



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

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

SANS GIAC
Certified Firewall Analyst (GCFW)
Practical Assignment
Version 1.9 (Revised January 20, 2003)

Atul Sharma
May 12, 2003

Table Of Contents

Abstract.....	5
1. SECURITY ARCHITECTURE	6
1.1 Operational Considerations	6
1.1.1 Customers	6
1.1.2 Suppliers.....	6
1.1.3 Partners	6
1.1.4 Employees.....	7
1.1.5 Mobile Employees	7
1.2 IP Addressing and Network Infrastructure	7
1.2.1 Managed PKI	8
1.3 Technical and Financial Feasibility	9
1.4 Network Architecture	10
1.4.1 Border Router.....	11
1.4.2 Nortel Contivity VPN Switch	11
1.4.3 External Pix Firewall	11
1.4.4 Internal CheckPoint Firewall.....	11
1.4.5 Intrusion Detection Servers	11
1.4.6 Web Servers	12
1.4.7 Mail Gateway	12
1.4.8 Proxy Server	12
1.4.9 Database server	12
1.4.10 Internal Domain Server	12
1.4.11 Internal Email Server.....	13
2: SECURITY POLICY AND TUTORIAL.....	14
2.1 Border Router	14
2.1.1 Border Router Configuration.....	14
2.1.2 Explanation of Border Router Configuration	15
2.2. External Firewall	18
2.2.1 External Firewall Access Control List	19
2.2.2 External Firewall Configuration	20
2.2.3 External Firewall Configuration Explanation	22
2.3 VPN Policy and Tutorial	25
2.3.1 VPN Tutorial.....	25
2.4 Internal Firewall.....	40
1.4.1 Internal Firewall Policy	40
2.4.2 Object Listing	41
2.4.3 Explanation of Checkpoint rules.....	41
3: VERIFY THE FIREWALL POLICY.....	43
3.1 Plan the Audit	43
3.1.1 Approach and Logistics.....	43
3.1.2 What will be reviewed.....	43

3.1.3	Costs and Effort Level.....	45
3.2	Conducting The Audit	46
3.2.1	Auditing Documentation.....	46
3.2.2	Auditing Physical Security	46
3.2.3	Auditing Rule Base	46
3.3	Evaluating the Audit	52
4:	DESIGN UNDER FIRE.....	54
4.1	Design to Attack.....	54
4.2	Denial of Service	55
4.3	Compromising an Internal Machine	56
4.3.1	Description of Vulnerability	57
4.3.2	Recommendation.....	57
4.4	Attacking the Firewall.....	58
4.4.1	Vulnerability Details.....	58
4.4.2	Exploit	58
4.4.3	Conclusion.....	59
5.0	REFERENCES.....	60

© SANS Institute 2003, Author retains full rights

Table of Figures

CONFIGURATION 1: BORDER ROUTER CONFIGURATION	15
CONFIGURATION 2: EXTERNAL FIREWALL CONFIGURATION	21
DIAGRAM 1: PROPOSED NETWORK ARCHITECTURE FOR GIAC	10
DIAGRAM 2: IP SCHEMA FOR BORDER ROUTER AND EXTERNAL FIREWALL INTERFACES	14
DIAGRAM 3: IP SCHEMA FOR EXTERNAL FIREWALL AND VPN SWITCH INTERFACES	19
DIAGRAM 4: IP SCHEMA FOR INTERNAL FIREWALL INTERFACES	40
DIAGRAM 5: INTERNAL FIREWALL RULES	40
DIAGRAM 6: INTERNAL FIREWALL OBJECTS	41
DIAGRAM 7: GIAC NETWORK ARCHITECTURE AS PROPOSED AFTER THE AUDIT	53
TABLE 1: IP SCHEME	8
TABLE 2: SERVER IP ADDRESSES	13
TABLE 3: A STEP-BY-STEP EXPLANATION OF BORDER ROUTER CONFIGURATION	17
TABLE 4: ILLUSTRATION OF HOW PIX HANDLES NAT	18
TABLE 5: ILLUSTRATION OF PIX ACL'S	19
TABLE 6: A STEP-BY-STEP EXPLANATION OF THE EXTERNAL FIREWALL CONFIGURATION	24
TABLE 7: COSTS AND EFFORTS REQUIRED	45
TABLE 8: NMAP SCAN RESULTS FOR PUBLIC SERVERS	47

© SANS Institute 2003, Author retains full rights.

Abstract

This document has been written to cover the Practical Assignment for my GCFW certification from GIAC. The main assignment has been sub-divided into four assignments

Assignment #1 Security Architecture

This section sets the tone for the sections 2 and 3. It defines GIAC security policy and network architecture to implement the defined requirements.

Assignment #2 Security Policy and Tutorial

This section describes the router, firewall and VPN policies for GIAC in detail.

Assignment #3 Auditing the Firewall Policy

Once the security policy has been defined and network infrastructure put in place to implement the GIAC security policy, auditing the technical work done will assist GIAC management in determining whether their policies have been implemented properly or not. This section deals with auditing the external firewall to verify implemented policies.

Assignment #4 Design under Fire

This section deals with attacking a network design from a practical assignment submitted in the last six months.

© SANS Institute 2003. All rights reserved. SANS Institute 2003. All rights reserved.

1. SECURITY ARCHITECTURE

1.1 Operational Considerations

According to the GIAC enterprise definition, there are five different user groups inside and outside of GIAC.

1.1.1 Customers

Customers, accessing GIAC information systems from Internet to buy fortunes online, will have to be reasonably assured of the security around the information being submitted by them. The credit card information has to be securely processed for payment and stored encrypted in a database server. GIAC's customer facing web portal <https://giac.com> will be enabled with SSL to provide an encrypted tunnel to process credit card transactions. To automate the payment process GIAC will be using Verisign's Payment Pro product. This software enables the enterprise to automate the processing of online credit card payments securely.

1.1.2 Suppliers

GIAC will create an online web portal for their suppliers to submit fortune sayings over the Internet. The suppliers will be able to upload the fortune sayings by cutting and pasting onto a browser-based application. Also they will be able to use the same application to securely upload a file. In order to strongly authenticate the authorized supplier personnel GIAC will issue them strong two-factor authentication smart card technology based USB tokens. These tokens will be used to store certificates issued by the GIAC Private Extranet CA. GIAC will buy a Managed PKI service from Soltrus, the Canadian affiliate of VeriSign, to issue client certificates. The supplier portal application will be hosted at <https://giac.com/suppliers>. All the data will be securely stored in a database housed in a secure internal LAN segment.

1.1.3 Partners

GIAC has a fairly static base of partners who will need access to the GIAC database to translate the supplied fortune sayings into different languages. The partner access will also be secured using a web portal application that will use 128-bit SSL authentication using client certificates. In order to strongly authenticate the authorized supplier personnel GIAC will issue them strong two-factor authentication smart card technology based USB tokens. These tokens will be used to store certificates issued by the GIAC Private CA. GIAC will buy a Managed PKI service from Soltrus, the Canadian affiliate of VeriSign, to issue client certificates. The partner portal application will be hosted at

<https://giac.com/partners>. All the data will be securely stored in a database housed in a secure internal LAN segment.

1.1.4 Employees

GIAC employees will be provided outbound web access as well as to the corporate email. All outbound web access will be controlled and restricted to http, DNS. All web access from the office network for the employees will be channeled through a proxy that will be hosted in the DMZ. No direct access to the Internet will be available from the office network. Developers who maintain the GIAC web application will be provided monitored physical access to the application server. Proper physical access control measure will be put in place to control the access to the GIAC network equipment. The core database and business systems will reside in a very secure internal network. Employees will not have any logical access the database network. Administrators will have to physically go to the data center for maintenance tasks such as OS installation, patching, hardware changes etc.

1.1.5 Mobile Employees

GIAC's mobile sales force will be provided with VPN access using Nortel Contivity Switch. They will use Nortel's extranet client to access the corporate network over IPSec. Client certificates stored on smart card technology enabled eTokens will be used to provide strong two-factor authentication. GIAC will provision smart card technology based tokens from eAlladin.

1.2 IP Addressing and Network Infrastructure

We have designed a three-tiered network. This design approach provides GIAC with a modular network that will be easy to scale, maintain and troubleshoot. The ultimate goal is to provide an always-online network infrastructure without a single point of failure. This is very critical because GIAC is an E-Commerce company that does all its business through the Internet. Firewalls from two different vendors have been used to make it difficult to intrude. All the Internet available servers for example the Marketing Web Server, Secure Business Server, DNS and Mail Gateway will be hosted in the GIAC DMZ. All the business critical servers like databases will be hosted in a network segment protected by a dedicated checkpoint firewall. The only logical access allowed to this segment will be from the business web server to the application server. Only application server is allowed to communicate to the database server that also resides on this network.

The office network will also be attached to a separate interface on the CheckPoint firewall. No logical access is allowed between the office and the internal network. A separate network management network has been created to implement the Intrusion Detection Systems that will monitor network access to different network segments. The Firewall Management workstation for the

CheckPoint firewall is located on this segment. This management segment will use the Private IP addresses from 192.168.1.0 – 192.168.1.254 (Refer to Table 1). GIAC Enterprises will use Private 10.x.x.x ranges for different internal network segments.

Network Name	Network Address	Netmask	Default Gateway
DMZ	10.10.10.0	255.255.255.0	10.10.10.1
Office LAN	10.10.20.0	255.255.254.0	10.10.20.1
Internal Server LAN	10.10.30.0	255.255.255.0	10.10.30.1
VPN LAN	10.10.40.0	255.255.255.0	10.10.40.1
LAN between two firewalls	10.10.50.0	255.255.255.0	10.10.50.1
IDS LAN	192.168.1.0	255.255.255.0	
Public IP	132.96.238.0	255.255.255.0	

TABLE 1: IP SCHEME

1.2.1 Managed PKI

GIAC is going to provision a MPKI solution from Soltrus. We are going to buy two private CA's.

- The first CA will be used to issue certificates for the employees of Suppliers and Partners who will access the GIAC extranet site to submit their respective works online.
- The second CA will be used to issue IPSec certificates for the VPN switch and GIAC remote sales force.

GIAC is an online business. Therefore they want to strongly authenticate the supplier and partner employees before they access the GIAC extranet applications. Strong authentication is a requirement for GIAC because these users have the ability to modify the GIAC database through the extranet application. GIAC has therefore decided to also procure 50 USB etokens from eAlladin. Of these 10 tokens will be issued to GIAC Remote Sales Force for two-factor authentication to the VPN Switch. 10 tokens will be given to the partners and suppliers each for authentication to the extranet application.

The Managed PKI accounts will be configured to generate the public/private key pair directly on the eTokens. Key pairs that are generated directly on the USB tokens (tamper proof) are not exportable which makes the user credentials impossible to duplicate.

1.3 Technical and Financial Feasibility

The internal network includes all production data, and business system, such as ordering, inventory, accounting, etc. This data is very critical to company's business. The data integrity and availability should be protected at all times. We have decided to house these servers separately in a completely isolated internal network. Only limited business protocols (such as database access) and indirect access (for example, from the business application server in internal network) are allowed. Pre-authorized employees will be allowed physical access to these machines secured in a separate network room. All data in the database will be stored encrypted by the application server.

The office network is built for all employees, as well as roaming employees. All the business applications, such as order processing, office documentation, printing, is in this segment. This network does not include critical business data, and all systems can have a mirror to provide high availability. Also each system will enforce strong authentication and auditing to assure accountability.

Employees can only access Internet via proxy (SQUID on Linux) servers, with limited protocols (FTP, Web, DNS, etc). More restriction on Internet access will improve system effectiveness and efficiency.

DMZ is an open environment to Internet access on some protocol, such as Web, DNS and Email. These protocols are required for GIAC to manage its business efficiently. GIAC web servers only provide web pages to Internet users (include customers, suppliers, and partners), with very strong authentication and authorization measures (e.g. certificates and USB tokens). No customer related and critical business data is stored on these web servers. Business Web Server is the only machine in the DMZ that is allowed to access the business application servers in secure internal network via proprietary restricted business protocols, not well-known Internet protocol. Except for marketing web server and Email, all ordering, supplier and partner traffic will be encrypted with 128 bits SSL.

GIAC being an E-Commerce shop, securely authenticating customers, partners, suppliers and remote employees is of paramount concern. In order to mitigate this risk we propose to provision a managed PKI solution from Soltrus, Canadian Affiliate of Verisign. Certificates stored on a USB smart card will help GIAC achieve a two-factor authentication.

From a financial perspective the initial costs in procuring a managed PKI solution will be high. However, considering GIAC is an online business, strong authentication will boost the confidence and trust of the people that they do business with. In the long run GIAC will benefit from this solution.

