Global Information Assurance Certification Paper

Securing Cisco Routers

Nicholas Vigil
CCNP, MCSE, A+
July 29, 2003
Version 1.4b

Abstract

A local area network (LAN) is a group of computers sharing a common communication media that spans a small geographical area. In local area networks it is fairly simple for computers to communicate with one another using rules for communication called protocols. For example, in an ethernet LAN computers using the TCP/IP protocol stack can share information by broadcasting it out onto the media. However, on large networks a simple broadcast will not guarantee the successful delivery of information. On larger networks comprised of many LANs routers are responsible for directing information between devices on different networks. On these wide area networks (WAN) routers assume the responsibility of routing traffic between networks. Routers can be thought of as gateways. They provide computers on LANs with a doorway out of the LAN onto a much bigger WAN such as the Internet. Routers run routing protocols that enable them to learn about other networks so that they can direct traffic to any given destination network. Using these routing protocols routers maintain routing tables that enable them to determine the best path a packet should take in order to get to its destination network. Large networks live off these routing tables in order to route information between networks. “Without robust routing, most modern networks cannot function. Therefore, the security of routers and their configuration settings is vital to network operation” (Antoine 7). The security of the router in a network is critical. Routers are often placed on the borders of networks connecting our internal networks to the outside world. Being on the perimeter means that the router is the first device to be seen by intruders that would try to penetrate our networks. Since the router is the first device an intruder would encounter the router also acts as our first line of defense. The purpose of this paper is to familiarize the novice administrator on what steps they can take to secure their Cisco router from ever being compromised by intruders and to protect their internal networks. This paper is not intended to be a complete reference on securing routers but to be more of a beginner’s guide, as it will address only some of the more common yet critical security configurations.

Background

Cisco Systems has become know world wide as one of the leading manufactures of routers. Cisco routers are Internetwork devices, which allow separate networks to connect together and communicate. Much of the Internet today is run through Cisco routers. Routers operate on the network layer of the OSI model. Since routers run at layer three of the OSI model they are mainly concerned with network addressing and delivering traffic between networks.

Routers like computers are run by an operating system. Cisco routers are run by Cisco’s Internetwork Operating System (IOS). The IOS comes in many

versions and depending on the needs of your network you should select carefully what version of IOS you have running on your router. The IOS comes in three main classifications. The three main classifications are general deployment, early deployment, and maintenance release.

The general deployment IOS are intended for most customers and are good operating systems. This class of IOS is generally very stable and free of any major bugs.

The early deployment IOS class contains newer operating systems. These IOS versions often contain new features supported by the IOS or new hardware support. Because these operating systems have not been in use very long it cannot be said for sure that all the major bugs have been worked out. I recommend that you should only use these IOS if they contain some of the new features you need for your network. Otherwise, if it is not critical wait for the general deployment.

Maintenance releases are intended to replace general deployment releases. These IOS versions have many of the fixes to bugs that have been discovered in the general deployments.

Before deploying any IOS I always recommend reading over the IOS documentation. If you need detailed information on a particular version of IOS or just want to read up more on them you can find information on Cisco's web site at http://www.cisco.com/univercd/cc/td/doc/product/software/index.htm.

It is important to remember that the IOS is an operating system just like Windows or Linux. Since operating systems are never perfect they are always subject to exploits and vulnerabilities. Your networks gateway router is not exactly the one device you would want an intruder to compromise. If an intruder was able to gain control of your router they could easily alter the path of traffic flow, capture data flowing through the router, or disable the router resulting in a denial of service on your network. Providing router security is as much a concern as configuring the router to provide routing services. Luckily, Cisco knows the importance of network security and has built some tools into the routers IOS that will enable you to properly secure your router and protect your network. However, using all the built in security features available in the IOS will not protect the router if an intruder is able to gain physical access to the router itself.

Physical Security

Providing physical security for a router is a very important step in hardening a routers defense against intruders. A good physical security plan will provide for the routers safety against both people and environmental hazards. Environmental hazards that need to be addressed include power surges, extreme temperatures, humidity, and electrostatic discharge. In order to protect a router from these hazards you should place the router in an area that is free from electrostatic discharge and humidity, temperature controlled, and plug the router into an uninterruptible power supply (UPS). The area that the router resides should provide for a very secure controlled location. Access to this area should be limited to only personnel who administer the routers. Some type of authentication system can be set up to ensure that only authorized personnel can

gain access to this protected room. For example, smartcards with passcodes can be a good authentication mechanism to ensure someone is whom they say they are to allow them to enter the controlled area. If the router administrators tend to connect to the router remotely for administration purposes then security should be put in place to protect the workstations that the administrators use to connect to the router.

