Global Information Assurance Certification Paper

Firewalls, Perimeter Protection, and VPNs
GCFW Practical Assignment

Version 1.6a (revised October 26, 2001)

By Rajesh Singh
SANS Sydney JAN 2002
March 26,2002

Abstract

This paper represents the practical assignment requirement for the GIAC Certified Firewall Analyst (GCFW) certification program (version 1.6a.)

The solution presented here is split into four parts as per the practice's requirements.

Briefly
Assignment 1 provides:

The security architecture for GIAC s, an e-business company which deals in the online sale of fortune cookie sayings. We will refer to all references to GIAC s as GIACE from here on.

Assignment 2 provides:

The security policy as implemented on the routers, firewalls and switches, which were, described in assignment one and also presents a tutorial on how this policy is implemented.

Assignment 3 provides

A technical audit of the Primary firewall

Assignment 4 provides

An attack scheme on one of the previously presented firewall assignments.

Contents

Assignment 1

Security Architecture

Overview

GIACE key business relationship between the customers, suppliers and partners will be the basis for defining GIACS security architecture.

- Customers and Suppliers of GIACE

  The customers and suppliers of GIACE will perform business transactions with GIACE in a similar manner. Basically the customers would type in a URL e.g. http://www.onlinefurtunes.com and they will be presented with web pages, which they can navigate to order online cookies.
  Similarly suppliers can log onto an appropriate page and transfer the cookies that they would like to sell.
  The front-end web servers will interact via some business logic with the backend data servers and retrieve the cookies that a client wants. There will be functions that GIACE will provide and will include options on payments types.
- Partners of GIACE

  The partners of GIACE will administer their own I.T infrastructures and the main function they will require of GIACE is to provide them with a secure link to download database files containing cookies and other information. This function will be provided by host-to-host VPN connections from their systems to GIACES networks.

- Employees of GIACE

  The employees of GIACE s will have their workstations on the same LAN as the GIACES server and database systems. They will use in-house applications to access the contents of the database and their access to data contained in these databases will be controlled by permissions and access control lists.

  Remote employees including sales staff will connect via their host-to-host VPN through their Internet service providers. Dial-in access directly to GIACE will not be provided initially

Security Policies
The following policies will help secure the E-business infrastructure for GIACE and provide a framework for the design of GIACE network

General Access

A Firewall that provides stateful packet filtering should be used to control data flow into and out of GIACE network. The firewall should be configured to prevent access from spoofed IP addresses. Data traffic information must be logged between the Internet and GIACES services network. Traffic must also be logged between the services network and internal network and traffic between internal network and business partners.
Any changes to the firewall configuration will only be granted via GIACE s change and Problem management process.

Remote employee Access

Employees of GIACE s must access their servers for content management via a secure private internal network or via authenticated and encrypted connection over the Internet. A minimum of 64-bit encryption must be used to transport the data

Database Access

A database in the internal network needs to be synchronized over the Internet then encryption must be provided by the network layer (VPN) or SQL. Database authentication must be used. Appropriate request must be requested and security forms must be filled before any such connections are approved.

Specific protocol access requirements

Domain Name Service (DNS)

Split-Split DNS design will be used for this Architecture. The Advertiser and Resolver services will be separated in the external DNS The advertiser services will answer to queries from the Internet for the zones that the DNS server is authoritative for i.e. local zones only. Recursion will be also disabled on these Advertiser systems.
The Resolver services will resolve queries from internal DNS servers.

The reason for using this design is to protect GIACE s from Cache poisoning

External DNS services

- Zone transfers are not allowed between internal and external DNS servers

- DNS queries from the internet will not be allowed to pass through to the internal name servers
- Zone transfers are not allowed between external DNS servers and any DNS server on the Internet. The exception to this rule is that the transfer of zones maybe permitted between ISP DNS and the external DNS servers. Initially the zone transfer to the IPS DNS will not be permitted

Internal DNS services

- Internal DNS servers are configured to forward all DNS queries to external servers for resolution

Simple Mail Transfer Protocol (SMTP)

- Inbound SMTP traffic will be restricted to the mail relay in DMZ
- Only SMTP connections may be initiated from the Internet-accessible SMTP server to other servers in the internal LAN.
- Servers with Internet connectivity configured for outbound only SMTP.
- The SMTP daemon must not be run under root access and must not support the debug mode
- Connecting SMTP must have a valid host name and domain name
- . Where possible, GIACE internal addresses must be hidden in outbound messages.
- Virus scanners must be used to check all email
- .SPAM sites and spammers must be blocked by mail servers

File Transfer Protocol (FTP)

- FTP will be only allowed within the internal network and via a VPN connection
- FTP will be allowed between business partners and GIACE via a VPN connection

Network File System (NFS)

- No NFS traffic is permitted through the external firewall
- NFS is only supported within the internal network or within the DMZ. No nfs traffic is allowed between the internal network and DMZ

Network Time Protocol (NTP)

- Time synchronization would be done via NTP servers within the GIACEC infrastructure.
- NTP servers in the internal network will be master servers for the servers in the DMZ or other VLANS

Pings and Traceroute

- Inbound ICMP echo requests from the Internet to the DMZ layer is not allowed
- Outbound ICMP echo requests are allowed from the internal network

Simple Network Management Protocol (SNMP)
SNMP is not allowed from the Internet into GIACE

Recommended Policies
The above policies do not comprehensively define the security policy for GIACE but defines policies that are crucial for GIACE business to be conducted. To facilitate a secure environment for GIACE s and its customers and suppliers, we can use templates from http://www.sans.org/newlook/resources/policies/policies.htm.

Logical Network Diagram

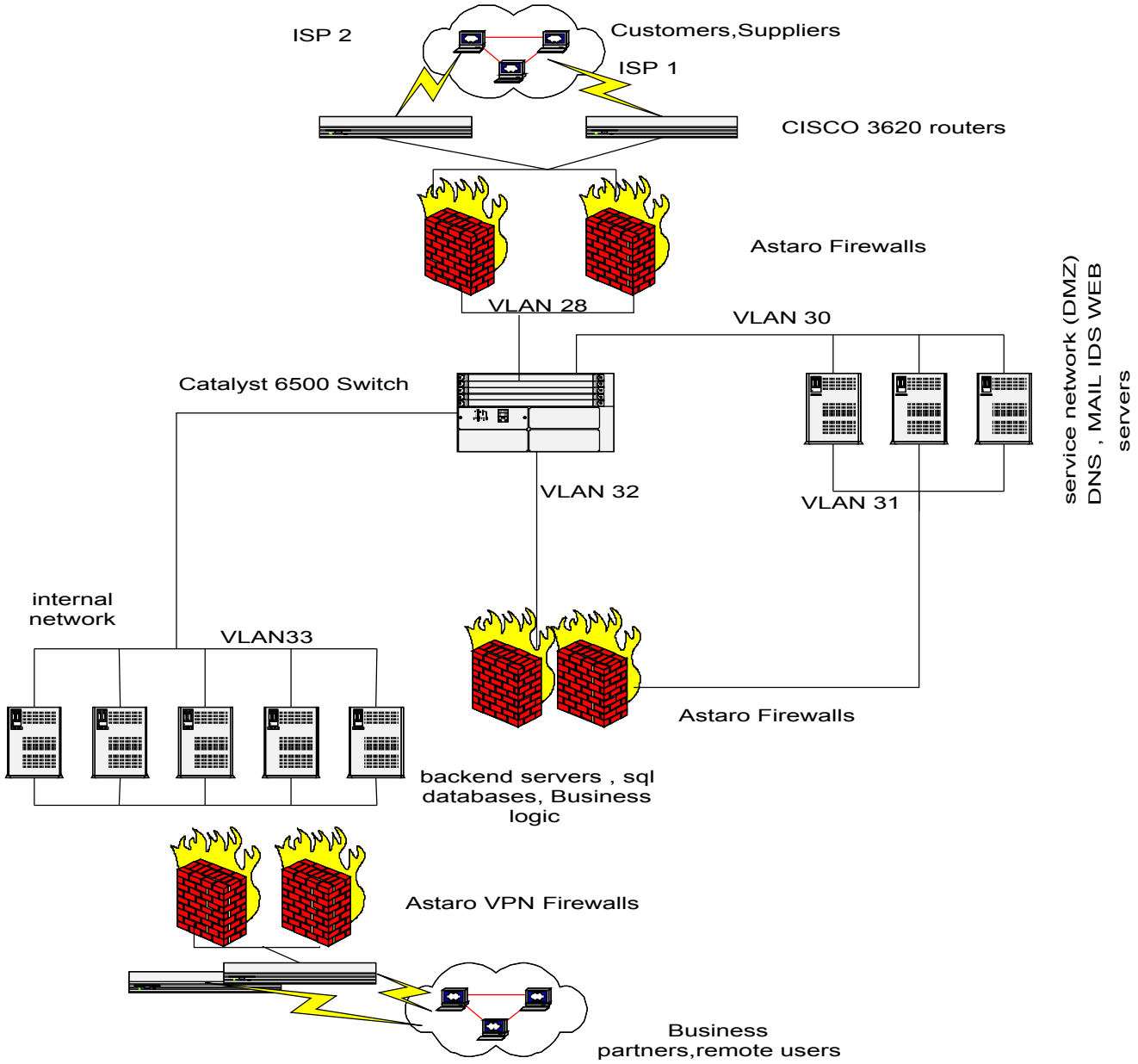


Figure 1 The logical Network Diagram for GIAC Enterprises

Network DESIGN

The key architectural elements of GIACE s network include perimeter routers, web servers, multi-layer switch and firewalls as seen in Figure 1 above