1.4 Network Architecture

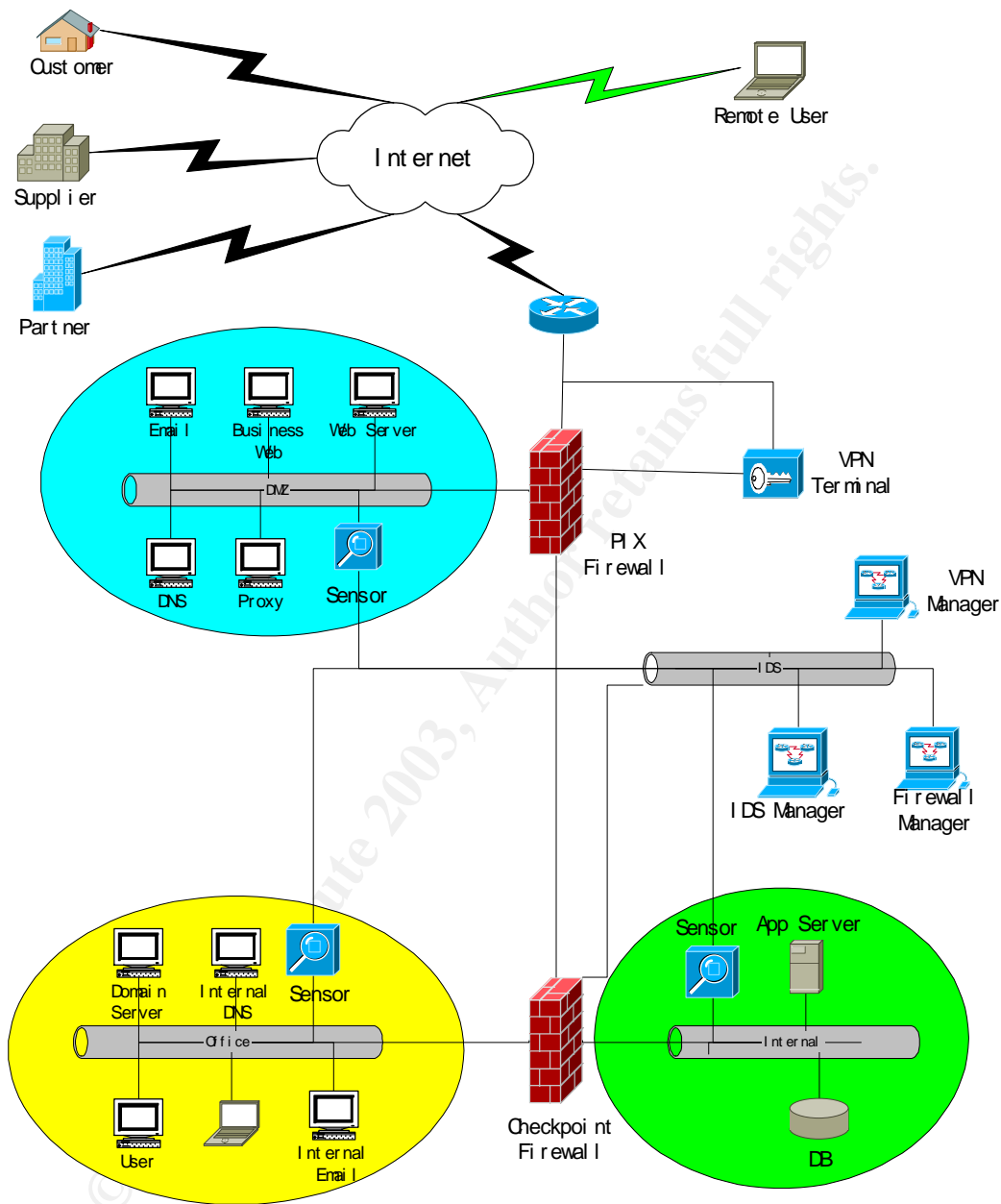


DIAGRAM 1: PROPOSED NETWORK ARCHITECTURE FOR GIAC

Below is a brief description of each of the components being used by the GIAC Enterprise Network.

1.4.1 Border Router

A Cisco 3600 router was chosen as the border router. This router will be responsible to connect the GAIC office to its ISP. Cisco 3600 is a mid sized router and will run the latest major version IOS (12.1). The reason version 12.1 is being used is because GIAC wants to use a stable IOS version. The router will be properly hardened based on Cisco's recommendations to prevent hack attacks. Cisco's 3600 router will help design a highly available, secure and scalable network. This will account for any future business needs of GIAC Enterprises.

1.4.2 Nortel Contivity VPN Switch

Nortel Contivity 1700 VPN Switch was chosen to provide VPN Access to the GIAC internal network for the mobile employees and system administrators. It will run version 4.06.200 of the Nortel VPN software. This is a mid sized VPN device that provides Stateful Packet Inspection. This VPN switch will allow GIAC to use strong two-factor authentication schemes like RSA SecureID, certificates stored on eTokens etc. Nortel Extranet version 4.65.21 will be used to access the VPN. Client certificates stored on eToken's will be used to provide strong hardware based two-factor authentication.

1.4.3 External Pix Firewall

Cisco Pix 520 running version 6.2(2) was chosen. PIX firewall will block all traffic; only allow limited inbound and outbound access. Pix firewall provides excellent performance and is easy to configure. It will implement NAT to translate the internal IP address to published IP address. Each publishing server inside the DMZ will have a static public IP, and the outbound access will share a single public IP.

1.4.4 Internal CheckPoint Firewall

Checkpoint Firewall-1 on NOKIA platform (IP440) was chosen as the second firewall to protect internal network. Major latest software version (IPSO 3.6 and Checkpoint NG FP2) will be applied on this box. Checkpoint firewall will filter the access from DMZ, VPN, and office to internal business network.

1.4.5 Intrusion Detection Servers

ISS Real Secure 7.0 is used as IDS platform. It's a leading technical provider in the intrusion detection market. We use Real Secure for Nokia 7.0 as IDS

manager and Real Secure Network Sensor 7.0 as probe. This tool can be installed on Windows 2000, Solaris and Linux. We choose Nokia security platform as server to enhance the performance and provide better security assurance. And the probe software is installed on windows 2000 boxes with SP3.

1.4.6 Web Servers

GIAC will run redundant Iplanet version 4.1 SP9 web servers on Solaris 8 machines. Sun 220R machines will be used for this purpose. OS on the web server will be properly hardened and will run only the services necessary to support web server functionality. These web servers will run separate SSL enable sites for Customers, Suppliers and Partners. All auditing will be turned on these machines. Also we will run file integrity checking software on the html directories to detect unauthorized change in content.

1.4.7 Mail Gateway

SendMail version 8.12.6 will be used as the SMTP relay to send and receive email over the Internet. SendMail was chosen because of low cost, wider install base and ease of configuration. It will be installed on Netra machine running Solaris 8, with the latest recommend patches.

1.4.8 Proxy Server

We will use Squid 2.5 on Solaris 8 as the outbound proxy to provide controlled Internet access to the GIAC employees. Internet access will be restricted to http, https and ftp ports. Squid was the proxy of choice because it is a high performance proxy server with extensive RAM caching of files and DNS. Also it supports pass through SSL and has highly configurable ACL's and can filter on IP, domain, URL, browser etc. Squid also writes extensive logs and many free log analyzers are available to analyze the logs. The service will be running on TCP port 3000.

1.4.9 Database server

Oracle 9i is being used as the database server. It is being run on Solaris 8 on a 220R platform. It will be installed on an isolated network and all access to it will be restricted logically from the Application Server. Pre-Authorized Database Administrators will require physical access for all maintenance and backup purposes.

1.4.10 Internal Domain Server

Microsoft Windows 2000 server running Active Directory is used as Internal Domain server. It's very typical use for an enterprise such as GIAC to establish office domain to manage all his users. It provides domain authentication, file

sharing and printing functions. Also it can be integrated with Internal Email Server (Microsoft Exchange Server) to share authentication and authorization information. It's installed on Windows 2000 Server with SP3.

1.4.11 Internal Email Server

Microsoft Exchange Server 2000 (with SP1) is used as Internal Email Server. It's installed on a Windows 2000 Server with SP3.

Table 2 illustrates the internal IP addresses for GIAC servers.

SERVER NAME	IP ADDRESS	EXTERNAL IP	DESCRIPTION
PUBLIC WEB SERVER	10.10.10.5/24	132.96.238.129	Provides HTTP server to Internet
ONLINE ORDERING WEB	10.10.10.6/24	132.96.238.130	Provides HTTP/HTTPS to Internet
DNS SERVER	10.10.10.7/24	132.96.238.131	Provides DNS Service to Internet
EXTERNAL EMAIL SERVER	10.10.10.8/24	132.96.238.132	Allows Internet Email access, and can access Internal Email Server
PROXY SERVER	10.10.10.9/24	132.96.238.201	Proxy server is running on port 3000
VPN TERMINAL	10.10.40.2/24	132.96.238.11/29	
INTERNAL EMAIL SERVER	10.10.20.5/23		Can be accessed from External Email server and office
INTERNAL DNS SERVER	10.10.20.10/23		For office users.
INTERNAL DOMAIN SERVER	10.10.20.15/23		For domain user authentication
APPLICATION SERVER	10.10.30.5/24		Only be accessed from Online ordering server and office clients (at port 3234)
DB SERVER	10.10.30.10/24		Only access from Application server
VPN MANAGER	192.168.1.5/24		
FIREWALL MANAGER	192.168.1.10/24		
IDS MANAGER	192.168.1.15/24		

TABLE 2: SERVER IP ADDRESSES

2: SECURITY POLICY AND TUTORIAL

2.1 Border Router

In our design, the border router is only responsible for communication; it connects the GIAC office to ISP and then to Internet. A CISCO high-end router (3600) and latest major version IOS (12.1) will be used in this scenario. Also we will do a lot of hardening job on that box before it goes to production to prevent it from hacking. Since GIAC only connects to one ISP, static routing is used in this case.

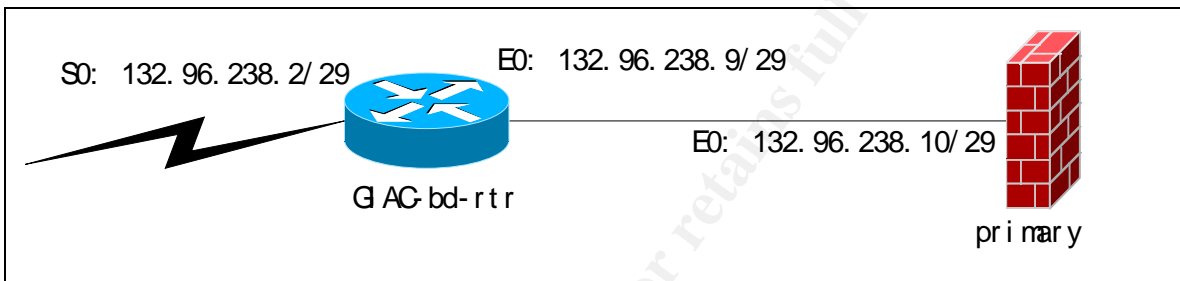


DIAGRAM 2: IP SCHEMA FOR BORDER ROUTER AND EXTERNAL FIREWALL INTERFACES

2.1.1 Border Router Configuration

```
!  
! NVRAM config last updated at 13:58:41 EST Fri Feb 8 2002  
!  
version 12.1  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption  
!  
no service tcp-small-servers  
no service udp-small-servers  
no ip bootp server  
no service finger  
no ip source-route  
no ip identd  
no ip http server  
no cdp run  
ntp disable  
no ip direct-broadcast  
no ip redirects  
no ip unreachablees  
!  
hostname GIAC-bd-rtr  
!
```

```

boot system flash ios1207.bin
logging buffered 4096 debugging
enable secret 5 $1$C2zm$5/KweBkvUR5D5rOs.kod.
enable password 54jkt3Ty
!
clock timezone EST -5
ip subnet-zero
!
interface Ethernet0
ip address 132.96.238.9 255.255.255.248
no ip route-cache
no ip mroute-cache
!
interface Serial0
ip address 132.96.238.2 255.255.255.248
!
ip classless
ip route 0.0.0.0 0.0.0.0 132.96.238.1
ip route 132.96.238.128 255.255.255.128 132.96.238.6
!
line con 0
transport input none
line vty 0 4
password sjT0lsk
login
!
end

```

CONFIGURATION 1: BORDER ROUTER CONFIGURATION

2.1.2 Explanation of Border Router Configuration

Table 3 below provides a step-by-step explanation of the border router configuration. A complete command set for Cisco IOS 12.1 is available at http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a0080087e3e.html

Command	Description
no service tcp-small-servers no service udp-small-servers	When you disable the minor TCP/IP servers, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS® software to send a TCP RESET packet to the sender and discard the original incoming packet. When you disable the UDP servers, access to Echo, Discard, and Chargen

	ports causes the Cisco IOS® software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
no ip direct-broadcast no ip redirects no ip unreachable	Disable sending "ICMP unreachable" , "ICMP redirect" packets.
no ip bootp server	When you disable the BOOTP server, access to the BOOTP ports cause the Cisco IOS software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
no service finger	To disallow Finger protocol requests (defined in RFC 742) to be made of the network server, use this global configuration command. This service is equivalent to issuing a remote show users command.
no ip source-route	To discard any IP datagram containing a source-route option use this command. It is not good practice to allow IP source routing due to implicit tunneling attacks.
no ip identd	The ip identd (RFC 1413) command returns accurate information about the host TCP port; however, no attempt is made to protect against unauthorized queries.
no ip http server	To remove the ability to use http to manage Cisco routers. This is very important considering IOS® HTTP Authorization vulnerability.
no cdp run	To prevent information gathering about routers.
ntp disable	If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain

	specified peers.
boot system flash ios1207.bin logging buffered 4096 debugging	Configure the IOS image where router boots. And configure buffer to hold logging information.
enable secret 5 \$1\$C2zm\$5/KweBkvURe5D5rOs.kod. enable password 54jkst3Ty	Set enable password what is encrypted.
service password-encryption	All the passwords are in encryption format
ip subnet-zero ip classless	Set router to recognize subnet zero, such as 10.10.0.0/24. Set router to recognize CIDR address.
ip route 0.0.0.0 0.0.0.0 132.96.238.1 ip route 132.96.238.128 255.255.255.128 132.96.238.6	Configure default router to Internet. And route DMZ packets to firewall port.
interface Ethernet0 ip address 132.96.238.9 255.255.255.252 no ip route-cache no ip mroute-cache	Configure E0 interface.
line con 0 transport input none password akdf45ty line vty 0 4 password sjT0lsk login	Configure console and VTY password.

