp
 description Allowed Citis Services
 port-object eq 6000
 port-object eq https
 port-object eq 3443
 port-object range 10000 10300
object-group service AdminServices tcp
 description ServicesAdministator
 group-object MailServices
 group-object FTPServices
 group-object VCTCPServices
 group-object WebServices
 port-object eq h323
 port-object eq 8098
 port-object eq 8089
 port-object eq 4662
 port-object eq 500
 port-object eq pptp
 port-object eq 47
object-group service Virus_Containment tcp
 description Used to keep from sending Virus to down stream internet providers.
object-group service L2TP-Services udp
 description VPN Services using pre-share Auth.
 port-object eq 4500
 port-object eq isakmp
access-list compiled
access-list outside_access_in permit gre any host P.U.B.26
access-list outside_access_in permit tcp any host P.U.B.26 eq pptp
access-list outside_access_in permit gre any host P.U.B.25
access-list outside_access_in permit tcp any host P.U.B.25 eq pptp
access-list outside_access_in permit udp any host P.U.B.14 eq syslog
access-list outside_access_in permit tcp any host P.U.B.14 eq 1470
access-list outside_access_in permit ip P.U.B.4 255.255.255.192 host P.U.B.14
access-list outside_access_in permit tcp any host P.U.B.14 eq 81
access-list outside_access_in permit ip any host P.U.B.16
access-list outside_access_in permit gre any host P.U.B.15
access-list outside_access_in permit tcp any host P.U.B.15 object-group AdminServices
access-list outside_access_in permit tcp any host P.U.B.22 object-group VCTCPServices
access-list outside_access_in permit udp any host P.U.B.22 object-group VCUDPServices
access-list outside_access_in permit tcp any host P.U.B.20 object-group VCTCPServices
access-list outside_access_in permit udp any host P.U.B.20 object-group VCUDPServices
access-list outside_access_in permit tcp any host P.U.B.21 object-group VCTCPServices
access-list outside_access_in permit udp any host P.U.B.21 object-group VCUDPServices
access-list outside_access_in permit tcp any host P.U.B.39 object-group FTPServices
access-list outside_access_in permit tcp any host P.U.B.39 object-group WebServices
```


© SANS Institute 2000 - 2005 Author retains full rights.

access-list outside_access_in permit tcp any host P.U.B.28 object-group WebServices
access-list outside_access_in permit tcp any host P.U.B.29 object-group MailServices
access-list outside_access_in permit tcp any host P.U.B.30 object-group MailServices
access-list outside_access_in permit icmp P.U.B.0 255.255.255.192 P.U.B.0 255.255.255.0
access-list outside_access_in permit tcp any host P.U.B.50 object-group WebServices
access-list outside_access_in permit icmp any any unreachable
access-list outside_access_in permit icmp any any time-exceeded
access-list outside_access_in permit tcp any host P.U.B.91 object-group MailServices
access-list outside_access_in permit udp host B.P.H.194 host P.U.B.83 eq isakmp
access-list outside_access_in permit esp host B.P.H.194 host P.U.B.83
access-list outside_access_in permit icmp any any
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 E.D.C.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 E.D.C.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.255.0 E.D.C.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 E.D.C.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 P.R.V.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 P.R.V.0