The network architecture can be broken up into 4 key layers. Layer

The Perimeter Network

This layer connects GIACE s network to the Internet Service Providers (ISP). The perimeter network provides a separation layer and protection of GIACEE network from the public. This layer includes the border routers and external firewalls. We will use two Cisco 3620 routers http://www.cisco.com/ and two ASTARO Firewall. http://www.astaro.org/The Astaro firewalls use the netfilter http://www.netfilter.org/engine from open source community. The hardware specifications for the Cisco router and the firewall is shown in table 1

Model	Description	Software Version
Cisco 3620	2-slot multiservice access router, with optional 4-port fast Ethernet module (NM-4E)*** Required 2	IOS 12.2(5) T
System	**Hardware Requirements**	**Software Version**
Astaro Firewall	Intel 1.4 GHZ processor 1 gbyte memory 40 Gbyte IDE hard drive 2 pci 100 Mbit pci network cards Required 2	Astaro 2.016

Table 1 Hardware specification of border routers and main firewall

Multilayer Switch

This design will incorporate the Cisco 6509 multilayer switch. This switch will enable us to separate the architecture into VLANS, which will provide us with the network segmentation that we require between the different server systems or layers. The network will be divided into the DMZ layer and Internal layer initially. The Cisco 6509 does have the capacity to provide further functional VLANS, but we would like to keep the initial design simple.[1]The traffic is routed

between the different VLANS using the router feature of the Cisco switch and will apply acls to provide the access controls that we require. [2]

The following table shows the switch configuration that we will use

Product Number	Description
WS-C6506-1300AC	Catalyst 6506 Chassis w/1300W AC power Supply
WS-X6k-S2-MSFC2	Catalyst 6500 supervisor Engine-2, 2GE,plus MSFC-2 & PFC-2
S6MSFC2C-12205E	Catalyst 6000 MSFC2 IOS Enterprise w/VIP
WS-X6348-RJ45	Catalyst 6000 48-ort 10/100 X 2
MEM-MSFC2-128MB	Catalyst 6000 128 MB DRAM option

We can create separate VLANS and allocate servers groups to each VLAN

We will create the following VLANS for our design

VLAN name	VLAN Number
Front end perimeter firewall	28
Back end perimeter firewall	29
Front end DMZ (web,dns.mail)	30
Back end DMZ (web,dns,mail)	31
Internal network	32
Back end of internal firewall	33

Traffic flow between the VLANS

1. HTTP and HTTPS are redirected from the perimeter firewall to the web servers in the DMZ i.e. traffic clients opening up a browser application using port 80 or 443 from the internet get redirected from perimeter firewall to the front –end VLAN 30 in the DMZ

DMZ

[1] To provide redundancy we can utilise two Cisco 6509 switches instead of one
[2] Instead of using a VLAN switch we can physically separate the networks to provide maximum security

The DMZ or screened network provides a secure space between the Internet and GIACES internal network, it contains servers, which provide core web services , such HTTP and HTTPS to GIACES customers or suppliers. The web servers can be cloned , which can be configured for load balancing or provide redundancy .These web servers will run the Apache web server software. This layer will house DNS servers providing services to internal systems as well as Internet requests. This zone will also contain SNORT based IDS systems

Internal Network:

This Internal network is separated from the DMZ by two ASTARO®™ Firewalls. Here the servers with business logic, i.e. systems that act as back ends to the web servers in the DMZ zone reside. We will use SQL database systems for the storage of business data.

There will be tape backup systems and an internal DNS server in this region.

As part of the GIACE architecture, we will utilize a set of management servers that are used to monitor the whole network, providing means of uploading the DMZ web servers with new data. These will also provide us with a remote interface and backup systems

Several IDS will be running snort will be placed in this layer

IP Address Assignment

GIACE has been public addresses in the range 203.10.90.10 to 203.10.90.255

The following chart is an example of the IP address assignment we will use for public address Internet space with subnet mask 255.255.255.0

System or Service	IP Address
First border router, internal side	203.10.90.3
Second border router, internal side	203.10.90.4
First Perimeter firewall external	203.10.90.1
Second Perimeter Firewall external	203.10.90.2
First web server	203.10.90.5
Second web server	203.10.90.6
First VPN	203.10.90.7
Second VPN	203.10.90.8

Assignment 2

DNS	203.10.90.9

The internal IP addressing scheme assign to GIACE is based on RFC 1597 private addressing scheme. The VLAN have been assigned addresses in the range 192.168.0.0 to 192.168.255.0 and therefore will use Class C subnet mask of 255.255.255.0

Subnet assignment	VLAN	Purpose
192.168.28.0	VLAN 28	Back end of perimeter firewall interface
192.168.30.0	VLAN 30	Front –end service network DMZ)for web servers, DNS and SMTP
192.168.31.0	VLAN 31	Backend service network interface
192.168.32.0	VLAN 32	Backend of internal firewalls
192.168.33.0	VLAN 33	Internal network, SQL server database server, internal DNS

The IP addressing scheme for the GIACE architecture is defined in the following manner

- Network 192.168.x.0
- Subnet Mask 255.255.255.0
- Default Gateway 192.168.x.255
- Broadcast Address 192.168.x.255
- Primary DNS 192.168.33.72
- Secondary DNS 192.168.33.73

Where x replaces the VLAN networks defined above

The Cisco 3620 is chosen to provide the routing between the ISP and GIACEE network. It is connected to the two different ISP via T1 connections. Its main function apart from being a routing gateway for GIACE is to the function as the first line of defense for GIACE using the IOS firewall feature set .Simple access list controls will be placed on the router to provide access restrictions according to GIACE security policy.

The process of installing and configuring the border routers is discussed in this section. The full configuration script is provided in appendix 1

Installing the Border Router

The border router is installed and configured as per documentation received with the product or via documentation included at the Cisco Web site: http://www.cisco.com

Configuring the Router

To configure the router, you first need to build a configuration file, log on to the router, and then upload the configuration.

To build a router configuration file:

We will use the copy and paste method of uploading the border routers with the configuration file. The configuration file we will use is shown in appendix 1.

Figure 4 below shows a sample output of how we will upload the router. It must be noted that configuration files for the router can be also loaded by using TFTP

Sample Configuration Output

Router>**en**

Password:

Router#**conf t**

< Enter configuration commands, one per line. End with **end**>

Router(config) < Copy and paste edited router configuration. >

Router(config)# **end**

Router#

*Mar 8 18:25:32.500: %SYS-5-CONFIG_I: Configured from console by console

Router# **copy run start**

Building configuration...

[OK]

Router#**reload**

Proceed with reload? [confirm]

*Mar 8 18:30:15.231: %SYS-5-RELOAD: Reload requested

Router Access rules configuration

The following commands are used to configure the border routers. All examples are for the true values of GIACS network

To configure the router interfaces

Command

interface used to choose which interface to configure

IP address used to assign an address to the interface.

