Global Information Assurance Certification Paper

GIAC Enterprises
Firewalls, Perimeter Protection and VPN's
Practical Assignment

Network Architecture Plan

Produced by: Brian Rickle
Group: Capital Sans 2000 Practical

Dates of Course: December 10 - 15, 2000
Date submitted: February 19, 2001

Introduction

This paper is my submission to complete the practical assignment given for the Capital SANS December 2000 GIAC level two Firewalls, Perimeter Protection and VPN course of study.

The practical exam is split up into four individual assignments. This paper will follow the same structure and address each of the assignments in the order they were given.

The assignment list is as follows:

- Assignment 1 - Security Architecture
- Assignment 2 - Security Policy
- Assignment 3 - Audit your Security Architecture
- Assignment 4 - Design under fire

The first three assignments will deal with a fictional company, GIAC Enterprises, which is a wholesale dealer of fortune cookie sayings. Directions for the fourth assignment include choosing a previously delivered practical exam and describing a method of attack against that security architecture. Details for each of these assignments will be given at the beginning of each section.

Assignment 1

Assignment 1 Details - Security Architecture

The details given for this part of the practical exam are as follows:

> Define a security architecture for GIAC Enterprises, a new Internet startup that expects to earn $200 million per year in online sales of fortune cookie sayings. Produce a diagram or set of diagrams with explanatory text that define how to use perimeter technologies to implement your security architecture.
>
> You must consider and define access for:
> - Customers (the companies that purchase bulk online fortunes);
> - Suppliers (the authors of fortune cookie sayings that connect to supply fortunes);
> - Partners (the international partners that translate and resell fortunes).
>
> Your architecture must specify filtering routers, firewalls, VPNs to partners, secure remote access, and internal firewalls. Be explicit about the brand and version of each perimeter defense component.

Assumptions

Given the sparse nature of the information given concerning GIAC Enterprises in the above assignment details, certain assumptions are going to be made for purposes of this paper. These assumptions include the following:

Customer Assumptions

- GIAC Enterprise customers will browse to the GIAC Enterprise web server using HTTP (Hypertext transport protocol) port 80 and when ready to order fortune cookie sayings will be switched to a secure web connection HTTPS port 443.

- Customers will have no other input capability other than input through a web form. The web development team designs this web form and the process has undergone a code review to provide assurance that the code on the machines is secure.

Supplier Assumptions

- Suppliers are the creative business resources that supply GIAC Enterprises with new fortune cookie sayings to add to the GIAC database.

- Suppliers could be other corporations or individual contributors.

- Any new sayings contributed will have to go through a quality control process before being added to the database. This process includes inspection for quality and appropriateness of

contribution. This process will also weed out any duplicate entries to the database.

- The database application has security built in to allow the suppliers to write to a small database of their own. It is this small database that quality assurance will look at and work with before any of the suppliers sayings are added to the GIAC Enterprises production database.

- Each supplier is provided with, and accepts, a written security policy agreement. In that agreement the suppliers rights and responsibilities for interaction with GIAC Enterprise systems are well defined.

Partner Assumptions

- The role of GIAC Enterprise partners is to translate sayings from the GIAC database and resell them to the partners customers.

- The database has security measures in place that protects GIAC by not allowing any partner to write into the database.

- The database application is written with enough intelligence to send the partners new sayings with each request. That is, the partner will not make more than one request and get the same fortune cookie sayings each time.

- Each partner is provided with, and accepts, a written security policy agreement. In that agreement the partners rights and responsibilities for interaction with GIAC Enterprise systems are well defined.

Remote Access Assumptions

- GIAC Enterprise employees may have need for remote connectivity to the corporate internal LAN (Local Area Network). Remote connectivity is provided for this purpose.

- Each employee is provided with, and accepts, a written security policy agreement. In that agreement the employee rights and responsibilities for interaction with GIAC Enterprise systems are well defined. This is a prerequisite for every employee whether they require remote access or not. This agreement must be finalized before a user account for the employee is created on the GIAC system.

GIAC Enterprises Assumptions

- GIAC Enterprises has credit acceptance procedures in place. These procedures have already been tested and secured. All confidential information from this process is stored within servers inside the corporate LAN structure.

- No confidential or sensitive information will be stored on the web server, or any other machine on the service network. (The service network will be defined in the section after this.)

- A full written corporate security policy will be in place. This includes distribution to all employees, partners and suppliers in addition to being accepted and agreed to by the CEO (Chief Executive Officer) and other members of the senior management team.

- GIAC has set up procedures for physical security of network components and servers. This includes environmental controls; fire protection and physical access restrictions.

- GIAC has defined full disaster recovery procedures that include backup and restoration testing for production servers and database machines.

- GIAC will be responsible to harden all machines on the network.

Security Architecture

A suggested high-level network architecture diagram is provided in figure 1 below. This architecture is based upon the information provided by GIAC Enterprises, in addition to the assumptions described above. The architecture includes security devices throughout the design. Each of these security measures adds to increasing the level of protection for confidential and sensitive information and resources owned by GIAC Enterprises.

