



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 GCFW CERTIFICATION

SANS SECURITY 2001 – BALTIMORE, MD

PRACTICAL ASSIGNMENT VERSION 1.5e

LORING ROSE

JULY 25, 2001

TABLE OF CONTENTS

I. Assignment 1: GIAC Enterprises, Security Architecture	3
A. What is GIAC Enterprises?	3
B. Business requirements	3
C. The architecture	4
D. General design decisions	4
E. Business solutions	5
II. Assignment 2: GIAC Enterprises, Security Policy	6
A. Assumptions	6
B. Border Router	6
C. Firewall and VPN	9
III. Assignment 3: GIAC Enterprises, Perimeter Audit	17
A. Requirements	17
B. Audit Planning	17
C. Process	18
IV. Assignment 4: Design Under Fire	22
A. The Firewall	22
B. Denial of Service	23
C. Compromised host	24
Appendix A: Complete Router Configuration and ACLs	26
Appendix B: Recommended Lockdown List for Windows NT (for FireWall-1)	30
Appendix C: Recommended Lockdown List for Microsoft IIS 5	33
Appendix D: Complete FireWall-1 Rulebase	35
Appendix E: References and Recommended Reading	37

I. ASSIGNMENT 1: GIAC ENTERPRISES, SECURITY ARCHITECTURE

A. What is “GIAC Enterprises”?

GIAC Enterprises is “a growing internet startup that expects to earn \$200 million per year in online sales of fortune cookie sayings” (http://www.sans.org/giactc/GCFW_assignment.htm). They have recently completed the acquisition of an established fortune cookie sayings company (in this design, the company is “China Sayings, Inc.”).

For the purposes of this design, it is assumed that GIAC Enterprises is a Microsoft-centric company, and the dominant platform is a version of Windows. In particular, the design will focus on running the security architecture on Windows NT and Windows 2000-based systems. It is the author’s belief that *properly configured* Windows-based systems can be as secure as any other (i.e. “*nix”) systems.

The following caveats must be kept in mind during the design:

GIAC Enterprises is a total Microsoft shop, with Microsoft-certified engineers managing the network. The design must leverage the existing knowledge of the current support staff.

The customer base, suppliers and partners of the company need access to data on the GIAC Enterprises network.

The design must be as cost-effective as possible given the above, but must not fall below a minimum security standard. The standard that the management of GIAC Enterprises has chosen is detailed in VISA’s Cardholder Information Security Program (see http://www.visabrc.com/doc.phtml?2,0,932,932a_cisp.html for an overview).

B. Business requirements.

The security architecture must encompass the following business requirements:

- GIAC Enterprises wants to establish a publicly-accessible website to provide potential customers with information about available products.
- Customers need to be able to securely place orders with GIAC Enterprises.

- GIAC Enterprises needs to be able to exchange e-mail with clients across the public Internet.
- GIAC Enterprises needs to securely share e-mail and other sensitive data with China Sayings.
- GIAC Enterprises needs to securely share data with its partners and suppliers.