TABLE 3: A STEP-BY-STEP EXPLANATION OF BORDER ROUTER CONFIGURATION

2.2. External Firewall

The primary PIX firewall will perform the following two main functions:

1. NAT, Network Address Translation
2. Traffic Filter, all inbound and outbound traffic will be monitored and filtered according to the policy design.

Table 4 demonstrates how we are handling NAT in order to make services available online.

SOURCE IP	DESTINATION IP	PROTOCOL	TRANSLATE SOURCE IP	TRANSLATE DESTINATION IP	TRANSLATE PROTOCOL	REMARK
Any	132.96.238.129	HTTP	Any	10.10.10.5	HTTP	GIAC public web server
Any	132.96.238.130	HTTP HTTPS	Any	10.10.10.6	HTTP HTTPS	GIAC online ordering web server
Any	132.96.238.131	DNS	Any	10.10.10.7	DNS	GIAC DNS server
Any	132.96.238.132	Email	Any	10.10.10.8	Email	GIAC Email Gateway
10.10.10.9	Any	HTTP HTTPS DNS	132.96.238.201	Any	HTTP HTTPS DNS	Proxy access to Internet
10.10.20.0/23	Any	ICMP	132.96.238.202	Internet	ICMP	For office network to test Internet activity
10.10.10.8	Any	Email	132.96.238.132	Any	Email	Access to Internet Email Server

TABLE 4: ILLUSTRATION OF HOW PIX HANDLES NAT

2.2.1 External Firewall Access Control List

Table 5 provides a simplified view of the access control lists as they are being implemented on the external firewall.

SOURCE IP	DESTINATION IP	PROTOCOL	ACTION	REMARK
Any	10.10.10.5 10.10.10.6 10.10.10.7 10.10.10.8	HTTP HTTPS Email DNS	Allow	Permit access from Internet to DMZ, especially allow icmp for connectivity testing
10.10.10.6	10.10.30.5	TCP 3234	Allow	Permit business web access application server in Internal segment
10.10.10.8	10.10.20.5	Email	Allow	Permit access from Email Gateway to Internal Email server
10.10.10.8	Any	Email	Allow	Permit Email server sent out Email
10.10.10.9	Any	HTTP HTTPS FTP	Allow	Permit proxy access Internet
10.10.20.0/23	Any	ICMP	Allow	Permit connectivity test from Office
10.10.40.0/24	10.10.20.0/24	Any	Allow	Permit VPN connection to office
Any	Any	Any	Deny	Deny any other access

TABLE 5: ILLUSTRATION OF PIX ACL'S

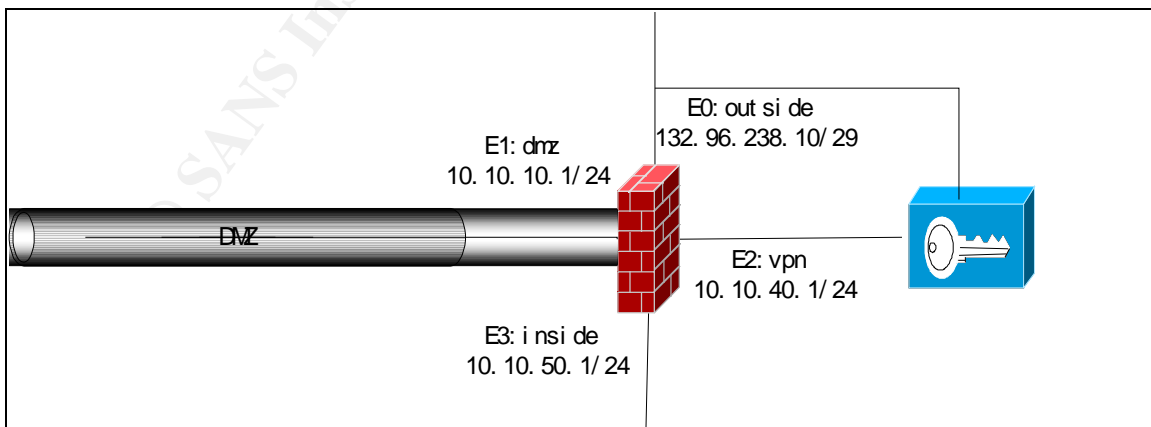


DIAGRAM 3: IP SCHEMA FOR EXTERNAL FIREWALL AND VPN SWITCH INTERFACES

2.2.2 External Firewall Configuration

```
primary# show run

PIX Version 6.2(2)

nameif ethernet0 outside security0
nameif ethernet1 dmz security50
nameif ethernet2 vpn security60
nameif ethernet3 inside security100

enable password xAJ5.yJk9/GRElWH encrypted
passwd 2KFQnbNIdI.2KYOU encrypted

hostname primary
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521

pager lines 24
logging on
logging trap debugging

interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto

mtu outside 1500
mtu dmz 1500
mtu vpn 1500
mtu inside 1500

ip address outside 132.96.238.10 255.255.255.248
ip address inside 10.10.50.1 255.255.255.0
ip address dmz 10.10.10.1 255.255.255.0
ip address vpn 10.10.40.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover

static (dmz, outside) 132.96.238.129 10.10.10.5 netmask 255.255.255.255
0 0
static (dmz, outside) 132.96.238.130 10.10.10.6 netmask 255.255.255.255
0 0
static (dmz, outside) 132.96.238.131 10.10.10.7 netmask 255.255.255.255
0 0
static (dmz, outside) 132.96.238.132 10.10.10.8 netmask 255.255.255.255
0 0

access-list acl dmz in permit tcp any host 132.96.238.129 eq www
```

```

access-list acl_dmz_in permit tcp any host 132.96.238.130 eq www
access-list acl_dmz_in permit tcp any host 132.96.238.130 eq 443
access-list acl_dmz_in permit tcp any host 132.96.238.131 eq 53
access-list acl_dmz_in permit tcp any host 132.96.238.132 eq smtp
access-list acl_dmz_in deny any any
access-group acl_dmz_in in interface outside

nat (dmz) 2 0 0
global (outside) 2 132.96.238.201 255.255.255.255

access-list acl_dmz_out permit tcp host 10.10.10.9 any eq www
access-list acl_dmz_out permit tcp host 10.10.10.9 any eq 443
access-list acl_dmz_out permit tcp host 10.10.10.9 any eq 25
access-list acl_dmz_out permit tcp host 10.10.10.7 any eq 53
access-list acl_dmz_out permit tcp host 10.10.10.8 any eq smtp
access-group acl_dmz_out deny any any
access-group acl_dmz_out in interface dmz

nat (inside) 3 0 0
global (outside) 3 132.96.238.202 255.255.255.255

static (inside, dmz) 10.10.20.0 10.10.20.0 netmask 255.255.254.0 0 0
static (inside, dmz) 10.10.30.0 10.10.30.0 netmask 255.255.255.0 0 0
static (inside, vpn) 10.10.20.0 10.10.20.0 netmask 255.255.254.0 0 0
access-list acl_to_office permit ip 10.10.40.0 255.255.255.0 10.10.20.0
255.255.255.0
access-list acl_to_office permit tcp host 10.10.10.8 host 10.10.20.5 eq
smtp
access-list acl_to_office permit tcp host 10.10.10.6 host 10.10.30.5 eq
3234
access-group acl_to_office out interface inside

arp timeout 14400

route outside 0.0.0.0 0.0.0.0 132.96.238.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323
0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
no snmp-server enable traps
floodguard enable
no sysopt route dnat
telnet timeout 5

terminal width 80

Cryptochecksum:500ffb58b0bd85e89dcad134365d9e87
: end

```

CONFIGURATION 2: EXTERNAL FIREWALL CONFIGURATION

2.2.3 External Firewall Configuration Explanation

Table 6 below displays a step-by-step explanation of the external firewall configuration shown above.

COMMAND	DESCRIPTION
<pre>Nameif ethernet0 outside security0 nameif ethernet1 dmz security50 nameif ethernet1 vpn security60 nameif ethernet2 inside security100</pre>	Map logical interfaces to physical interfaces.
<pre>mtu outside 1500 mtu dmz 1500 mtu vpn 1500 mtu inside 1500</pre>	Configure logical interface parameters.
<pre>ip address outside 32.96.236.6 255.255.255.252 ip address inside 10.10.20.1 255.255.254.0 ip address dmz 10.10.10.1 255.255.255.0 ip address vpn 10.10.40.1 255.255.255.0</pre>	Assign IP addressed to three logical interfaces.
<pre>fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol rsh 514 fixup protocol rtsp 554 fixup protocol smtp 25 fixup protocol sqlnet 1521</pre>	Enable FTP, HTTP, and SMTP services to use CISCO Adaptive Security Algorithm.
<pre>ip audit info action alarm ip audit attack action alarm no failover</pre>	Enable IP auditing on PIX and disable failover feature.
<pre>enable password xAJ5.yJk9/GRElWH encrypted passwd 2KFQnbNIdI.2KYOU encrypted</pre>	Set password and keep it in encrypted format.
<pre>static (dmz, outside) 132.96.238.129 10.10.10.5 netmask 255.255.255.255 0 0 static (dmz, outside) 132.96.238.130 10.10.10.6 netmask 255.255.255.255 0 0 static (dmz, outside) 132.96.238.131 10.10.10.7 netmask 255.255.255.255 0 0 static (dmz, outside)</pre>	All inbound traffic from Internet to DMZ. These rules will translate DMZ IP to global IP and allow certain service access to DMZ.

<pre> 132.96.238.132 10.10.10.8 netmask 255.255.255.255 0 0 access-list acl_dmz_in permit tcp any host 132.96.238.129 eq www access-list acl_dmz_in permit tcp any host 132.96.238.130 eq www access-list acl_dmz_in permit tcp any host 132.96.238.130 eq 443 access-list acl_dmz_in permit tcp any host 132.96.238.131 eq 53 access-list acl_dmz_in permit tcp any host 132.96.238.132 eq smtp access-list acl_dmz_in deny any any access-group acl_dmz_in in interface outside </pre>	
<pre> nat (dmz) 2 0 0 global (outside) 2 132.96.238.201 255.255.255.255 access-list acl_dmz_out permit tcp host 10.10.10.9 any eq www access-list acl_dmz_out permit tcp host 10.10.10.9 any eq 443 access-list acl_dmz_out permit tcp host 10.10.10.9 any eq 25 access-list acl_dmz_out permit tcp host 10.10.10.7 any eq 53 access-list acl_dmz_out permit tcp host 10.10.10.8 any eq smtp access-group acl_dmz_out deny any any access-group acl_dmz_out in interface dmz </pre>	<p>Enable some DMZ access to Internet. All the DMZ address will be translated to global address 132.96.238.201. But only proxy and email are allowed to go out.</p>
<pre> nat (inside) 3 0 0 global (outside) 3 132.96.238.202 255.255.255.255 </pre>	<p>All office traffic to DMZ, VPN segments and Internet. Only ICMP traffic is allowed from office to Internet and 132.96.238.202 will be used a original IP.</p> <p>From office, users can access proxy server in DMZ.</p> <p>Inside interface is in higher security level than DMZ, so it's always allowed to access DMZ from office.</p>
<pre> static (inside, dmz) 10.10.20.0 10.10.20.0 netmask 255.255.254.0 0 0 static (inside, dmz) 10.10.30.0 10.10.30.0 netmask 255.255.255.0 0 0 </pre>	<p>External Email server in DMZ can access Internal Email server. And VPN users can access office with full authorization.</p> <p>All these access use original IP address. No translation needed.</p>

<pre>static (inside, vpn) 10.10.20.0 10.10.20.0 netmask 255.255.254.0 0 0 access-list acl_to_office permit ip 10.10.40.0 255.255.255.0 10.10.20.0 255.255.255.0 access-list acl_to_office permit tcp host 10.10.10.8 host 10.10.20.5 eq smtp access-list acl_to_office permit tcp host 10.10.10.6 host 10.10.30.5 eq 3234 access-group acl_to_office out interface inside</pre>	
<pre>route outside 0.0.0.0 0.0.0.0 132.96.238.5 1 timeout xlate 3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute</pre>	<p>Configure default route to the border gateway 132.96.238.5.</p> <p>And configure parameters for address translation and connection.</p>
<pre>telnet timeout 5</pre>	<p>Restrict telnet</p>

TABLE 6: A STEP-BY-STEP EXPLANATION OF THE EXTERNAL FIREWALL CONFIGURATION

2.3 VPN Policy and Tutorial

Next step is to implement GIAC VPN policy. A Nortel Contivity 1700 series switch has been bought GIAC to allow its remote sales users access to the internal GIAC applications like Corporate Email, Intranets etc. An address pool will be created on the contivity switch and the VPN users will be assigned an IP address in the 10.10.40.0/24 network after they have successfully authenticated to the Nortel Switch using their certificates stored on an eToken. Both external firewall and Internal firewall have been configured to allow the VPN traffic from 10.10.40.0/24 through to the office network.

This section provides a step-by-step tutorial on How to configure the Contivity Switch to use certificates in order to Authenticate Users.

2.3.1 VPN Tutorial

To manage the switch using web browser, connect to the console and add the management IP.