255.255.255.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 host N.E.T.31
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 host N.E.T.3
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 P.V.80.0
255.255.252.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 N.E.T.0 255.255.0.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 P.V.80.0
255.255.252.0
access-list inside_outbound_nat0_acl permit ip P.R.V.0 255.255.252.0 N.E.T.0 255.255.0.0
access-list dmz_outbound_nat0_acl permit ip D.M.Z.0 255.255.255.0 P.V.80.0
255.255.255.0
access-list dmz_outbound_nat0_acl permit ip D.M.Z.0 255.255.255.0 E.D.C.0 255.255.255.0
access-list dmz_outbound_nat0_acl permit ip host D.M.Z.99 host D.M.Z.142
access-list outside_cryptomap_20 permit ip P.R.V.0 255.255.252.0 E.D.C.0 255.255.255.0
access-list outside_cryptomap_20 permit ip P.R.V.0 255.255.252.0 E.D.C.0 255.255.255.0
access-list outside_cryptomap_20 permit ip P.R.V.0 255.255.252.0 E.D.C.0 255.255.255.0
access-list outside_cryptomap_20 permit ip D.M.Z.0 255.255.255.0 E.D.C.0 255.255.255.0
access-list FTA.com-dmz_access_in permit ip any any
access-list inside_access_in permit ip any any
access-list inside_access_in permit ip host P.R.V.51 any
access-list dmz_access_in permit ip any any
access-list dmz_access_in permit ip host D.M.Z.61 host D.M.Z.63
access-list dmz_access_in permit ip host D.M.Z.62 host D.M.Z.63
access-list dmz_access_in permit tcp D.M.Z.0 255.255.255.0 object-group MailServices host
D.M.Z.20 object-group MailServices
access-list FTA-net-dmz_access_in permit ip any any
access-list FTA-net-dmz_access_in permit ip host N.E.T.3 host P.R.V.2
access-list outside_cryptomap_70 remark All Ports are open and secured via VPN-IPSEC
access-list outside_cryptomap_70 permit tcp host D.M.Z.99 host B.P.N.142
access-list FTA_tn-net_access_in permit ip any any
access-list FTA_tn-net_access_in permit ip host P.R.V.2 host N.E.T.3

© SANS Institute 2000 - 2005 Author retains full rights.

```
access-list FTA_tn-net_access_in permit ip host P.R.V.9 host D.M.Z.61
access-list FTA_tn-net_cryptomap_20 permit ip P.R.V.0 255.255.252.0 P.R.V.0
255.255.255.0
access-list FTA_tn-net_cryptomap_20 permit ip P.R.V.0 255.255.252.0 P.R.V.0
255.255.255.0
access-list FTA_tn-net_cryptomap_20 permit ip D.M.Z.0 255.255.255.0 P.R.V.0
255.255.255.0
access-list dmz_nat0_inbound permit ip D.M.Z.0 255.255.255.0 P.R.V.0 255.255.255.0
access-list dmz_nat0_inbound permit ip D.M.Z.0 255.255.255.0 any
access-list outside_cryptomap_60 permit ip P.R.V.0 255.255.252.0 host B.P.N.31
access-list outside_cryptomap_60 permit ip P.R.V.0 255.255.252.0 host B.P.N.1.3
access-list FTA.com-dmz_cryptomap_1 permit ip D.M.Z.0 255.255.255.0 P.V.80.0
255.255.252.0
access-list FTA.com-dmz_cryptomap_1 permit ip D.M.Z.0 255.255.255.0 N.E.T.0
255.255.0.0
access-list FTA.com-dmz_cryptomap_1 permit ip P.R.V.0 255.255.252.0 P.V.80.0
255.255.252.0
access-list FTA.com-dmz_cryptomap_1 permit ip P.R.V.0 255.255.252.0 P.V.80.0
255.255.252.0
access-list FTA.com-dmz_cryptomap_1 permit ip P.R.V.0 255.255.252.0 N.E.T.0
255.255.0.0
access-list FTA.com-dmz_cryptomap_1 permit ip D.M.Z.0 255.255.255.0 N.E.T.0
255.255.255.0
pager lines 24
logging on
logging timestamp
logging console emergencies
logging monitor critical
logging buffered debugging
logging trap debugging
logging facility 23
logging device-id hostname
logging host inside P.R.V.4
mtu outside 1500