The syntax for the commands is as follows:

interface ***interface-name***

IP address ***address-address netmask***

e.g. for the external (internet facing) interface

interface FASTEthernet0/0

ip address 203.10.90.254 255.255.255.240

for the internal facing Ethernet card

interface FASTEthernet0/1

ip address 203.10.90.253 255.255.255.240

Default Route Configuration

Command

ip route used to enter a default route for the router.
ip route 0.0.0.0 0.0.0.0 ***your-gateway-IP-address***
e.g. ip route 0.0.0.0 0.0.0.0 203.40.90.254

Password Configuration
Command

enable secret used to configure the password
enable secret ***your-password***
e.g. enable secret BR7edc4ab

Console Password Configuration
Command to configure the console password by using the

line con choose the console interface
password used to set console password

the syntax for the commands is as follows

line con 0
password ***your-console-password***

line con 0

password BR7edc4ab

Password Encryption
Command
service command is used to encrypt the password while viewing config

service ***password-encryption***

Router Naming
Command

hostname used to give your router a name
hostname ***your-router-name***
hostname kurra01

Timestamps
For debugging and logging purposes, a timestamp is important. The following commands are used for timestamp entries:

service timestamps debug uptime
service timestamps log uptime

Synwait Time
Allow this wait time for Cisco IOS to fully establish TCP/IP connections

ip tcp synwait-time ***number-of seconds***
eg ip tcp synwait-time

BGP is used to provide the most efficient path to and from an Internet client. It is a way of providing optimized routing for router devices. This design that GIACE will negotiate with its Internet service provider to provide BGP services for itself. The router is configured for BGP , by using the router bgp command in the configuration mode

HSRP will be used to between the router do provide fail over features. When one of the 3620 router fails, the other router will automatically take over and perform the functions of the failed router.

In GIACE design only on router will be active at a time. This router will have a higher priority according to the HSRP priority scheme. When an interface of one router changes, this lowers its priority and the other inactive router will compare this with its priority number. If the backup routers priority is higher then the failed routers, the backup router will take the role of the master router. This design thus allows for the business to continue until problems with the lowered priority router is fixed.

We will connect the two routers together with a cross over cable and provide an interface address .

HSRP configuration on the Routers:
To enter the HSRP mode use the following command
we will configure the fast Ethernet 0/1 using the commands below

Standby 1 ip 203.10.90.253

All routers configured for HSRP , need to wait a certain time before a failed router can

be declared inactive. We use the hello-time and hold time to define this time variants.

This is done with the command below

standby 1 timers 1 2

The priorities of the routers are set by using the priority command.. With our two border 3620 routers we can assign the first one a priority of 110 while the other can be assign a priority of 95

standby 1 priority 110

We than use the track command to check the interfaces of the router to monitor when the priority goes down.

standby 1 track FastEthernet0/0

A detailed explanation of HSRP protocol can be found at the Cisco Internet site

Locking down the Border Router

It is very important to fully secure the router itself the configuration file used in appendix 1 includes the commands used for securing the Cisco 3620. These commands will now be explained here

Disable Finger Service

This can be used to determine who is logged onto the router.
command:
no service finger

Disable TCP-Small-Servers

Chargen, Echo, and Daytime require TCP-Small-Servers. These services are not required and have been used by hacker exploits or can be used by scanning tools to provide information about the router.
command:

no service tcp-small-servers

Disable UDP-Small-Servers

Again Chargen and Echo services require UDP-Small-servers and should be disabled as they are not usually needed .

command:
no service udp-small-servers

Disable BOOTP

You should disable BOOTP server on the border router.
command:
no ip bootp server

Disable Proxy Arp

Proxy Arp helps hosts to find media access control (MAC) addresses of other hosts on attached subnets. Because this feature can be exploited, you should disable Proxy ARP by using the following command:
no ip proxy arp

Disable Forwarding

Disable forwarding of directed broadcasts, as these can be used for exploits or DD0s attacks
no ip directed-broadcast

Disable Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) which can be used to determine router configuration information should

be disabled
command:
no cdp enable

Disable HTTP Management Interface
Using the HTTP management interface provides go interface for router management via a browser. But enabling this feature you enable the exploits through http , and you don't want this on your border router. Disable it
command:
no ip http server

Disable Redirection of Traffic by ICMP
Disable icmp redirects as they can be used for malicious rerouting of networking traffic
command:
ip access-list extended access-list-name
deny icmp any redirect

Disable snmp
No snmp

Very recent CERT advisories have found several vulnerabilities when this protocol is enabled on the router

Disable ip source route
No ip source-route

Source routing provides a way for the intruder to exploit any weaknesses in the network design, by overlooking routes that permit entry into the network

Using the HTTP management interface provides go interface for router management via a browser. But enabling this feature you enable the exploits through http , and you don't want this on your border router. Disable it
command:
no ip http server

We will also enable tcp intercept and nbar recognition. Tcp intercept allows us to stop tcp sync DOS attacks while nbar can be used to filter NIMDA/RED code type of worms.

TCP intercept is implemented as shown below

e.g. ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.0.0 0.0.0.255

NBAR

```
#class-map match-any http-hacks
                    #match protocol http url “*.ida*"
                  #match protocol http url “*cmd.exe*"
                  #match protocol http url “*.ida*"
                  #match protocol http url “*root.exe*"
                  #match protocol http url “readme.eml*"
```

We will define GIACE domain and nameservers to prevent anyone spoofing the DNS server

```
ip domain name giace.com
ip name-server 203.10.90.72
ip name server 203.10.90.73
!
```

We then create an extended acl list called internet

```
ip access-list extended internet
 remark =====================================
 remark Access restrictions from the internet
 remark =====================================
```

We will only allow http and https access to the web servers .

```
 permit tcp any host 203.10.90.70 eq www
 permit tcp any host 203.10.90.70  eq 443
 permit tcp any host 203.10.90.71  eq www
 permit tcp any host 203.10.90.71  eq 443
```

we will allow DNS access in

```
permit udp any host 203.10.90.72 eq 53
permit udp any host 203.10.90.73 eq 53
```

we will also allow SMTP access in

```
permit udp any host 203.10.90.73 eq 25
permit udp any host 203.10.90.74 eq 25
```

Then we will deny any other access into GIACE network by applying the following acl

```
access-list 115 deny ip any any
```

These statements are essential as they allow public users to access the GIACE’s web servers. We need to

allow HTTP and HTTPS

ip access-list extended *access-list-name*

permit tcp any host *VIP-ADDRESS-GOES-HERE* eq www

permit tcp any host *VIP-ADDRESS-GOES-HERE* eq 443

Block External Use of Reserved and Internal Addresses
It To prevent spoofing of addresses from the internal network and reserved addresses , we use the deny command for example:
ip access-list extended *access-list-name*

deny ip 127.0.0.0 0.255.255.255 any

deny ip 10.0.0.0 0.255.255.255 any

deny ip 172.16.0.0 0.240.255.255 any

deny ip 192.168.0.0 0.0.255.255 any

deny ip *your-internal-network netmask* any
e.g. deny ip 192.168.0.0 0.0.255.255 any
Password-Protected LogOn
To enable password protected logon from the console port add we use the following commands

.
You will need to set your own password by using the following commands:
line con 0
password *your-password-goes-here*
login
transport input none

Disable Auxiliary Port Configuration
Disable the auxiliary port on the router , which can be used as a dialin port for modem connections. We do not allow remote administration of the border router via dial-in
command:
line aux 0
no exec
transport input none

Define a Message of the Day Banner
As part of our security policy , we want to warn users who are authorized to use the router
command:
banner motd ^C

Main FIREWALL

Restricted to GIACE s Business use only, or for purposes approved by GIACE s management
^C

Astaro Firewall will be used for all the firewall requirements of this architecture. Astaro firewall is a Linux based firewall solution containing GPL'ed software with some parts proprietary from http//www.astaro.org

The Astaro Firewalls was chosen because it provides

1) stateful inspection packet filtering using NETFILTER, where the packet payload is analyzed and recorded.
2) Application level gateways e.g. SMTP proxy, which will be used in our design for email distribution and also contains a virus engine. The virus engine can be automatically be updated so it can be kept up to date all the time .
3) HTTP proxy with Java, JavaScript & ActiveX-Filter as well as banner filtering.
4) Socks proxy that can be used with ICQ, IRC and ftp clients. This wont enabled for this design as we will not allows theses protocols into our network from the internet.
5) VPN capabilities using IPSEC and PPTP. This functionality of the firewall is based on Linux Free/Swan from http://www.freeswan.org

The main Astaro firewall is configured using the WebAdmin interface from within a browser . The WebAdmin interface is started with a HTTPS connection to the Astaro firewall on port 443.
This connection is protected by generating a CA certificate for the WebAdmin interface. Information about this certificate and how to install it is provided in the User Manual for Astaro Security Linux 2.0

The following is the main page of WebAdmin when you log into Astaro.


main.jpeg

The System Option

In this page we can setup several important general functions of the router.