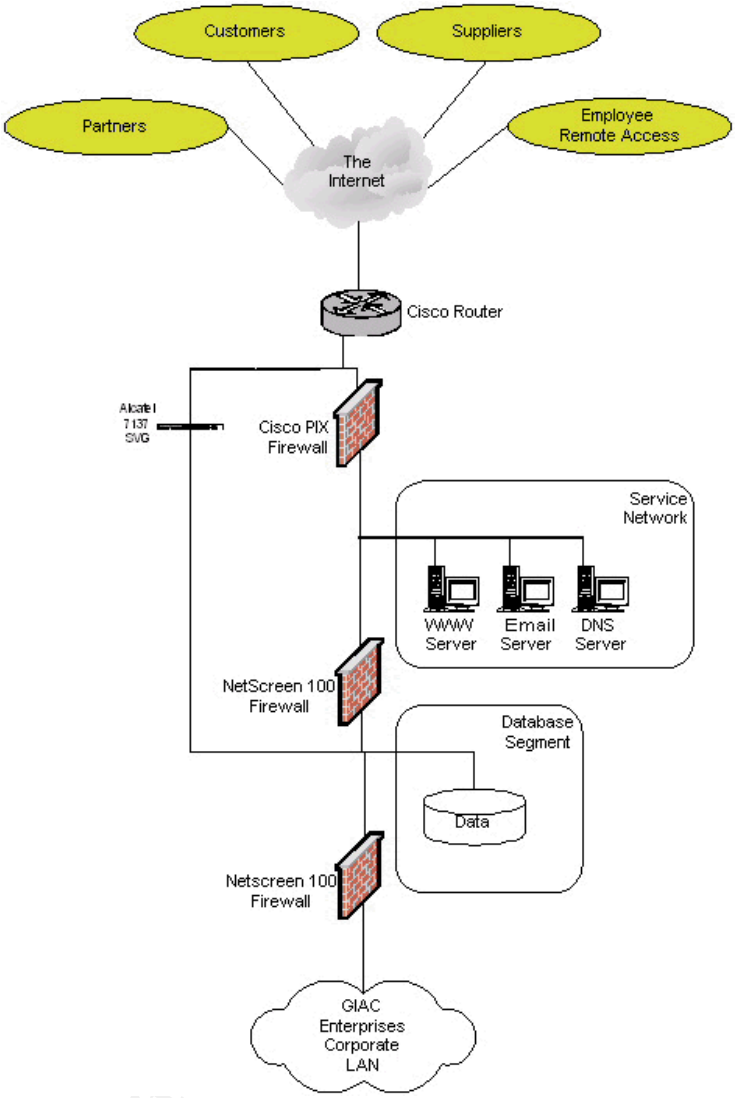

Figure 1 - High Level Diagram for GIAC Enterprises

Architecture Details

Looking at the high level diagram we can walk through the design starting at the top and working our way down.

At the top we see that customers, partners, suppliers and remote access users need access to GIAC Enterprise systems for various reasons. The cloud in the diagram represents the Internet, which is the primary delivery mechanism for all of the systems services.

The first device under GIAC Enterprises control is the router. The Cisco 4000 router has been chosen for this application. Specific details for this router can be found at http://www.cisco.com/univercd/cc/td/doc/pcat/4700m.htm#CIHCIDDI. The router will serve as a filtering gateway to the GIAC network. As such a policy will be implemented that will allow communications destined to the GIAC network in. It will drop any traffic from the outside that has internal source or loopback addresses.

After the router, there are three paths that the communication can take, depending upon whom is on the source side of the communication. This report will first detail the path of public access, that is the path taken by customers, websurfers and email for GIAC enterprises that will travel through the Cisco PIX firewall.

The Cisco PIX 525 firewall was chosen because it was engineered for reliability, speed and scalability. It can handle security requirements for large enterprise organizations and complex, high-end traffic environments. It has a throughput of up to 370 Mbps with the ability to handle 250,000 simultaneous sessions. Specific details for this firewall appliance can be found at http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/.

This device will be configured to allow HTTP (port 80), HTTPS (port 443), SMTP (port 25) and DNS (port 53) to specific machines on the GIAC service network. This device will also be providing the NAT (network address translation) function for the GIAC web site network. By utilizing NAT, the actual IP addresses of the machine on the GIAC service network will be kept private. By keeping these addresses private an additional level of security is provided because any would be attacker would not know true addresses for an intended target machine.

Beyond the PIX firewall is the service network. This is the first level of the architecture where anyone from the outside has any type of true access. That is, this is the first level where anyone in the public sector has access to the machine, as opposed to communication just being accepted or denied by the front-end components. Attached to this network are the GIAC web server, E-mail server and a DNS server. The web server, E-mail server and DNS server will be chosen by GIAC personnel to fit into their operational design. It is strongly suggested here that GIAC Enterprises adopt a policy of utilizing split DNS architecture. This keeps the internal DNS out of the public knowledge and therefore doesn't provide any specific information about the internal structure of the GIAC network architecture.

In addition, each of these boxes on the service network should be given special attention during the build and operational processes to rigorously harden the OS and application programs. That is any service not required on the boxes should be eliminated, good strong passwords utilized, up to date security patches installed, auditing and logging enabled. Baselines of the systems should be taken before the boxes are installed on the network. This can be accomplished with the Tripwire product, or a similar package. Once put on the network, baseline comparisons should be run regularly. These boxes should be installed and maintained as "bastion" boxes. That is, they should be thought of as sacrificial, in that if they are attacked, a quick rebuild is an elementary process that doesn't take long to get the site back up and running quickly. This requires distribution media and current backups are available at a moment's notice. No sensitive or confidential data will reside on any machine within this network segment. Keeping in line with these criteria will be a function of the GIAC Enterprises operations staff.

After the service network there is a second firewall installed. This firewall provides protection for the database from any would be attacker should they be successful at cracking any of the boxes on the service network layer. The Netscreen 100 was chosen for installation at this location in the architecture. The decision to implement this firewall appliance was based on several criteria. First, a different manufacturer than the Cisco PIX produces it. This eliminates the possibility of a would be attacker taking advantage of an exploit on the outer firewall and using it to compromise the inner firewall to the database segment of the network. Other criteria used include its performance, management and reliability. More information about this appliance can be found at http://www.netscreen.com/products/appliances.html#ns100.

This first Netscreen firewall appliance will be configured to allow only the webserver to query the database (probably ODBC). Note here that it is important that database security measures be implemented also. The firewall will also allow email (SMTP) to pass to the internal mail server and

web traffic to pass from internal systems to the outside for employees of GIAC Enterprises.

Between the database segment and the GIAC Corporate network is another Netscreen 100 firewall. This will provide protection for the corporate network from any supplier, partner, and customer who may stray from the provisions of their security agreement or any would be attacker who is able to successfully compromise the security chain this far. This supplies another hurdle that must be negotiated to gain access to GIAC enterprises. This firewall will also limit database accessibility to specific members of the internal GIAC team.

Moving back to the top of the high level diagram and on to the other communication paths open for use after the Cisco router, there is an Alcatel 7137 SVG's (Secure VPN Gateway). Alcatel is the VPN device supplier that has been chosen for installation on the GIAC network. These devices were chosen over other alternatives for several reasons. Including the fact that they are not integrated with any other part of the security architecture. That is, the VPN capability is not incorporated within the physical router or firewall components. Having the VPN components integrated with routers or firewalls may decrease the operational production of these components. This in combination with the thought of if anyone is able to compromise the router or firewall with the VPN component installed, they could very well compromise the VPN capabilities of that specific machine also. Tunnels will be provided for partner and supplier accesses to the database segment. This is represented in figure 2 below.