mtu inside 1500
mtu FTA-net-dmz 1500
mtu FTA_tn-net 1500
mtu FTA.com-dmz 1500
mtu dmz 1500
ip address outside P.U.B.11 255.255.255.192
ip address inside P.R.V.1 255.255.252.0
ip address FTA-net-dmz N.E.T.17 255.255.255.240
ip address FTA_tn-net P.V.217.1 255.255.255.0
ip address FTA.com-dmz P.V.218.1 255.255.255.248
ip address dmz D.M.Z.1 255.255.255.0
ip verify reverse-path interface outside
ip audit info action alarm
ip audit attack action alarm
failover
failover timeout 0:00:00
failover poll 15
failover replication http
failover ip address outside P.U.B.13
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
failover ip address inside P.V.209.1
failover ip address FTA-net-dmz N.E.T.20
failover ip address FTA_tn-net P.V.217.254
failover ip address FTA.com-dmz P.V.218.4
failover ip address dmz D.M.Z.2
failover link inside
pdm logging debugging 100
pdm history enable
arp timeout 14400
global (outside) 10 P.U.B.61-P.U.B.62
global (outside) 20 P.U.B.63
global (inside) 1 interface
global (FTA-net-dmz) 10 interface
global (FTA-net-dmz) 20 N.E.T.20
global (FTA_tn-net) 20 interface
global (FTA_tn-net) 10 P.V.217.4
global (FTA.com-dmz) 20 interface
global (FTA.com-dmz) 10 P.V.218.4
global (dmz) 10 interface
nat (inside) 0 access-list inside_outbound_nat0_acl
nat (inside) 10 0.0.0.0 0.0.0.0 0 0
nat (FTA_tn-net) 10 0.0.0.0 0.0.0.0 0 0
nat (FTA.com-dmz) 0 access-list cisco_test
nat (FTA.com-dmz) 10 0.0.0.0 0.0.0.0 0 0
nat (dmz) 0 access-list dmz_outbound_nat0_acl
nat (dmz) 20 0.0.0.0 0.0.0.0 0 0
static (inside,outside) P.U.B.25 P.R.V.7 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.30 D.M.Z.26 dns netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.20 D.M.Z.61 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.21 D.M.Z.62 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.15 D.M.Z.254 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.29 D.M.Z.25 netmask 255.255.255.255 0 0
static (inside,outside) P.U.B.74 P.R.V.4 netmask 255.255.255.255 0 0
static (inside,outside) P.U.B.88 P.R.V.122 netmask 255.255.255.255 0 0
static (inside,dmz) D.M.Z.64 P.R.V.51 netmask 255.255.255.255 0 0
static (dmz,fta-net-dmz) P.U.B.15 D.M.Z.254 netmask 255.255.255.255 0 0
static (inside,fta-net-dmz) P.U.B.14 P.R.V.4 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.16 D.M.Z.250 netmask 255.255.255.255 0 0
static (inside,outside) P.U.B.60 P.R.V.71 netmask 255.255.255.255 0 0
static (edc_tn-net,dmz) D.M.Z.63 P.R.V.9 netmask 255.255.255.255 0 0
static (edc_tn-net,outside) P.U.B.22 P.R.V.9 netmask 255.255.255.255 0 0
static (edc_tn-net,fta-net-dmz) P.R.V.2 P.R.V.2 netmask 255.255.255.255 0 0
static (edc_tn-net,outside) D.M.Z.99 P.R.V.14 netmask 255.255.255.255 0 0
static (dmz,outside) P.U.B.31 D.M.Z.22 netmask 255.255.255.255 0 0
static (inside,outside) P.U.B.26 P.R.V.121 netmask 255.255.255.255 0 0
static (inside,outside) P.U.B.39 P.V.210.36 netmask 255.255.255.255 0 0
static (inside,dmz) D.M.Z.20 P.R.V.52 netmask 255.255.255.255 0 0
static (edc_tn-net,outside) P.U.B.23 P.R.V.2 netmask 255.255.255.255 0 0
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
access-group FTA-net-dmz_access_in in interface FTA-net-dmz
access-group FTA_tn-net_access_in in interface FTA_tn-net
access-group FTA.com-dmz_access_in in interface FTA.com-dmz
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
access-group dmz_access_in in interface dmz
route outside 0.0.0.0 0.0.0.0 P.U.B.66 1