Event Notification

Port scans, invalid password attempts, and self-monitoring alerts can be sent to an email address

Remote syslog

We will use this facility to enable logging to a remote system with GIACES DMZ. A better solution would be to use a third interface card and provide a separate subnet where the logging system can be placed. In

our design we will simply put the logging system in the DMZ. The problem here is that if the DMZ is compromised , most likely the intruder will attempt to attack the syslog server.

Secure Shell (ssh)

For remote management of the firewall, we can enable ssh . This will allow administrators to access the firewall from the internet using a SSH client. We will restrict management of the firewall via https login from a single system in the DMZ, or alternatively . We will need to define the ip address of this single pc using the Definitions /Networks function of the firewall.

Traffic is filtered by Astaro firewalls using iptables version V 1.2.2

The following excerpt has been taken from Astaro online help

```
      All rules are entered according to the principle: source IP - service -
destination IP - action. To be able to differentiate rules, the appropriate
networks/-groups and services/-groups must first be
      defined.



      Enter new packet filter rules:
      New packet filter rules are created by choosing from four drop-down lists.
All services, networks and groups previously created in DEFINITIONS are presented
for selection. With the button Save
      rule the appropriate rule is created as a new line at the end of the table.
The status of the new rule is initially inactive, and can be manually activated
afterwards. The new rule automatically receives the
      next available number in the table. The effectivity of the rule is decided
by its position in the table. Move the new rule within the tabel with move, if
necessary.

      From (Client):
      Here, choose the network from which the data packets are sent.

      Service:
      Here, choose the service that exists between client and server.

      To (Server):
      Here, choose the network to which the data packets are sent.

      Action:
      Here, choose the action that is to be performed in the case of a successful
      matching (applicable filter rule).
      Select from:
      Allow:
      All packets that meet these requirements are routed.
      There are two cases here.
      Either there is a service listening on that port or not.

      No service listening:
      The response to the syn-packet(S) is a connection reset(R)
```

```
      Note: This is clearly different from what you get form a ipchains firewall.

      Service is listening:
      A successfully established TCP connection. The hosts have exchanged and
acknowledged their respective syn-packets.

      Drop:
      All packets that meet these requirements are discarded, dropped to the
floor, assigned to oblivion. No reply packet of any kind is sent.

      Deny:
      All packets that meet these requirements are first logged and then dropped.

electing open Packetfilter-violation-LiveLog you are able to watch violations in
real-time.
```

Analysis of the packet filter rules

The main INPUT chain used by iptables is divided into four sub chains as shown below.

Local,FIX_CONNTRACK,AUTO_INPUT , TTT_ACCEPT and LOGDROP.

The INPUT rules handles all traffic destined for the firewall. The traffic will pass through the four sub chains define above until a rule matches.

The sub chain local will accept all traffic destined for the firewall initially.

- Local
  This chain accepts all traffic that is going from the one local interfaces of the firewall to other local interfaces

  e.g. of how this is implemented is shown below

```
Chain LOCAL (3 references)
 target     prot opt in     out     source               destination
ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0
```

Next the incoming traffic goes through the PSD_Matcher rule that We have enabled to detect port scans. The action of what should be done when a port scan is detected is further defined by rule PSD_ACTION. In our configuration we have decided to send all port scan traffic to a black hole, i.e. log the port scan and drop the traffic.

If the above two rules don't match, then FIX_CONNTRACK rules is checked to , which basically keeps a track of valid, related or established connections.

Should the packets be part of a valid connection, then the AUTO_INPUT rule is checked which allows traffic for DNS , ssh ,https,smtp,http proxy 8080

Finally if packets don't match, than all traffic is logged and dropped.

- FIX_CONNTRACK
  This is a module-based rule that fixes connections that are no longer established or valid
- AUTO_INPUT
  This chain defines the rules that are for services that run on the firewall. Theses services are SMTP , ssh, web proxy and DNS proxy. The stateful inspection rule, that all established and related connections are accepted are listed here. Rules are modified here by using the Web admin interface by enabling and disabling services.

- TTT_ACCEPT
  This sub chain defines rules for interfaces on the firewall that have either source or destination ip defined for them

- LOGDROP
  In this chain every packet is logged with the protocol as the prefix. All packets are dropped then.

  This rules basically defines As taro's functionality as below
  Generally the following is valid: 'Everything that is not explicitly allowed is forbidden'. [3]

```
Chain LOGDROP (8 references)
target     prot opt in     out     source               destination
LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        udp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        esp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        ah   --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        icmp --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        all  -f  *      *       0.0.0.0/0            0.0.0.0/0
DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

The FORWARD rule that defines rules for traffic that needs to forwarded to another interface on the firewall, is probably the main rule that will be hit most often.

This chain has four sub rules as well. The first two rules local and fix_conntrack function as described for the input rule. The third rule , AUTO_FORWARD , checks for established and related packets. The USR_FORWARD rule is then applied to any packets as they move down the chain. In this packet we define the traffic between different systems in the different VLANS.

[3] Astaro online help

In this Chain you find the ICMP-Forward accept rule, as well as the Statefull Inspection rule, that accepts all ESTABLISHED and RELATED connections.

```
 USR_FORWARD:
This is the chain that we can use to define filter rules by using
WebAdmin/Packet Filer/Rules.
```

```
   Chain USR_FORWARD (1 references)
target     prot opt in     out     source               destination
DROP       all  --  *      *       10.0.0.0/8           192.168.33.0/24
DROP       all  --  *      *       172.16.0.0/12        192.168.33.0/24
DROP       all  --  *      *       192.168.0.0/16       192.168.33.0/24
DROP       all  --  *      *       10.0.0.0/8           192.168.30.0/24
DROP       all  --  *      *       172.16.0.0/12        192.168.30.0/24
DROP       all  --  *      *       192.168.0.0/16       192.168.30.0/24
```

#the above rules will not allow forwarding of packets from public networks

```
ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.30.2        tcp spts:1:65535 dpt:53
ACCEPT     udp  --  *      *       0.0.0.0/0            192.168.30.2        udp spts:1:65535 dpt:53
```

#the above rules enable DNS access to the DNS servers in the DMZ

```
ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.30.1        tcp spts:1024:65535 dpt:443
```

#The above rules allows https access to the web servers

```
ACCEPT     tcp  --  *      *       0.0.0.0/0            192.168.30.2        tcp spts:1024:65535 dpt:25
```

#we allow access from the mail relay server to the mail server in the internal network

```
ACCEPT     icmp --  *      *       192.168.33.0/24      0.0.0.0/0           icmp type 0 code 0
ACCEPT     icmp --  *      *       192.168.33.0/24      0.0.0.0/0           icmp type 8 code 0
ACCEPT     icmp --  *      *       192.168.33.0/24      0.0.0.0/0           icmp type 11 code 0
```

pings are allowed from systems in the internal network

Configuring the Cisco 6509
The Cisco 6509 catalyst series will be configured in two parts. It contains layer2 , which performs the switching component and layer 3 that performs the routing component. The routing component of the 6509 switches , is configured with commands identical to those of the 3620 Cisco router.

Configuring the Cisco 6509 Part 1(Layer-2)
The commands for configuring the 6509 switch can be written using a notepad, and then cut and pasted onto the router in the configuration mode. We will not provide the complete configuration file for the switch but will show the commands used to configure some important aspects of the switch configuration. A complete reference guide on how to configure the 6500 catalyst series of switches can be found at the Cisco web site.

Global system settings

Basic configuration setting can be set with the following commands

```
set system name mainswitch      -use this to set system name
set time mm/dd/yy hh:mm:ss      -this sets the system time
set password                    -use this to set console password
set enablepass                  -used to set password to get to enable
mode
```

set interface sc0 192.168.20.1/255.255.255.0 -sets an ip address of switch for admin function
set interface sc0 20 -this assigns a VLAN number to the switch itself

We can now create VLAN segments and assign ports to a segment
We can Create a VLAN and assign ports by using the **set vlan** command.

set vlan 20 name VLAN20 type Ethernet mtu 1500 said 100020 state active
set VLAN 31 name VLAN31 type Ethernet mtu 1500 said 100031 state active
set VLAN 32 name VLAN32 type Ethernet mtu 1500 said 100032 state active
set VLAN 33 name VLAN33 type Ethernet mtu 1500 said 100033 state active

Using the *set vlan vlan-number module/port-number or range of ports command* we setup our vlans

#module 2 : 48-port 10/100BaseTX Ethernet
set vlan 30 2/1-12
set vlan 31 2/13-25