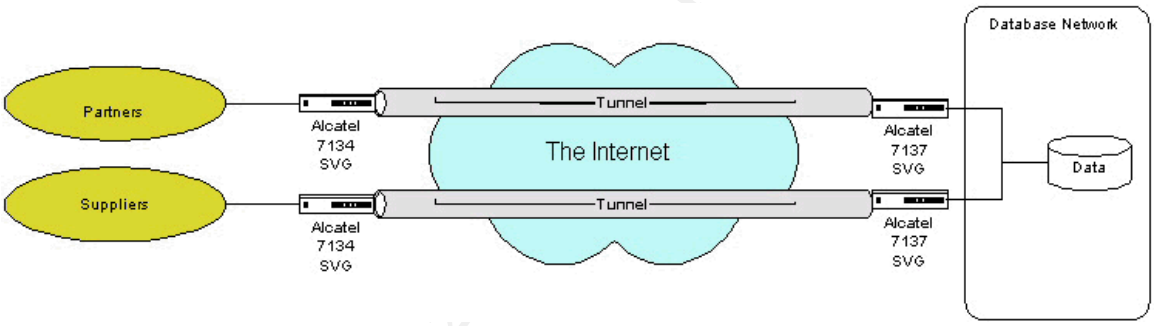

Figure 2 - Secure tunnels for Supplier and Partner access to the GIAC database

While it is the job of the secure VPN to control and secure access and communication to and from the database segment, it is important to note that data input by suppliers and data retrieval by partners should be controlled by database interface applications. Databases have their own level of security that can be implemented and it is highly recommended that these security functions and interfaces be reviewed by a third party code review process.

Additionally, secure VPN tunnels will be provided for remote access employees also. There are two different scenarios of remote access employees that are taken into account in figure 3 below. These include employees who work at home and are connecting to the corporate LAN via a dialup connection through an ISP's POP location. These users will use a secured VPN client application installed on their computer, whether it is a laptop or desktop machine. The other scenario covered is that of a small home office or telecommuter with a cable modem connection. These users can take advantage of the Alcatel 7132 SVG for use in connecting through to the Corporate LAN.

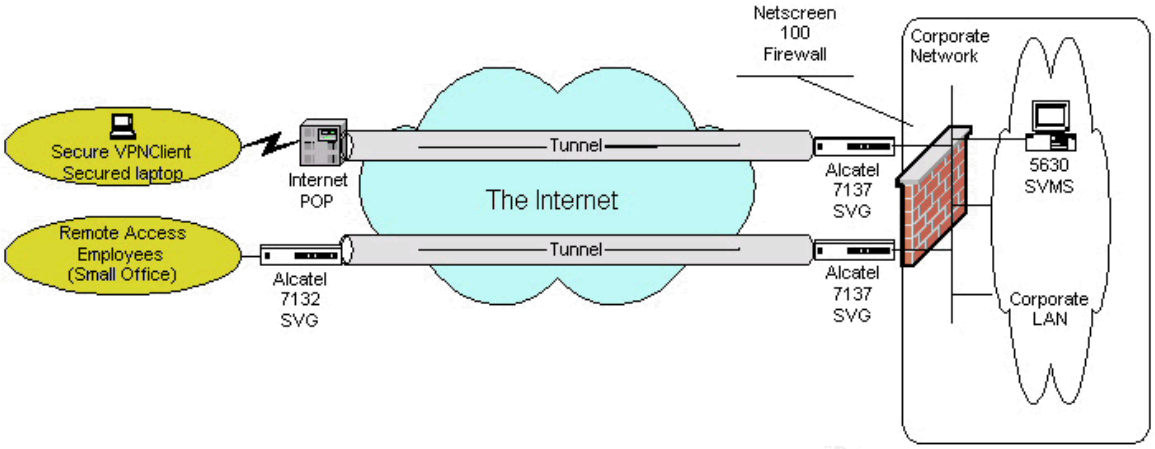

Figure 3 - Remote Access Employee Tunneling

The 5630 SVMS shown if figure 3 is the Alcatel Secure VPN Management Suite. As noted on the Alcatel web site, this suite is "a component of the Alcatel Secure VPN Solution, offers a turnkey solution with an integrated public key infrastructure (PKI) for automated certificate management and support for LDAP-compliant X.500 directories. The Alcatel 5630 includes the Entrust/PKI 4.0, which acts as the Certification Authority, PeerLogic's LDAP-compliant i500 directory, and the Alcatel 5631 Secure VPN Policy Manager. The Alcatel 5631 Secure VPN Policy Manager, which manages attribute certificates that define VPN policies for the user, allows you to control communication between users and devices to guarantee a high degree of access control."

There is also capabilities for the Alcatel solution to provide access for branch office connectivity should GIAC Enterprises require that kind of service in the future.

The Alcatel system offers solutions for all of the current GIAC Enterprise secure VPN needs and is scalable for any future requirements that may arise. More information about the Alcatel Secure VPN products can be found at the Alcatel web site http://www.cid.alcatel.com/frames/solutionsummary.jhtml?solution=Secure%20VPNs.

This concludes the high level description of the proposed security architecture for GIAC Enterprises.

Assignment 2

Assignment 2 Details - Security Policy

The details for this part of the practical exam are as follows:

> Based on the security architecture that you defined in Assignment 1, provide a security policy for AT LEAST the following three components:
>
> - Border Router
> - Primary Firewall
> - VPN
>
> You may also wish to include one or more internal firewalls used to implement defense in depth or to separate business functions.
>
> By 'security policy' we mean the specific ACLs, firewall ruleset, IPSec policy, etc. (as appropriate) for the specific component used in your architecture. For each component, be sure to consider internal business operations, customers, suppliers and partners. Keep in mind you are an E-Business with customers, suppliers, and partners - you MAY NOT simply block everything!
>
> (Special note VPNs: since IPSec VPNs are still a bit flaky when it comes to implementation, that component will be graded more loosely than the border router and primary firewall. However, be sure to define whether split-horizon is implemented, key exchange parameters, the choice of AH or ESP and why. PPP-based VPNs are also fully acceptable as long as they are well defined.)
>
> For each security policy, write a tutorial on how to implement each ACL, rule, or policy measure on your specific component. Please use screen shots, network traffic traces, firewall log information, and/or URLs to find further information as appropriate. Be certain to include the following:
>
> 1. The service or protocol addressed by the ACL or rule, and the reason these services might be considered a vulnerability.
> 2. Any relevant information about the behavior of the service or protocol on the network.
> 3. The syntax of the ACL, filter, rule, etc.
> 4. A description of each of the parts of the filter.
> 5. An explanation of how to apply the filter.
> 6. If the filter is order-dependent, list any rules that should precede and/or follow this filter, and why this order is important. (Note: instead of explaining order dependencies for each individual rule, you may wish to create a separate section of your practical that describes the order in which ALL of the rules should be applied, and why.)
> 7. Explain how to test the ACL/filter/rule.
>
> Be certain to point out any tips, tricks, or "gotchas".