Evaluating Current Router Security

One of the first steps you should take in securing a router is to test the routers current security posture. What you need to be looking for during this security screening is what services are running and what exploits and vulnerabilities have been identified with the routers current Internetwork Operating System. In order to discover any known vulnerabilities with the routers IOS you can refer to the Cisco web site Cisco Product Security Advisories and Notices page at http://www.cisco.com/warp/public/707/advisory.html.

Next, you should find out what ports are open on the router that an intruder could see from the outside and possibly exploit. The best way to determine what ports are open is to perform a port scan on the router. Nmap is a great port scanning utility that you can use to perform this port scan and can be downloaded for free at http://www.insecure.org/nmap/. Once you perform the port scan you should review the results to see what ports are open and determine what ports you need open so that you can close all unnecessary ports. If you cannot get a hold of a port scanner you can always use the routers IOS to discover running services by issuing the IOS command *show processes.* This command will display all the current processes being processed by the router CPU.

Other options that I use and find very handy are Cisco's bug toolkit and output interpreter. The bug toolkit allows you to search for software bugs in your routers IOS. The output interpreter will give you recommendations, warnings, and fixes to configuration and security settings on your router based on certain show commands that you copy from the router into the interpreter.

Disabling Unneeded Services and Security Risk

Cisco routers by default have many types of services, protocols, and processes running. Once you have evaluated your current router security and know what is running on the router, you should start turning off all unnecessary settings. We will now take a look at some of the more common services, protocols, and processes that are running and walk through how to shut them off.

Cisco Discovery Protocol is a layer two protocol that is enabled on all Cisco routers by default. In most cases CDP is not necessary and can be disabled without any problems. CDP poses a security threat because it shares your routers information with neighboring devices. By default, CDP will send broadcast information about your router out each interface every 60 seconds. This information includes router addresses, protocols running, IOS version, platform, capabilities, and port ID. Any intruder could easily take this information and use it to exploit your router. In order to disable CDP on the router go to

global configuration mode and enter the command *no cdp run.* If you wish to leave CDP enabled but disable it from only select interfaces then enter the correct interface mode and enter the command *no cdp enable* to turn CDP off for that particular interface.

Finger is another service enabled by default that an intruder could use to gather useful information about the router. Using finger an intruder could find information about what lines are currently open to the router and where they are coming from. For example, if someone had established a telnet session to the router from a remote location an intruder using finger could determine what vty line was in use, what IP address the remote connection is coming from, and if the session was idle or not. Using such information an intruder could try and spoof the source IP address that the session was established from to try and gain access to the router. To avoid an intruder from using finger to gather information about who is logged in to the router it should be either blocked using an access list or just disabled. To disable finger go to global configuration mode and enter the commands *no ip finger* and *no service finger.* If you would rather block finger using an access list be sure to use an extended access list blocking tcp port 79.

By default Cisco routers run udp and tcp diagnostic services. Such services are usually not necessary on a router and need to be disabled. These services include echo (port7), discard (port9), and chargen (port19). By disabling these services you will help to prevent denial of service attacks on your router that are commonly launched using both echo and chargen ports. To disable these services on the router go to global configuration mode and enter the commands *no service tcp-small-servers* and *no service udp-small-servers*. According to Cisco's web site these commands became the default settings beginning with Cisco IOS release 12.0 and later (Improving Security on Cisco Routers).

The Simple Network Management Protocol (SNMP) is another service that can pose a big security threat to a router. This protocol is primarily used for gathering statistics and making configuration changes. However, SNMP can be used for malicious purposes. An intruder can create malformed SNMP messages and send them to your router causing various processes to fail, resulting in the router crashing or rebooting. If SNMP is not be utilized it is best to completely disable this protocol. However, Chris Benton, author of Mastering Cisco Routers, recommends that if you do have a need to use SNMP you should try to use SNMPv2 as this version has the capability to utilize MD5 authentication (358). SNMPv2 became available in Cisco router IOS version 10.3 and up. In order to disable SNMP you should delete all community strings, disable SNMP system shutdown and trap features, and disable the SNMP process. In order to accomplish these steps enter the following commands from global configuration mode:

```
Router(config)#no snmp-server community public RO
Router(config)#no snmp-server community admin RW
Router(config)#no snmp-server enable traps
Router(config)#no snmp-server system-shutdown
```

```
Router(config)#no snmp-server trap-auth
Router(config)#no snmp-server
```