```
set vlan 32   2/26-30
set vlan 33   2/32-48
```

Securing the VLANS.

The Cisco switch provides us with the network segmentation that we desire. We have to make sure that the VLANS are only able to communicate with each other under the policies that we have defined.
To achieve this we define two groups of VLANS e.g.

Internal – VLANs 32 and 33

External – VLANs 28, 29, and 30

We will use acls, to restrict the internal VLAN group from communication with the external VLAN

Configuring the Virtual Interfaces
VLAN interfaces bind to the VLAN that corresponds to the interface name. Hosts that belong to VLANs with a VLAN interface as their gateway can communicate with other VLAN interfaces and corresponding hosts. Be careful which VLANs you configure with a VLAN interface.

To create a VLAN interface:

here we define the VLAN interfaces and the corresponding IP addresses:

```
interface vlan20
ip address 192.168.20.254 255.255.255.0
interface vlan28
ip address 192.168.28.254 255.255.255.0
interface vlan29
ip address 192.168.29.254 255.255.255.0
interface vlan30
ip address 192.168.30.254 255.255.255.0
interface vlan31
ip address 192.168.31.254 255.255.255.0
interface vlan32
ip address 192.168.32.254 255.255.255.0
interface vlan33
ip address 192.168.33.254 255.255.255.0
```

```
interface vlan30
 ip address 192.168.12.254 255.255.255.0
 ip access-group vlan30-in in
!
interface vlan31
 ip address 192.168.13.254 255.255.255.0
 ip access-group vlan31-in in
 no ip redirects
 no ip directed-broadcast
!
interface vlan32
 ip address 192.168.15.254 255.255.255.0
 ip access-group vlan32-in in
 no ip redirects
 no ip directed-broadcast

!
interface vlan33
 ip address 192.168.21.254 255.255.255.0
 ip access-group vlan33-in in
 no ip redirects
 no ip directed-broadcast
 no ip mroute-cache
!
```

Isolating Particular VLANS

We will use ACLS, similar to those we have used for the routers to restrict the traffic between the VLANS according to our security policy

The ACL appears as follows:

We are permitting traffic from the internal network into the DMZ and the backend VLAN of the internal firewall

```
ip access-list extended vlan33-in
 permit ip 192.168.33.0 0.0.0.255 192.168.31.0 0.0.0.255
 permit ip 192.168.33.0 0.0.0.255 192.168.32.0 0.0.0.255
 permit ip 192.168.33.0 0.0.0.255 224.0.0.0 0.0.0.255
```

Allow access from the backend of internal firewall to the internal VLN33 network

```
ip access-list extended vlan32-in
permit ip 192.168.32.0 0.0.0.255 192.168.33.0 0.0.0.255
permit ip 192.168.31.0 0.0.0.255 192.168.33.0 0.0.0.255
permit ip 192.168.32.0 0.0.0.255 224.0.0.0 0.0.0.255
```

We allow traffic on VANs from the internet to access servers in the DMZ

```
ip access-list extended vlan30-inbounds
 permit ip 192.168.28.0 0.0.0.255 192.168.30.0 0.0.0.255
 permit ip 192.168.30.0 0.0.0.255 224.0.0.0 0.0.0.255
```

We apply the rules to the switch with the following commands
command:

```
interface Vlan32
 ip access-group vlan32-in in
```

Internal network access to the DMZ

We have to add static route for servers on the internal network, VLAN 33 to reach the DMZ. All traffic is routed to the internal firewalls, which in turn based upon its rules either allow or disallow traffic to systems in the service network. To configure the static route, use the **ip route** command with the following syntax:

ip route *destination-address network-mask gateway-address*

Securing the Switch

We will disable services that are not needed and those that can be exploited. These reasons for disabling these services have been explained in the section Configuring the border router, assignment 2

Command:

```
no service finger
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no ip proxy arp
no ip directed-broadcast
no cdp enable
```

Banner

Internal Firewall

The internal firewalls are Astaro firewalls, and they can be configured using the WebAdmin interface as described under the section , Main firewall

Configuration

Using the internal firewall The following rules will be implemented

Define using the WebAdmin pages

Add the routes to allow the firewall to access the servers on the internal network

Choose Routing→Network—Interface route
Where the Interface is the internal interface eth1 of the Astaro internal firewalls

Route add 192.168.13.0/24 –i eth1
Route add 192.168.13.0/24 –i eth1

Add ip addresses of the internal and external interface

Choose Routing→Network—Interface route

External ip address device eth0 192.168.31.254 255.255.255.0
Internal ip address device eth1 192.168.33.254 255.255.255.0

Define the traffic that is allowed from the DMZ (via VLAN 31) into internal network (VLAN 33)

For a Microsoft SQL server allow access to port 1433 from DMZ servers

Choose Packet Filter Rules →from(client)--→server--→port(services) -→action allow

```
0     0 ACCEPT     tcp  --  *      *   192.168.31.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:1433
```

Allow DNS access into internal network

```
0     0 ACCEPT     tcp  --  *      *   192.168.31.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:53
```

Define the traffic that is allowed from the internal network (VLAN 33) into DMZ (via VLAN 31)

```
Allow www,proxy http,https,smtp ,dns from employees and server systems
in the internal network to the internet
```