Step 1: Setup the LAN connection

In this section we will assign IP Addresses to the switch's public and private interfaces:

1.1 Open the Nortel Management Web Pages

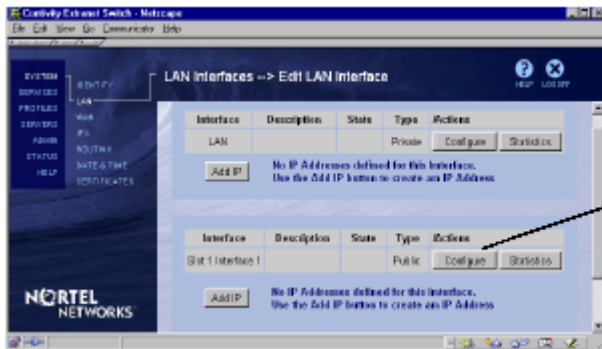
Open System->LAN. The LAN Interfaces Page opens



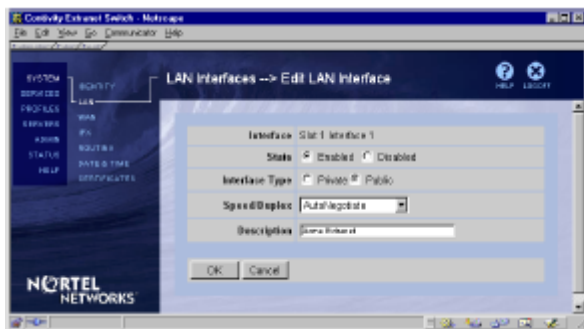
For the LAN (private) interface, click **Configure**.



Enter a description of the LAN interface.
Click OK.



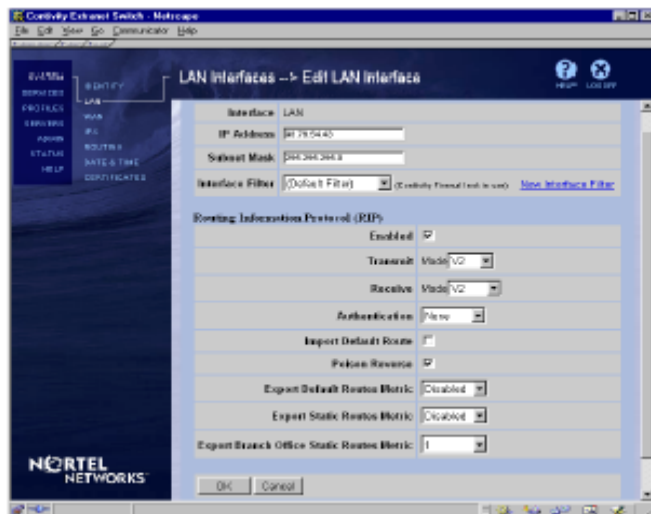
For the Slot 1 (public) interface, click Configure.



Enter a description of the public interface.
Click OK.



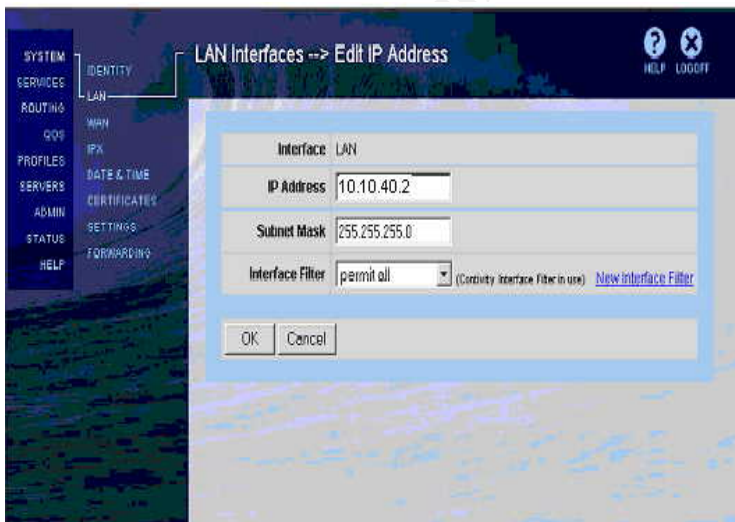
For the public (external) interface, click Add IP.



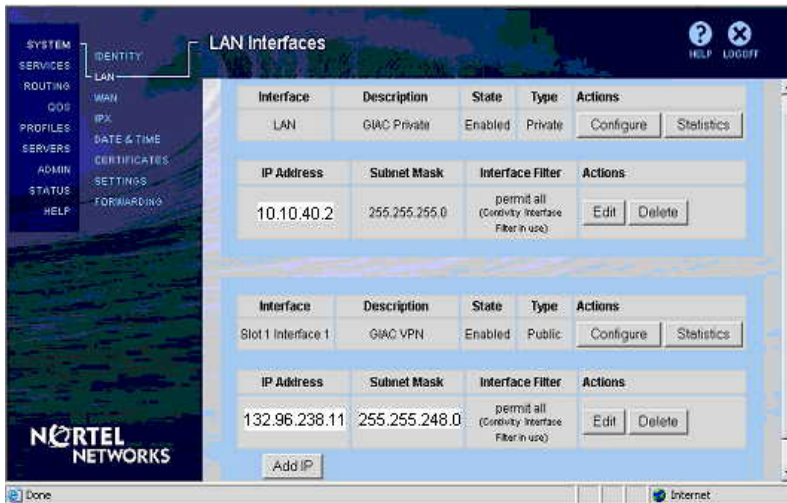
Enter the IP address of the public interface.
Click OK.



Optional:
For the private (internal) interface, click **Add IP** and enter the appropriate information.



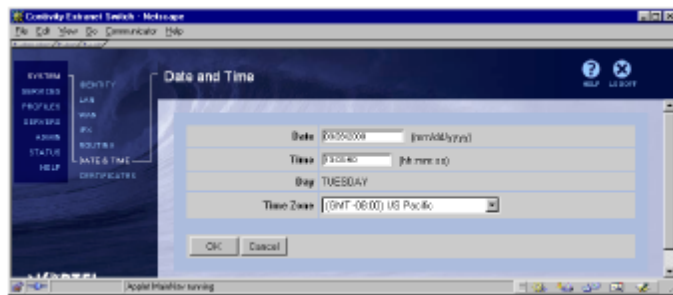
Add the IP Address and Click OK



This finishes the configuration of the public and private LAN interfaces of the Nortel Contivity Switch.

Step 2 Setup system Date and Time

Click System-> Date and Time



Enter the current date and time.
Select a time zone.
Click OK.

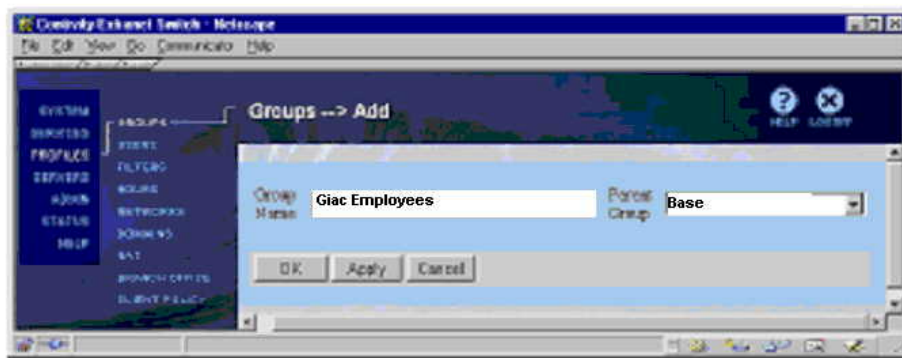
Step 3 Create a group

By creating a group we can combine the end-users that are allowed to access the VPN.

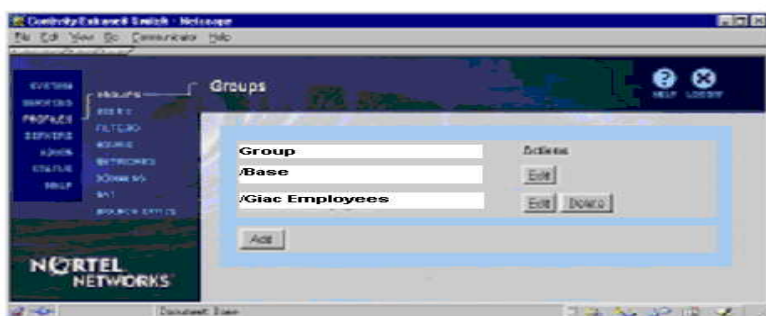
Click Profile->Groups.



Click Add.
The Groups → Add page opens.

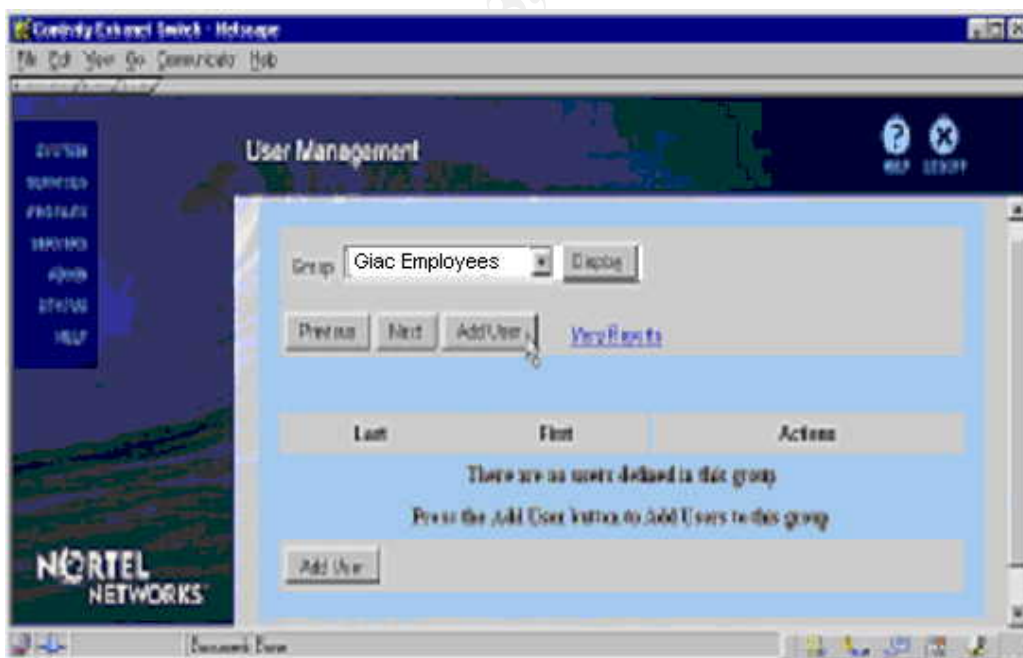


Enter a group name (Giac Employees in this example) and Click OK.



The Groups page now includes the Giac Employees group

Step 4 Add Users to the Group (or Enable All Option)



Click Add User

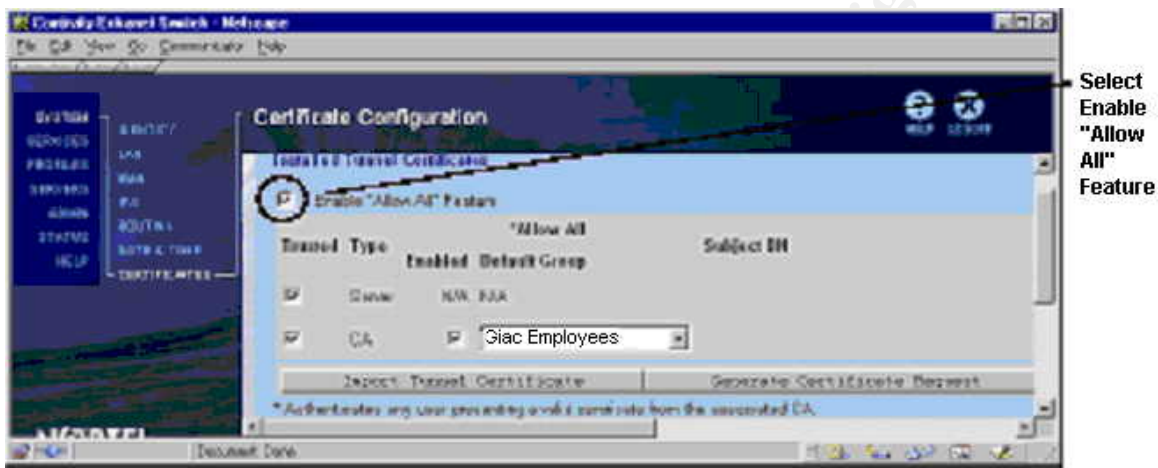
Once we have created a group we have two options

Add individual users to the group. As a result each individual user is added to the switch's internal LDAP directory as an entity that is allowed VPN access to specified network.

Enable the *Allow All* feature to allow VPN access to any user whose certificate is signed by the CA whose CA certificate is configured on the switch.

GIAC is going to create a separate VPN CA and only remote sales force is going to be allowed to access the VPN, we are going to enable *Allow All* feature.

To configure *Allow All* feature **Click System-> Certificates**



Step 5 Load the CA certificate into the switch

In this step, we retrieve the root certificate of the GIAC VPN CA (from Soltrus hosted Web Site) that issues IPsec device and client certificates for GIAC, and save it on the switch. Extranet Access Client uses this certificate to authenticate the signature on the encrypted 3DES key presented by the switch when initiating VPN sessions.

The switch will use the CA certificate to authenticate digital signatures presented by clients. Extranet Access Client also uses this certificate to authenticate the digital signatures presented by the switch when initiating VPN sessions.

GIAC's VPN CA can be downloaded from GIAC MPKI Control center hosted by Soltrus.