Cisco routers provide administrators the ability to configure the router through a web-based client using HTTP. This service should be avoided if possible because it has security concerns as well. For example, like telnet all traffic sent over the HTTP connection is sent in clear text including passwords. If this service is not needed you should ensure it is turned off on the router. In order to disable this service you need to enter the commands *no ip http server* from the global configuration mode.

The bootp protocol allows other network devices to download a copy of an IOS image from a Cisco router. The risk here being that an intruder might be able to download a copy of the IOS that your network devices are using. If not being utilized this service should be disabled. This is done from global configuration mode by entering the command *no ip bootp server*.

Source routing allows packets to specify their own routes by including route information in the header. When a router receives a source-routed packet it will forward the packet according to the information in the header of the packet. Source routed packets can be dangerous and used by intruders to possibly bypass security points in your network. Unless source routing is needed you should turn off the routers ability to forward source-routed packets. To disable this feature enter the command *no ip source-route* from global configuration mode.

IP directed broadcast could be used in denial of service attacks. Earlier Cisco IOS support the forwarding of directed broadcast by default. This feature was later turned off on later versions. However, you should still ensure that this feature is turned off if not absolutely needed on your network. To disable this service go to interface configuration mode and enter the command *no ip directed-broadcast.*

Finally, the last service I am going to mention is the network time protocol (NTP). This service allows routers to stay in synch with other devices clocks to include date and time. If you do not run NTP on your network or this router does not participate in NTP it should be disabled. This is done from interface configuration mode by entering the command *ntp disable*.

Setting Passwords

Hardening your routers defense against intruders includes establishing good strong passwords. Cisco routers allow you to create several passwords to help maintain security on the router. These passwords include the enable secret password, console port password, auxiliary port password, and vty passwords. Cisco routers also support an enable password that uses a Cisco created algorithm, however research has shown that this has proven to be a weak algorithm (McClure Scambray Kurtz 460). It is better to use the enable secret password instead as this supports the MD5 hash, which is a lot stronger. The enable secret password allows a user to access privilege exec mode on the router. The enable secret password should always be set to protect access to the

privilege exec mode. In order to set the enable secret password and unset any enable password that may be in place perform the following steps:

Router#Configure terminal
Router(config)#enable secret *password*
Router(config)#no enable password

The console and auxiliary port passwords help to protect unauthorized users from connecting to the router through the console and auxiliary ports. The console port is used to directly connect to the router for administration and the auxiliary port is used to support dial-in capabilities for administration. However, if the auxiliary port is not being utilized it should be shut down to prevent unauthorized access. Another difference in these two ports is the ability to perform password recovery. If an administrator forgets the enable secret password on the router and as a last resort must perform the password recovery procedure it can only be done from the console port. To set the console or auxiliary port password perform the following steps for the correct port:

Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password *password*

If you have no need for the auxiliary port then here are the steps to disable the auxiliary port:

Router(config)#line aux 0
Router(config-line)#transport input none
Router(config-line)#exec-timeout 0 1
Router(config-line)#no exec
Router(config-line)#login local

Routers also support numerous vty lines for telnet sessions. The number of vty lines varies depending on your version of IOS. To see how many vty lines your router has enter the command *show lines.* If you wish to connect to the router through telnet you should set vty line passwords. The example below sets the vty passwords for five vty lines:

Router(config)#line vty 0 4
Router(config-line)#password *password*

Once you have set all the above passwords you will notice that upon entering the command *show running-config* on the router that all the passwords besides the enable secret password are displayed in clear text in the configuration file. In order to encrypt all system passwords so that none of them will show in clear text enter the *service password-encryption* command from the global configuration mode.

When setting all the above passwords be sure to choose good strong passwords. The best passwords follow the four criteria for strong password complexity and are a good size in length. It is recommended that when creating passwords use both lowercase and uppercase letters, numbers, and special characters (Cole et al 415). An example of using all the four mentioned criteria might be something like Pa$%w0rD.