```
0     0 ACCEPT     tcp  --  *      *   192.168.33.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:443
0     0 ACCEPT     tcp  --  *      *   192.168.33.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:80
0     0 ACCEPT     tcp  --  *      *   192.168.33.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:8080
0     0 ACCEPT     tcp  --  *      *   192.168.33.0/24   192.168.33.0/24     tcp spts:1024:65535 dpt:25
```

PPTP Solution

We will again use two multihomed Astaro firewalls and implement our VPN using PPTP protocol. Detailed information on PPTP can be found in RFC 26 The reason for choosing this is that we will only allow a few pc's from business partners to connect to GIACES network. The initial demand from business partners is predicted to be minimal and, they will only connect once a day to GIACES site and download database files .

Administrators and Sales Persons will need to connect via their laptops from hotels or from their homes.

The internal interface of the VPN firewall is connected to VLAN 33 and the external interface connected to the Cisco 2610 routers. We will need to create static routes on the VPN servers to VLAN 31 .The Cisco routers will need to open the port 1723 for both inbound and outbound connection.

We will use the PPTP protocol instead of the L2TP protocol. PPTP is chosen because it can be used over NAT systems. We will use 128-bit encryption certificates or MS-CHAPV2 and long passwords. Also EAP cannot be used with windows NT 4.0 or Windows 98 operating systems, This can be argued to be not as secure as with using EAP and certificates, but our aim here is to initially provide a solution that is easy to implement. This VPN solution will need to be reviewed in the future .

The other advantage in using PPTP VPN is that, our clients will most probably be MS Windows 98 or windows 2000.

Configuring Astaro VPN

The Web Admin interface can be used to configure the VPN. In the VPN directory open PPTP remote access window. Choose the enable button to enable **PPTP Road Warrior VPN**. We then can choose the encryption level under **Encryption Strength.** We will choose the highest level of 128 bits. We have confirmed with our international business partners, that they can install clients supporting this level of encryption. We will need all windows 2000 clients to install the service pack 2 to support 128-bit

encryption level.

PPTP IP Pool

The users of the PPTP service are defined under Definitions/Users. Over here they will also be assigned private addresses in 10.5.0.1 to 10.5.0.100 range. We will also need to create Masquerading rules for the address we assign to the VPN clients.

We can use the VPN live log to monitor or trouble shoot VPN connections.

How is a client setup

In order to setup a windows 200 client we need to follow the following steps

1) choose start→settings→network and dialup connections
2) choose make new connection
3) choose next and chose to connect to a private network through the internet
4) if dialing through an ISP choose DIAL other connections first
5) enter the ip address of the VPN server of GIACE
6) in the connection availability window , restrict access to oneself
7) finish the setup by giving it a name for the VPN connection
8) By right clicking on DUN connections properties choose security→ advanced and choose MSCHAPv2 protocol and under network properties select PPTP.

This basically sets up the client and their server for dial engaging in a VPN communication tunnel.

Our first test in establishing an audit process for the Primary firewall, or for any host system, requires a complete written procedure for the audit process. We will only provide an outline for the audit process, but the complete documentation will contain items like the scope of the audit. How often the audit should be performed and whose responsibility is to perform this audits. The documentation should also provide a detailed baseline of the system or the systems that are to be audited. This baseline should not only include a picture of what the audit system files are but also should include detailed logs and network traffic usages. These baseline measurements will be able to help us determine what is the 'normal' data of a system or network.

Other important contents of this documentation procedure should include sections on

- Reporting Security incidents.
  This defines what happens when intrusions or incidents occur . Included in this section management and technical contact points, phone numbers and email Addresses
- Security/Integrity Advisory Process
  This will define the process of how to keep up to date with the latest security patches

- Virus protection
  This should define the processes for maintaining anti virus software on the firewalls and ways to keep it up-to-date with the latest virus signatures

In this technical audit of the primary firewall we will take the following approach.

The initial audit will be performed over a period of 2 weeks over two phases.

- Phase1
  An initial meeting will be held with the client to determine a time when the audit will be performed. We would like to perform the audit when network usage is the least so the business impact on GIACE is minimal. (The security architecture that we have designed for GIACE has two firewalls , with one used as a backup firewall. With both firewall having the same configuration, we can take it offline and perform scans by attaching a scanner to its external interface. This scan will provide us with a better result of the firewall, because if we perform scans from the outside of the router, we are not really fully testing the firewall, the router has extensive filtering rules as well.) To determine average network usage we will run the iptraf utility to measure bandwidth over a week. All the tools we use will be burned onto cd , keeping inline with recommendations from GIACE study guide page 226.
  We will ensure that all logs are appropriately enabled on the firewall. We don't want to end up with no logs to check. From the logs we should be able to determine the following

    Logins, login failures, permission changes, rules changes, web (squid) logs, DNS logs etc

- Phase 2
  In this phase we will actually perform the penetrations test using NMAP, retrieve all flog files and produce a detailed report of our findings. This report will contain recommendations.

  Costs.

  The main cost will be the man-hours involved in running data collection tools and analyzing the results. The total cost involved will be approximately 3 full days consultation charges, which will be approximately $1500, plus other cost of $500.

Audit Exercise
The audit exercise that we will perform will only contain results of port scans on the main firewall. Other security policies like DNS access, mail access and http and https access , virus detection was not possible to be tested with the setup available

The main tool used for the scans was nap from Fodor http://www.insecure.org/nmap

- Performing a port scan of the primary firewall external interface , will prove what ports are open and hence what access is allowed from the internet.

Using the following command
Nmap –s T –O –P0 –n –v 203.10.90.1

Where the options define the following perimeters
-sT – used to perform a connect scan
-O - attempts to determine the OS of the target
-P0 - performs the scan without using ping. We need to use this as firewalls normally have pings disabled against their external interface
-n - we are turning off name resolution of the target . This can be used to speed up scans
-v - Produce verbose output

The output obtained from the scan result is shown in figure 5 below. Nmap.jpeg is page one of the output and nmap2.jpeg is page 2.

Figure 5 Shows the output of nmap port scan on the main firewall.

from the results we can see that only ports 53,25,443 and 80 are open. This verifies that our security policy is applied by the external firewalls.

The interesting result is that the Operating System fingerprinting is able to determine that it is RedHat Linux. Although this isn't totally true for the Astaro firewall, as it is a Linux variant, hackers will have some ideas as to what type of firewall is installed. This will enable them to guess what type of filters can run on these types of Linux systems and hence go searching for exploits and vulnerabilities for this particular architecture.

- Spoofing
  We will scan the firewall port 443 from spoofed addresses

  Nmap –s S –P0 –s 10.5.0.5 –p 443 –v –n 203.10.90.1

  Where the options
  -s S –define a sync scan
  -s -defines the source we are scanning from i.e. a private address
  -v - verbose mode
  -n - don't resolve names
  -p 443 – we are scanning port 443 in this example

  We are deliberately scanning port 443 because we know that it is open, and if our filter rules are filtering spoofing addresses, then we should see a different response to a scan

  The results obtained are shown below in figures 6


spoof3.jpeg

Figure 6 Output of nmap scan using a spoofed private address

The output shows that port 443, is in a filtered mode. This determines that our iptables rules are being hit.

- Pinging the external interface of the firewall

  The security policy states that users from the internet users should not be able to ping the firewall . We tested this rule using the following command

  Ping –U 203.10.09.1

  The results obtained is shown in figure 7 below


ping.jpeg

Figure 7 nmap ping scan output for the primary firewall

The output shows the two parts of the ping scan
The Astaro firewall has two options, one to enable ICMP FORWARDING that allows all users to ping systems through the firewall to systems inside the GIAC network. This has

been disabled
The second option allows a user to enable/disable pinging the firewall itself.

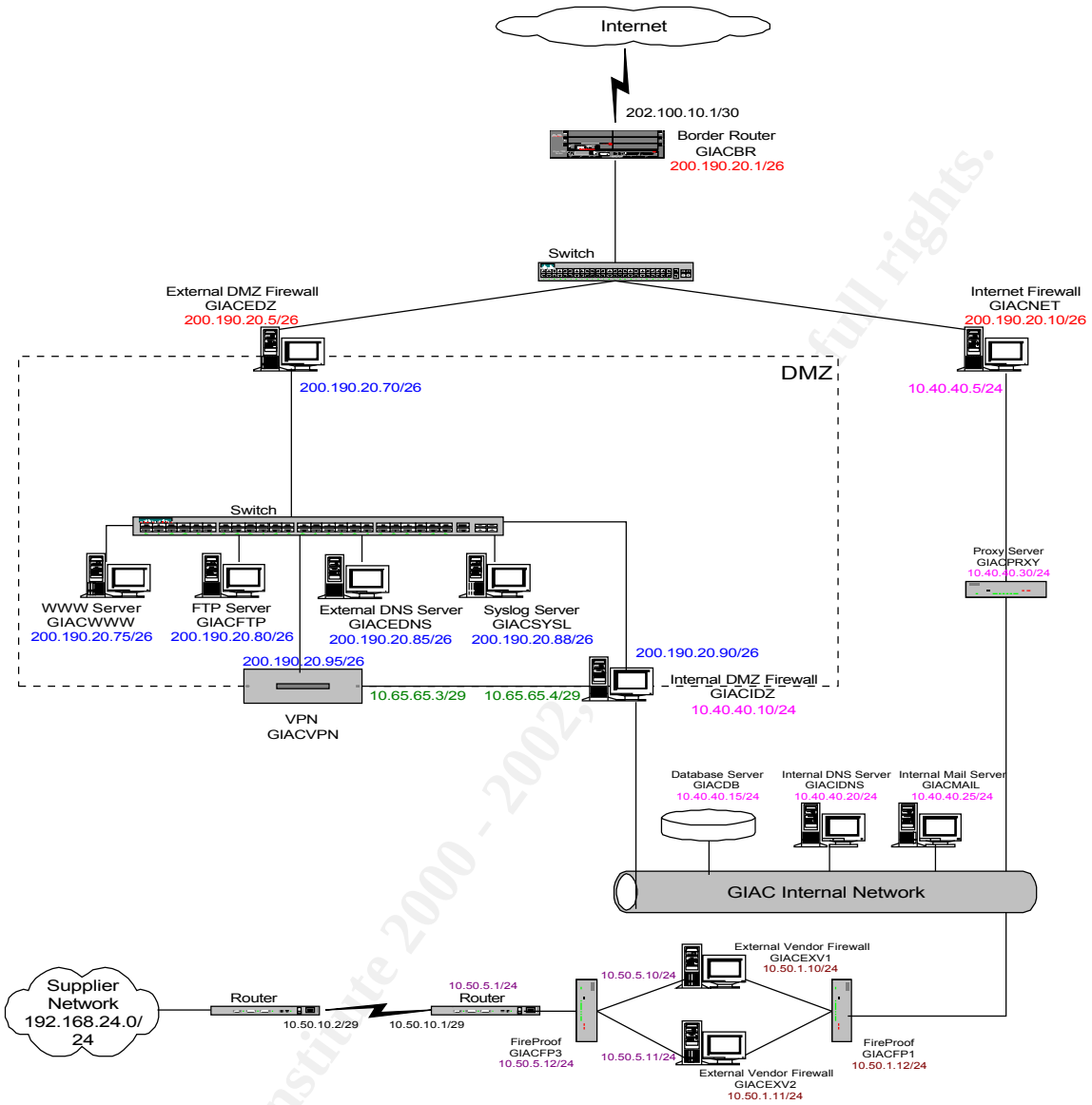
We performed our scans by initially enabling the ICMP on the firewall itself. This resulted in ICMP echo replies as shown in the top half of the output in figure 7. When the ICMP on the firewall option was disabled, this stopped all ping replies as shown in the bottom part of the screen output in figure 7 above.

It must be noted that we have specifically added rules to allow internal uses to ping the firewall via specific firewall rules discussed in assignment 2 .

