# Global Information Assurance Certification Paper

GSEC Assignment Ver 1.3 7/5/2002 – Michael Galvin
First Line of Defence – Cisco Internet Router Configuration.


Abstract

One of the main areas that the SANS GSEC course teaches is the concept of 'defence in depth'. The idea behind this is to protect your information assets from internal and external compromise by deploying not one, but multiple layers of defence. In doing this, it makes it more difficult for the would be attacker to reach your valuable assets should any one layer be compromised. The purpose of this paper is to give an example of a Cisco router configuration that can be used as the first layer of protection from external attack. The example organisation ACME, has single mail server and a small web site that contains static content. ACME consists of approx. 100 employees, all of which send and receive email and access the internet on a daily basis.


ACME Network Diagram

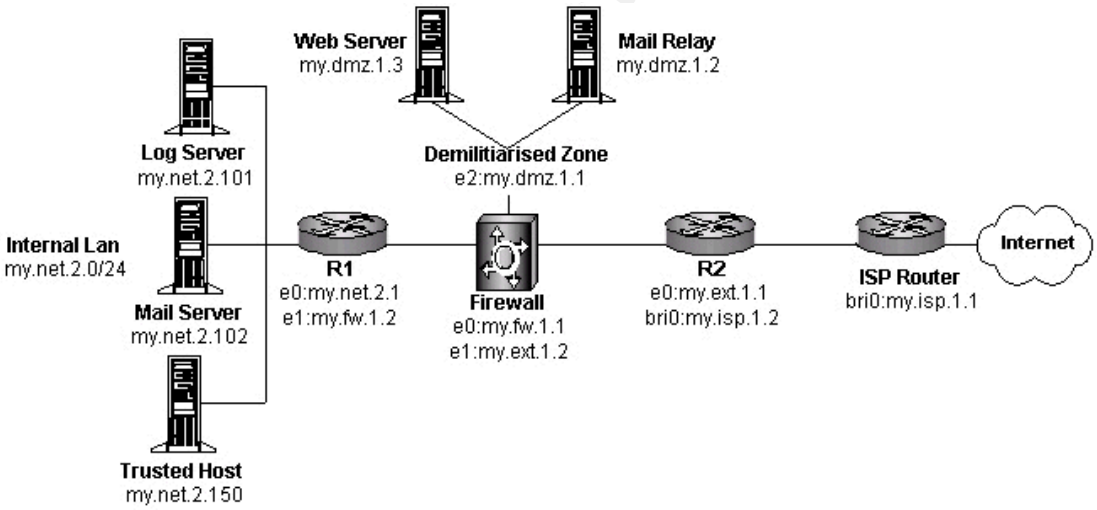


Diagram Source: Original by author.

Hardware/Software Specification.

The following hardware and software was chosen for the ACME Internet/border router:

Cisco 2620
32k NVRAM
8192k Flash Memory
1 x Fast Ethernet interface
1 x BRI interface
Cisco IOS Version 12.1

Router Access.

In order to enquire on, or modify the router configuration, a connection to the device must be established. This can be achieved in a number of different ways, either by connecting directly to the serial port at the back of the router or using a telnet program to connect to the IP address of one of the router interfaces.

Inputting Commands.

The router configuration can be input or updated by manually typing the commands into the Cisco command line interface (CLI) or by cutting and pasting the commands from a text file, or uploading them from a TFTP server.

Commands entered into the CLI are used to input, update or enquire upon the routers status. The commands are applied globally to the router or to a specific router interface.

Document Conventions.

The following conventions will be used within this document to show the command line structure.

- All router prompts will be shown in normal case.
- Commands will be shown in their long form in italics *long version of command* .
- An explanation on the command will be shown, along with the short form of the command in brackets (*short command)*.