Open the MPKI Control Center to the *Configuration Menu*





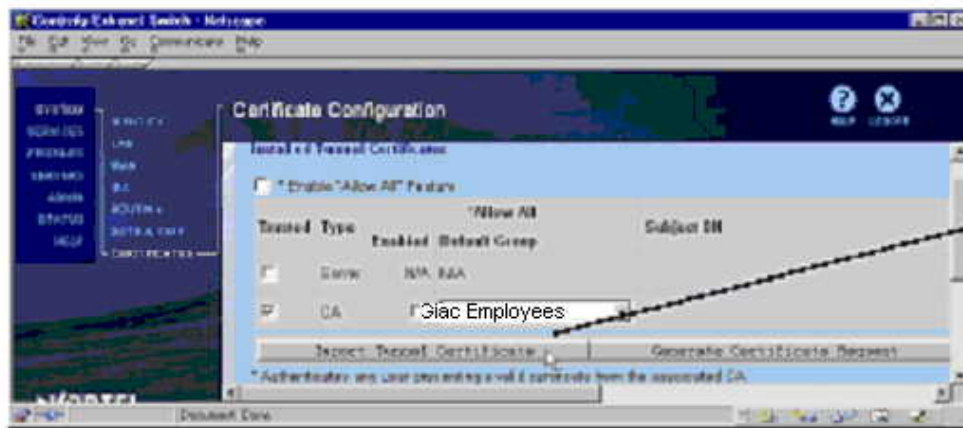
The *Install CA* page opens.

Select the entire text of the CA certificate, including the **Begin** and **End** comments.

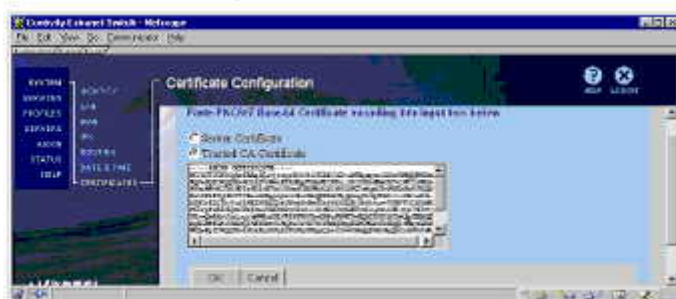
Copy the text (Ctrl-C).

In the next step, you paste this text into the **Conivity Switch Management** pages.

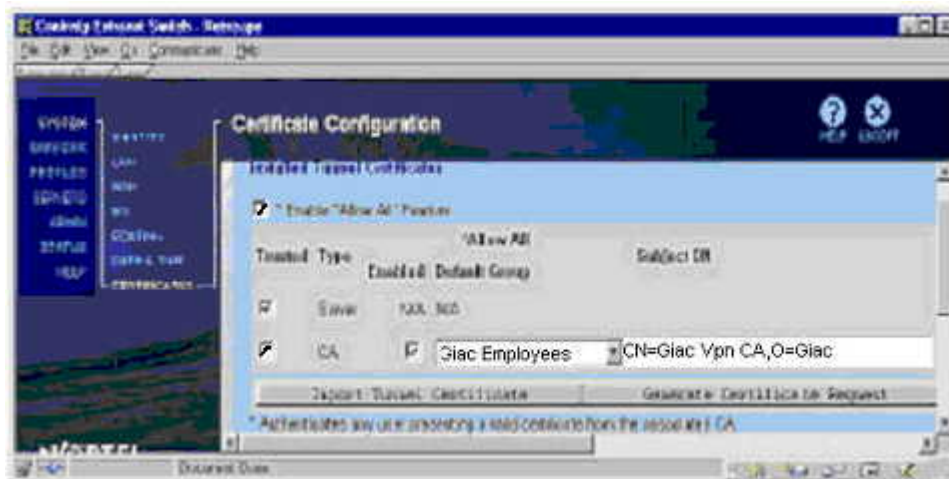
Next Click System-> Certificates



Ensure that the correct group is selected, and click **Import Tunnel Certificate**



Select **Trusted CA Certificate**. Paste the certificate into the text box, and click **OK**.



The O and OU values for the CA certificate now appear.

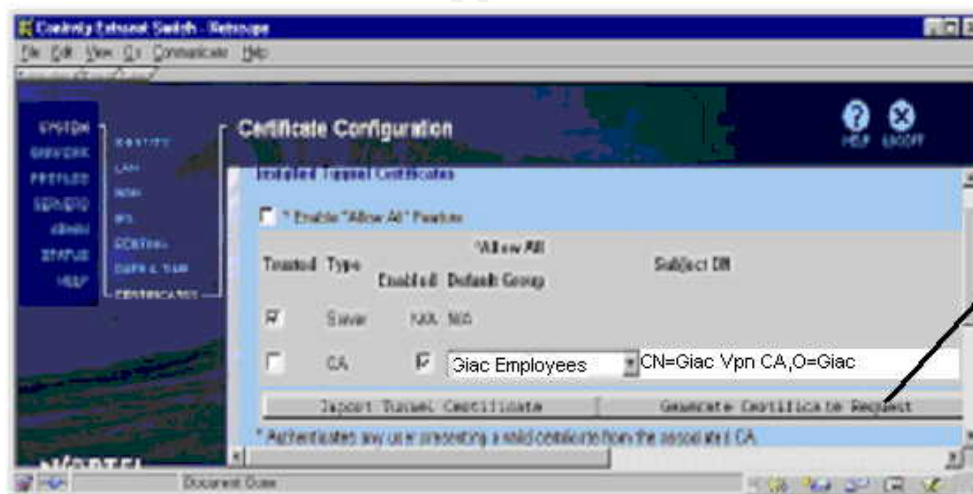
Select both the Trusted and Enabled check boxes

Now we have successfully stored GIAC Private VPN CA hosted as a managed service by Soltrus, the Canadian Affiliate of Verisign.

Step 6 Generate Certificate Signing Request

In this step, we will use the Contivity Management pages to generate a certificate signing request (CSR). The CSR contains the switch's public key, uniquely identifies the switch, and enables Soltrus to generate the unique IPsec device certificate for this switch.

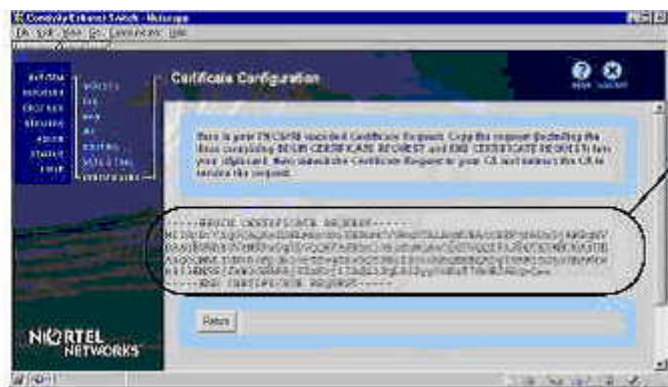
Click System-> Certificates



Click Generate Certificate Request



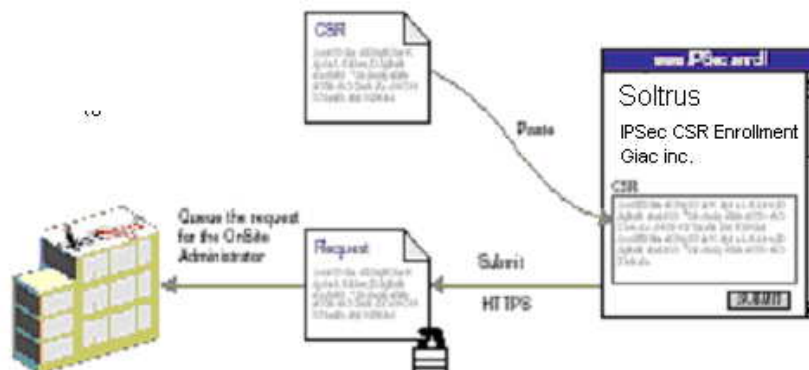
Enter the values for the switch name and organization.
Click OK



Select and copy the full text of the certificate request (including the Begin and End comments).
Click return

Step 7 Request an IPsec device certificate for the switch

In this step, we will use the CSR to request a Soltrus IPsec device certificate for the switch. We browse to the IPsec Device certificate enrollment form, paste the CSR into the form, and submit the form to Soltrus. Soltrus stores the request and places notification of the request in the MPKI administrator's queue.



From the *Certificate Management* page of the OnSite Control Center, click the **User (or Lifecycle) Services** link.



The Lifecycle Services page opens.

Click the link to the Lifecycle Services Web page.



The Digital ID Center page opens.

Click the Enroll for a Digital ID for a VPN device link.

Caution: Do not click the Enroll link in this step.

VeriSign OnSite Enrollment

[Help with this Page](#)

Complete Enrollment Form

Submit Certificate Signing Request File
Your Administrator should have sent you email knowledge that explains how to send for a Digital ID. The message includes information on how to find the Certificate Signing Request (CSR) file that holds the public key. If you have questions about this file, [Contact Your Administrator](#).

Enter Path to CSR File:

Information for the Digital ID
Fill in fields. Use only the English alphabet without accents here. The information entered with a "*" is included in your Digital ID and is available to the public.

First Name: *	<input type="text"/>
Last Name: *	<input type="text"/>
E-mail Address: *	<input type="text"/>
FQDN: *	<input type="text"/>
Employee ID Number: *	<input type="text"/>
Fully Qualified Domain Name: *	<input type="text"/>
IP Address: *	<input type="text"/>

Challenge Please
This screen provides instructions for your next step in your action on your Digital ID and should not be shared with anyone. Do not leave it if it is required to enroll and name your Digital ID.

Enter Challenge Response:

Optional: Enter Comments
In some cases, your Administrator will contact you to enter Shared Secret information (keys only to you and the Administrator) information in this field. The Administrator does this shared secret to verify that it only is you submitting the application. This comment will not be included in your Digital ID.

© 2000 VeriSign, Inc. All Rights Reserved

The IPsec CSR Enrollment page opens.

Following the instructions on the page, fill in the enrollment form:

- Browse to the CSR file and select it.
- Fill in the other enrollment fields.
- Be sure to enter the e-mail address (typically, yours) to which the certificate should be sent.
- When the form is complete, click **Submit** to submit the request.

In the next step, you approve this request.

Step 8 Using MPKI, approve the request for the switch certificate

As part of buying the MPKI service from Soltrus, a designated GIAC MPKI administrator enrolls for an MPKI account and Soltrus issues him an administrator certificate that will enable the GIAC MPKI administrator to manage the certificate lifecycle for all the GIAC VPN users.

From the MPKI Control Center, we will approve the request for the switch's certificate. Soltrus generates the certificate and e-mails it to VPN administrator.

Open the Control Center at
<https://xxx.soltrus.com/abc.htm>



The browser prompts for the OnSite administrator's certificate that enables access to the OnSite Control Center.
 Select the administrator certificate, and click Continue.



If you have protected your certificate database with a password, this dialog box appears.
 Enter the password, and click OK.



The OnSite Control Center opens.
 View the list of pending requests for certificates by clicking the **Process Requests** link on the **Certificate Management** page.



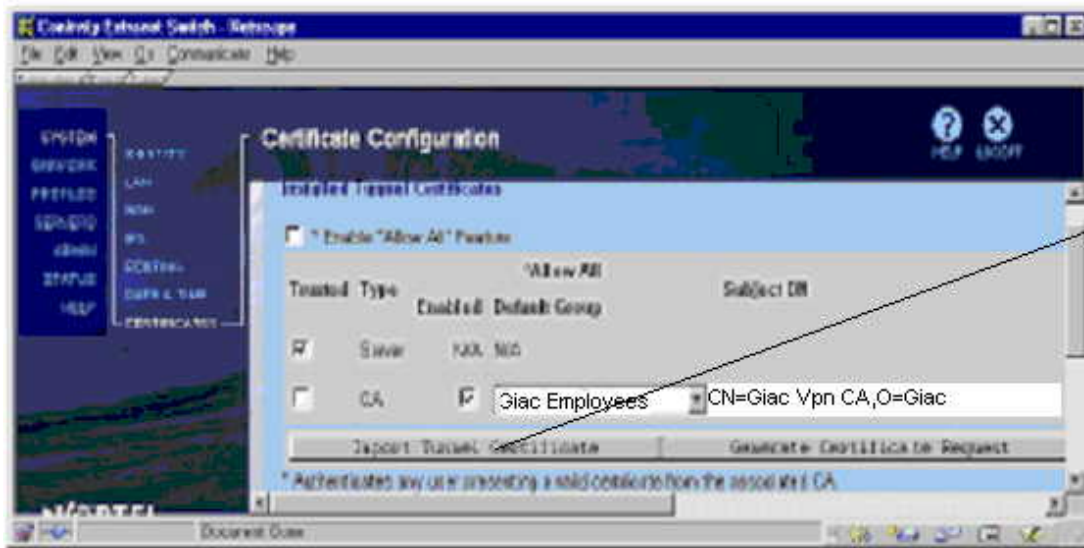
The **Process Requests** page opens.
 Find the request that you just submitted, and click the **Approve** link.

