Global Information Assurance Certification Paper

GIAC Certified Firewall Analyst (GCFW)
Practical Assignment 4.1

Rodney Rose
March 31, 2005

Outline

Abstract

The current design of most networks today defines a perimeter, an Internet Services area, and an internal Local Area Network (LAN). Traffic from the Internet usually comes through a filtering router, at least one firewall, and then to its destination. Generally speaking, the LAN traffic is considered safe with minimal security measures in place. Remote access is provided by IPSec VPN, SSL VPN, or Dial-in services. These services typically authenticate the user and then allow the user to perform certain tasks based on authorization policies in place on network devices.

There are currently products that run on the client computer which are based on a personal firewall concept and only allow certain network activity based on certain criteria. For example, if a wireless adapter is enabled, then the user can only connect via VPN to the corporate network. This concept will be critical in the future of securing networks.

The proposed solution is to build into the operating system network driver the function of establishing a connection to the home office as soon as the client gets an IP address. This session will authenticate the machine and start an SSL encrypted tunnel. Also, there will need to be a virtual interface that allows all client applications to connect via SSL to each server. The user then logs in using two-factor authentication and an encrypted session is launched to each server based on what application is launched. For example, if Outlook is opened, an SSL session is established between the client computer and the Exchange server. The Exchange server will only talk to clients that have been authenticated by both machine and user account. The only traffic the Exchange server will send/receive will be encrypted and therefore move the need for packet inspection to the upper layers of the OSI stack on each server. This solution will be more flexible than IPSec because it will not require special firewall rules to be in place.

This concept will allow organizations to have complete control over corporate owned computers. Secure network perimeters will be moved to each individual machine. The concept of a “trusted segment” will be eliminated and each client to server connection will be a virtual cable. It will become easier for servers to be securely available on the Internet at any hosting location.

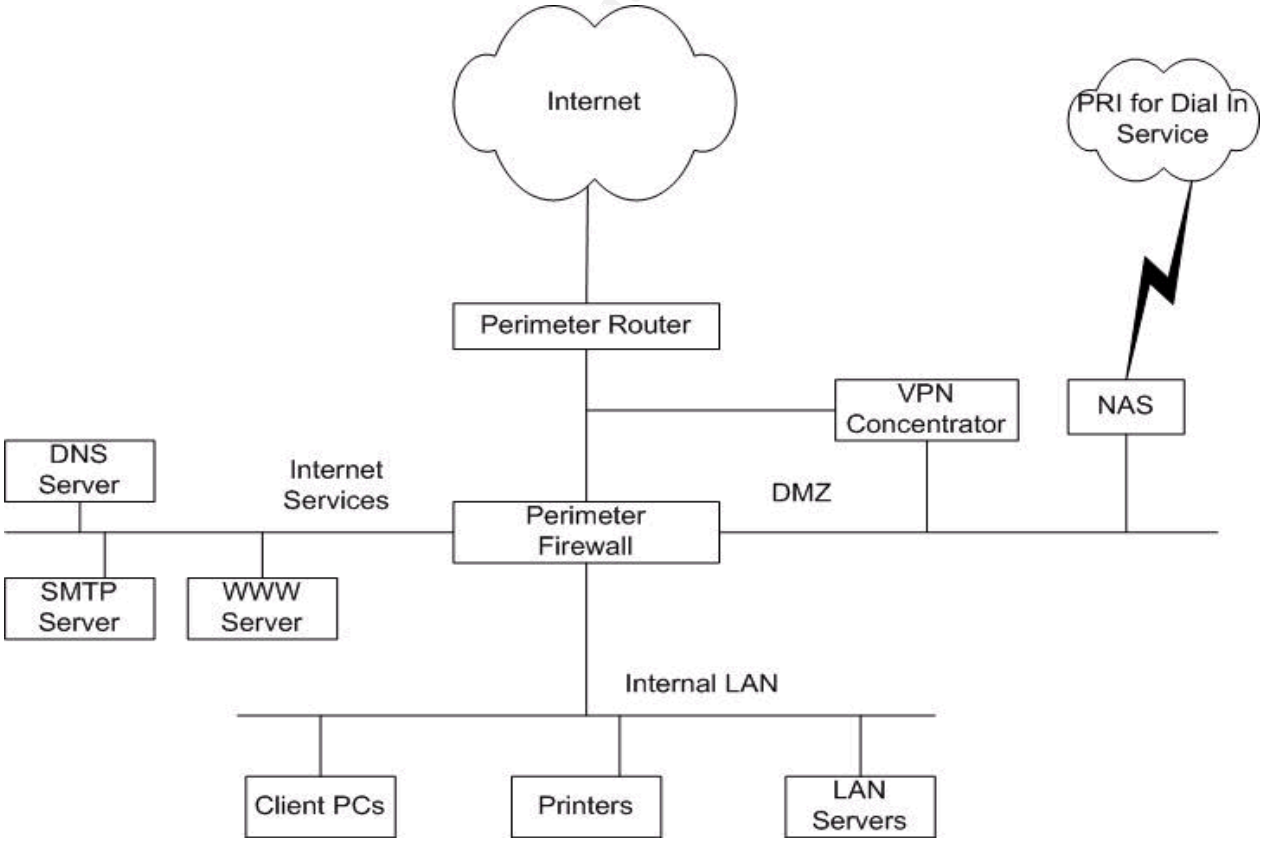
Assignment 1: Future State of Security Technology

1.1 Current Network Architecture

Assessing current security architectures is helpful in looking toward the future. The majority of networks today consist of at least one connection to the Internet and an Internal LAN segment for clients and servers. The connection to the Internet comes through a perimeter router and most likely at least one perimeter firewall. Then there is the LAN segment that is behind, or inside the firewall. There often is also an area between the perimeter router and inside LAN that is called a DMZ, or Internet Services, area that is designed for servers that are accessed from the Internet.

Also, incoming VPN or RAS connections are dropped off on this segment, so the traffic must pass through a firewall to reach the inside LAN. Figure 1 is a diagram of this typical configuration.

Figure 1: Current Network Design



While this is just an example of a typical design, there are many additional design options or components that can be deployed. For example, in more security oriented companies, there typically is some type of Network

Intrusion Detection (NIDS) or Prevention system in place. This would usually connect to the network between the perimeter router and firewall, as well as each additional segment that needed to be protected. In addition to a Network Intrusion system, there can be Host Intrusion Detection System (HIDS) that runs on individual servers. This will catch attacks against certain components of the host that would not be detected by a NIDS.

Another example of stronger designs is to implement internal firewalls, or multiple firewalls of different types. For example, a company could have an Application Layer Firewall at the perimeter protecting the Internet Services segment and have a Network Layer firewall controlling traffic inside the perimeter. This will provide additional security inside the perimeter and also allow deeper packet inspection going to the Internet accessible servers.

Even though this design has been relatively effective in the past, there are some concerns that should be addressed for the future.

1.2 Issues or Limitations of Current Architecture

The current network architecture is good at protecting traffic coming in from the Internet to the Internet Services segment and incoming VPN connections through the VPN concentrator. However, there is typically little control placed over the traffic inside the perimeter firewall. Once a device is connected to the Internal LAN, it usually can access every other device connected to the LAN with little or no restriction. If all of the corporate devices are always connected to the LAN, and have some type of personal firewall loaded, then this design is sufficient. Unfortunately, not many companies have that kind of control placed on each computer and there are laptop computers that pose a greater risk.

It is becoming increasingly convenient to connect any device to the Internet including home and company owned computers. Internet access is now available in most hotel rooms, shopping malls, coffee shops, and other public places. Corporate users easily can take their laptop computers and connect them to the Internet. In addition, most companies do not enforce their VPN policy to restrict users from connecting to the Corporate LAN from their home computer. Many of these home computers are constantly connected to the Internet via a cable or DSL line. This constant connection makes the computer vulnerable to Internet Trojans, worms, Spyware, or compromise.

Some companies have invested considerably in trying to protect corporate computers by purchasing client firewall software such as Sygate to control their assets at all times. With software such as this, a user can be restricted to only allow them to connect via VPN to the corporate network when they are off the LAN. To be effective, this policy would have to be put in place and not be disabled by the user. Also, this policy assumes that the client computer will always be allowed to connect using an IPSec VPN tunnel. If the computer is connected to another corporate network, or somewhere that has a firewall in place, they must have ports open for the IPSec VPN connection. This

is not always feasible and is rarely convenient. Also, this type of design places restrictions on the corporate network.