Command Line Basics

Once a connection to the router has been established, you will be required to enter the password to gain access:

| | |
|---|---|
| password: *password* | supply the router password. |

If a valid password is entered, the command prompt with the name of the router will appear:

acme_R2>

You are now connected to the router in unprivileged or exec mode. This mode allows limited examination of the router:

| | |
|---|---|
| acme_R2> *show version* | display information about the running software version. (*sh* |

| | |
|---|---|
| | *ver)* |
| acme_R2> *show memory* | display information about the routers memory. (*sh mem)* |

To update the router configuration, you must be in privileged exec or enable mode:

| | |
|---|---|
| acme_R2> *enable* | enter privileged mode. (*en)* |
| acme_R2> password : *password* | supply the privileged mode password. |

Once in enable mode, the router command prompt will change to the following:

acme_R2#

To configure the router from the command line, you must enter terminal configuration mode:

| | |
|---|---|
| acme_R2# *configure terminal* | enter terminal configuration mode (*conf t*). |

The command prompt will change to allow input of global configuration commands:

acme_R2(config)#

To configure specific interfaces on the router, enter the interface name at the global configuration command prompt:

| | |
|---|---|
| acme_R2(config)# *interface fast ethernet 0* | interface Fast Ethernet 0 (*int fast 0*). |

The command prompt will change to allow input of interface specific commands:

acme_R2(config-if)#

Once you have finished inputting your router configuration commands, you can exit to the previous configuration level by typing 'exit' at the command prompt or <cntrl-z> to exit configuration mode completely.

| | |
|---|---|
| acme_R2(config-if)# *exit* | exit to previous configuration level |
| acme_R2(config)# *^Z* | exit configuration mode completely <cntrl-z>. |

The routers running configuration is now updated. If you are happy that this

configuration is correct, you may now copy the running configuration to the start up configuration for use when the router is reloaded.

| | |
|---|---|
| acme_R2# *copy running startup* | copy running configuration to start up configuration (*copy run start*). |
| acme_R2# destination filename(startup-config) | specify the name of the filename for the startup configuration or default |

Now that we have covered the basics of accessing the router and inputting global and interface specific commands, we will move on to more the detailed security aspects that need to be addressed.

Preventing Physical Access to the Router.

Preventing physical access to the router will stop unauthorised persons from connecting locally to the console or aux port. As by default, no password is required for this type of connection, an attacker could logon on and attempt to enter privileged mode to change any aspect of the router configuration.
To restrict physical access to the router, it is recommended that the router is kept in a secure area where access is monitored.

Setting Passwords and Restricting Access.

To prevent unauthorised login, strong encrypted passwords should be used for login and privileged mode access.
To prevent unauthorised remote access, telnet should be restricted to specific workstations on your trusted network and Cisco http server should be disabled.

The above can be achieved using the following commands:

| | |
|---|---|
| acme_R2> *enable* | enter privileged mode (*en)*. |
| acme_R2> password : *password* | supply the privileged mode password. |
| acme_R2# *configure terminal* | enter terminal configuration mode (*conf t)*. |
| acme_R2(config)# *service password-encryption* | MD5 hashing on password. |
| acme_R2(config)# *enable secret password* | establish or change the privileged mode password. |
| acme_R2(config)# *access-list 1 permit my.net.2.150* | permit telnet access |

| | |
|---|---|
| only from host my.net.2.150. | |
| acme_R2(config)# *line vty 0 4* | set the vty to apply the access-list to. |
| acme_R2(config)# *access-class 1 in* | apply access-list 1 inbound. |
| acme_R2(config)# *no ip http server* | disable http access. |

Unauthorised Access Banner.

It is recommend that a logon banner is enabled on the router to warn any unauthorised persons that they have connected to a proprietry device.
The banner should state that unauthorised access and configuration is not allowed and may be subject to prosecution. An example banner for ACME:

'WARNING - You have logged on to an ACME proprietry device. If you are not authorised to use this device, please log off immediately. Anyone found using this device for any unauthorised purpose may be subject to disciplinary action, and/or prosecution'

To enable the banner, use the following command:

| | |
|---|---|
| acme_R2(config)# *banner login ^Cbanner text^C* | banner to display at logon. |

Disable Unnecessary Services.