IP Assignment

In order to specify security policy and ACL's it will be easier to assign IP designations for each device in the planned architecture. The diagram below assigns IP numbers for purposes of this report, these IP numbers are assigned in a strictly random way. Any conflict with legally assigned IP numbers is strictly coincidental.

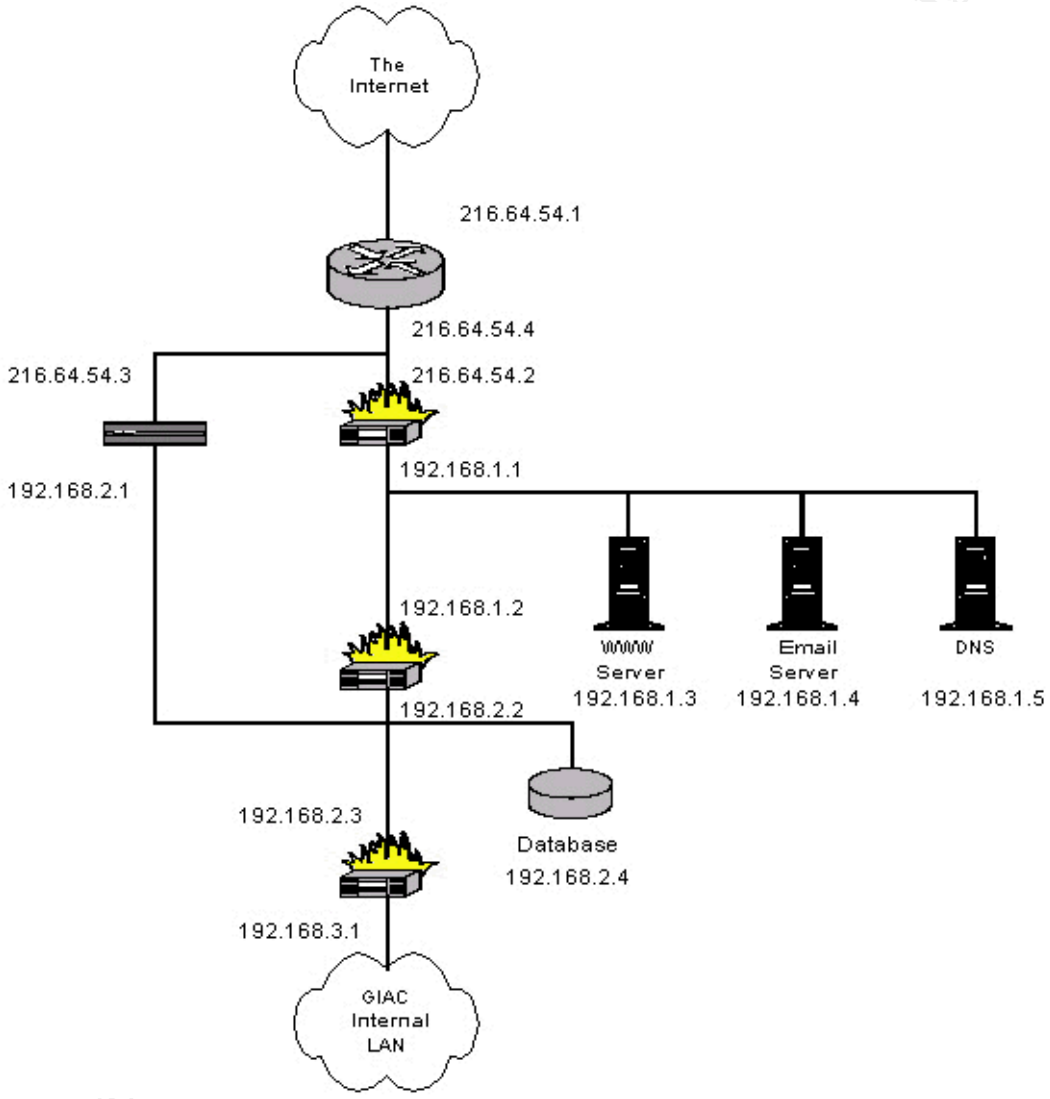

Figure 4 - Assigned IP's

Border Router - Cisco 4500

The Cisco 4500 router is located between the Internet and the service network and VPN device. The router will be the first line of defense for GIAC Enterprise systems. It will provide basic filtering for ingress and egress. By providing this filtering, the burden on the firewall system is decreased. By keeping the filtering simple the router can operate in an efficient manner.

Router management will be accomplished by using SSH (Secure Shell) and only from a limited

number of machines on the GIAC internal LAN. This device is also under the umbrella of the written corporate security policy, which means that password policies exist and should be adhered too. Additionally, this machine should be locked down or hardened. That is all unnecessary services should be deleted and or disabled. There is good documentation available from Cisco, which has specific steps to accomplishing this task. This documentation can be found at http://www.cisco.com/warp/public/707/21.html.

The acl's for the Cisco 4500 are set via the Cisco IOS. There are some basic filtering operations that the router will perform. These include:

Screening out packets that have private source addresses
Screening out packets that have the loopback address as a source address
Screening out packets that have GIAC internal LAN addresses as a source address
Screen out broadcast and mulitcast packets
Screen out SNMP requests and traps
Screen out ICMP packets
Screen out echo
Screen out finger
Drop packets not attempting to communicate with GIAC Enterprise systems
Drop source-routed packets
Screen outbound broadcasts and multicasts
Screen outbound packets from addresses other than GIAC Enterprises networks
Protect against SYN-flooding by running TCP intercept
Log dropped packets to a syslog server