In the architecture mentioned above, the network is usually in one physical location due to the cost of building the network infrastructure. This design requires a connection to the Internet, Router, Firewall, Servers, Intrusion Detection, VPN, NAS, and switch connections. Even if a company chooses not to purchase all this equipment, but rather to host their servers at a leased data center, the systems are all still in one location and that brings up disaster recovery issues.

With a single data center design, disaster recovery must be considered and usually costs a considerable amount of money each year. One common option is to have a contract with a disaster recovery facility to provide the critical hardware needed by the company within a specified period of time in the event of a disaster. The company usually has the option to purchase their own equipment and have it at the disaster recovery facility for use in the event of a disaster. Either option is very expensive and is only an insurance policy. Frequently, this is never used. Due to these considerations, some companies have built a second data center in a remote location and are using that location for load balancing. Not only is there an expense in building out the data center, but also in establishing connectivity. A dedicated circuit is very expensive and a VPN tunnel over the Internet can have unreliable speeds.

These are just a few of the current limitations placed on corporate networks because of the technology available. The future of security technology will address these issues and make it feasible for any company to distribute their data center across the Internet.

1.3 Proposed Network Architecture

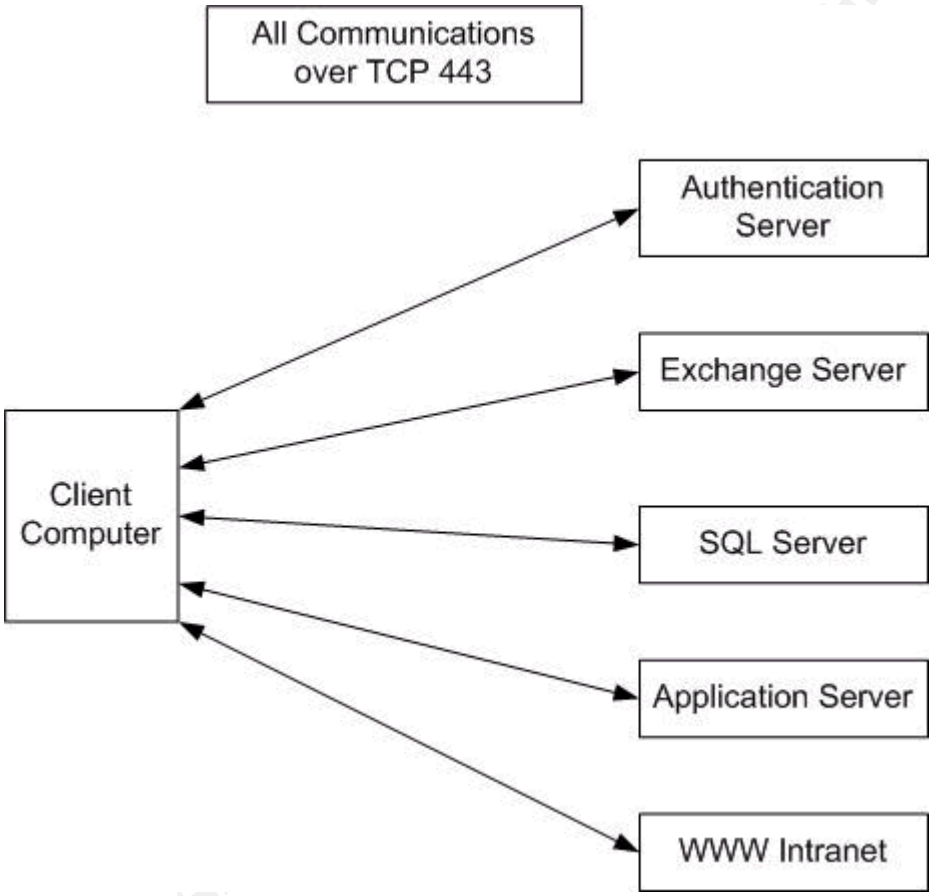
Imagine being able to take any corporate computer and connect it to the Internet from any location, having complete, secure, and seamless access to all devices on the corporate network. Also, imagine having a distributed data center across the state, United States, North America, or even the world. A corporate server could be placed anywhere on the Internet and could be securely available to all corporate users and other servers across the Internet. This could also be done without having to provision the server location with a Firewall, Domain Controller, VPN Concentrator, etc. The future of security technology is tearing down the great perimeters that have protected corporate networks for years and moving towards a decentralized, distributed approach to security.

With the new architecture, all laptops can be taken to any location including hotel rooms, shopping malls, home networks, other corporate networks, and connect securely to every corporate application without having a VPN client or concentrator and without having to write rules through corporate firewalls for IPSec connections for laptops to connect to an IPSec VPN. In addition to having complete mobility with corporate computers, the servers will be placed securely at any hosting location on the Internet without having to rely

on the hosting company to provide security. In Figure 2 below, a user's computer is connecting via port 443 to every server necessary for all client applications. The authentication server is necessary and the other servers are placed for illustration purposes.

While this seems like a pretty simple design, there are several components that need to be in place for these connections to be made securely.

Figure 2: Client SSL Communications



The following list contains components that need to be in place on the client computer. While some of these components are in production and available today, others are concepts that are not known to be available.

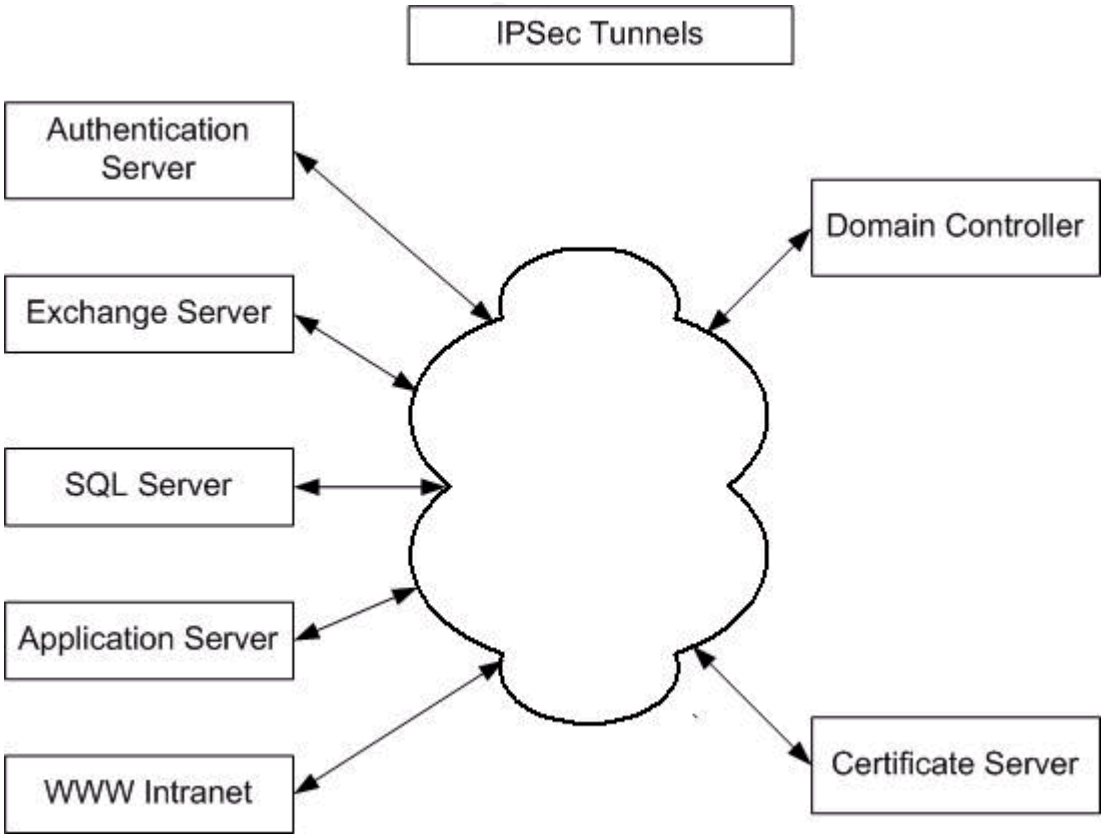
- Machine Certificate Issued by Corporate Certificate Server
- Process written in the Operating System boot procedures that authenticates the computer to Corporate Network prior to login

- Proprietary algorithm database using timed synchronization similar to RSA SecurID, except that it is not two-factor authentication. This database will be present on every corporate computer.
- Two factor authentication used for user login (hardware token a.k.a. key fob)
- Shim in Operating System TCP/IP stack that creates a connection table for each outgoing request and tunnels each request through TCP port 443
- Stateful firewall running at the network layer on the client computer that only allows return traffic that has a connection in the connection table. This is technology that is readily available in Microsoft Windows 2003.[1]

The client will continue to need Antivirus software loaded, as well as client software needed for business applications. The network shim on the client needs to be able to receive client side application requests on any port, build an entry in the connection table, and tunnel the request to the appropriate server on port 443. A similar technology is available today in products such as Stunnel.[2] The proposed solution will use the client's machine certificate to encrypt all traffic back to the corporate servers.