There are many services that are provided by the Cisco IOS that are not required or used in the ACME network scenario. The following services should be disabled to prevent the router from sending out information that may give a would be attacker clues as to the topology of the local network, or enable the router to be compromised. In addition, several known vulnerabilities exist which could be exploited by allowing access to these services/ports. Disabling unnecessary services will also prevent future as yet undiscovered vulnerabilities with these services being exploited.

| | |
|---|---|
| acme_R2(config)# *no service UDP-small-servers* | disable UDP ports echo, chargen, snmp etc |
| acme_R2(config)# *no service TCP-small-servers* | disable TCP ports echo, discard, chargen etc |
| acme_R2(config)# *no service finger* | disable finger service – could be used to provide router information to outside. |
| acme_R2(config)# *no cdp run* | disable Cisco Discovery Protocol – prevents router announcing information |

| | |
|---|---|
| | about itself. |
| acme_R2(config)# *no snmp-server* | disable SNMP |
| acme_R2(config)# *no ip bootp server* | disable bootp |
| acme_R2(config)# *no service dhcp* | disable dhcp |
| acme_R2(config)# *no service pad* | disable packet assembler/disassembler |
| acme_R2(config)# *no ip classless* | disable classless forwarding |
| acme_R2(config)# *no ip direct-broadcast* | disable direct broadcast possible DOS attack |
| acme_R2(config)# *no ip domain-lookup* | disable DNS queries |
| acme_R2(config)# *no ip source route* | disable source routing |
| acme_R2(config)# *no ip redirects* | disable ICMP redirects |
| acme_R2(config)# *no ip unreachables* | disable ICMP unreachables – prevents router from sending out network information. |

Access Control Lists.

One of the main security aspects that can be implemented on the router are Access Control Lists (referred to in the rest of this document as ACL).
ACLs are used to filter traffic in either direction on each router interface to which they are applied. There are 2 types of ACL, Standard and Extended. Standard ACLs are used to permit or deny traffic from a specific source address, whereas, Extended IP ACLs allow more flexibility as they can permit or deny traffic based on both source and destination address, port and protocol.
Each ACL is given a number, the number ranges are predefined according to the type of ACL and the protocol to which they apply. For example Standard IP ACLs number range is 1-99 and 1300 to 1999, and Extended IP ACLs range is 100 to 199 and 2000 to 2699.

Standard ACL Command Specification

**access-list** access-list-number **{permit | deny}** source source-wildcard

Extended ACL Command Specification

**access-list** access-list-number **{permit | deny}** protocol source source-wildcard destination destination-wildcard [**eq** [port]]

Rules that Apply to Access Control lists:

There are a few basic rules that apply to ACLs :

- ACLs are applied top down, therefore the most restrictive statements should be first.

- Only one ACL is allowed for each protocol, on each interface, in either direction to which it is applied.

- There is an implicit deny all at the end of each ACL, therefore, what is not explicitly allowed by the ACL is implicitly denied.

ACME Scenario

In our scenario for ACME we are going to apply 2 types of filters using ACLs. The first Ingress filter, will be applied inbound on the external or internet facing interface of the router. In the case of ACME this is the BRI0 interface. This filter will be used to block incoming traffic from any private, non-routable (RFC1918) address. It will also be used to block traffic destined for specific ports that are well known for malicious activity or vulnerable services.

The second, Egress filter will be applied inbound on the internal interface (E0) of the router. This will filter will be used to ensure that only ACMEs valid assigned address space passes out onto the internet. This prevents any malicious (DDOS) or unauthorised traffic from being generated on the internal network and sent out.

Both filters will use an extended IP Access Control List.

Ingress Filter

The Ingress filter that I will demonstrate is based on denying access to specific IP addresses and ports as opposed to only allowing access to specific ports and services.

To create the access list first connect and logon to the router:

| | |
|---|---|
| acme_R2> *enable* | Enter privileged mode (*en)*. |
| acme_R2> password : *password* | Supply the privileged mode password. |
| acme_R2# *configure terminal* | enter terminal configuration mode (*conf t)*. |

Once in terminal configuration mode, we can create our extended IP access list. As basis for the Ingress filter, I will use the SANS top ten Cisco ACL blocking recommendations plus additional blocking that I recommend for ACME. See Appendix A for the full list.