Step 9 Store the IPsec device certificate on the switch

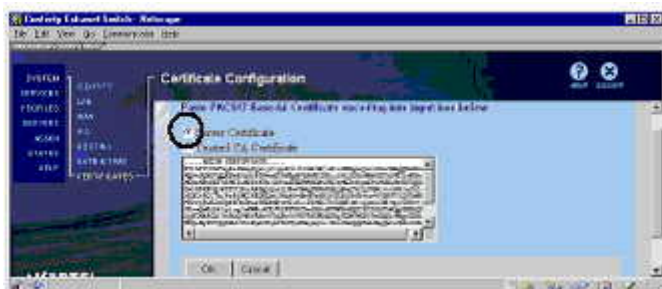
Next we will copy the certificate from the e-mail message, paste the certificate into the Contivity Management page, and import the certificate into the switch's certificate store.

Open Soltrus's e-mail message. Copy the full text of the certificate (including the Begin and End comments).

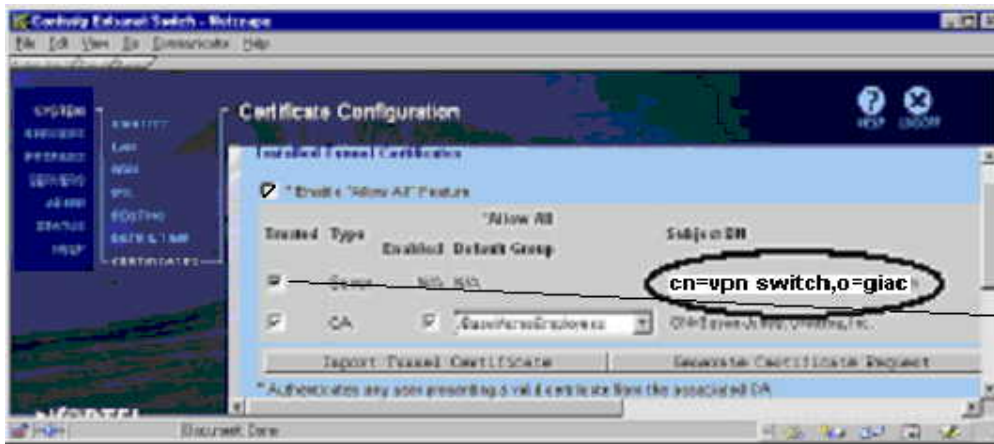
In the Management pages, **click System -> Certificates**.



Select Server Certificate. Click Import Tunnel Certificate



Select Server Certificate. Paste the certificate (copied from the email) into the text box, and click OK

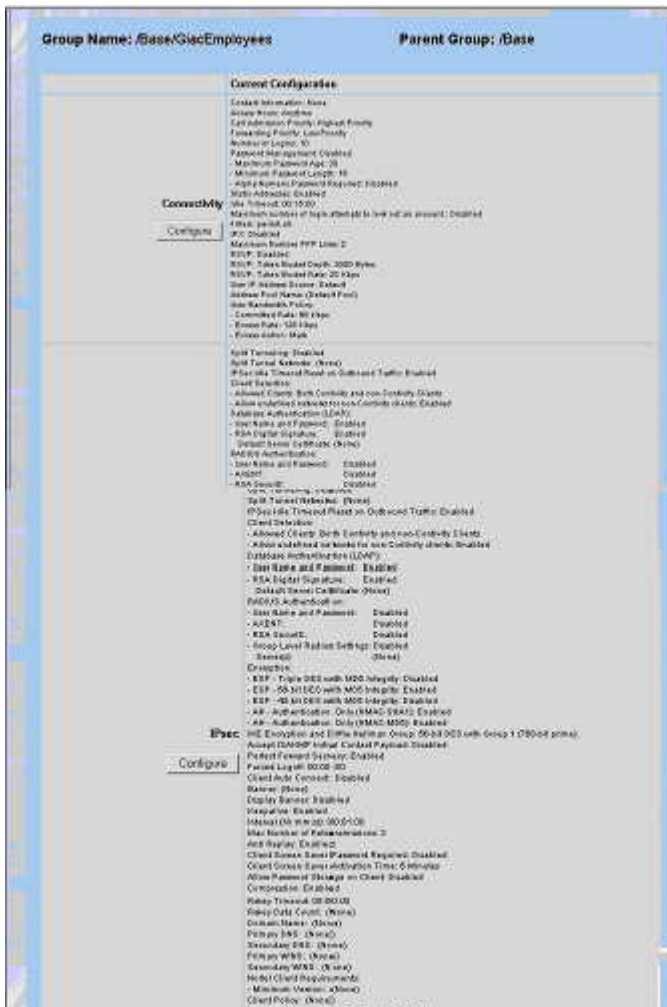


The Certificate appears on the page. Click the Trusted check box.

We have successfully stored the switch's IPsec device certificate.

Step 10 Configure the Giac Employees group to use Certificates for Authentication

Click Edit to configure the Policies for the group



Next step is to configure the Authentication mechanism for remote users. Click Configure Under IPsec section to configure IPsec Policies. RSA Digital Signatures will be the only authentication mechanism selected. We have chosen the IPsec switch certificate we enrolled for from before as the default server certificate.

Field	Value	Actions	Inherited From
Split Tunneling	Disabled	Configure	/Base
Split Tunnel Networks	(None)	Configure	/Base
IPsec Idle Timeout Reset on Outbound Traffic	Enabled	Configure	/Base
Client Selection	Allowed Clients: Both Contivity and non-Contivity Clients Allow undefined networks for non-Contivity clients: Enabled	Configure	/Base
Authentication	Database Authentication (LDAP): - User Name and Password: Disabled - RSA Digital Signature: Enabled Default Server Certificate: cn=vpn switch,o=giac * RADIUS Authentication: - User Name and Password: Disabled - AVERT: Disabled - RSA SecurID: Disabled - Group Level Radius Settings: Disabled Server(s): (None) Group ID: (None) LDAP Authentication: Group ID: (None)	Configure	/Base
Encryption	ESP - Triple DES with MD5 Integrity: Disabled ESP - 56-bit DES with MD5 Integrity: Enabled * ESP - 40-bit DES with MD5 Integrity: Disabled AH - Authentication Only (HMAC-SHA1): Enabled AH - Authentication Only (HMAC-MD5): Enabled	Configure	/Base

This completes the Nortel Switch configuration that will enable users to use certificates for authenticating to the VPN switch.

2.4 Internal Firewall

This section describes in detail the internal firewall rule set and interface configuration. Diagram 4 below displays the IP schema for all the interfaces on the internal firewall.

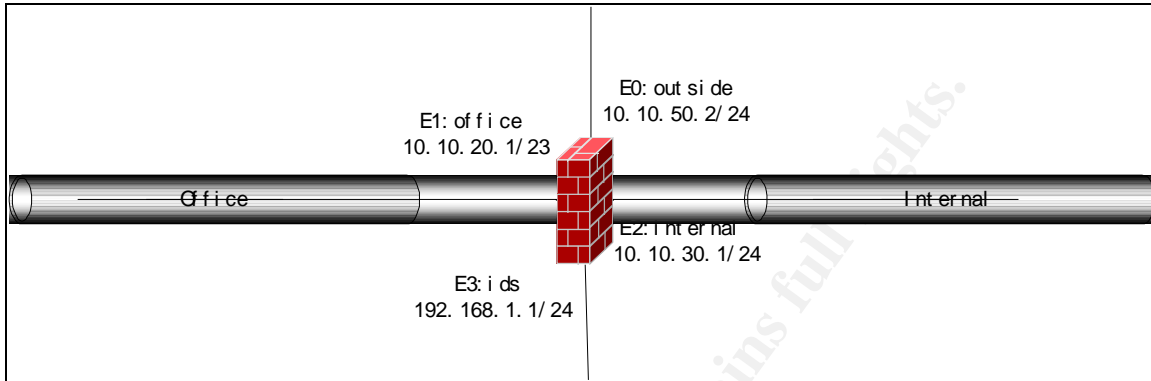


DIAGRAM 4: IP SCHEMA FOR INTERNAL FIREWALL INTERFACES

1.4.1 Internal Firewall Policy

RULE	SOURCE	DESTINATION	SERVICES	ACTION	TRACK	TIME	INSTALL ON	COMMENTS
1	Online_order	App_svr	TCP business	accept	Long	Any	Internal_FW	Allow access to business server via online ordering web
2	External_Email	Internal_Email	TCP SMTP	accept	Long	Any	Internal_FW	Allow External Email access Internal Email
3	Internal_DNS	External_DNS	TCP domain-tcp	accept	Long	Any	Internal_FW	Internal DNS connect to external DNS
4	Office	Proxy_server	TCP HTTP TCP HTTPS	accept	Long	Any	Internal_FW	Office can access proxy server
5	FW_mgmt	Internal_FW	Any	accept	Long	Any	Internal_FW	Firewall management
6	Internal_FW	FW_mgmt	TCP FW_Log	accept	Long	Any	Internal_FW	Firewall logging
7	VPN	Office	TCP SMTP	accept	Long	Any	Internal_FW	Allow vpn user access to office
8	Office	Any	ICMP ICMP	accept		Any	Internal_FW	Allow office to test connectivity
9	Any	Any	Any	drop	Long	Any	Gateways	

DIAGRAM 5: INTERNAL FIREWALL RULES

2.4.2 Object Listing
















Name	Type	FW-1	IP Address	Netmask	Comment
Internal_FW	 gateway	Yes	10.10.20.2	-	Internal Firewall (Checkpoint NG)
 Internal_FW.e0			10.10.50.2	255.255.255.0	Antispoofing: Any
 Internal_FW.e1			10.10.20.1	255.255.254.0	Antispoofing: Any
 Internal_FW.e2			10.10.30.1	255.255.255.0	Antispoofing: Any
 Internal_FW.e3			192.168.1.1	255.255.255.0	Antispoofing: Any
App_svr	 host	No	10.10.30.5	255.255.255.0	Application Server in Internal Network
Online_order	 host	No	10.10.10.6	255.255.255.0	Online Ordering Web server in DMZ
Proxy_server	 host	No	10.10.10.9	255.255.255.0	Proxy Server in DMZ
Internal_Email	 host	No	10.10.20.5	255.255.254.0	Internal Email in office segment
External_Email	 host	No	10.10.10.8	255.255.255.0	External Email server in DMZ
Internal_DNS	 host	No	10.10.20.10	255.255.254.0	Internal DNS Server in office
External_DNS	 host	No	10.10.10.7	255.255.255.0	External DNS Server in DMZ
FW_mgmt	 host	No	192.168.1.10	255.255.255.0	Checkpoint Firewall management station
Office	 network	No	10.10.20.0	255.255.254.0	Whole Office Network
VPN	 network	No	10.10.40.0	255.255.255.0	VPN user segment

DIAGRAM 6: INTERNAL FIREWALL OBJECTS

2.4.3 Explanation of Checkpoint rules

The order of these firewall rules is very important. If one mistakenly puts “deny all” into the prior order, all the access will be deny and won’t pass the next rule.

Rule 1 is to permit the traffic initiated from Online Ordering Web server in DMZ to the Business Application Server in Internal network. It enables the GIAC online business function.

Rule 2,3,4 are defined to allow communication between DMZ and office services, such as Email, DNS, etc. Rules 5 permits office users access to proxy server on port 3000.

Rules 6 and 7 are used for the management of Checkpoint firewall. There is a management station what provides policies and monitoring function. The firewall should communicate with it.

Rule 8 enables the users in VPN domain (who is remotely access from Internet via VPN terminal) to access office services.

Rule 9 permits all office users to test connectivity for Internet. We found it's quite useful since GIAC is an online service provider. The employers not only have to manage the online services, but also need to get information from Internet.

© SANS Institute 2003, Author retains full rights

3: VERIFY THE FIREWALL POLICY

3.1 Plan the Audit

The purpose of the Firewall in the network is to control traffic and enforce GIAC security policy. In order to verify that GIAC's security policy is effectively enforced we need to plan a thorough audit of the GIAC network. Also an independent audit will insure that all the components of GIAC Security Policy have been implemented properly.

3.1.1 Approach and Logistics

To ensure an independent and objective audit we propose that the audit be performed by two employees from the network team who were not part of the initial design and implementation of the GIAC network infrastructure. This will also help discover any shortcomings in security policy left by the implementation and design team.

GIAC has a regular maintenance window of 4 hours on Sunday Morning between 2 AM to 6 AM. We propose to do all the scanning work against the External PIX firewall during that period. This will ensure that there is minimal downtime for the customers as GIAC is an online business and cannot afford hindrance to day-to-day business. This will also provide the technical team to restore back to a fully functional network just in case the network scanning breaks it down.

Prior permissions will be taken from the authorized personnel to carry on the network scan. Part of the audit we want to make sure that GIAC network monitoring team takes necessary action once an attack has been identified. Proper personnel will be notified about the audit so that they continue to monitor the network for an actual attack. All alarms should be attended to as before.

3.1.2 What will be reviewed

To examine the external Firewall thoroughly we plan to audit the following:

- 1) Firewall Documentation
- 2) Physical Security
- 3) Rulebase

3.1.2.1 Firewall Documentation

The first step in the auditing process will be to review all the network and firewall documentation. This will include

- Detailed network diagrams for all local area networks within the audit scope, including all significant nodes such as the border router, the

- external firewall, VPN gateway, file servers, host processing systems (Unix, mainframe, etc.), with network and node IP addresses and link transmission methods (Ethernet, token ring, etc.).
- Narrative descriptions of significant applications in use, along with descriptions of TCP/IP services (telnet, ftp, NFS, TFTP, etc.) necessary to support these applications.
 - Firewall configuration files and logs
 - Network operations and security policies and procedures

3.1.2.2 Physical Security

The purpose of determining that adequate physical security is in place over network transmission media and a network device is to prevent unauthorized physical access and/or modifications to systems and data. Once the intruder has physical access to the firewall console or the network that firewall controls, it breaks the first line of defense and makes the network relatively vulnerable.