The next part of this solution is the backend server communications as seen in Figure 3. This concept is using IPSec tunnels which are commonly used today for server to server communications.

Figure 3: Server IPSec Communications



The following is a list of components that need to be in place on each server for backend communication to take place.

- Machine Certificates issued by Corporate Certificate Server
- Proprietary algorithm database using timed synchronization similar to RSA SecurID, except that it is not two-factor authentication. This database will be present on every corporate computer
- Operating System that can allow for IPSec rules to be configured for the network adapter. (e.g. Microsoft Windows 2000 Server)
- Routing mechanism on server to send all "backend" server communications over network adapter configured for IPSec communications to other servers.
- Shim in Operating System TCP/IP stack that encrypts outgoing and decrypts incoming requests using corporate machine certificates

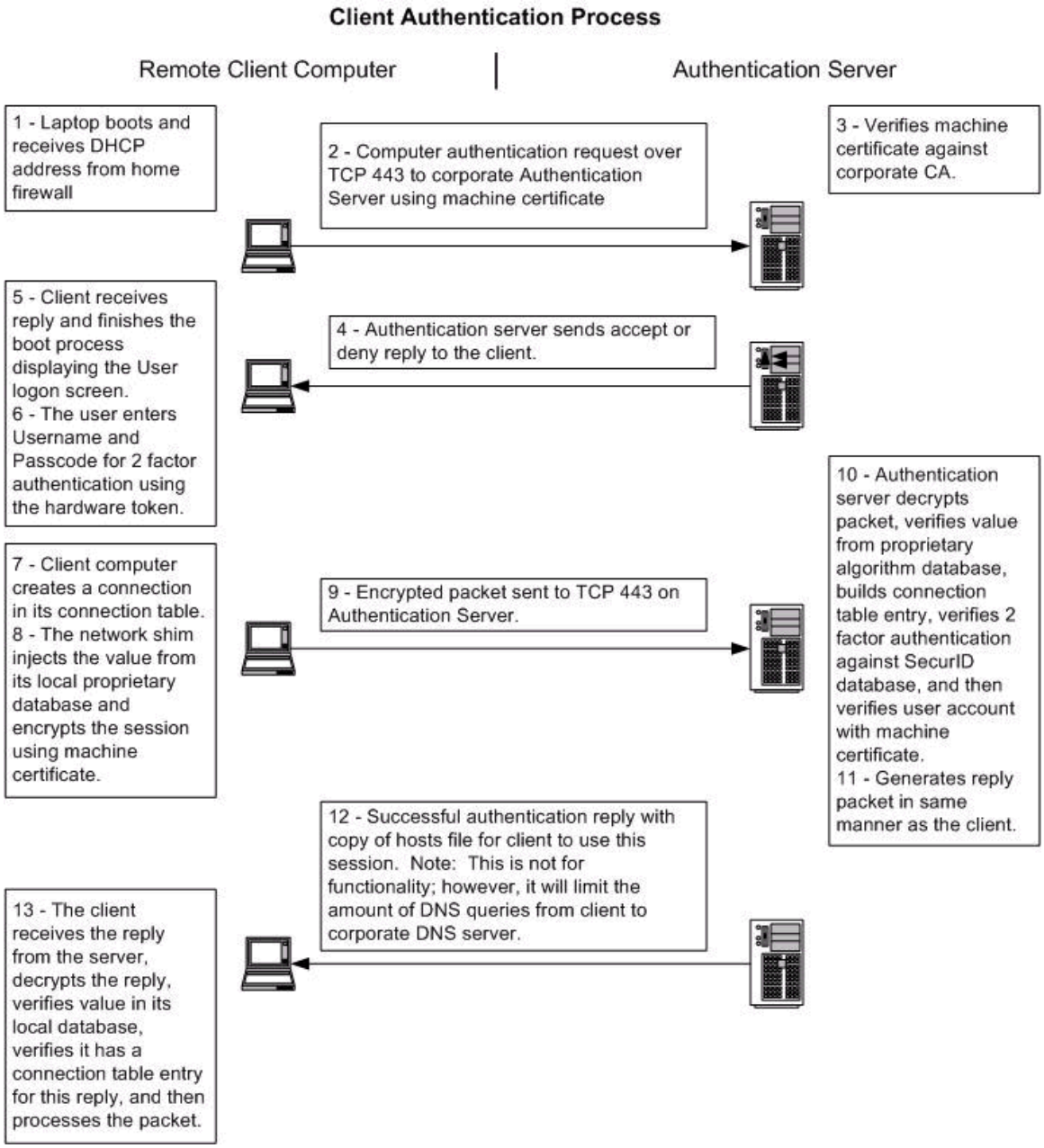
The Authentication server also will require:

- Two-factor authentication database that uses synchronized time (e.g. RSA SecurID)
- Updated hosts file to push to authenticated clients.

All IPSec communications are opened and terminated on the servers themselves; therefore, no need for firewalls or VPN concentrators to handle this traffic. If a server were located at a hosting facility that already had a firewall in place, the ports for IPSec would have to be opened to allow this communication.

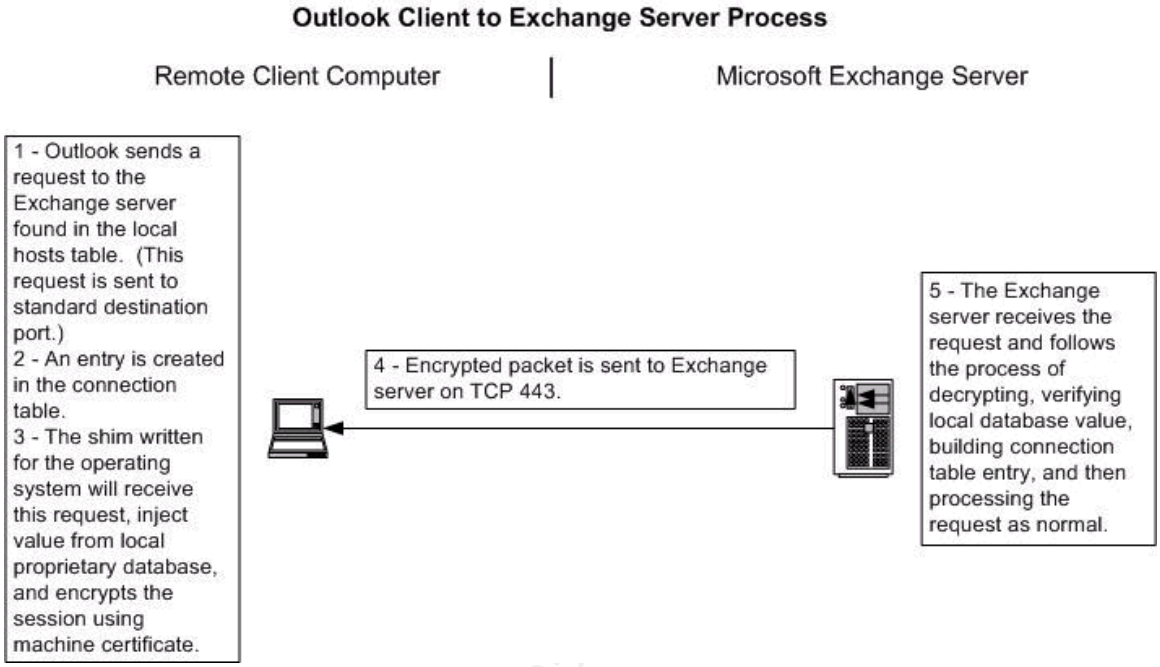
The following example in Figure 4 describes how the process works. In this example, we will use a corporate laptop connected to a home network behind a firewall that is connected to a Cable Modem.