route FTA-net-dmz P.R.V.0 255.255.255.0 P.V.32.18 1
route FTA.com-dmz P.V.80.0 255.255.252.0 P.V.218.2 1
route FTA.com-dmz P.V.96.0 255.255.255.248 P.V.218.2 1
route inside P.R.V.0 255.255.252.0 P.R.V.2 1
route FTA_tn-net P.R.V.0 255.255.255.0 P.V.217.2 1
route FTA_tn-net P.R.V.0 255.255.255.0 P.V.217.2 1
route FTA-net-dmz N.E.T.3 255.255.255.255 N.E.T.18 1
route FTA-net-dmz N.E.T.0 255.255.0.0 N.E.T.18 1
route FTA.com-dmz N.E.T.0 255.255.0.0 P.V.218.2 1
timeout xlate 1:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server RADIUS (inside) host P.R.V.5 pix-525 timeout 5
aaa-server LOCAL protocol local
aaa authentication http console LOCAL
aaa authentication ssh console LOCAL
aaa authentication telnet console LOCAL
aaa authorization command LOCAL
http server enable
http P.V.210.30 255.255.255.255 inside
http P.R.V.4 255.255.255.255 inside
http P.V.210.29 255.255.255.255 inside
tftp-server inside P.R.V.4 /tftpboot/pix/pix525.cfg
floodguard enable
sysopt connection permit-ipsec
sysopt connection permit-pptp
sysopt connection permit-l2tp
auth-prompt prompt !!!!! W A R N I N G !!!!! - This is a private computer system
auth-prompt accept This computer system, including all related equipment, networks, and
network devices are provided only for authorized use. Access is monitored at all times.
auth-prompt reject Unauthorized access of this system may be subject to civil and/or criminal
penalties.
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer B.P.A.1
crypto map outside_map 20 set transform-set ESP-DES-SHA
crypto map outside_map 60 ipsec-isakmp
crypto map outside_map 60 match address outside_cryptomap_60
crypto map outside_map 60 set peer B.P.B.2
crypto map outside_map 60 set transform-set ESP-3DES-SHA
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
crypto map outside_map 70 ipsec-isakmp
crypto map outside_map 70 match address outside_cryptomap_70
crypto map outside_map 70 set peer B.P.C.6
crypto map outside_map 70 set transform-set ESP-3DES-MD5
crypto map outside_map interface outside
crypto map edc_tn-net_map 20 ipsec-isakmp
crypto map edc_tn-net_map 20 match address edc_tn-net_cryptomap_20
crypto map edc_tn-net_map 20 set peer P.V.21.2
crypto map edc_tn-net_map 20 set transform-set ESP-3DES-SHA
crypto map edc_tn-net_map interface edc_tn-net
crypto map na.com-dmz_map 1 ipsec-isakmp
crypto map na.com-dmz_map 1 match address na.com-dmz_cryptomap_1
crypto map na.com-dmz_map 1 set peer P.V.96.1
crypto map na.com-dmz_map 1 set transform-set ESP-3DES-MD5
crypto map na.com-dmz_map interface na.com-dmz
isakmp enable outside
isakmp enable edc_tn-net
isakmp enable na.com-dmz
isakmp key ******** address B.P.A.1 netmask 255.255.255.255 no-xauth no-config-mode
isakmp key ******** address B.P.B.6 netmask 255.255.255.255 no-xauth no-config-mode
isakmp key ******** address P.V.21.2 netmask 255.255.255.255 no-xauth no-config-mode
isakmp key ******** address B.P.C.2 netmask 255.255.255.255 no-xauth no-config-mode
isakmp key ******** address P.V.96.1 netmask 255.255.255.255 no-xauth no-config-mode
isakmp policy 9 authentication rsa-sig
isakmp policy 9 encryption des
isakmp policy 9 hash sha
isakmp policy 9 group 1
isakmp policy 9 lifetime 86400
isakmp policy 29 authentication pre-share
isakmp policy 29 encryption des
isakmp policy 29 hash sha
isakmp policy 29 group 2
isakmp policy 29 lifetime 86400
isakmp policy 39 authentication pre-share