Auditing the physical security around the Firewall will include among other things the following:

- Review of the physical security access system to ensure that there are effective controls in place for granting authorized access to the secure rooms.
- Observing the network and systems operations center to determine that physical access is granted on an as-needed basis and is well controlled.
- Determining that wiring hubs and concentrators are located in secured areas accessible only by network support personnel.
- Determining whether network management software is used throughout the network to monitor the networks physical connections and traffic load proactively.
- Review wiring diagrams and compare them to a physical observation of hub connection labeling, multiplexer link labeling, modem labels, etc., to ensure that all physical connections are authorized and documented.

3.1.2.3 Rule Base

On majority of the properly configured firewalls, you should find no open ports with no required business service running on them, you should not even be able to ping it. The goal is to ensure that the firewall is enforcing what you expect it to; in other words, no surprises or no unwanted traffic can get through the firewall. This is achieved by scanning every network segment from every other network segment to see what packets can and cannot get through the firewall.

In order to verify that the Firewall Rule base is being properly enforced we propose to use Nmap running on a Linux machine to port scan the firewall for open ports from

- Internet,
- DMZ
- Internal Network between the two firewall

NMap can be downloaded from www.insecure.org/nmap/. It is an excellent tool to scan the network for open TCP and UDP ports. One can create all sorts of different TCP Packets in order to accomplish network reconnaissance. Security administrators can enforce the company security policy by performing regular and timely scans of their network to check it for unwanted open TCP and UDP ports. Also NMap can help fingerprint the OS that can further enhance the attackers chances to hack by exploiting the known vulnerabilities for that particular Operating System.

The objective of scanning the network using NMap is to verify that GIAC ACL's are being properly enforced at the primary firewall. The firewall will be scanned to verify the following:

1. Allows the required connections from the Internet to the DMZ
2. Allows the required connections from business web server to the application server.
3. Allows Email Gateway in the DMZ to talk to the internal email system
4. Permits connections to the Internet from the proxy server
5. Machines from office network can only access Internet through the proxy (in DMZ)

3.1.3 Costs and Effort Level

The table 7 below presents the costs associated with hiring two auditors to evaluate the GIAC network. GIAC personnel will provide two laptops loaded with Linux and NMap.

ITEM	NO OF HOURS	COST
Documentation Review	8 man hrs	8 x 200 = 1600 CDN
Physical Security Review	4 man hrs	4 x 200 = 800 CDN
Rule base Verification	16 man hrs	16 x 200 = 3200 CDN
Total costs	28 man hrs	28 x 200 = 5600 CDN

TABLE 7: COSTS AND EFFORTS REQUIRED

3.2 Conducting The Audit

The audit of firewall is a three-fold process. The auditor's will follow the approach we described as follows:

3.2.1 Auditing Documentation

Based on the detailed review of the firewall configuration documents, logs and network diagrams for GIAC network, It was found out that most of the support documentation is up to date. Some of the network diagrams and supporting documentation needs to be updated based on the current firewall configurations that were reviewed.

3.2.2 Auditing Physical Security

The auditor's reviewed the access control mechanisms put in place to physically secure the network equipment. They were properly logged and granted access into the secure processing center. The PIX firewall was found properly locked in a secure rack. All the supporting network equipment was locked up in secure racks. The network cabling was properly covered and no spare network connections were found available for the auditors to plug in their laptops.

It was noted that the firewall had the console keyboard plugged off and locked in a secured cabinet. The PIX has been configured with no remote access and the only way to make configuration changes is to be on the console.

3.2.3 Auditing Rule Base

To verify the firewall rule base the auditors are going to use NMap running on a laptop Linux. NMap can fingerprint the OS, conduct TCP and UDP scans for open ports. As mentioned above we will scan the external firewall from the Internet, DMZ, and Internal segment between the two firewalls to ensure that the configured firewall rule base is implementing GIAC security policy.

3.2.3.1 Scanning from the Internet

As per our proposed plan we connected the auditor's laptop on to the Internet. The objective was to scan the external interface of the firewall for possible open ports that could pave the way for a possible attack. We will scan the entire publicly available subnet that has been assigned to GIAC

Following is the NMap output for a command issued to scan the external interface of the firewall:

TCP Ports:

```
nmap -PO -sS -p1-65535 132.96.238.10
```

```
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Interesting ports on (132.96.238.10):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 759 seconds
```

In line with the GIAC security policy no ports are open on the Firewall.

Table 8 displays results of scanning the publicly available servers from the Internet with NMap:

SERVER	IP SCANNED	PORTS OPEN: TCP SCAN	PORTS OPEN: UDP SCAN
Public Web Server	132.96.238.129	80/http	None
Online Ordering Web Server	132.96.238.130	80/http 443/https	None
DNS Server	132.96.238.131	53/domain	53/domain
External Email Server	132.96.238.132	25/smtp	none
Proxy Server	132.96.238.201	none	none

TABLE 8: NMAP SCAN RESULTS FOR PUBLIC SERVERS

The results of the scans on the publicly available servers are found in accordance with the GIAC security policy.

3.2.3.2 Scanning from the DMZ

Next we plugged in the auditor's laptop onto the DMZ network. It was configured with an IP from the DMZ subnet i.e. 10.10.10.0/24 network. We scanned each of the configured hosts in the DMZ for TCP SYN and UDP and received the following output:

3.2.3.3 Scan the DMZ interface of the firewall

On scanning the firewall interface from the DMZ network we found out that the firewall is allowing TCP traffic for email, DNS, http, https, proxy and the business application. This was in accordance with the GIAC security policy.

Below are the NMap commands we issued and the output

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.1
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/)
Interesting ports on (10.10.10.1):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 1759 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.1
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/)
Interesting ports on (10.10.10.1):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 2435 seconds
```

3.2.3.4 Scan the Marketing Web Server

Upon scanning the marketing web server we found out that the operating system is properly hardened. The machine no ports other than port 80. Below is the NMap output for this scan.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.5
```

```
Interesting ports on (10.10.10.5):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
80/tcp    open       http
nmap run completed -- 1 IP address (1 host up) scanned in 726 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.5
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.5):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 1753 seconds
```

3.2.3.5 Scanning the Business Web Server

The business web server scans are presented below. The interesting port is 3233. This is the port the business application is listening on. This application talks to the application server through the two firewalls.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.6
```

```
Interesting ports on (10.10.10.6):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
80/tcp    open      http
443/tcp   open      https
nmap run completed -- 1 IP address (1 host up) scanned in 731 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.6
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.6):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 2845 seconds
```

3.2.3.6 Scanning the DNS

Below are the scan results for the DNS server. The DNS server shows UDP port 53 for client connections trying to resolve names using GIAC external DNS.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.7
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.7):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
53/tcp    open       domain
```

```
nmap run completed -- 1 IP address (1 host up) scanned in 419 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.7
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.7):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
53/UDP    open       domain
```

```
nmap run completed -- 1 IP address (1 host up) scanned in 1782 seconds
```

3.2.3.7 Scanning the Mail Gateway

Below are the results for the nmap scan for the mail gateway.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.8
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.8):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
25/tcp    open       domain
```

```
nmap run completed -- 1 IP address (1 host up) scanned in 1678 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.8
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.8):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
```

```
nmap run completed -- 1 IP address (1 host up) scanned in 2431 seconds
```

3.2.3.8 Scanning the Web Proxy

GIAC is running the web proxy listening on port 3000. The NMap scan shows no surprises.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.10.9
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.9):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
3000/tcp   open       unknown

nmap run completed -- 1 IP address (1 host up) scanned in 1423 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.10.9
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.10.9):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service

nmap run completed -- 1 IP address (1 host up) scanned in 1642 seconds
```

The NMap scanning of the GIAC DMZ proved that all the servers in the DMZ have been properly hardened in accordance with the company security policy. Also the firewall blocks all the unnecessary traffic traveling to and fro between the DMZ, Internet and the internal office network of GIAC.

3.2.3.9 Scanning from Internal Network between the two firewall

Finally we plugged in the auditor laptop on the internal network between the two firewalls that is the 10.10.50.0/24 segment. The laptop was given a static IP on this segment and NMap was run against the firewall interface and following output was received.

TCP Ports:

```
nmap -PO -sS -p1-65535 10.10.50.1
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.50.1):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
25/tcp     open       smtp
3000/tcp    open       unknown

nmap run completed -- 1 IP address (1 host up) scanned in 2357 seconds
```

UDP Ports:

```
nmap -PO -sU -p1-65535 10.10.50.1
```

```
Starting nmap V. 2.54BETA31 (www.insecure.org/nmap/ )
Interesting ports on (10.10.50.1):
(The 65535 ports scanned but not shown below are in state: filtered)
Port      State      Service
nmap run completed -- 1 IP address (1 host up) scanned in 1524 seconds
```

The NMap output conforms the GIAC security policy of not allowing any out bound connection from the internal network to any other host on the Internet. The only hosts in the DMZ that can be connected to from the office network are the proxy server and external mail gateway.

3.3 Evaluating the Audit

The audit was a complete success. The audit results provided an independent and objective assessment of the fact that GIAC Firewall rule base was consistent with the security policies.

The Firewall is a single point of failure and the recommendation would be to add a redundant firewall to eliminate the DOS threat. Also recommended is running of an NTP server for time synchronization. This will ensure synchronized logging of events by various network devices and servers. In order to consolidate the logs generated by all the network equipment, a Syslog server should be installed with a WORM drive. This will eliminate the risk for anyone to modify the logs once written on the drives.

Another issue that was noticed was that the documentation maintained by GIAC did not reflect the current status of the GIAC network. It is recommended that a frequent review of the network documentation be put in place (e.g. quarterly) so that the documents are updated on a regular basis.

Upon incorporating the recommendations offered by the auditors, the GIAC network will look as