C. The architecture.

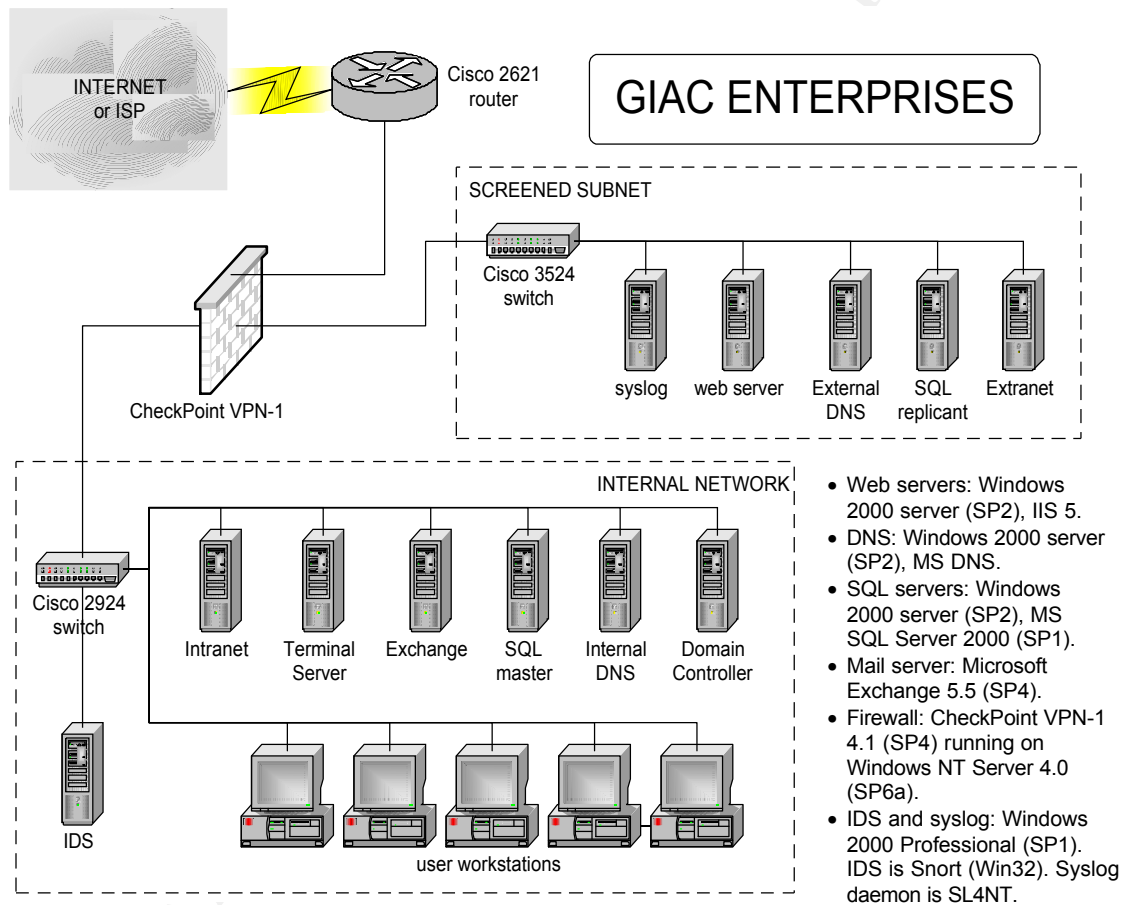


Figure 1.1: Security/Network Architecture diagram

D. General design decisions.

The border router will act as a screening router to provide an additional layer of security.

The central focus of the design is the choice of CheckPoint VPN-1 as the firewall. The VPN-1 product can be leveraged to fulfill a number of the business and security requirements without additional purchase. The product is also relatively easy to administer.

To help save some money, two freeware products will be implemented: SL4NT, a freeware syslog daemon (available from netal at <http://www.netal.com>, a more fully-featured version is available for purchase) and Snort for Win32, a free, lightweight IDS. The recommended installation of Snort requires logging to a MySQL database, and installation of Acid (Analysis Console for Intrusion Databases) for alert analysis. (See <http://www.snort.org/win2ksnort.htm> for detailed instructions on setting up this configuration on Windows 2000.)

Also to lower costs, the design uses Microsoft IIS 5.0 as the web server and Microsoft DNS, both included at no additional charge with Windows 2000. To help offset potential security issues with Microsoft DNS, split DNS will be implemented.

To help isolate the Microsoft SQL server from data corruption, data replication and an aggressive database backup regimen will be implemented.

The CheckPoint firewall will implement an SMTP Security Server as a mail relay, isolating the Exchange server from the Internet.

E. Business solutions.

The design presents the following solutions to the earlier specified business requirements:

- Potential customers will access GIAC Enterprises' public web site for product information.
- Customers will place orders with GIAC Enterprises via a secure extranet site.
- GIAC Enterprises will share data with its partners and suppliers via a secure extranet site.
- GIAC Enterprises will implement a VPN with China Sayings, Inc., to share sensitive data.