isakmp policy 39 encryption 3des
isakmp policy 39 hash md5
isakmp policy 39 group 2
isakmp policy 39 lifetime 86400
isakmp policy 49 authentication pre-share
isakmp policy 49 encryption 3des
isakmp policy 49 hash sha
isakmp policy 49 group 2
isakmp policy 49 lifetime 86400
telnet P.R.V.4 255.255.255.255 inside
telnet P.V.210.30 255.255.255.255 inside
telnet timeout 5
ssh P.V.210.30 255.255.255.255 inside
ssh timeout 5
management-access inside
console timeout 0
username INFOSYSpassword trxdrzere5fxgz encrypted privilege 15
username SYSADMIN password /GAEFG1PZ encrypted privilege 15
privilege show level 0 command version
```

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

```
privilege show level 0 command curpriv
privilege show level 3 command pdm
privilege show level 3 command blocks
privilege show level 3 command ssh
privilege configure level 3 command who
privilege show level 3 command isakmp
privilege show level 3 command ipsec
privilege show level 3 command vpdn
privilege show level 3 command local-host
privilege show level 3 command interface
privilege show level 3 command ip
privilege configure level 3 command ping
privilege configure level 5 mode enable command configure
privilege show level 5 command running-config
privilege show level 5 command privilege
privilege show level 5 command clock
privilege show level 5 command ntp
vpnclient server P.V.96.1
vpnclient mode network-extension-mode
vpnclient vpngroup FTA.fta.com password ********
terminal width 80
banner exec This computer system $(hostname).$(domain) is monitored at all times.
banner login !!!!!  W A R N I N G  !!!!!
banner login This is a private computer system. This computer system,
banner login including all related equipment, networks, and network
banner login devices are provided only for authorized use. Access
banner login is monitored at all times.
banner login Unauthorized use of this system may be subject to civil
banner login and/or criminal penalties.
banner motd Unauthorized use of this system may be subject to civil
banner motd and/or criminal penalties.
Cryptochecksum:d4fc13b4ebe71a37c3e0c5b5a586d396
: end
[OK]
```

© SANS Institute 2000 - 2005 Author retains full rights.

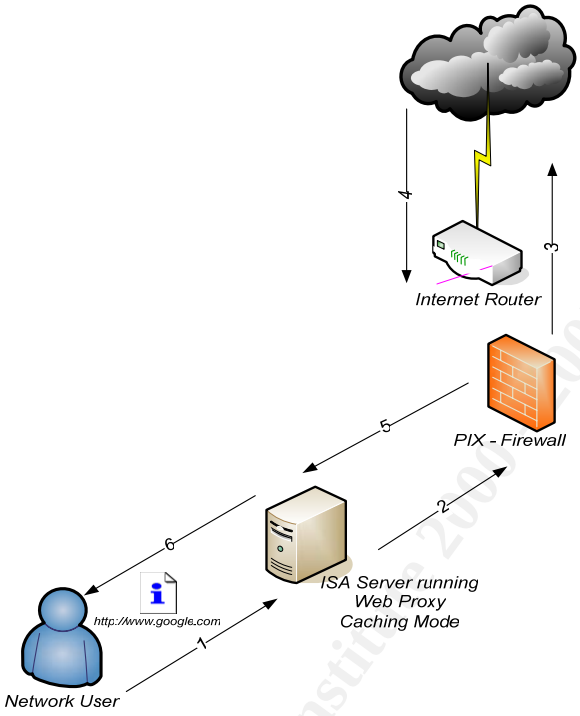
© SANS Institute 2000 - 2005 Author retains full rights.

F – ISA Server Installation and Configurations

Overview

FTA currently use a Cisco's firewall solution, but have a need to monitor, manage, and optimize the users Internet activity for all connected sites.

It is for these reasons that we decided to implement Microsoft's ISA Server. The ISA Server installation is on a machine with two network interface cards and the machine is both a Firewall and a Web proxy server. This multi-homed ISA Server can connect to the Internet through the existing PIX firewall.



This figure shows the basic infrastructure. You have a firewall that sits at the edge of the network. This is a PIX-525UR a packet-filtering device. The multi-homed ISA Server has one NIC in the DMZ and the other NIC is internal, trusted network. The multi-homed ISA Server is configured in Firewall and Web Proxy that accesses the Internet through the existing firewall solution. The ISA Server is configured to exert access control over the Web Proxy clients on the internal network, and the existing firewall is configured to exert its own access control over the ISA Server's outbound access attempts.