The first access list entry I will demonstrate will block access from any traffic originating from one of the private (RFC1918) addresses, in this case the reserved class A network range 10.0.0.0 – 10.255.255.255. These address ranges are reserved for use on internal

private networks, and therefore cannot come from outside of the ACME internal network.

acme_R2(config)# *access-list 102 deny ip 10.0.0.0 0.255.255.255 any*

The second access list entry I will demonstrate will block access to the telnet service,TCP and UDP port 23. Although useful, telnet poses a huge security threat as it allows remote command execution via a terminal window connected to the telnet server.

acme_R2(config)# *access-list 102 deny tcp 23*
acme_R2(config)# *access-list 102 deny udp 23*

The third access list entry will allow incoming mail traffic to the ACME mail relay only on port 25 (smtp) and incoming web traffic to the ACME web server only on port 80 (http).

acme_R2(config)# *access-list 102 permit tcp any my.dmz.1.2 0.0.0.0 eq 25*
acme_R2(config)# *access-list 102 permit tcp any my.dmz.1.3 0.0.0.0 eq 80*

Next we will apply the access-list inbound on the BRI0 interface:

| | |
|---|---|
| acme_R2(config)# *interface BRI0* | interface BRI0 (*int BRI0)*. |
| acme_R2(config-if)# *ip access-group 102 in* | apply the access list 102 inbound. |
| acme_R2(config-if)# *exit* | exit to previous configuration level or |
| acme_R2(config)# *^Z* | exit configuration mode completely <cntrl-z>. |

The filter is now applied to the running configuration and will come into effect immediately.

Egress Filter

The Egress filter is based on the valid IP address range and mask that are assigned to ACME. It is simple to set up and apply:

To create the access list first connect and logon to the router:

| | |
|---|---|
| acme_R2> *enable* | enter privileged mode (*en)*. |
| acme_R2> password : *password* | supply the privileged mode password. |
| acme_R2# *configure terminal* | enter terminal configuration mode (*conf t)*. |

acme_R2(config)# *access-list 101 permit ip my.ext.0.0 0.0.255.255 any*
acme_R2(config)# *access-list 101 deny ip any any*

| | |
|---|---|
| acme_R2(config)# *interface fastethernet 0* | interface fast ethernet 0 (*int fast 0)*. |
| acme_R2(config-if)# *ip access-group 101 in* inbound. | apply ACL 101 |
| acme_R2(config-if)# *exit* | exit to previous configuration level or |
| acme_R2(config)# ^*Z* | exit configuration mode completely <cntrl-z>. |

The filter is now applied to the running configuration and will come into effect immediately.

Testing the Configuration

Once applied, the configuration should be tested to ensure that it meets ACMEs security requirements:

To test the Ingress filter, a tool such as NMAP (http://www.insecure.org/nmap) should be used from outside of the network to run a port scan and check that only the required ports/services on the router are open/enabled.

To test the Egress filter, the logging option on the router should be enabled and a tool such as HPING2 (http://www.hping.org) can be used to craft invalid packets and try and send them out on to the internet.

To switch on logging:

| | |
|---|---|
| acme_R2(config)# *logging on* | |
| acme_R2(config)# *log my.net.2.101* | send logs to syslog server. |

If the tests prove to be satisfactory and achieve the required results, the running configuration should be saved for use as the startup configuration when the router is reloaded:

| | |
|---|---|
| acme_R2# *copy running startup* | copy running configuration to start up configuration (*copy run start*). |
| acme_R2# destination filename(startup-config) | specify the name of the filename for the startup configuration or default |

## Conclusion

Protecting your external router from unauthorised access and misconfiguration is a critical element in the defence of your network. If any unauthorised person should gain access to the router, they could reconfigure the system to remove any filtering in place and configure it for their own use.
Using ACLs as a first line of defence to filter inbound and outbound traffic in conjuntion with firewalls and intrusion detection systems will provide some of the multiple layers of defence and monitoring that are talked about in the SANS GSEC course. Performing regular scans on your network from an external source will enable you to check that only the ports/services that are required on the router are listening and available, thus minimising the risk of external attack/compromise.