Figure 4: Client Authentication Process



Now that the client has successfully logged on, the end user can launch any application as if it were on the Corporate LAN. For example, Figure 5 shows the user opening Microsoft Outlook to check email.

Figure 5: Client/Server Process



This process will continue for the entire session from the client. Since the shim on the client will accept any port and build a connection table entry for each packet, any client software application will work.

Figure 6 below, will help define the network architecture to support this design. To keep it simple, DNS names and zones will be used instead of IP addresses. All DNS names will be assigned to a registered IP address on the Internet. For example, company XYZ has three zones for client, server to server, and public.

Figure 6: Server DNS Names

Server Type	Client	Server to Server	Public Entry
Authentication	Auth1.client.xyz.com	Auth1.server.xyz.com	
Domain Controller	Dc1.client.xyz.com	Dc1.server.xyz.com	
Exchange	Email.client.xyz.com	Email.server.xyz.com	
SQL	Db.client.xyz.com	Db.server.xyz.com	
Application 1	App1.client.xyz.com	App1.server.xyz.com	
Intranet	Intranet.client.xyz.com	Intranet.server.xyz.com	
Certificate		Cert.server.xyz.com	
WWW Public		Web.server.xyz.com	www.xyz.com

SMTP Gateway		Smtp.server.xyz.com	Mx record for xyz.com
DNS Public		Name.server.xyz.com	Name.xyz.com

This table covers some basic servers that are deployed in most networks today. Each server is multi-homed, and one network card is dedicated to "inter server" communications. The other card accepts requests from either corporate clients, or clients on the Internet. If the second adapter is receiving requests from corporate clients, then it must be configured to verify all packets against local proprietary database.

The servers that must be able to communicate with any computer on the internet require additional security that is commonly deployed today. For example, the servers should be protected by an Application Layer firewall, Network Intrusion Detection System, or Host Intrusion Detection System. This will allow them to communicate and provide the same level of protection they have today.

1.4 Technical Issues of Proposed Architecture

This proposed architecture will provide companies with full control over every corporate computer and flexibility with housing corporate servers. There are some technical issues that need to be addressed for this design to be successful. First, there is the local proprietary database.

In the previous example, RSA SecurID product was used for two-factor authentication from the client to the Authentication server. A similar database that is used by RSA would have to be developed for this solution. This database would have to be encrypted on each local computer so it could not be tampered with or reverse engineered. Also, this database must be very time sensitive and would require that each device on the corporate network be synchronized to a reliable time source. The next technical hurdle is the shim for the TCP/IP stack of each device.

There are technologies available today that will somewhat achieve this effect. A similar process needs to be incorporated into the operating system so that every request from a client application can be encrypted and sent via SSL to its destination. Only if it is written at this level, will every application be supported. Finally, there will be issues with performance.

To have every computer handle this amount of encryption is going to require some type of additional resources. This could be done with some type of encryption card in the computer, or by using additional processor cycles. This is definitely technology that is available today for many vendors that have added encryption to their networking components. These components frequently have the option of adding an additional card to offload encryption.

These technical concerns, while valid, should not be difficult to overcome if the networking and security community will support the concept.

Assignment 2: Security Architecture

2.1 Overview of GIAC Business Operations

GIAC Enterprises business operations revolve around a set of SQL database clusters. The first database cluster is called SQLPROD and is the Production SQL database that provides fortune cooking sayings for customers and partners. The second database cluster is called SQLDEV and is the staging database for SQLPROD. All database updates to SQLPROD must come from SQLDEV. Since these two servers are the heart of GIAC, they are well protected by firewalls, Network Intrusion Detection, and various other components that help achieve defense in depth. Instead of risking customers directly accessing the fortunes database, GIAC provides a web server front end which is accessible from the Internet.

2.2 Details of Connections to GIAC Enterprises

2.2.1 Customers

The customers of GIAC enterprises connect to the web server to purchase online fortune cookie sayings. The initial connection is unencrypted; however, once the customer chooses to "login" from the main web page, they are redirected to an SSL encrypted page. At this point, if it is a new user, they are required to fill in the appropriate fields to setup a user account and password on the system. The user is also required to setup a default method of payment which can include a credit card or a direct bill service. If it is a direct bill, then the user must wait for a confirmation email saying their credit is approved. GIAC runs a credit report on the user/company to verify they are a not a credit risk. If the user chooses to pay by credit card, then they are redirected to an order screen where they can immediately purchase and download fortune cookie sayings.

Customers also have the option of a monthly service plan. If a customer subscribes to this plan, then the predefined amount of fortune cookie sayings will be automatically available to them via the secured website. Once the user logs in, the sayings are available for download over the SSL session. This method will be either billed directly to them, or to their credit card on a monthly basis. This is the preferred method for GIAC due to the ability to project revenue.

The online user accounts for customers are stored on the RSA/ACE server as local users. Authentication requests using these accounts are sent from the web server to the Ace server. Figure 7 shows access requirements from customers to GIAC.

Figure 7: Customer Connections to GIAC

Source	Destination	Port(s)/Protocols	Description

Any IP	GIAC Web Server	80/TCP – HTTP	Initial connection to GIAC's website
Any IP	GIAC Web Server	443/TCP – SSL	Secure Web Pages

2.2.2 Suppliers

GIAC currently receives its fortune cookie sayings from Unlimited Fortunes in Boston, MA. GIAC signs an annual agreement that estimates the amount of expected fortune purchases and a quarterly bill is sent based on fortunes received. There is a VPN to VPN tunnel between GIAC Enterprises and Unlimited Fortunes. All traffic between these two organizations is sent over this encrypted VPN tunnel. The traffic in this tunnel is originated from GIAC to Unlimited Fortunes and the tunnel is opened only when traffic is present. GIAC has a SQL download that is performed when the number of unused fortunes reaches 10 percent. This download is performed by the Staging SQL cluster and the data is immediately saved to the database. Once the data is confirmed to be valid, it is then replicated to the Production SQL cluster. This process ensures data integrity and helps protect against database corruption. Details of connection requirements are shown in Figure 8.

Figure 8: Supplier Connections to GIAC

Source	Destination	Port(s)/Protocols	Description
GIAC VPN	Supplier VPN	500/UDP – ISAKMP	Tunnel Negotiations for VPN Connection
GIAC VPN	Supplier VPN	IP 50 – ESP	Encrypted traffic between VPN concentrators
GIAC Staging SQL Cluster	Supplier SQL Database	1433/TCP – SQL	Download of Fortunes through VPN Tunnel

2.2.3 Partners

The two partner companies are Fortunes of Germany and English Fortunes. These companies both connect to GIAC via a VPN to VPN tunnel. GIAC has configured the Cisco VPN concentrator with a group named Partners and has put the remote VPN devices in this group. Although this tunnel is always up, only partner VPN IP addresses are allowed to come through the VPN concentrator. Also, this traffic can only go to the Production SQL cluster for SQL downloads. Each partner has signed an agreement stating they will pay for each downloaded fortune from their source IP address. This procedure is in place to give a financial interest to each partner company to keep their network and hosts secure. Partner connection requirements are listed in Figure 9 below.

Figure 9: Partner Connections to GIAC

Source	Destination	Port(s)/Protocols	Description
Partner VPN – (Both Partners)	GIAC VPN	500/UDP – ISAKMP	Tunnel Negotiations for VPN Connection
Partner VPN – (Both Partners)	GIAC VPN	IP 50 – ESP	Encrypted traffic between VPN concentrators
Partner SQL Client (Both Partners)	GIAC Production SQL Cluster	1433/TCP – SQL	Download of fortunes through VPN Tunnel

2.2.4 GIAC Enterprise Employees – Internal Network

GIAC Enterprise's business model places emphasis on minimal staff being on location at the headquarters building in Newark, De and the four regional offices. The main purpose of this is to keep office overhead at a minimum, as well as providing mobility for disaster recovery or office relocation. Therefore, only about ten employees total are in the office on a daily basis. These employees include Human Resources, Finance, Management and few Information Technology staff.

The regional offices are connected via a VPN to VPN tunnel over the Internet. Each regional office has a Cisco Pix firewall which is the VPN endpoint for the remote office. Only the headquarters office has servers and the remote offices connect back to the headquarters office for email, files, and Internet access. The tunnel to the remote office is always up; however, these employees must pass through the Sygate Gateway Enforcer to access all services on the network. Figure 10 shows all Internal LAN access requirements for users.