The PIX firewall does not understand higher-level protocols, or it does so on a superficial level.

We will allow Web Publishing Rules and will publish SSL Web sites, including Outlook Web Access sites.

Configure the PIX Firewall

The PIX Firewall is configured to allow the ISA Server to access HTTP, HTTPS, and FTP content only. The ISA Server is a client to the PIX just like any other client on the internal network. It is not expected that the PIX and the ISA Server share any special information with one another.

© SANS Institute 2000 - 2005 Author retains full rights.

We are allowing the multi-homed ISA Server FTP downloads for the Web Proxy clients in Standard mode FTP. To do so we have to force the Web Proxy service to use PASV mode FTP connections to the Internet.

To force FTP connections to be PASV mode the following steps were completed on the ISA Server

1. Open **regedit.**
2. Locate the following registry key:

HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/W3Proxy/Parameters

3. In the right pane of the **Registry Editor**, right-click **NonPassiveFTPTransfer**, and click **Modify.**
4. In the **Value data** box, type **0** (zero), then click **OK**. **Note**: the default value of this setting is **1**.
5. Quit Registry Editor, and then restart the ISA Server Web Proxy service. You do not need to restart the server.

Configure the Supporting TRUSTING Network Infrastructure

DNS is critical to the success of the network infrastructure. We will configure the internal DNS infrastructure so that internal network clients are able to identify the ISA Server by its Fully Qualified Domain Name (sec-fta-01). All network clients should be able to do this, including those clients belonging to domains different from the ISA Server's domain. Web Proxy clients are configured to resolve the name of the ISA Server by its host name only, we took care to make sure that when the clients fully qualify the unqualified name that the result is the correct name of the ISA Server.

This is especially important since we are using WPAD entries to support the Auto discovery network feature. When the Web Proxy client is configured to use Auto discovery to find the Web Proxy server, it will send a DNS query for wpad.FTA. The "FTA" is based on how the Web Proxy client computer fully qualifies unqualified names. For Windows 2000 and Windows XP clients, the DNS client software will append the Web Proxy client computer's primary domain name to the unqualified names before sending them for name resolution. The important thing to remember is that Web Proxy clients need to resolve both the ISA Server's host name and WPAD correctly.

The nice thing about the Web Proxy client configuration is that you do not have to make profound changes to your network's routing infrastructure to support it.

© SANS Institute 2000 - 2005 Author retains full rights.

Configure the ISA Server for Outbound Access

- Configure the TCP/IP Settings on the ISA Server
- Install ISA Server in Integrated Mode
- Configure the Site and Content and Protocol Rules

All that needs to be done is to assign the ISA Server a valid IP address and subnet mask, a default gateway that will route internet bound requests to your internet access device, and a DNS server that can resolve internet host names. In this case, we used the following information:

The best option for the DNS server is an internal network server that is configured to use a Forwarder to resolve internet host names.

Perform the following steps to install ISA Server in cache-only mode:

1. Let the ISA Server CD autorun, or open **ISAAutorun.exe** from the CD.
2. Click the **Install ISA Server** link on the install page.
3. Click **Continue** on the **Welcome to the Microsoft ISA Server installation page**.
4. Enter your CD Key in the CD Key dialog box. Click **OK**.
5. Note your product ID. **Write it down just in case.** Click **OK**.
6. On the **License Agreement** page, read the **EULA** and click **I Agree**.
7. On the installation type page, click on the **Custom Installation** button.
8. On the Options list page, click **Continue**.
9. We are installing ISA Server as a stand-alone server. Click **Yes** in the dialog box that explains that you have not performed the enterprise initialization.
10. On the **ISA Server Mode** page, select the **Cache Mode** option and click **Continue**.
11. If IIS is installed on the ISA Server, click **OK** to allow the ISA Server to stop the IIS WWW service during installation. Note that the WWW service be stopped only until the ISA Server is restarted. You should disable IIS on the ISA Server, or configure the ISA Server with multiple IP addresses and configure all Web sites to listen on IP addresses not used by the Web Proxy listeners. Click **OK**.