Recommendation for ports cans
Astaro firewalls provides a feature which can be used to monitor port scans as they happen and the actions to perform when a port scan is detected. We recommend this to be enabled as shown in figure 8 below Disabling port scans will prevent OS fingerprinting that was determined by port scan above

Figure 8 How to disable port scans on firewall

Design Under Fire



The above network design by Asad Alsader posted at http://www.giac.org/practical/Asad_Alsader_GCFW.zip will be used for our attack network

A distributed denial of service attack

The whole idea of a distributed denial of service attack (DDOS) is to flood a company's web server and communication links temporarily halting access.

There are numerous DDOS methods , the most common being

- Floodnet (netstrike)
  This attack uses a java-based application to overwhelm web servers for non-existent pages and queries to search engines. It uses a tcp/ip flooding attack which saturates the CPU and the network. It will also generate massive logs and fill up the server disks.

  This attack can be detected using and IDS system and then needs to be filtered using a packet filter
- Trinoo
  This method of attack uses master and agent configuration on several compromised computers, which will then be used to flood victims using UDP flood. There are tools available, which can detect agents via remote scanning with tools such as NIPC's find_ddos from http://www.fbi.gov/nipc/trinoo.htm

- Tribal Flood Network (TFN)
  This is an attack using many DOS attacks, utilizing SMURF,TCP syn flood,UDP flood and ICMP flood attack. More information on this type of attack can be found at http://staff.washington.edu/dittrich/misc/tfn.analysis
- TFN2k
  This is a similar attack to TFN but uses encryption between its master and agents. Its agents can be detected using NIPC,s find_ddos tool.

We will base our attack using the Stacheldraht tool http://staff.washington.edu/dittrich/misc/stacheldraht.analysis ,which uses multiple DOS attacks using Smurf,TCP SYN flood,Udp flood and ICMP flood. In its original form its agents can be detected with remote scanning

A little bit of Background

The first stacheldraht attacks surfaced in late august/early September of 1999 . A CERT incident note 99-04 was released describing this attack .; http://www.cert.org/incident_notes/IN-99-04.html

The captured source code for stacheldraht, which is available according to Dittrich, has to be obtained and certain keyword modified before we can successfully utilize it to perform an attack on or target network.

The stacheldraht network consists of the following components

- Clients
  These are the control systems, which communicate with the handlers via an encrypted telnet like program
- Handlers
  These are the systems that control the agents. Of the 50 systems that we have compromised we will use two systems as handlers
- Agents
  These are the systems that compromised systems, which actually perform the DDOS attack. We will have 48 clients to perform the attack for us
- victims
  The victim in our case is the border Cisco router of XXXXXXXXXX

We will modify the stacheldraht source code and change some of the known keywords. For example when an agent starts up it wants to know which handler will control it. It sends an ICMP_ECHOREPLY packet with an ID field value of 666 and data field containing string “skillz”

We will modify the code to use a different port and a different string for this communication.

If the master handler gets this packet , it sends a ICMP_ECHOREPLY packet with an id field of value 667 and data field containing string “ficken”

We will modify this behavior as well. This means that any monitoring of ICMP packets on attack network will require more time to figure out what’s happening.

We will also alter other strings, which can identify the original stacheldraht. Some of the keywords are spoofworks, niggahbitch, which are not encrypted.ICMP_ECHOREPLY packets with ID values of 666,667,689 and 1000 will also be modified before we launch our attack.

On the compromised systems , we will install our root kits , and use hidden directories to conceal them. Once our handlers and agents are set up we will proceed to attack GIACS network using the following commands

1) .madd ip
   This command will allow us to add the ip address of the GIAC's network as the victim
2) .micmp
   This command will allow us to use the ICMP flood attack. we can use .setisize to modify the size of UDP packets. We will try several variations here
3) .mudp
   This will enable us to use udp attacks. We can use .setusize to modify the packet size of our udp attacks.

How to protect against DDOS attacks

It is important that all systems are kept up-to-date with the security patches. Several new tools that are available now can be used to prevent this type of attacks. These tools are available from Captus Networks Corp, Foundry networks, Mazu Networks, radware, reactive Network solutions and Top Layer network. The paper, Fireproofing Against Dos Attacks by Jeff Forristal from networkcomputing.com describes the functionality of the above commercial products and how they can be used against preventing DDOS attacks. It must be noted that the above tools do not completely stop a DDOS attack on its tracks. The DDOS attacks can stopped completely only at the expense of shutting down the business network.

TCP Intercept

We can stop tcp sync attacks with using the tcp intercept feature of the Cisco routers.

To enable this feature on routers , we need to define an IP extended access list using the command

In the router config mode
 # access-list *access-list-number* {**deny | permit**} **tcp any** *destination destination wildcard*

enable TCP intercept
#ip tcp intercept list *access-list-number*
e.g. ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.0.0 0.0.0.255

More information can be found at
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrsfw

NBAR

Since the nimda /code red worm, is a newer threat we would recommend protecting against it as well. This can be done using the Network-based application recognition(NBAR) feature of Cisco routers. The minimum Cisco IOS software versions required is 12.1(5) T for most routers. We can apply nbar commands as follows using ingress filtering as follows

In the router config mode#class-map match-any http-hacks
#match protocol http url “*.ida*"
#match protocol http url “*cmd.exe*"
#match protocol http url “*.ida*"
#match protocol http url “*root.exe*"
#match protocol http url “readme.eml*"

An Attack on an Internal System

Our first approach to compromising an internal system will be to use several reconnaissance techniques to learn more about the network.

- We will need to determine what remote access devices does GIAC use. This may require social engineering to determine how sales staff connect to the network
- We will review information available on GIAC public website. Any company information posted here will help us create a picture of the network. The location information of the company may be enough to determine the IPS providers for the company for example, and via this information we can further research and find out through which ISP's remote employees may be connecting through.
- We can look at the source code of GIACS website, and see if comments imbedded in it can provide us with some clues to vulnerabilities.
- We can attempt a zone transfer to determine if that reveals anything.
- We will connect to the ports 25 and 53 to see if the banner reveals anything about the software version of bind or sendmail .
- We can run a stealth port scan

We will assume that most of the above reconnaissance techniques haven't revealed much to us as the network designer is a certified GCFW and his network is well protected from these techniques.

But from our reconnaissance we have determined that a sales staff uses a VPN connection from his laptop at home and connects to GIAC Enterprises network via the largest service provider the location he lives in. This sales staff uses a DSL modem for connection and we have obtained his email address as it was listed on GIACS website.

Our next step will be to obtain a temporary account with the same ISP as the sales staff , obviously using false information, and proceed to perform an attack on the sales staffs laptop from a hotel room.

We will email the sales staff, masquerading as a potential big customer wanting to buy cookies for a big organization with the promise of continuing sales in the future. This will form a basis of our initial conversation with the sales staff. We will then attempt to deceive the sales staff to install a backdoor program like Back Orifice on the impression that he is installing a spreadsheet of our companies projected requirements for cookies that we would like to buy

This action may or may not be successful, as a good virus checker may be able to identify this agent that we want to install, however new versions of Back Orifice may not be that easily detected. If the sales staff is duped into clicking on the attachment, we will basically have control over his workstation. Now we will proceed to attack the server he connects to inside GIACs perimeter. This can be any systems the sales staff has access to and even through the VPN connection.

Our Next move will be to monitor the sales staffs action for several days learning as much as possible about his employers network. The sales staff may even have a Web Cam attached to his laptop, thus providing us with details when he has left the room, his pc connected and at our disposal.

There are several ways this type of attack can be prevented

- Running a good virus tool, such as Norton's Antivirus, and keeping it up to date with the latest patches.
- Educating all the staff about content sent over email, and restricting the execution of unknown attachments. Basically all users must be educated about security in general, videos of common security vulnerabilities and attacks may be of more attractive option of a means of education for the non-technical staff.
- For the GIAC network, running scanning tools, which can detect hacker tools
- Using personnel firewalls on remote users workstations. If possible restrict laptops provided to employees for strictly business use only.

Appendix 1

Border router configuration