Figure 10: LAN Employee Connection Requirements

Source	Destination	Port(s)/Protocols	Description
Remote Office Firewall/VPN Peer (4 Remote Offices)	GIAC HQ VPN Concentrator	500/UDP – ISAKMP	Tunnel Negotiations for VPN Connection
Remote Office Firewall/VPN Peer (4 Remote Offices)	GIAC HQ VPN Concentrator	IP 50 – ESP	Encrypted traffic between VPN concentrators

ISA Server	ANY	21, 22, 80, 443/TCP	Internet Traffic

2.2.5 GIAC Enterprise Mobile Employees – Remote Sales Force

The majority of GIAC's remote employees connect via VPN to the network at headquarters. All employees have this ability and are encouraged to work remotely when possible. All employees also have Dell laptops that are loaded with the Sygate client[3] and are assigned SecurID key fobs. When the remote clients connect in to the VPN server, they are authenticated via SecurID to the RSA/ACE server. Once they pass authentication, the Sygate enforcer ensures the client passes the security policy, and then they are permitted access to the internal network. If the Sygate client fails the security check, they are forwarded to the VPN Client Update VLAN (VLAN 9 in Figure 13) where they can download required updates. Once their computer is up to date, they are permitted access to network resources. Each Sygate client has personal firewall running which contains filters to only allow connections to approved servers.

Figure 11: Remote Employee Connections to GIAC

Source	Destination	Port(s)/Protocols	Description
Any	GIAC VPN	500/UDP – ISAKMP	Tunnel Negotiations for VPN Connection
Any	GIAC VPN	IP 50 – ESP	Encrypted traffic from VPN client to VPN Concentrator
Any	GIAC VPN	UDP 4500	Nat Traversal[4]
Any	GIAC VPN	UDP 10000	IPSec Through NAT

2.2.6 The General Public

The general public is permitted access to GIAC Enterprises website that is hosted on the WWW server in the Internet services VLAN. From this website they can get information on GIAC's business plan, how to become a customer or partner, and the annual statement. Other information such as contact information and open employment opportunities are also available on the public website.

GIAC also hosts its own DNS records for both the website and mail server with a secondary DNS being located at GIAC's ISP. All queries are

permitted to the DNS server for this purpose. All inbound and outbound mail must pass through the SMTP gateway that is on the Internet Services VLAN. This keeps limited IP addresses from unnecessarily accessing the Internet. Connection requirements for the general public are provided below in Figure 12.

Figure 12: General Public Connections to GIAC

Source	Destination	Port(s)/Protocols	Description
Any	GIAC Public Web Server	80/TCP – HTTP	Access to website for general information about GIAC
Any	GIAC DNS Server	53/UDP – DNS	DNS queries for giac.com domain
Any	GIAC SMTP Server	25/TCP – SMTP	Inbound mail for giac.com domain

2.3 Network Diagram

Figure 11 is the network diagram for GIAC's corporate network. Included in the diagram are servers located at the headquarters' data center, and a network map including all VLANs defined in GIAC's switches. Each VLAN has an associated router port defined and access-list applied to help control traffic flow. Also, the second domain controller is located on the same VLAN as the SQL clusters to provide domain services locally and allow more restrictive rules on the VLAN access-list.

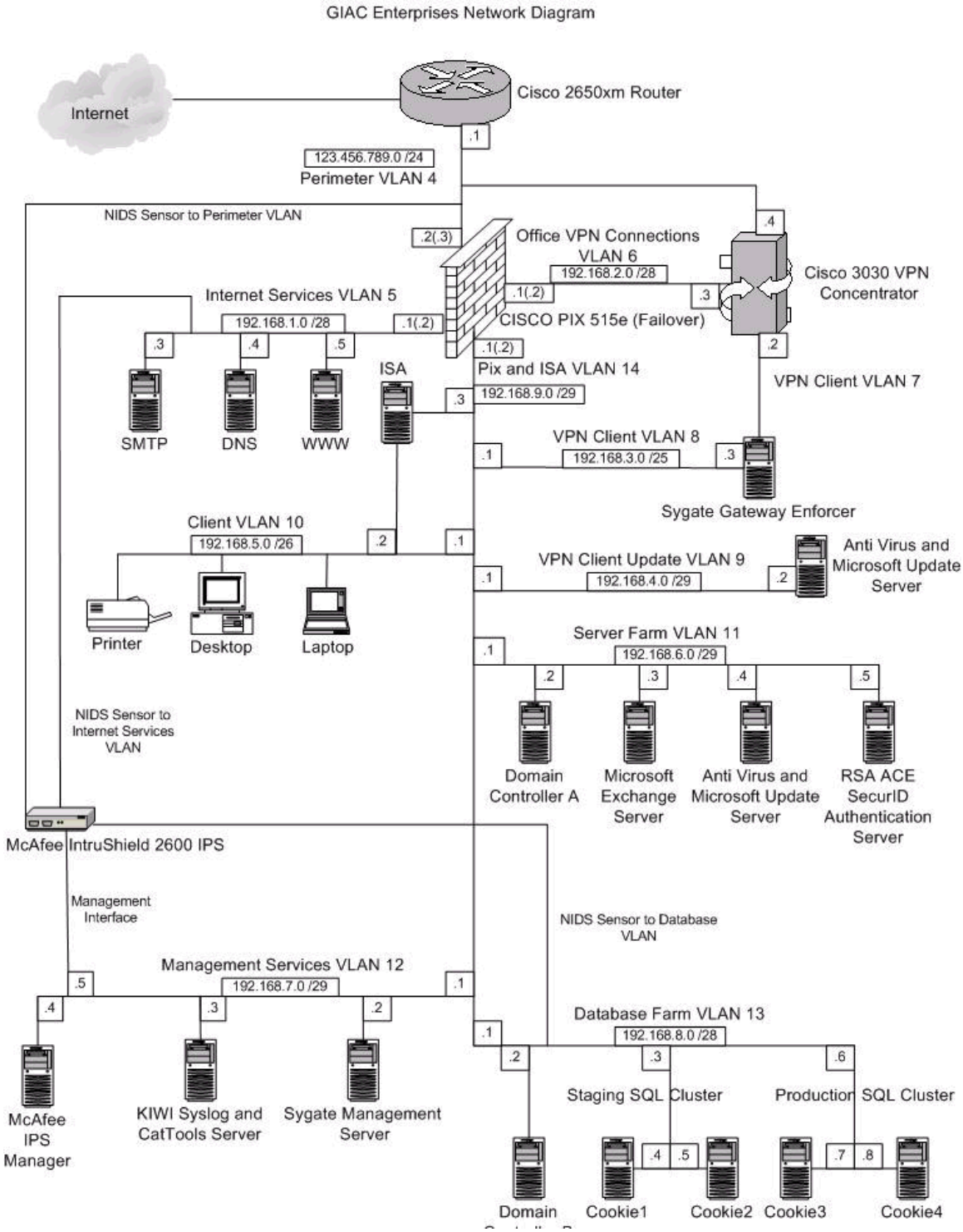


Figure 13: GIAC Enterprises Network Diagram

2.4 IP Address Table

GIAC Enterprises has a registered class C subnet mask assigned to them from their Internet provider for the headquarters office, and reserved public addresses for each remote office. RFC 1918 addresses are used inside of the firewalls at headquarters and each remote office. Each remote office has a registered IP address assigned to them for their firewall. The table shown in Figure 15 illustrates GIAC's registered IP addresses in use and the registered addresses relevant to GIAC. The complete IP address table can be found in Appendix A.