Here is a copy of the router configuration file:

```
!
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no service tcp-small-servers
no service udp-small-servers
!Set no SNMP
no snmp
!Set no finger
no service finger
! Set router hostname
hostname Fortunes
! Set password and password security
enable secret 5 crumbs
! Set no ip source-routing
no ip source-route
!Set DNS server
ip name-server 206.54.123.35
!
ip subnet-zero
ip domain-lookup
ip routing
!
! Context-Based Access Control
!Set the basic firewall protections
no ip inspect audit-trail
ip inspect tcp synwait-time 30
ip inspect tcp finwait-time 5
```

```
ip inspect tcp idle-time 3600
ip inspect udp idle-time 30
ip inspect dns-timeout 5
ip inspect one-minute low 900
ip inspect one-minute high 1100
ip inspect max-incomplete low 900
ip inspect max-incomplete high 1100
ip inspect tcp max-incomplete host 50 block-time 0
!
! IP inspect Ethernet_0
!
no ip inspect name Ethernet_0
ip inspect name Ethernet_0 tcp
ip inspect name Ethernet_0 smtp
ip inspect name Ethernet_0 udp
!
! IP inspect Ethernet_1
!
no ip inspect name Ethernet_1
ip inspect name Ethernet_1 tcp
ip inspect name Ethernet_1 smtp
ip inspect name Ethernet_1 udp
!
controller E1 0
!
interface Ethernet 1
 no shutdown
 description connected to Internet
 media-type 10BaseT
 ip address 216.64.54.67 255.255.255.240
 ip inspect Ethernet_1 in
 ip access-group 101 in
 keepalive 10
!
interface Ethernet 0
 no shutdown
 description connected to EthernetLAN
 media-type 10BaseT
 ip address 216.64.54.4 255.255.255.192
 ip inspect Ethernet_0 in
 ip access-group 100 in
 keepalive 10
!
! Access Control List 100
! The following Access Control  lists set up network to accept HTTP, HTTPS, DNS, SMTP and VPN
! Since I don' t have any of the Alcatel equipment, I made a fictitious service of 4774 for VPN access
!
no access-list 100
access-list 100 permit udp any eq rip any eq rip
access-list 100 permit tcp host 216.64.54.3 any eq 4774
access-list 100 deny ip host 216.64.54.3 any
access-list 100 permit tcp host 216.64.54.2 any eq 80
access-list 100 permit tcp host 216.64.54.2 any eq 443
access-list 100 permit tcp host 216.64.54.2 any eq 25
access-list 100 permit udp host 216.64.54.2 any eq domain
access-list 100 deny ip host 216.64.54.2 any
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any any eq 443
access-list 100 permit tcp any any eq 25
```

```
access-list 100 permit tcp any any eq 4774
access-list 100 permit udp any any eq domain
!
! Access Control List 101
!
no access-list 101
access-list 101 deny ip 216.64.54.0 0.0.0.63 any
access-list 101 permit tcp any host 216.64.54.3 eq 443
access-list 101 permit tcp any host 216.64.54.3 eq 25
access-list 101 permit tcp any host 216.64.54.3 eq 80
access-list 101 permit tcp any host 216.64.54.3 eq 4774
access-list 101 permit udp any host 216.64.54.3 eq domain
access-list 101 deny ip any host 216.64.54.3
access-list 101 permit tcp any host 216.64.54.2 eq 25
access-list 101 permit tcp any host 216.64.54.2 eq 443
access-list 101 permit tcp any host 216.64.54.2 eq 80
access-list 101 permit udp any host 216.64.54.2 eq domain
access-list 101 deny ip any host 216.64.54.2
access-list 101 permit tcp any 216.64.54.0 0.0.0.63 eq 25
access-list 101 permit tcp any 216.64.54.0 0.0.0.63 eq 4774
access-list 101 permit tcp any 216.64.54.0 0.0.0.63 eq 443
access-list 101 permit udp any 216.64.54.0 0.0.0.63 eq domain
access-list 101 permit tcp any 216.64.54.0 0.0.0.63 eq 80
!
router rip
 version 2
 network 216.64.54.0
 passive-interface Ethernet 1
 no auto-summary
!
!
ip classless
!
! IP Static Routes
ip route 0.0.0.0 0.0.0.0 Ethernet 1
no ip http server
no snmp-server location
no snmp-server contact
! Set a warning banner. If this is not here, there is legal ramifications
banner motd #You are not welcome here. This is a warning banner bla bla bla. Keep out
Survivors will be prosecuted !#
!
line console 0
 exec-timeout 0 0
 password crumbs
 login
!
line vty 0 4
 password crumbs
 login
!
end
```

The router configuration was set up by using the Cisco configmaker application. It is a GUI driven application that allows for building block type network creation. After the network is assembled on the desktop, a configuration file is created. This file can then be moved to the

Cisco device that is being installed. It is an easy program to work with once you get used to it. More information and the configmaker tool can be found at http://www.cisco.com/warp/public/cc/pd/nemnsw/cm/index.shtml.

Below is figure 5, which is a screen capture made while working with the Cisco Configmaker.