ASSIGNMENT 2: GIAC ENTERPRISES, SECURITY POLICY

A. Assumptions.

For purposes of the design, the following networks are assumed:

- GIAC Enterprises' internal network is 192.168.100.0/24
- GIAC Enterprises' screened subnet is 214.160.100.0/25
- China Sayings, Inc.'s internal network is 207.168.200.0/24
- GIAC Enterprises' external router interface is 214.170.10.10

B. Border router.

The border router will be configured with both ingress and egress filters to aggressively control traffic. Only that specifically permitted by the business requirements will be allowed inbound. Although we will restrict some of the same traffic with the firewall rulebase, it is important to implement the filters for (at least) two reasons: to lock down the router, and to reduce load on the firewall.

As part of the router configuration, unused services will be disabled, and configuration access will be restricted as much as possible.

To implement the configuration, the following brief tutorial is provided:

- 1) Connect to the router: use your favorite Telnet client to establish a connection to the router (the client in Figure 2.1 is PuTTY, freely available from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>). Our router's name is "chicago."

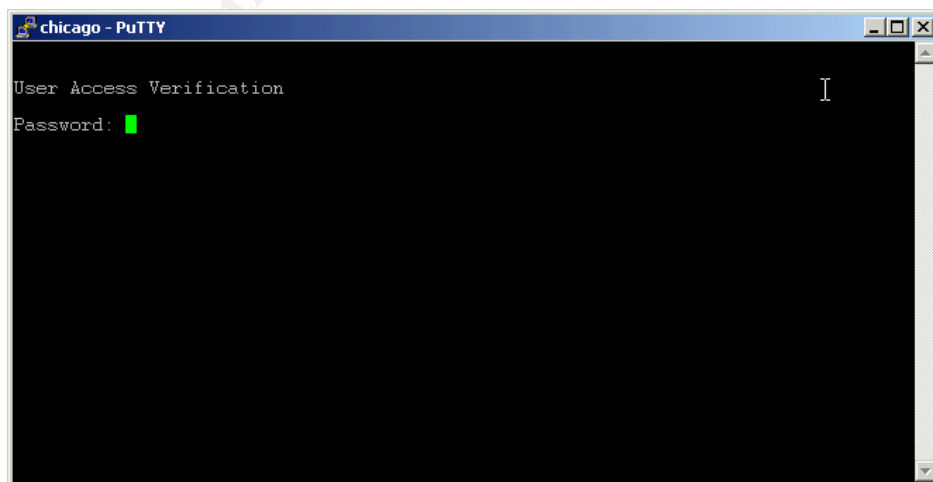


Figure 2.1: initial router connection

- 2) Enter the VTY access password and press ENTER (Figure 2.2). To enter Enable mode (required for configuration), type the command "en" and press ENTER

(Figure 2.3). Provide the enable password and press enter (Figure 2.4).

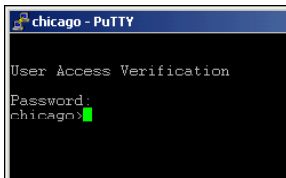


Figure 2.2: VTY access

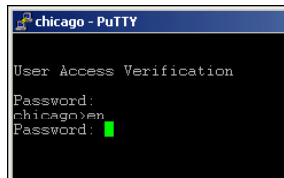


Figure 2.3: Enable command

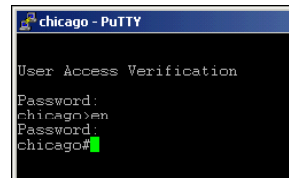


Figure 2.4: Enable password

- 3) Once in Enable mode (indicated by a hash as the command prompt), use the command "config t" to enter Global Configuration mode (Figure 2.5). We can now type in the recommended Global Configuration commands (as shown in Appendix A: Router Configuration and ACLs). Exit Global Configuration mode by pressing "Control-Z".