Figure 14: GIAC IP Address Table

Office Location	Network Device	IP Address	Subnet Mask
Headquarters	Perimeter Router	123.456.789.1	255.255.255.0
	Firewall (Primary) Outside Interface	123.456.789.2	255.255.255.0
	Firewall (Secondary) Outside Interface	123.456.789.3	255.255.255.0
	VPN Concentrator Outside Interface	123.456.789.4	255.255.255.0
	SMTP Gateway	123.456.789.5	255.255.255.0
	DNS Server	123.456.789.6	255.255.255.0
	WWW Server	123.456.789.7	255.255.255.0
	Kiwi Syslog	123.456.789.8	255.255.255.0
	ISA Server	123.456.789.9	255.255.255.0
Unlimited Fortunes (Supplier)	VPN Server	1.2.3.4	255.255.255.255
Fortunes of Germany (Partner)	VPN Server	1.2.3.5	255.255.255.252
English Fortunes (Partner)	VPN Server	1.2.3.6	255.255.255.252
GIAC Remote Office 1	VPN Server	1.2.3.7	255.255.255.252
GIAC Remote Office 2	VPN Server	1.2.3.8	255.255.255.252
GIAC Remote Office 3	VPN Server	1.2.3.9	255.255.255.252
GIAC Remote Office 4	VPN Server	1.2.3.10	255.255.255.252

2.5 Defense In Depth

GIAC Enterprises practices the concept of Defense in Depth by leveraging the strengths of each network device and mitigating the weaknesses of each with their location in the network. The perimeter router is the first line of defense which is followed by the VPN concentrator and firewall. The core switch leverages VLANs with router ports and access lists to control traffic inside the perimeter. In addition, the Network Intrusion Detection system monitors traffic at key points in the entire network. Finally, each host has some type of packet filters or host firewall to protect it against unauthorized packets. This concept of defense in depth is detailed further in the following section.

2.5.1 Filtering Router

The perimeter router at GIAC's headquarters is a Cisco 2650xm[5] with a serial connection to the Internet provider supporting a T3 line. The purpose of this device is to provide reliable network routing and support some packet filtering. The Internet connection has an ingress access list that performs filtering of incoming traffic from the Internet and an egress access list to filter outbound traffic. The purpose of the egress access list is to limit the amount of traffic on the segment outside the perimeter firewall and VPN concentrator. The strength of the perimeter router is that it is able to restrict some traffic at a general level, while permitting all other traffic to GIAC's firewall. Also, the Cisco routers can be hardened to allow them to sit securely at the Internet border. The weakness of the perimeter router is that it does not perform deep packet inspection and only restricts at layer 3 of the OSI model. This weakness is mitigated by having a stateful firewall and a network intrusion detection sensor between the router and inside network.

2.5.2 Firewall

The firewall chosen by GIAC's administrator is a Cisco Pix 515e failover bundle.[6] One reason this firewall was chosen is that it has a proven record of great performance and reliability. The security function of the perimeter firewall is that it restricts all traffic coming and going from GIAC's corporate network. The firewall also restricts traffic coming in over the VPN concentrator from the supplier's and partners' networks. The main security strength of the Pix is that it performs stateful packet inspection and builds a connection table entry for each connection through it in any direction. A return packet will only be allowed to pass from one interface to another if there is a connection table entry for the previous packet in the conversation. The firewall controls all perimeter traffic coming in and out of the Internet Services, VPN, and internal LAN segments.

The security weakness of the Pix firewall is that it only inspects packets at the Transport Layer of the OSI model. This firewall will not detect an attack at the upper layers of the OSI model as an Application Layer firewall would. This weakness is mitigated by implementing Defense in Depth and deploying a

Network Intrusion Detection System.

2.5.3 Network Intrusion Detection System

The Network Intrusion Detection System (NIDS) chosen by GIAC is McAfee IntruShield 2600 IPS.[7] Although this device can be configured in line to be an Intrusion Prevention System, GIAC has it implemented to monitor and alert the Administrator in the event of possible attack. This is due to the lack of trust in general to Intrusion Prevention systems and the fear of false positives terminating a valid session. This viewpoint may change over time if the amount of false positives is minimal and the potential for attack is greater than risk of killing a valid session. The security function of this device is to provide Application layer inspection at key hotspots of the GIAC network. These hotspots are at the perimeter, in the Internet Services segment, and in the Database VLAN. Again, the traffic in two of these segments will have passed through the Pix firewall and therefore will have gone through some type of packet inspection.

The weakness of the NIDS is that it cannot be on every device in the network. This device is designed to monitor a great deal of traffic and provide alerting or other action if a detection is noticed; however, there will still be traffic on the GIAC LAN that will not pass through this sensor. The implementation of defense in depth handles this weakness by utilizing some type of host firewall or packet filters on every device connected to the network. Although GIAC has used Cisco for all other Network devices, they wanted to leverage a different vendor for the NIDS to implement the policy of security by diversity. If a vulnerability were to be reported in Cisco Products, the NIDS would not be susceptible to this and would still provide protection.

2.5.4 VPN

The VPN device selected by GIAC is the Cisco 3030 VPN Concentrator.[8] The performance of the VPN concentrator was a major concern since the core of GIAC's business occurs over this connection. This device would handle all traffic to and from the Supplier, Partners, Remote Office, and employees that were out of the office. The security function this device provides is that it must handle encryption and decryption of all VPN traffic to GIAC. Also, it must support putting users into groups, assigning reserved IP addresses, and implementing access lists to restrict where the users are allowed to go on the network. In addition, this device must be able to authenticate some users using ACE SecurID two-factor authentication. Finally, this device can also be hardened to stand facing the Internet with only the IPSec ports open on the outside interface.

The security weakness of this component is that it also will not do stateful packet inspection. Again, the implementation of GIAC's Defense in Depth requires non trusted connections over this VPN device to also pass through the

Pix firewall prior to connection to any devices on GIAC's corporate network.

2.5.5 Additional components

The additional components in use by GIAC for security are Sygate Secure Enterprise, Symantec AntiVirus, Microsoft's ISA Server, VLANs with access lists on the Cisco switches, Kiwi Syslog and Kiwi CatTools. The most critical of these components is the Sygate Secure Enterprise solution.

Sygate Secure Enterprise

Sygate runs on every client machine owned by GIAC enterprises. Each laptop has a set of policies that provides restrictions based on the DHCP server that issued the client an IP Address. If the DHCP server is not GIAC's, then the clients can only connect to GIAC's VPN server. This keeps users from surfing the web, or connecting to other networks which would potentially put their computer at risk by being unprotected on a foreign network or the Internet. In addition, this client is a personal firewall on the computer and will protect each computer from any other device initiating inbound connections, as well as the computer making unauthorized outbound connections. This is critical since GIAC does most of its work remotely and has users connecting to the Internet all over the world. Also, this policy applies to the users in remote offices. The VPN tunnel is always up, but the VPN policy on the Cisco concentrator forces them to pass through the Sygate Gateway Enforcer and meet the security policy before connecting to the LAN.

The Sygate Gateway Enforcer is a bridge device that intercepts all packets at layer 2 and requires them to pass through the security policy before proceeding to the next hop. If a client does not pass the security policy because of a security update or Antivirus update needed, then Sygate will permit them to access the server in the VPN Client Update VLAN only. Once the client has updated its security requirements, it will be permitted access to GIAC's network. GIAC also implements policies to the client firewall upon successful completion of the security attributes. The clients are only permitted access to the Server Farm (VLAN 11), the production SQL database (VLAN 13), and the ISA server (VLAN 10). This policy is also enforced on the access list applied to VLAN 8 which is the VPN client VLAN.

Symantec AntiVirus Corporate Edition

GIAC also uses Symantec AntiVirus[9] for all clients and servers in the Enterprise. Symantec has a reputation of being quick with antivirus updates and it works well with the Sygate client. Also, having an enterprise implementation of Symantec allows for strict policy control over installing, managing, and updating each client.

Microsoft ISA Server

The next component that enforces defense in depth is Microsoft ISA server for outbound Internet Access. Every device inside the firewall, including clients at remote offices and VPN clients, are configured to connect to the Internet through this ISA server. This allows for very granular firewall rules and prevents multiple devices from connecting directly to the internet. This server is also running Burst Technologies bt-WebFilter[10] software to enforce corporate policy regarding acceptable Internet use. The outside interface of the ISA server is in a VLAN with only the Inside interfaces of the firewall. This further contains traffic from the Internet by leveraging access lists on the inside switches.

Cisco Switches with Trunked VLANs and Access-lists

GIAC's implementation of defense in depth also includes the use of VLANs and access lists on all switches. Although traffic can be controlled here, the switches are not going to provide the same functionality as a firewall and are only in place to provide general traffic filtering. The access lists on each VLAN provide general permit rules and then a deny all. The network administrator has provided all necessary traffic permission to go through the VLANs and logs all denied traffic. This will alert him to any unusual traffic from either a rogue network attached device, or a malicious user.

Kiwi Syslogd and CatTools

GIAC uses KIWI Syslog daemon[11] to receive logs and alert on events from the router, firewall, and switches. Also, GIAC uses KIWI CatTools[12] to periodically perform configuration backups of all network devices.