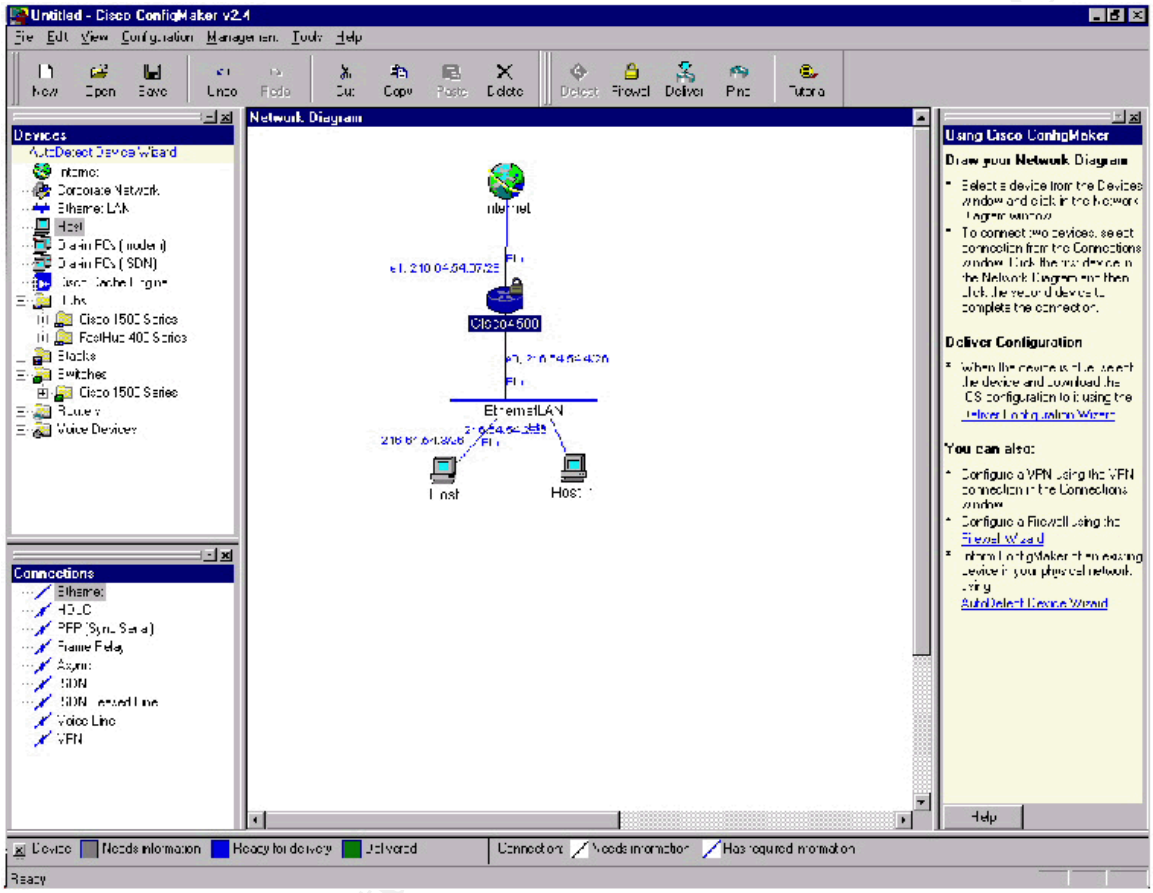

Figure 5 - Cisco Configmaker Screen Capture

Primary Firewall - Cisco PIX

Between the border router and the service network a Cisco PIX 525 firewall is installed. Management of this box should be accomplished via SSH from a limited number of machines on the GIAC internal LAN on the internal interface of the PIX box. Operational and management procedures of the PIX machine should be addressed in the written security policy. This will include password protection and change control procedures.

The incoming firewall policies are implemented to ensure only legitimate traffic gets to GIAC Enterprise machines. It will allow web (HTTP 80, HTTPS 443), mail (SMTP 25) and DNS (53) through to the service network. All other traffic trying to get to the service network will be blocked.

The outgoing policies should allow outgoing mail and DNS queries from the service network; all other connections should be blocked and logged. Depending upon a decision to be made by GIAC Enterprises management, an outgoing policy may be implemented that will allow web surfing from the internal network.

Following is a copy of the firewall ruleset generated for the GIAC Enterprises network design implemented for this paper.

```
# Name the interfaces and give a security level
nameif  ethernet0 outside security0
nameif  ethernet1 webnet security100

# Identify network interfaces
interface ethernet0 auto
interface ethernet1 auto

# Assign and identify the IP Addresses of each of the three interfaces
ip address outside 216.64.54.1 255.255.255.0
ip address webnet 192.168.1.1 255.0.0.0

# Name the PIX firewall. This will appear in the command line prompt.
hostname cookies

#PIX fixup protocol enable for default
 fixup protocol http 80
fixup protocol smtp 25


# Disable the RIP attributes so no routing takes place
no rip webnet passive
no rip outside passive
no rip webnet default
no rip outside default

# Set the outside default route to the router attached to the Internet.
route outside 0.0.0.0 0.0.0.0 216.64.54.4

#Let Internal users start connections on the service network and outside interfaces
nat (webnet) 1 192.168.3.0 255.0.0.0

# Name the webserver.
name 192.168.1.3 fortuneserver

# Allow outside access to fortuneserver on ports 80 and 443
conduit permit tcp host fortuneserver eq 80 any
conduit permit tcp host fortuneserver eq 443 any

# Name the mailserver
name 192.168.1.4 fortunemail

# Allow outside SMTP access to fortunemail
conduit permit tcp host fortunemail eq smtp any

# Name the DNS machine
name 192.168.1.4 fortunenames
```

Allow DNS access to fortunenames
conduit permit tcp host fortunemail eq 53 any

VPN - Alcatel Secure VPN Gateway

The Alcatel Secure VPN solution is designed as a total solution for the networking needs of enterprise customers today. Making cost effective use of the Internet to securely connect mobile users, partners and suppliers to the enterprise systems.

The Alcatel VPG (VPN Gateways) are tamper resistant gateways that secure communications for intranets, extranets and Internet remote access. Alcatel products offer a turnkey solution with integrated PKI (Public Key Infrastructure) for automated certificate management and support for LDAP compliant (Lightweight Directory Access Protocol) X.500 directories. The Alcatel VPN solution gives the flexibility to centrally manage secure VPN deployments with a choice of PKI's and directories. Support for certificates from Entrust, GTE Cybertrust, VeriSign, Netscape, Baltimore, RSA Security and Xcert.

Some of the benefits of the Alcatel VPN products are as follows:

- Data encryption prevents anyone from reading data as it travels across the Internet.
- Cryptographic checksums ensure that no one tampers with data as it travels across the Internet.
- X.509 Certificates ensure that data is coming from the source it claims to be coming from.
- Directory-based policy management restricts users to only those parts of the network they are authorized to see.

More information about these components can be found at http://www.cid.alcatel.com.

Assignment 3

Assignment 3 Details - Audit Your Security Architecture

You have been assigned to provide technical support for a comprehensive information systems audit for GIAC Enterprises. You are required to audit the Border Router and Primary Firewall described in Assignments 1 and 2. Your assignment is to:

1. Plan the assessment. Describe the technical approach you recommend to assess your perimeter. Be certain to include considerations such as what shift or day you would do the assessment. Estimate costs and level of effort. Identify risks and considerations.
2. Implement the assessment. Validate that the Border Router and Primary Firewall are actually implementing the security policy. Be certain to state exactly how you do this, including the tools and commands used. Include screen shots in your report if possible.
3. Conduct a perimeter analysis. Based on your assessment (and referring to data from your assessment), analyze the perimeter defense and make recommendations for improvements or alternate architectures. Diagrams are strongly recommended for this part of the assignment.

Note: DO NOT simply submit the output of nmap or a similar tool here. It is fine to use any assessment tool you choose, but annotate the output.