```
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname kurra01
!
logging rate-limit console 10 except errors
```

```
enable secret  BR7edc4ab
enable password BR7edc4ab
!
ip subnet-zero
!
no ip finger
!
no snmp
!
no ip source-route
!
no ip bootp server
!
call rsvp-sync
cns event-service server
!
interface FastEthernet0/0
description : This interface connects to the internet
ip address 203.10.90.4  255.255.255.240
 ip access-group internet in
 no ip redirects
 no ip proxy-arp
 speed 100
 full-duplex
 no cdp enable
!
 interface FastEthernet0/1
 description : This Interface connects to Firewall1
 ip address 203.10.90.253 255.255.255.240
 speed 100
 full-duplex
 standby 1 timers 1 2
 standby 1 priority 105 preempt
 standby 1 ip 203.10.90.253
 standby 1 track Fastethernet 0/0
!
interface FastEthernet1/0
description : This interface connects to Kurra02 (X cable)
ip address 192.168.10.5  255.255.255.0
duplex auto
speed auto
!
ip classless
no ip http server
```

```
!
ip domain name giace.com
ip name-server 203.10.90.72
ip name server 203.10.90.73
!
ip access-list extended internet
 remark =======================================
 remark Access restrictions from the internet
 remark =======================================
 permit tcp any host 203.10.90.70 eq www
 permit tcp any host 203.10.90.70  eq 443
 permit tcp any host 203.10.90.71  eq www
 permit tcp any host 203.10.90.71  eq 443
 permit udp any host 203.10.90.72 eq 53
 permit udp any host 203.10.90.73 eq 53
permit udp any host 203.10.90.74 eq 25
 permit udp any host 203.10.90.75 eq 53

 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.0.0.0 0.240.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
access-list 115 deny ip any any
!
!
banner motd

#############################################################

 Restricted to GIACE s Business use only,or for purposes approved by GIACE s management

#############################################################

!
line con 0
 password  BR7edc4ab
 login
 transport input none
line aux 0
line vty 0 4
 access-class 115 in
 password BR7edc4ab
 login
!
```

end

Appendix 2

Main Firewall configuration

```
Chain INPUT (policy DROP )
target     prot opt in     out     source               destination
LOCAL      all  --  *      *       0.0.0.0/0            0.0.0.0/0
PSD_MATCHER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
FIX_CONNTRACK  all  --  *      *       0.0.0.0/0            0.0.0.0/0
AUTO_INPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0
TTT_ACCEPT  all  --  *      *       0.0.0.0/0            0.0.0.0/0
LOGDROP    all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy DROP )
target     prot opt in     out     source               destination
LOCAL      all  --  *      *       0.0.0.0/0            0.0.0.0/0
PSD_MATCHER  all  --  *      *       0.0.0.0/0            0.0.0.0/0
FIX_CONNTRACK  all  --  *      *       0.0.0.0/0            0.0.0.0/0
AUTO_FORWARD  all  --  *      *       0.0.0.0/0            0.0.0.0/0
USR_FORWARD  all  --  *      *       0.0.0.0/0            0.0.0.0/0
LOGDROP    all  --  *      *       0.0.0.0/0            0.0.0.0/0

 Chain OUTPUT (policy DROP )
target     prot opt in     out     source              destination
LOCAL      all  --  *      *       0.0.0.0/0            0.0.0.0/0
FIX_CONNTRACK  all  --  *      *       0.0.0.0/0            0.0.0.0/0
AUTO_OUTPUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0
TTT_ACCEPT  all  --  *      *       0.0.0.0/0            0.0.0.0/0
LOGDROP    all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain AUTO_FORWARD (1 references)
target     prot opt in     out     source               destination
ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0          state RELATED,ESTABLISHED

Chain AUTO_INPUT (1 references)
target     prot opt in     out     source               destination
LOGDROP    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          tcp dpt:53
LOGDROP    udp  --  *      *       0.0.0.0/0            0.0.0.0/0          udp dpt:53
LOGDROP    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          tcp dpt:22
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          tcp spts:1024:65535 dpt:443
LOGDROP    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0          tcp spts:1024:65535 dpt:443
ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0          state RELATED,ESTABLISHED

Chain AUTO_OUTPUT (1 references)
pkts bytes target     prot opt in     out     source               destination
ACCEPT     esp  --  *      *       203.10.90.1          0.0.0.0/0          esp
ACCEPT     udp  --  *      *       203.10.90.1          0.0.0.0/0          udp spt:500 dpt:500
ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0          state RELATED,ESTABLISHED

Chain FIX_CONNTRACK (3 references)
pkts bytes target     prot opt in     out     source               destination

Chain LOCAL (3 references)
 target     prot opt in     out     source               destination
ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0

Chain LOGDROP (8 references)
target     prot opt in     out     source               destination
LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        udp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        esp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        ah   --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
LOG        icmp --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        all  -f  *      *       0.0.0.0/0            0.0.0.0/0
DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain PSD_ACTION (2 references)
target     prot opt in     out     source               destination
LOG        all  --  *      *       0.0.0.0/0            0.0.0.0/0
DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain PSD_MATCHER (2 references)
target     prot opt in     out     source               destination
0     0 RETURN     all  --  *      *       192.168.33.0/24      0.0.0.0/0
0     0 PSD_ACTION  tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           psd options
0     0 PSD_ACTION  udp  --  *      *       0.0.0.0/0            0.0.0.0/0           psd options
Chain TTT_ACCEPT (2 references)
target     prot opt in     out     source               destination

ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:25
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1:65535 dpt:53
0.0.0.0/0          udp spts:1:65535 dpt:53
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:8080
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:80
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:443
ACCEPT      udp   --  *       *        0.0.0.0/0              0.0.0.0/0            udp spts:1024:65535
dpts:33000:34000
ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0           icmp type 11 code 0
ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:113

b
Current NAT rules

target      prot opt in      out      source          SPOOF_DROP   all   --  *       *         0.0.0.0/0
0.0.0.0/0
AUTO_NAT_PRE  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain POSTROUTING (policy ACCEPT 20160 packets, 957K bytes)
pkts bytes target     prot opt in     out     source               destination
AUTO_NAT_POST  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT 20160 packets, 957K bytes)
target     prot opt in     out     source               destination
AUTO_NAT_OUT  all  --  *      *       0.0.0.0/0            0.0.0.0/0

Chain AUTO_NAT_OUT (1 references)
target      prot opt in      out      source                DNAT        tcp  --  *       *       0.0.0.0/0
203.10.90.5        tcp spts:1024:65535 dpt:80 to:192.168.30.1:80

Chain AUTO_NAT_POST (1 references)
target     prot opt in     out     source               destination

Chain AUTO_NAT_PRE (1 references)
target     prot opt in     out     source               destination
REDIRECT   tcp  --  *      *       192.168.30.0/24      0.0.0.0/0           tcp spts:1024:65535 dpt:80
redir ports 8080
ACCEPT     tcp  --  *      *       192.168.30.0/24      0.0.0.0/0           tcp spts:1024:65535 dpt:8080
LOGDROP    tcp  --  *      *       0.0.0.0/0            0.0.0.0/0           tcp spts:1024:65535 dpt:8080
DNAT        tcp  --  *      *       0.0.0.0/0            203.10.90.1         tcp spts:1024:65535 dpt:80
to:192.168.30.1:80

Chain LOGDROP (1 references)
pkts bytes target     prot opt in     out     source               destination
LOG        tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        udp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        esp  --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        ah   --  *      *       0.0.0.0/0            0.0.0.0/0
LOG        icmp --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
LOG        all  -f  *      *       0.0.0.0/0           0.0.0.0/0
DROP       all  --  *      *       0.0.0.0/0           0.0.0.0/0

Chain SPOOF_DROP (1 references)
target     prot opt in     out     source              destination
LOG        all  --  eth0   *       192.168.29.1        0.0.0.0/0
DROP       all  --  eth0   *       192.168.29.1        0.0.0.0/0
LOG        all  --  eth0   *       203.10.90.0/24      0.0.0.0/0
DROP       all  --  eth0   *       203.10.90.0/24      0.0.0.0/0
LOG        all  --  eth1   *       203.10.90.1         0.0.0.0/0
DROP       all  --  eth1   *       203.10.90.1         0.0.0.0/0
LOG        all  --  eth1   *       192.168.29.0/24     0.0.0.0/0
DROP       all  --  eth1   *       192.168.29.0/24     0.0.0.0/0
```

References

Online Sources

Smurf
http://www.cert.org/advisories/CA-98.01.smuf.html

TCP-SYN flood information
ftp:/info.cert.org/pub/cert_advisories/CA-96.21.tcp_syn_flooding

CERT analysis of DDOS
http://www.cert.org/advisories/CA-2000-01.html
http://staff.washington.edu/dittrich/talks/cert/
http://www.cert.org/reports/dsit_workshop.pdf

Stacheldraht
http://staff.washington.edu/dittrich/misc/stacheldraht.analysis

Cisco CBAC explained
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt3/sccbac.htm#3974

Configuring Cisco Access Control Lists
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt3/scacls.htm

Microsoft Systems Architecture: Internet Data Center
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/architect/default.asp

Microsoft Systems Architecture: Internet Data Center : Reference architecture Guide
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/ittasks/architect/default.asp