These items all have strengths and weaknesses, but together they form a solid network architecture. GIAC has realized that it's workforce is mostly mobile, or not in the corporate office and therefore must have control at the machine level. Also, GIAC has tried to keep the cost at a manageable level and not over complicate the network architecture unless necessary.

Assignment 3: Router and Firewall Policies

3.1 Router and Firewall Policies

The perimeter router is the first line of defense for GIAC Enterprises network. The security function of this device is to only allow valid traffic based on source and destination IP address and port. The ingress acl, which is on the Internet connection, blocks the most commonly used ports for viruses and worms. Also, this acl denies any traffic that is known to be invalid and permits only valid traffic to GIAC's network. The egress acl is on the port coming from GIAC's network and is in place to prevent any known invalid traffic from leaving the network. This acl also restricts the most commonly used ports from viruses and worms as part of GIAC's due diligence to protect the Internet in case their own computers get compromised. This is the last line of defense for outbound traffic and should have minimal hits. Since the default policy of the router is to permit IP traffic, these access lists need to be periodically updated with any deny rules based on information about malicious traffic on the Internet. One source used is SANS Internet Storm Center found at http://isc.sans.org/ .

The firewall policy is very similar to the router and is the second line of defense for inbound traffic from the Internet. The firewall also restricts outbound connections from LAN devices to prevent any unauthorized connections to the Internet or through VPN tunnel. Since the default policy of the firewall is to deny all IP traffic, the access lists are only changed when a new service is needed inbound or outbound. Since the firewall provides deep packet inspection, it is a critical device in GIAC's implementation of Defense in Depth.

3.2 Router Configuration

3.2.1 Ingress ACL

Source	Destination	Port/Protocol	Action	Description
Any	Any	1433/TCP	Deny	SQL connections
Any	Any	445/TCP	Deny	MS Directory Service Connections
Any	Any	137-139/ TCP & UDP	Deny	NetBIOS Services
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Any	Any	Deny	RFC 1918 Source Address
224.0.0.0/8	Any	Any	Deny	Multicast Source Address

123.456.789.0/24	Any	Any	Deny	GIAC as Source Address
Any	123.456.789.5	25/TCP	Permit	Inbound Email
Any	123.456.789.6	53/TCP & UDP	Permit	Inbound DNS queries
Any	123.456.789.7	80/TCP	Permit	Inbound http queries
Any	123.456.789.7	443/TCP	Permit	Inbound https queries
Any	123.456.789.9	TCP Established	Permit	Return traffic originating from ISA Server
Any	123.456.789.4	500/UDP	Permit	ISAKMP to VPN
Any	123.456.789.4	IP 50	Permit	ESP to VPN
Any	123.456.789.4	4500/UDP	Permit	Nat Traversal
Any	123.456.789.4	10000/UDP	Permit	IPSec Through NAT
Any	Any	Any	Deny	Deny All

3.2.2 Egress ACL

Source	Destination	Port/Protocol	Action	Description
Any	Any	1433/TCP	Deny	Outbound SQL Connections
Any	Any	445/TCP	Deny	Microsoft DS
Any	Any	137-139/ TCP & UDP	Deny	NetBIOS Services
10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Any	Any	Deny	RFC 1918 Source Address
224.0.0.0/8	Any	Any	Deny	Multicast Source Address
123.456.789.4	Any	500/UDP	Permit	ISAKMP from VPN
123.456.789.5	Any	25/TCP	Permit	Outbound Email
123.456.789.6	Any	53/UDP & TCP	Permit	DNS queries outbound
123.456.789.7	Any	Source Port 80/TCP Established	Permit	Return http traffic from Web Server

123.456.789.7	Any	Source Port 443/TCP Established	Permit	Return https traffic from Web Server
123.456.789.9	Any	20, 21, 22, 80, 443/TCP	Permit	Outbound traffic from ISA server
123.456.789.4	Any	IP 50	Permit	ESP from VPN
123.456.789.4	Any	4500/UDP	Permit	Nat Traversal
123.456.789.4	Any	10000/UDP	Permit	IPSec through NAT
Any	Any	Any	Deny	Deny All

3.2.3 Order of rules for Router

The order of rules on both access lists is important since they are parsed from the top to the bottom. The ingress access list, which is from the Internet, begins with a series of denies for common ports used by viruses, worms, and malicious attacks. Then there are rules denying traffic with invalid source addresses. The next series of rules are permitting valid traffic to the servers in the Internet Services VLAN. The next rule allows all traffic that originated from the LAN ISA server to return; however, it will not allow connections to be initiated from the Internet to the ISA server. The next few rules are to allow traffic to the VPN concentrator, and finally the last rule denies all other traffic.

The egress access list is very similar to the ingress access list. The first set of rules denies commonly used ports for viruses, worms, etc. The next series of rules denies traffic with an invalid source IP address. Then there are rules allowing valid traffic from the Internet services VLAN and the ISA server from the LAN. Finally, there are rules allowing VPN traffic from the concentrator and then a rule that denies all other traffic.

3.3 Firewall Configuration

3.3.1 Outside Interface ACL

Source	Destination	Port/Protocol	Action	Description
Any	123.456.789.5	25/TCP	Permit	Inbound Email
Any	123.456.789.6	53/TCP 53/UDP	Permit	Inbound DNS Queries
Any	123.456.789.7	80/TCP	Permit	HTTP to Web Server
Any	123.456.789.7	443/TCP	Permit	HTTPS to Web Server

123.456.789.1	123.456.789.8	514/UDP	Permit	Router Syslog to Kiwi

3.3.2 Internet Service ACL

Source	Destination	Port/Protocol	Action	Description
192.168.1.3	Any	25/TCP	Permit	Email
192.168.1.4	Any	53/TCP & UDP	Permit	DNS Queries
192.168.1.5	192.168.6.5	5500/UDP	Permit	Authentication request to ACE Server
192.168.1.5	192.168.8.6	1433/TCP	Permit	SQL Queries to Production Cluster
192.168.1.0/28	192.168.6.4	2967/UDP 38293/UDP	Permit	Symantec AntiVirus[13]

3.3.3 VPN ACL

Source	Destination	Protocol	Action	Description
192.168.2.3	192.168.6.5	UDP 5500	Permit	ACE Authentication Request
192.168.2.4-7	192.168.8.6	TCP 1433	Permit	Partner Access to Production SQL Cluster

3.3.4 Inside ACL

Source	Destination	Protocol	Action	Description
192.168.6.3	192.168.1.3	TCP 25	Permit	Outbound Email
192.168.9.3	192.168.1.4	53/UDP & TCP	Permit	DNS queries for Internet Access
192.168.6.2	192.168.1.4	53/UDP & TCP	Permit	DNS forwarding from LAN DNS Server

192.168.9.3	Any	TCP 21, 22, 80, 443	Permit	Outbound Traffic from ISA Server
192.168.8.3	10.10.10.10	TCP 1433	Permit	Staging SQL Cluster Updates through VPN to Supplier

3.3.5 Order of Rules for Firewall

The order of rules in the firewall is not significant since they are all permit rules with the implicit deny all at the end. GIAC arranges the firewall rules for readability, management, and performance purposes only. All access lists on the firewall start with any global, or "Any", rules and then proceed with predicted most hit rules. Finally, the last rules are generally those used for GIAC management or monitoring purposes.

Conclusion

GIAC Enterprises has invested considerably in providing a safe computing environment from the perimeter to the desktop. Although additional funds could have been spent procuring additional security equipment; however, GIAC management feels that by leveraging defense in depth their security stance is very strong.