Assessment Plan

Because the assignment calls for "a comprehensive" audit, it is important that all areas of the network be audited. This plan will call for both human interaction and the use of automated tools.

Plan Steps

1. Meet with the GIAC Enterprises Systems Management staff. This meeting will kick of the auditing effort. It is important that the management team know what is going to happen, what they can expect as a result. During this meeting a detailed discussion of the network should take place. Included in this meeting will be discussion of times, dates and places for auditing efforts to take place. In addition, because some social engineering will take place, it is important that no one besides management be informed of the processes. Any leak of information about social engineering efforts could skew the results.

2. Gather and review all written security policy documentation. Verify that this documentation has been distributed throughout the organization and to all suppliers and partners.

3. Gather and review logs from all security-related equipment. This will include logs from routers, firewalls, VPN devices and machines on the service network and database segment. The written security policy should define the logging processes and procedures. These procedures should include specific information about log review, rotation and retention.

4. Verify physical security of the network machines. Routers, firewalls, VPN devices, service network and database network machines should be physically secured and protected. Power, environmental conditioning and fire protection should be addressed. This should be noted in the written security policy.

5. Review all operational procedures. These include change control, backup and recovery procedures. All of these items should be defined within the written security document, and should be adhered too.

6. Review procedures for keeping machines up to date in regard to security patches and updates. These procedures should be defined in the written security policy and adhered too. From a security perspective, it is extremely important to keep up with the patching of systems; new security vulnerabilities are found and published frequently. Not defending the systems against these vulnerabilities is a dereliction of duty. In addition, keeping systems up to date helps operational personnel by keeping machines in sync with each other.

7. Set up and perform some social engineering experiments. Try calling system operators on differing shifts and try to get them to supply information that would be useful to an attacker. This information would include things such as IP address information, password information, and modem information (although there shouldn't be any). Try walking into a department and seeing who has left their machine logged on to the network and unprotected. Basically, befriend anyone in the organization that may be able to help get into the system from any point.

8. Using automated tools scan the network from the outside world. There are numerous automated tools that can be used to scan the machines on the different network segments. For purposes of this auditing effort the nessus product is suggested. It is free, easy to use and can be modified easily to include new tests. (Much more information about the nessus project can be found at http://www.nessus.org/index.html.) This should not take longer than a few hours. Since the GIAC Enterprise website is a 24 hours 365 day a year operation, there is probably no time that is completely clear of risking site operations. However, GIAC Enterprise Management should be able to come to a consensus of the best time for this scanning effort to take place. Also, discuss the ramifications of running destructive type tests, such as DOS (Denial of Service) operations which could take the site down, and password cracking tests which could impact site operations. Make a determination with management of which tests will be run and when.

9. Using automated tools scan the network from somewhere within the corporate LAN boundaries. This is important from a security standpoint, as it is well known that many security breaches are accomplished from within the security perimeter. This will also provide the GIAC Enterprise management team with a good baseline of where their internal systems are on the security scale. It is important that security measures permeate the whole LAN environment. Depending upon the size of the internal LAN this could be quite time consuming. It can probably be conservatively estimated to take 2 hours per 10 machines being scanned. This will include setting up the scanning machine and taking care of any tool modification needed. Again, discuss whether destructive tests will be run on the internal segments of GIAC Enterprises LAN environment.

10. Using tools such as Hping packets can be crafted to test the router and firewall rulesets. Using tools such as tcpdump or etherpeek, a monitor can be set up on the inside of the network protection mechanisms to see if any attempt to thwart the security is successful.

11. Combine information collected into a clear and concise report along with a summarization of the top security issues found, and recommendations for mitigating these risks. Depending upon the number of machines being audited internally, this could be a very time consuming task. Estimate 8 hours for each 10 machines scanned.

12. Meet with GIAC Enterprises Management team and discuss the report findings.

Assessment Implementation

Any time a control system is in place, it's important to audit it appropriately to confirm that it is meeting your needs. To assess the border router and primary firewall the following tests can be run.

Set up a monitor on the inside of the protection device. This can be a machine running tcpdump, etherpeek or numerous other sniffer programs. Find one that you are comfortable with and has a friendly output.

Validate that border protection mechanisms are performing as expected. Using a copy of the border and firewall rulesets check that each rule is performing its specific function. For instance, from the outside try to gain access utilizing an internal address and a loopback address. Spoofing an internal or loopback address in the source field of the TCP/IP packet can complete this. The Hping tool can accomplish this.

Check each rule in the ruleset. Be sure to check for access by services other than those that are explicitly allowed.

Check for machines that are loosely configured. By scanning the machines from the outside with tools such as nessus or Fyodor's nmap or other scanning tools vulnerabilities, and pertinent information can be found in an automated way. Once found; try to exploit the vulnerabilities from a machine outside. If they are successful, determine what protection mechanism failed and fix it. It is important to scan the machines from inside the boundary protection mechanisms as well. Vulnerabilities are often found here that can't be seen from the outside world. However, should anyone successfully get inside, they will be able to exploit any vulnerability that exists.

Assignment 4

Assignment 4 Details - Design Under Fire

The purpose of this exercise is to help you think about threats to your network and therefore develop a more robust design. Keep in mind that the next certification group will be attacking your architecture!
Select a network design from any previously posted GCFW practical (http://www.sans.org/giactc/gcfw.htm) and paste the graphic into your submission. Be certain to list the URL of the practical you are using. Design the following three attacks against the architecture:

1. An attack against the firewall itself. Research vulnerabilities that have been found for the type of firewall chosen for the design. Choose an attack and explain the results of running that attack against the firewall.
2. A denial of service attack. Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods. Describe the countermeasures that can be put into place to mitigate the attack that you chose.
3. An attack plan to compromise an internal system through the perimeter system. Select a target, explain your reasons for choosing that target, and describe the process to compromise the target.

Attack Network

For this portion of the assignment, I chose to look deeper into the network design of Alexander Usenko. His paper and network design can be found at http://www.sans.org/y2k/practical/Alexander_Usenko_GCFW.doc.

I have attached a copy of the network architecture below in figure 6. Basically, the site is being protected by a front end Cisco border router, a corporate firewall that allows access from the internet and a VPN. The publicly accessible web site has basic protections provided by the border router and a pair of F5 Labs BigIP load balancers. The Production machines are protected by a second firewall which separates the backend of the webservers from the DB / Application servers and the corporate network segments.