## References


1. Configuring passwords and privileges on Cisco IOS.
   http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt5/scpass.htm
2. SANS Reading Room.
   http://rr.sans.org/index.php
3. Cole, Eric. "GSEC Course – SANS GIAC Certification Program", January 2002.
4. Graesser, Dana. "Cisco Router Hardening Step-by-Step", 25 July 2001
   http://rr.sans.org/firewall/router2.php
5. SANS Institute. "How to Eliminate The Ten Most Critical Internet Security Threats ver 1.33", June 2001.
   http://www.sans.org/topten.htm
6. Brett and Variable K, "Building Bastion Routers Using Cisco IOS" Phrack Magazine, Vol 9, Issue 9, September 1999.
   http://www.phrack.com/show.php?p=55&a=10
7. Middleton, James, "Hybrid Threats overtake DOS Attacks", April 2002.
   http://www.vnunet.com/News/1131294
8. NMAP.
   http://www.insecure.org/nmap
9. HPING2.
   http://www.hping.org


## Appendix A - Top ten block Cisco ACL blocking recommendations from SANS

Source: http://www.sans.org/topten.htm

1. Block "spoofed" addresses-- packets coming from outside your company sourced from internal addresses, private (RFC1918 and network 127) and IANA reserved addresses.

Also block source routed packets.
2. Login services-- telnet (23/TCP), SSH (22/TCP), FTP (21/TCP), NetBIOS (139/TCP), rlogin et al (512/TCP through 514/TCP)
3. RPC and NFS-- Portmap/rpcbind (111/TCP and 111/UDP), NFS (2049/TCP and 2049/UDP), lockd (4045/TCP and 4045/UDP)
4. NetBIOS in Windows NT -- 135 (TCP and UDP), 137 (UDP), 138 (UDP), 139 (TCP). Windows 2000 – earlier ports plus 445(TCP and UDP)
X Windows -- 6000/TCP through 6255/TCP
5. Naming services-- DNS (53/UDP) to all machines which are not DNS servers, DNS zone transfers (53/TCP) except from external secondaries, LDAP (389/TCP and 389/UDP)
6. Mail-- SMTP (25/TCP) to all machines, which are not external mail relays, POP (109/TCP and 110/TCP), IMAP (143/TCP)
7. Web-- HTTP (80/TCP) and SSL (443/TCP) except to external Web servers, may also want to block common high-order HTTP port choices (8000/TCP, 8080/TCP, 8888/TCP, etc.)
8. "Small Services"-- ports below 20/TCP and 20/UDP, time (37/TCP and 37/UDP)
9. Miscellaneous-- TFTP (69/UDP), finger (79/TCP), NNTP (119/TCP), NTP (123/TCP), LPD (515/TCP), syslog (514/UDP), SNMP (161/TCP and 161/UDP, 162/TCP and 162/UDP), BGP (179/TCP), SOCKS (1080/TCP)
10. ICMP-- block incoming echo request (ping and Windows traceroute), block outgoing echo replies, time exceeded, and destination unreachable messages except "packet too big" messages (type 3, code 4). (This item assumes that you are willing to forego the legitimate uses of ICMP echo request in order to block some known malicious uses)

Additional Blocking Recommendations:

| Port(s) | Protocol | Description |
|---|---|---|
| 2222, 6669, 7000 | TCP | Serbian badman/backdoor.subseven |
| 16959, 27274, 6711, 6712, 6776 | TCP | Subseven |
| 16660, 65000 | TCP | Stacheldrant |
| 27665 | TCP | Trinoo |
| 27444, 31335 | UDP | Trinoo |
| 33270, 39168 | TCP | Trinity V3 |
| 1993 | UDP | Cisco SNMP |
| 6660 - 6669 | TCP | IRC |
| 5190 | TCP | AIM |
| 1027, 1029, 1032 | TCP | ICQ |

Source: Original by Author.