Appendix A: Complete IP Address Table for GIAC Enterprises

Headquarters Network				
	Network Device	**IP Address**	**Subnet Mask**	**Translated / Public Address**
VLAN 4 – Perimeter	Perimeter Router Serial	1.2.3.2	255.255.255.252	
	Perimeter Router ethernet1	123.456.789.1	255.255.255.0	123.456.789.1
	Pix Firewall Primary ethernet0 (Outside)	123.456.789.2	255.255.255.0	123.456.789.2
	Pix Firewall ethernet0 (Outside)	123.456.789.3	255.255.255.0	123.456.789.3
	VPN Concentrator Outside	123.456.789.4	255.255.255.0	123.456.789.4
VLAN 5 – Internet Services	Pix Firewall Primary ethernet2	192.168.1.1	255.255.255.240	
	Pix Firewall Secondary ethernet2	192.168.1.2	255.255.255.240	
	SMTP Server	192.168.1.3	255.255.255.240	123.456.789.5
	DNS Server	192.168.1.4	255.255.255.240	123.456.789.6
	Web Server	192.168.1.5	255.255.255.240	123.456.789.7
VLAN 6 – Partner and Supplier VPN Connections	Pix Firewall Primary ethernet3	192.168.2.1	255.255.255.240	

	Pix Firewall Secondary ethernet3	192.168.2.2	255.255.255.240	
	VPN Concentrator Interface 2	192.168.2.3	255.255.255.240	
	Fortunes of Germany Clients	192.168.2.4 – 192.168.2.5	255.255.255.240	
	English Fortunes Clients	192.168.2.6 – 192.168.2.7	255.255.255.240	
	Staging SQL Cluster Outbound	192.168.2.11	255.255.255.240	
VLAN 7 and 8 – VPN Client Segment	Router port on core switch for VLAN 8	192.168.3.1	255.255.255.192	
	VPN Concentrator Interface 3	192.168.3.2	255.255.255.192	
	Sygate Enforcer Interface 2	192.168.3.3	255.255.255.192	
	VPN Client Pool	192.168.3.9 – 192.168.3.50	255.255.255.192	
VLAN 9 – VPN Client Updates	Router port on core switch for VLAN 9	192.168.4.1	255.255.255.248	
	AntiVirus and Microsoft Update Server	192.168.4.2	255.255.255.248	
VLAN 10 – Client VLAN	Router port on core switch for VLAN 10	192.168.5.1	255.255.255.192	

	ISA Server Interface 1	192.168.5.2	255.255.255.192	
	Reserved for Static IP	192.168.5.3 – 192.168.5.14	255.255.255.192	
	LAN Client DHCP Pool	192.168.5.15 – 192.168.5.30	255.255.255.192	
VLAN 11 – LAN Server Farm	Router port on core switch for VLAN 11	192.168.6.1	255.255.255.192	
	Domain Controller A	192.168.6.2	255.255.255.192	
	Exchange Server	192.168.6.3	255.255.255.192	
	AntiVirus and Microsoft Update Server	192.168.6.4	255.255.255.192	
	RSA ACE SecurID Authentication Server	192.168.6.5	255.255.255.192	
VLAN 12 – Management Services	Router port on core switch for VLAN 12	192.168.7.1	255.255.255.248	
	Sygate Management Server	192.168.7.2	255.255.255.248	
	Kiwi Syslog, CatTools, and Network Device Management Server	192.168.7.3	255.255.255.248	
	McAfee IPS Manager	192.168.7.4	255.255.255.248	

VLAN 13 – Database Farm	Router port on core switch for VLAN 13	192.168.8.1	255.255.255.240	
	Domain Controller B	192.168.8.2	255.255.255.240	
	Staging SQL Cluster IP	192.168.8.3	255.255.255.240	
	Staging SQL Server A	192.168.8.4	255.255.255.240	
	Staging SQL Server B	192.168.8.5	255.255.255.240	
	Production SQL Cluster IP	192.168.8.6	255.255.255.240	
	Production SQL Server A	192.168.8.7	255.255.255.240	
	Production SQL Server B	192.168.8.8	255.255.255.240	
VLAN 14	Pix Firewall Primary ethernet1 (Inside)	192.168.9.1	255.255.255.248	
	Pix Firewall Secondary ethernet1 (Inside)	192.168.9.2	255.255.255.248	
	ISA Server Outside Interface	192.168.9.3	255.255.255.248	

GIAC Remote Office 1				

	Network Device	**IP Address**	**Subnet Mask**	**Translated / Public Address**
	Pix Ethernet0 (Outside)	1.2.3.7	255.255.255.252	1.2.3.7
	Pix ethernet1 (Inside)	192.168.15.1	255.255.255.224	
	Client DHCP Pool	192.168.15.5 - 15	255.255.255.224	
GIAC Remote Office 2				
	Network Device	**IP Address**	**Subnet Mask**	**Translated / Public Address**
	Pix ethernet0 (Outside)	1.2.3.8	255.255.255.252	1.2.3.8
	Pix ethernet1 (Inside)	192.168.16.1	255.255.255.224	
	Client DHCP Pool	192.168.16.5 - 15	255.255.255.224	
GIAC Remote Office 3				
	Network Device	**IP Address**	**Subnet Mask**	**Translated / Public Address**
	Pix ethernet0 (Outside)	1.2.3.9	255.255.255.252	1.2.3.9
	Pix ethernet1 (Inside)	192.168.17.1	255.255.255.224	
	Client DHCP Pool	192.168.17.5 – 15	255.255.255.224	
GIAC Remote Office 4				
	Network Device	**IP Address**	**Subnet Mask**	**Translated / Public Address**
	Pix ethernet0 (Outside)	1.2.3.10	255.255.255.252	1.2.3.10
	Pix ethernet1 (Inside)	192.168.18.1	255.255.255.224	

	Client DHCP Pool	192.168.18.5 – 15	255.255.255.224	

Unlimited Fortunes (GIAC's Supplier)	VPN Remote Peer	1.2.3.4	255.255.255.255	1.2.3.4
Fortunes of Germany (Partner)	VPN Remote Peer	1.2.3.5	255.255.255.255	1.2.3.5
English Fortunes (Partner)	VPN Remote Peer	1.2.3.6	255.255.255.255	1.2.3.6

References

[1] "Securing your network with Basic Firewall. Windows Server 2003, Standard Edition." Microsoft Corporation, 2005. March 28, 2005. <http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/mpr_und_basicfw.asp>

[2] Hatch, Brian. "Stunnel – Universal SSL Wrapper." Stunnel Home Page. March 17, 2004. March 28, 2005. <http://www.stunnel.org/>

[3] Eng, Audra. "Sygate Secure Enterprise 4.0." Whitepaper. Sygate. July 2004. March 28, 2005. <http://www.sygate.com/solutions/datasheets/wp/WP-Sygate-Secure-Enterprise.pdf>

[4] "Cisco – Configuring NAT Transparent Mode for IPSec on the VPN 3000 Concentrator." Cisco Systems. March 2, 2004. March 28, 2005. <http://www.cisco.com/warp/public/471/nat_trans.html>

[5] "Cisco 2600 Series Modular Access Router [Cisco 2600 Series Multiservice Platforms]." Product Data Sheet. Cisco Systems. December 30, 2004. March 28, 2005. <http://www.cisco.com/en/US/products/hw/routers/ps259/products_data_sheet0900aecd800fa5be.html>

[6] "Cisco PIX 515E Security Appliance [Cisco PIX 500 Series Security Appliance] – Cisco Systems." Product Data Sheet. Cisco Systems. February 4, 2005. March 28, 2005. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080091b15.html>

[7] "McAfee IntruShield Network IPS Sensor." Data Sheet. McAfee Corporation. 2005. March 28, 2005. <http://www.mcafeesecurity.com/us/local_content/datasheets/ds_intrushield_ips_app.pdf>

[8] "Cisco VPN 3030 Concentrator – Cisco Systems." Cisco Systems. February 10, 2005. March 28, 2005. <http://www.cisco.com/en/US/products/hw/vpndevc/ps2284/ps2292/index.html>

[9] "Symantec AntiVirus Corporate Edition." Symantec Corporation. 2005. March 28, 2005. <http://enterprisesecurity.symantec.com/products/products.cfm?productid=155>

[10] "Burst Technology : btWebfilter – The Only Web Filtering Application that Blocks Spyware." Burst Technology, Inc. 2005. March 28, 2005. < http://www.burstek.com/products/btwebfilter.htm>

[11] "Syslog Daemon for Windows, Free Syslog Server, Firewall Logging, Kiwi Syslog Daemon." Kiwi Enterprises. August 24, 2004. March 28, 2005. < http://www.kiwisyslog.com/info_syslog.htm>

[12] "Free network configuration management tool – automate configuration backups and more with." Kiwi Enterprises. January 17, 2005. March 28, 2005. <http://www.kiwisyslog.com/cattools2.htm>

[13] "Ports used for communication in Symantec AntiVirus Corporate Edition 8.x and 9.x." Symantec Corporation. January 28, 2005. March 28, 2005. <http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002091816450048>