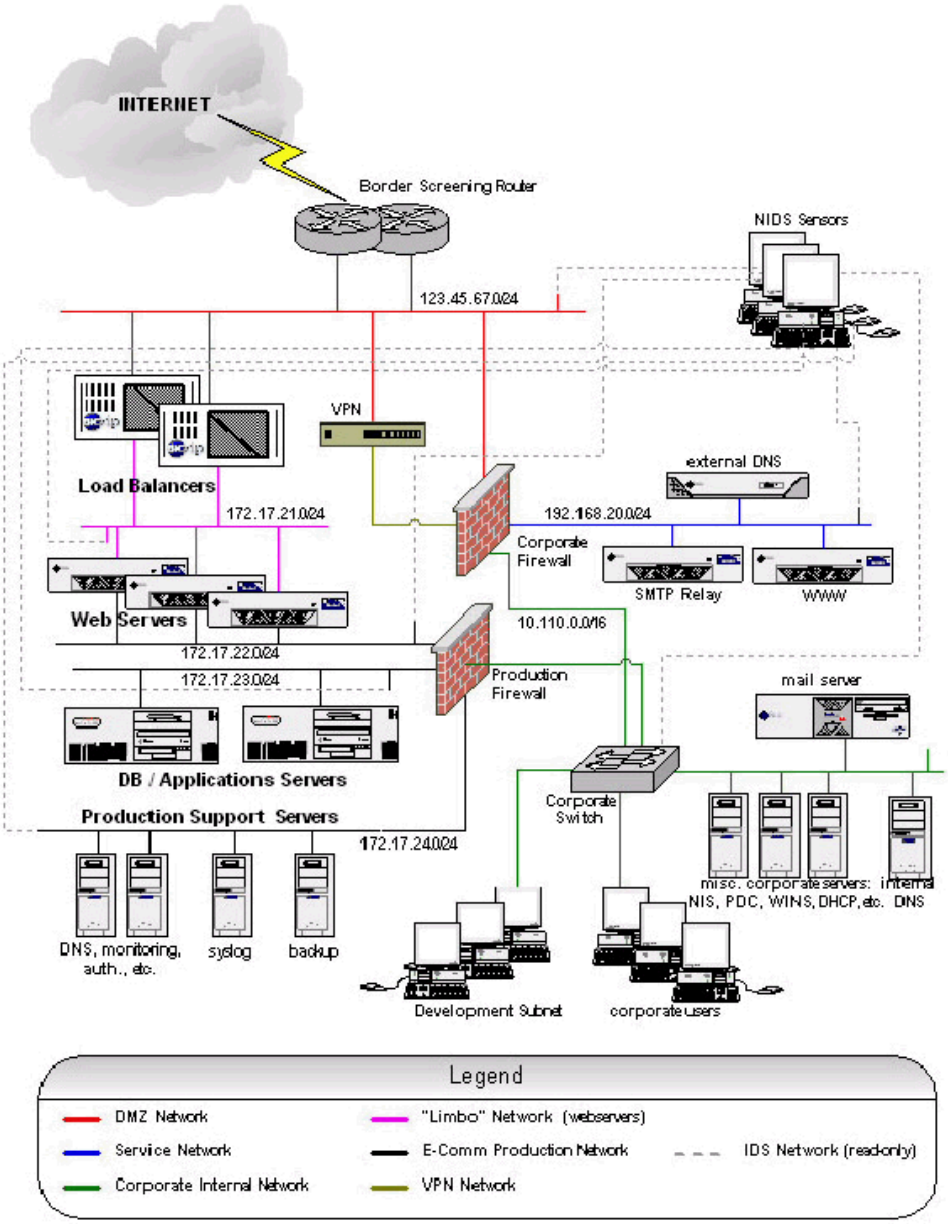

Figure 6 - Network Architecture under Attack

Sneaking in the Gates - Firewall Attack

While researching for this paper I came across a great paper by Ofir Arkin. This paper can be found at http://www.hideaway.net/Server_Security/Library/Firewalls/firewall/unverified.pdf. In this paper Arkin explains the deficiency in many firewalls that are in the market place today. By crafting an ICMP packet, Arkin has managed to penetrate defense mechanisms and gain valuable information about the systems that lie behind them. While Alexander does block ICMP packets from his network, Arkin makes a valuable point that the process described in his paper is not limited to use with ICMP protocol. In fact there are numerous protocols that can be used and while there is not a complete ruleset included in Alexander's paper, there is a high probability that one of the protocols allowed will accommodate an attack similar to the one experimented with by

Arkin. With this type of attack valuable information concerning the systems behind the firewall can be ascertained.

In addition there is a very good and detailed paper titled " A Stateful Inspection of FireWall-1" by Thomas Lopatic, John McDonald TUV data protect and Dug Song, Center for Information Technology Integration University of Michigan. This paper can be found at http://www.hideaway.net/Server_Security/Library/Firewalls/firewall/stateful_firewall-1.txt. It is meant to complement slides that were presented at the Black Hat briefings 2000. The slides can be found at http://www.dataprotect.com/bh2000/ . This presentation defines numerous holes in the Checkpoint FW1 product. Checkpoint has since released patches that are supposed to address all of the issues discussed, but if Alexander hasn't loaded these patches, then the firewalls in his network are vulnerable to all of the attacks described.

Flood the Gates - A Denial of Service attack

Alexander's design is full of twists and turns. Both firewalls have 4 interfaces; the border routers are directly connected to a VPN device, a firewall and a set of BigIP load balancers. The webservers themselves are being protected only by the border router and the pair of load balancers, that are performing IP filtering. Doing a little reading and research, and talking with someone from F5 I have found that the BigIP load balancers are built on a BSDI kernel. And while the literature for these machines states the capability to filter IP, it is not recommended because the kernel is not optimized to handle this operation.

In keeping with the scenario of " Subject the design to a theoretical attack from 50 compromised cable modem/DSL systems using TCP SYN, UDP, or ICMP floods", my guess is that we could deny service to the webservers from the outside very easily by flooding the load balancers.

This scenario could be mitigated by placing limits on traffic to the BigIP's on the border router.

The Gates are Flooded - Can we come in?

If our attack above successfully crashes the BigIP's, there is a good chance that they will be sent into an unstable state, which of course is always good for a would be attacker. Compromise of the load balancing machines could quickly lead to compromise of the webservers. Looking at the design of this network, we see that there is a valid backend connection to the production firewall. From there all the doors are open in the kingdom, and the jewels are at risk.