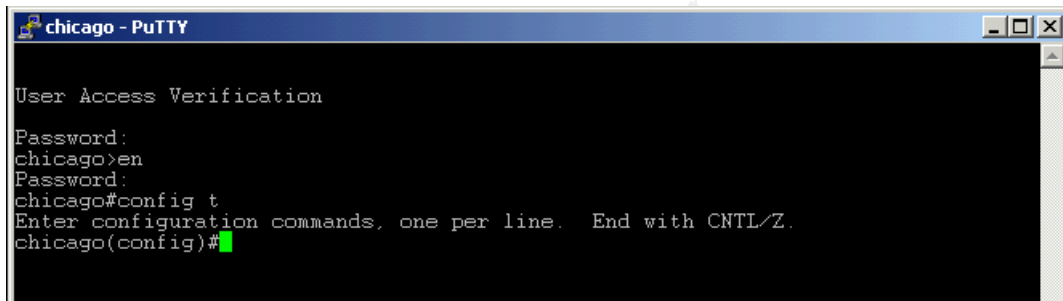
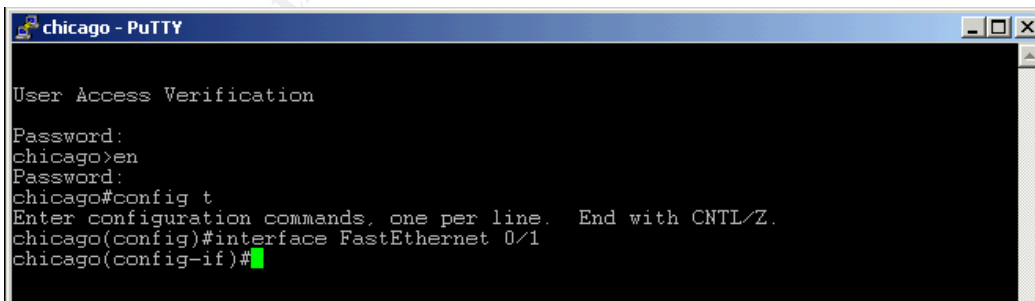


Figure 2.5: Global Configuration mode

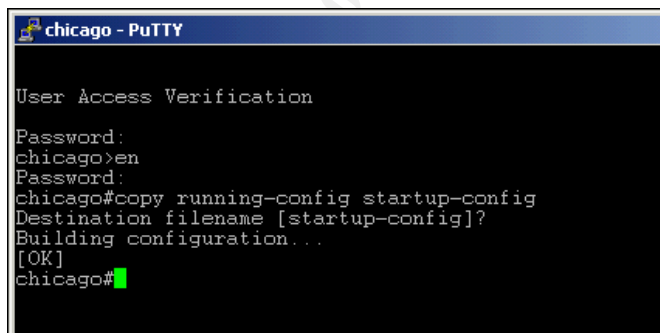
- 4) To configure the individual interfaces, first enter Global Configuration mode. Then specify the interface to configure with the "interface" command (Figure 2.6). Type in the interface configuration commands and press "Control-Z" when done to exit the configuration mode.



```
access-list list-number {deny|permit} protocol source
destination
```

```
ip access-group 101 in
```

in



```
chicago - PuTTY
User Access Verification
Password:
chicago>en
Password:
chicago#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
chicago#
```

```
copy running-config startup-config
```

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

Implied Rules

<input type="checkbox"/> Accept VPN-1 & FireWall-1 Control Connections:	First
<input type="checkbox"/> Accept RIP:	First
<input type="checkbox"/> Accept Domain Name Over UDP (Queries):	First
<input type="checkbox"/> Accept Domain Name Over TCP (Zone Transfer):	First
<input checked="" type="checkbox"/> Accept ICMP:	Last
<input checked="" type="checkbox"/> Accept Outgoing Packets Originating From Gateway:	Before Last

IKE

Renegotiate IKE Security Associations every minutes

Renegotiate IPSEC Security Associations every seconds

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Guardian	Any	drop	Long	Guardian	Any	Stealth Rule
Any	Any	Any	drop	Short	Guardian	Any	Cleanup Rule

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Web	http	accept		Guardian	Any	permit TCP80 (HTTP) access to web server for all users

Source	Destination	Service	Action	Track	Install On	Time	Comment
Any	Extranet	https	accept		Guardian	Any	Allow TCP443 (HTTPS) to extranet server for all users

Network Objects...

Services...

Resources...

Servers...

Users...

Users on account unit...

Time...

Keys...

UFP...

CVP...

RADIUS...

RADIUS Group...

TACACS...

DEFENDER...

LDAP Account Unit...

CA...

Policy Server...

CA Properties

General | VPN-1 LM

Name: VeriSign

Comment: VeriSign Certificate Authority

Color:

CA Type: **VPN-1 Certificate Manager**

VPN-1 Certificate Manager

Entrust PKI

IPSEC PKI

OK Cancel Help