12. On the cache size page, select the drive and configure the size of the cache. Click **OK**.
13. The files are installed. Leave the checkmark in the **Start ISA Server Getting Started Wizard** checkbox and click **OK**.
14. If everything works out, you will be taken to the **Getting Started** page.
15. Now install Service Pack 1.

© SANS Institute 2000 - 2005 Author retains full rights.

Completing the initial installation

In the Integrated mode, there is a button you can press to create an "Limited Outbound Access – All Open" Protocol Rule:

1. Expand the **Servers and Arrays** node and expand your server name.
2. Expand the **Access Policy** node and click on the **Protocol Rules** node. Click on the **Create a Protocol Rule for Internet Access** icon.
3. On the **Welcome to the New Protocol Rule Wizard** page, type in a name for the rule "*Limited Outbound Access – All Open*". Click **Next**.
4. On the **Protocols** page, remove the checkmarks from any protocols you do not want applied to this rule. Since we are creating an All Open rule, we will leave all the protocols selected. Click **Next**.
5. On the **Schedule** page, select the **Always** schedule. *You would change this based on your network's requirements*. Click **Next**.
6. On the **Client Type** page, select the appropriate option. In most circumstances, you will select the **Specific users and groups** option. *You would select this option because the Web Proxy client can leverage user/group membership to control outbound access*. Select **Specific users and groups** and. Click **Next.**
7. On the **Users and Groups** page, click the **Add** button. Select your domain and then select the **Domain Users** group. Double click on the group and click **OK**. This will allow members of the domain to access the Internet via this Protocol Rule. If users cannot authenticate, they will not be able to connect to the Web. Click **Next**.
8. On the **Completing the New Protocol Rule Wizard** page, review your settings and click **Finish**.

You do not need to create any packet filters or Site and Content Rules at this point. There is a default Site and Content Rule that allows everyone access to all sites at all times. You will want to change this site and content rule or disable it later so that you can have better control over what sites users can access.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Configure the Clients for Proxy Use

Browsers must be configured to use the ISA Server as their Proxy server. This is what makes them Web Proxy clients. You can manually configure the browsers or you can take advantage of WPAD entries and allow the browsers to automatically detect the address of the Web Proxy server. Automatic discovery is supported by Internet Explorer 5.0 and above. The following steps take place when the IE 6+ attempts to auto discover the Web Proxy server:

1. When the client makes a web request, the client connects to a DNS or DHCP server.
2. The DNS server or the DHCP server has a WPAD entry that points to a WPAD server, which is the ISA Server computer.
3. The ISA Server computer that was identified by the WPAD entry in the DNS server or DHCP server fulfills client requests. The ISA Server can also provide the Autoconfiguration script if it is configured to advertise Autodiscovery information.

The **Automatically detect settings** option behaves in different ways, depending on how the ISA Server is configured.

The default setting is to *disable* Autodiscovery. If the **Automatically detect settings** option is configured on the Web browser *and* Autodiscovery is *disabled* on the ISA Server, the Web browser will only receive the IP address of the Web Proxy server. This has the same effect as selecting *only* the **Use a proxy server for you LAN** option and typing in the IP address; no Autoconfiguration information is sent to the Web browser.

However, if you configure the ISA Server to **Publish automatic discovery information** by putting a checkmark in the checkbox, the Web browser configured to **Automatically detect settings** will get the IP address of the ISA Server and will also receive the Autoconfiguration script. This has the same effect as selecting the **Use automatic configuration script** option and manually inputting the Autoconfiguration script address. You can see the Browser requesting the Autoconfiguration script in the figure below.

You can configure WPAD entries in either DNS or DHCP.

We choose to use both DNS and DHCP to deliver wpad information as a redundant configuration to each other.

© SANS Institute 2000 - 2005 Author retains full rights.

Configure the WPAD Information

Web Proxy clients can use either a DHCP server or a DNS server to obtain Autoconfiguration information.