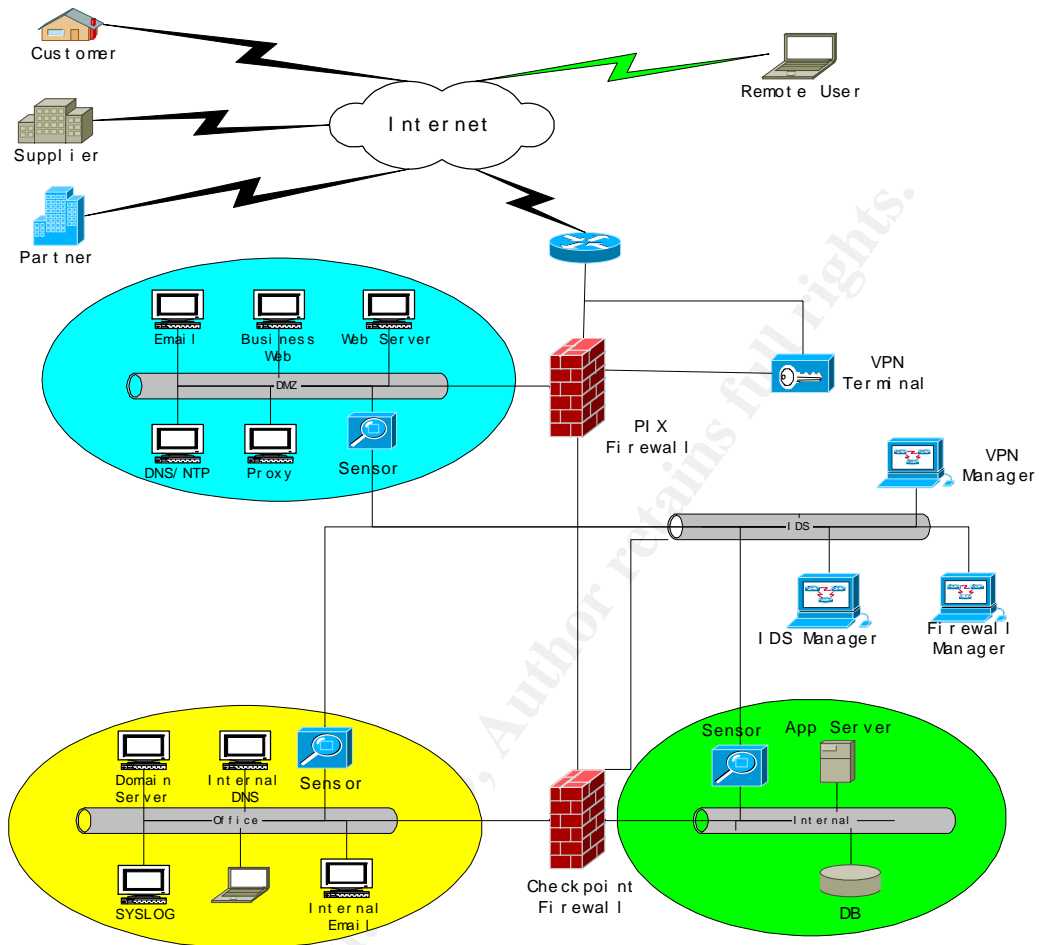


DIAGRAM 7: GIAC NETWORK ARCHITECTURE AS PROPOSED AFTER THE AUDIT

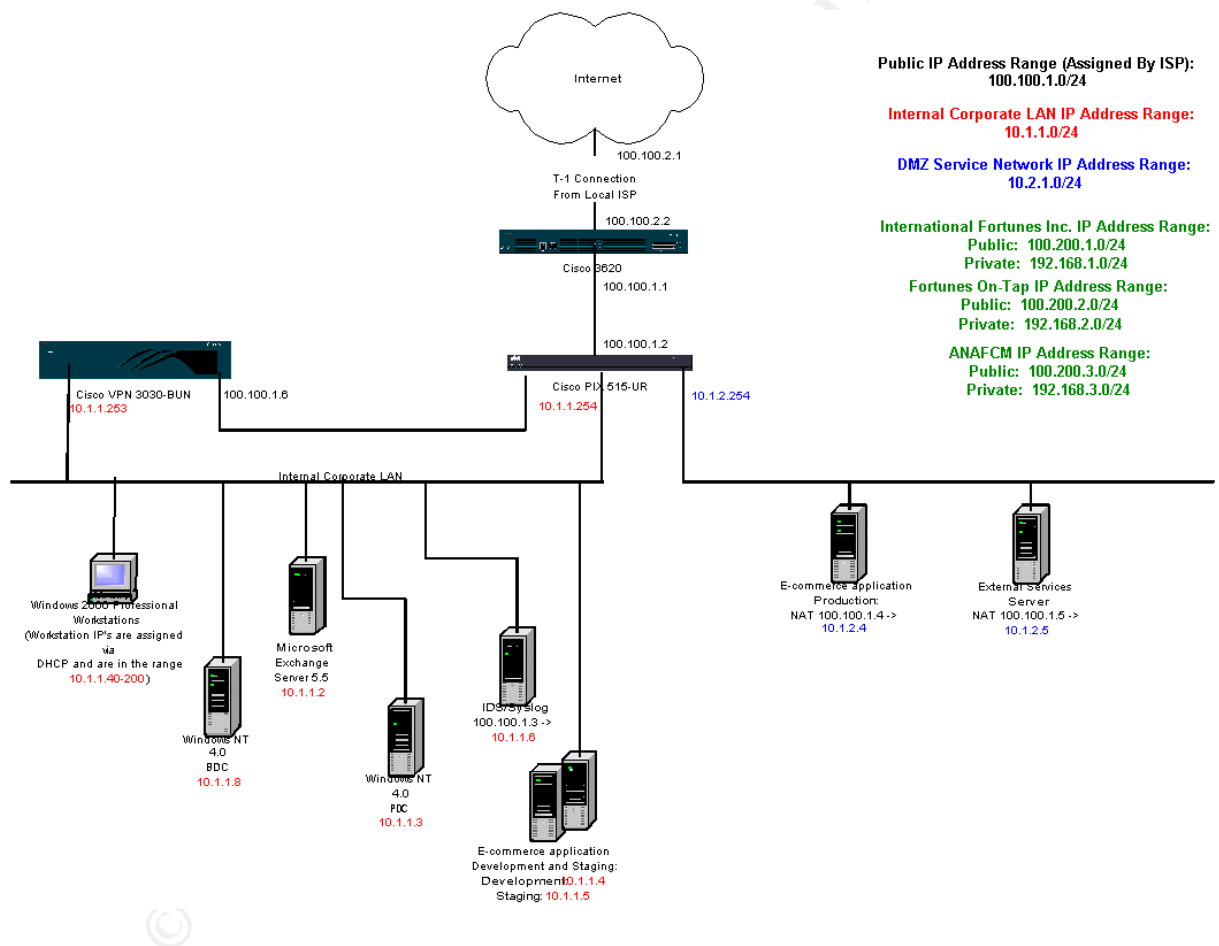
4: DESIGN UNDER FIRE

4.1 Design to Attack

I have chosen to attack Matt Pogue's design submitted on Nov 19, 2002. It is available for review at http://www.giac.org/practical/Matt_Pogue_GCFW.doc

Here is the Network Diagram from his proposal. He is running PIX 515-UR with Cisco PIX firewall software version 6.1.

1



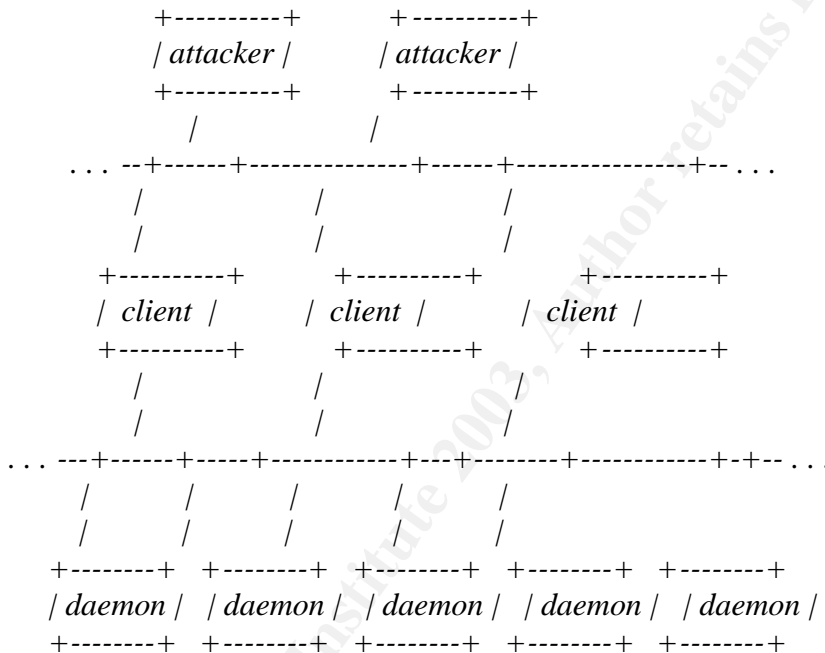
¹ http://www.giac.org/practical/Matt_Pogue_GCFW.doc

4.2 Denial of Service

We will use Denial of Service tool called Tribe Flood Network to create an attack against GIAC External PIX Firewall.

²*TFN is made up of client and daemon programs, which implement a distributed network denial of service tool capable of waging ICMP flood, SYN flood, UDP flood, and Smurf style attacks, as well as providing an "on demand" root shell bound to a TCP port.*

The TFN network is made up of a tribe client program ("tribe.c") and the tribe daemon ("td.c"). A TFN network would look like this:



The attacker(s) control one or more clients, each of which can control many daemons. The daemons are all instructed to coordinate a packet-based attack against one or more victim systems by the client.

The Detailed analysis of the TFN tool can be found at

<http://staff.washington.edu/dittrich/misc/tfn.analysis>

For the purpose of this assignment we have 50 compromised cable modem/DSL systems with clients and daemons installed on them. GIAC web site

² <http://staff.washington.edu/dittrich/misc/tfn.analysis>

www.giacenterprises.com is publicly available over the Internet. We will target this machine with a TCP SYN attack for Denial of Service. The Web server will be flooded with TCP SYN packets from the TFN Daemons being run on the compromised cable modems.

This kind of attack is difficult to defend against. Cisco has incorporated protection against such attacks in to the router IOS and PIX OS software. More PIX related marketing information can be found at

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a0080124551.html

Matt has done a good job at enabling tcp-intercept feature at the border router, available with the Cisco IOS, to minimize denial of service to the web server and the firewall.

The following commands from Matt's router configuration reflect enabling of this feature.

³We will enable tcp intercept for connections destined for our public IP address range (100.100.1.0/24) with the following access list:

```
access-list 101 permit tcp any 100.100.1.0 0.0.0.255
```

We will then enable tcp intercept and define its mode of operation:

```
ip tcp intercept mode intercept
ip tcp intercept list 101
```

Enabling these commands at the Border Router will enable GIAC website to reduce the initial impact of the Denial of Service attack mounted by us. All though our initial DOS attack at the GIAC web site was not completely successful we were still able to slow down the border router considerably. We kept the attack going for a little longer and finally managed to reboot the router itself.

4.3 Compromising an Internal Machine

Matt is running an E-commerce Web Application Server in the DMZ. I plan to exploit known vulnerabilities for Apache 2.0.43 web server running on Linux.

“⁴This server runs Red Hat Linux 7.2, Apache 2.0.43, Tomcat Java Application Server 4.1.12, and PostgreSQL 7.2.3 serving GIAC's e-commerce web application. This application is Java servlet-based and is developed and maintained by GIAC's team of developers. “

³ http://www.giac.org/practical/Matt_Pogue_GCFW.doc

⁴ http://www.giac.org/practical/Matt_Pogue_GCFW.doc

Upon researching known issues around Apache Web Server running on Linux platforms I was able to find multiple vulnerabilities with well-documented exploits.

4.3.1 Description of Vulnerability

⁵A memory leak in Apache 2.0 through 2.0.44 allows remote attackers to cause a significant denial of service (DoS) by sending requests containing lots of linefeed characters.

Apache 2.0 does not filter terminal escape sequences from its access logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

Apache does not filter terminal escape sequences from its error logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences. This could include denial of service attacks, file modification, data modification, and possibly the execution of arbitrary commands.

Details of these exploits and references can be found at the

<https://rhn.redhat.com/errata/RHSA-2003-139.html>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0083>

Further research into these vulnerabilities led us to a well-documented exploit to compromise the system and gain access. This exploit is explained in detail in the document published at the following URL.

<http://www.digitaldefense.net/labs/papers/Termulation.txt>

We will emulate the Case Study of “A Fictitious Company “ mentioned and base our attack on the Apache Web Server version 2.0.43 being run by Matt.

Once we have compromised the web server in the above-explained manner we can run more code to further expose the system. More attacks to exploit this vulnerability can be found at

http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=82142

4.3.2 Recommendation

⁵ <https://rhn.redhat.com/errata/RHSA-2003-139.html>

Red Hat has issued an advisory for these vulnerabilities. The details are available at

<https://rhn.redhat.com/errata/RHSA-2003-139.html>

Based on these advisories we would recommend Matt to upgrade to the latest version of Linux OS and also apply the patches to the apache web server that are mentioned in the document. Patching up the web server should prevent any more attackers to exploit the system

4.4 Attacking the Firewall

Matt is running PIX 515 UR with PIX OS 6.1. After searching the Cisco site, I found out that version 6.1 of the PIX OS is susceptible to a denial of service attack if it has SSH running on it.

4.4.1 Vulnerability Details

“⁶While fixing vulnerabilities mentioned in the Cisco Security Advisory: Multiple SSH Vulnerabilities (<http://www.cisco.com/warp/public/707/SSH-multiple-pub.html>) we inadvertently introduced an instability in some products. When an attacker tries to exploit the vulnerability VU#945216 (described in the CERT/CC Vulnerability Note at <http://www.kb.cert.org/vuls/id/945216>) the SSH module will consume too much of the processor's time, effectively causing a Denial of Service. In some cases the device will reboot. In order to be exposed SSH must be enabled on the device. “

The vulnerability VU#945216 has well documented attacks. One of the exploits can be found at <http://www.securityfocus.com/bid/2347/exploit/>. This exploit leads the attacker to execute arbitrary code with the privileges of the SSH daemon, typically root.

4.4.2 Exploit

From Matt's PIX configuration we already know that he is running SSH on the device. The following rules in the configuration allow any computer from the internal network to SSH on to the PIX to make configuration changes.

```
7ssh 10.1.1.0 255.255.255.0 inside
ssh timeout 20
```

In order to exploit the above documented vulnerability and launch a successful attack we have to get on to Matt's internal network as that is the only segment that has access to the SSH server running on the PIX.

⁶ <http://www.cisco.com/warp/public/707/SSH-scanning.shtml>

⁷ http://www.giac.org/practical/Matt_Pogue_GCFW.doc

I have already compromised the external E-Commerce Web Server. This puts me right in Matt's DMZ. This provides me better access to the network to exploit it for further vulnerabilities. A scan from DMZ against the internal network revealed that a syslog server is running and listening on UDP 514. Matt is running a fairly updated version of the syslog server. I was unable to find any latest vulnerability for that particular syslog version.

4.4.3 Conclusion

Matt has fairly up to date and patched systems and that makes it real hard to find well-known exploits that his network is vulnerable to. He has good checks and balances in place in his device configurations. The DOS vulnerability for PIX we described above can be fixed by simply upgrading the PIX to a newer version of the OS that can be downloaded from www.cisco.com. We will need more time to research for possible exploits that went unnoticed during this initial phase of attacking.

© SANS Institute 2003, Author retains full rights.

5.0 REFERENCES

Cisco Router Hardening Step-by-Step By Dana Graesser

<http://www.sans.org/rr/firewall/router2.php>

Practical Assignment chosen to attack

http://www.giac.org/practical/Matt_Pogue_GCFW.doc

Cisco Security Advisory: Scanning for SSH Can Cause a Crash

<http://www.cisco.com/warp/public/707/SSH-scanning.shtml>

Vulnerability Notes VU# 945216 - SSH CRC32 attack detection code contains remote integer overflow

<http://www.kb.cert.org/vuls/id/945216>

SSH CRC-32 Compensation Attack Detector Vulnerability

<http://www.securityfocus.com/bid/2347/exploit/>.

Apache Web Server Vulnerabilities

<https://rhn.redhat.com/errata/RHSA-2003-139.html>

http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=82142

<http://www.digitaldefense.net/labs/papers/Termulation.txt>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0020>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0083>

The "Tribe Flood Network" distributed denial of service attack tool By David Dittrich

<http://staff.washington.edu/dittrich/misc/tfn.analysis>

Cisco IOS Command Reference, Version 12.1

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_command_reference_chapter09186a0080087e3e.html

Cisco PIX Firewall Command Reference, Version 6.2

http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_command_reference_book09186a0080104234.html

Auditing your Firewall Setup, By Lance Spitzner

<http://www.spitzner.net/audit.html>

Soltrus Inc., Canadian Affiliate of Verisign

www.soltrus.com

Go Secure for Nortel Administrator's Guide from Verisign