To configure the DNS server to send the Autoconfiguration URL to the Web Proxy and Firewall client:

1. Start the DNS snap-in.
2. In the console tree, click your server name, and then click **Forward Lookup Zones**.
3. Right-click the forward lookup zone that you want to support Web Proxy client Autoconfiguration, and then click **New Alias**.
4. Type ***wpad*** in the **Alias name** box.
5. Type in the Fully Qualified Domain Name of the ISA Server (sec-fta-01.FTA) internal interface.

    - Use the **Browse** button to minimize the chance of making an error.

6. Click **OK**.

To configure the DHCP server to send the Autoconfiguration URL to the Web Proxy and Firewall client:

1. Start the DHCP snap-in.
2. Right-click the **DHCP** name, and then click **Set Predefined Options**.
3. Click **Add**.
4. Type **wpad** in the **Name** box.
5. Click **String** in the **Data Type** box.
6. Type **252** in the **Code** box.
7. Click **OK**.
8. Type **http://*wpad*/wpad.dat** in the **String** box in the **Predefined Option and Values** dialog box.
9. Click **OK**.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

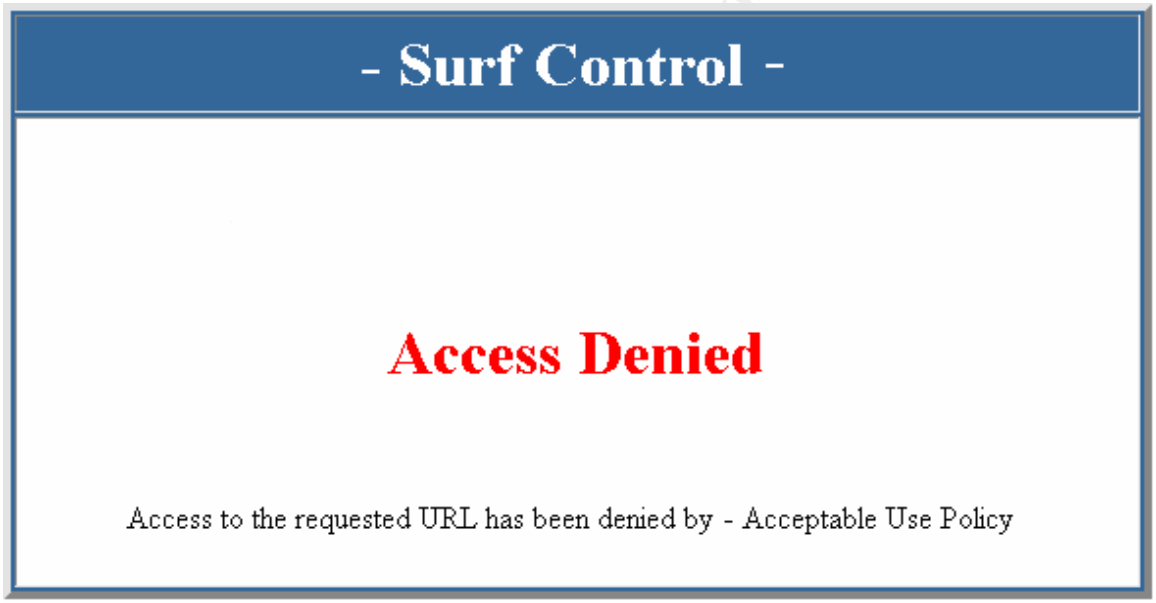
Configure the Web Proxy Client Information

To configure the Web Proxy client browser to automatically detect its settings:

1. Start Internet Explorer 6.0 or later.
2. On the **Tools** menu, click **Internet Options**.
3. Click the **Connections** tab.
4. Click **LAN Settings**.
5. Click to select the **Automatically detect settings** check box, click **OK**, and then click **OK** again.

Test Web Proxy client configuration by pointing your browser to www.google.com

Web Proxy clients that try to access sites which are in violation of the Acceptable Use policy will receive the following page instead of their requested page:



Web Filtering is provided by Surf Control Software which has an ISA integrated interface.

© SANS Institute 2000 - 2005 Author retains full rights.