Access List

Cisco routers have the ability to perform packet filtering using access control list. These access lists allow us to use the router as not just a device to route traffic, but also as a means of keeping unwanted traffic out of our network and preventing internal traffic from leaking out. Cisco routers support two main types of access list, which you can be bound to either incoming or outgoing traffic of a particular interface.

The first type of access control list is the standard access list. A standard access list uses the source IP address in a packet header to filter traffic.

The second type of access control list is the extended access list. Extended access list have the ability to filter traffic using source and destination IP address, port number, protocol field in the layer 3 header, and socket numbers in the layer 4 header.

This paper assumes that the reader already has an understanding of how access list work and how to configure them. If you are new to access list or just want a refresher you can view detailed information at Cisco's web site at http://www.cisco.com/warp/public/105/acl_wp.html. Now, lets look at some recommended access list that administrators should implement to protect their network. The recommendations listed in the following paragraphs are recommendations from the SANS Institute's SANS Security Essentials with CISSP CBK Volume 1 training manual.

First, we will look at some recommended access list that might be configured on an interface to restrict inbound traffic coming from the Internet. It is recommended that on your Internet interface that inbound access list should be created that block traffic whose source addresses belong to any of the private address ranges defined in RFC 1918 (Cole et al 246). Any packet coming from the Internet should have a valid source IP address and not a reserved address. Loopback addresses should be blocked as well. Another recommendation is to block all multicast traffic from the Internet from entering your network unless you have a specific need for multicast traffic (Cole et al 415). Also, blocking packets with a source IP address of all zeros is another good filter to apply to inbound traffic access list. Examples of all access list mentioned above are provided below:

```
access-list 7 deny ip 10.0.0.0 0.255.255.255
access-list 7 deny ip 172.16.0.0 0.15.255.255
access-list 7 deny ip 192.168.0.0 0.0.255.255
access-list 7 deny ip 224.0.0.0 0.255.255.255
access-list 7 deny ip host 0.0.0.0
```

Second, we will examine recommended access list for permitting inbound traffic from the Internet. Some of the most common types of access list to be applied for permitting inbound traffic are list permitting web traffic, mail traffic, and DNS traffic. In order to allow these packets through the router and only these types of packets you need to set up extended access list. Below are examples of extended access list that allow web, mail, and DNS packets through the router and to their perspective servers.

```
access-list 101 permit tcp any host  192.168.100.2 eq 80
access-list 101 permit tcp any host  192.168.100.3 eq 25
access-list 101 permit tcp host 4.1.2.2 host 192.168.100.4 eq 53
access-list 101 permit udp any host 192.168.100.4 eq 53
```

Remember when setting up access list on the router that their purpose is to filter what type of traffic is allowed in and out of your network. Also, at the end of every access list is an explicit deny all statement.

We looked at some very common recommended access list for filtering traffic. However, what is allowed in and out is ultimately the responsibility of the administrator. It is better to be to restrictive than to be vulnerable to attack. Allow only necessary traffic to pass through the router that is essential for your network. If the traffic is not necessary block it.

Logging

Another important aspect of router security is maintaining logs. Log files enable us to keep track of what is going on with the router and can often give us valuable information about what is going on in our network. Cisco routers support different types of logs. These logs are Authentication Authorization Accounting logging, SNMP trap logging, and system logging. AAA logging is used to record information such as user dial-in connections, logins, logouts, privilege level changes, and HTTP access. SNMP trap logging will send information about major changes in the routers status to SNMP management stations. System logging records a variety of events such as router configuration changes, router reboots, access list violations, interface changes, and many other items as well. These system logs can be viewed by directing the message to various locations. System log messages can be sent directly to the console port, over terminal lines, to local buffers, or to a syslog server. When you enable logging and these messages are created the messages are grouped into various categories of severity. The table below shows the different logging levels and what type of information each displays.

Log Level	Name	Description
0	Emergencies	System is unusable
1	Alerts	Immediate action needed
2	Critical	Critical condition
3	Errors	Error condition

4	Warnings	Warning condition
5	Notifications	Normal but significant event
6	Informational	Informational message
7	Debugging	Debugging messages

You can have the router send the various log messages to any number of locations mentioned above and can log various types of events corresponding to each log level.

Now that we have become familiar with the different types of logs and logging levels available on a Cisco router lets look at how to enable logging to the various locations. In order to send logs to the console port you would enter the *logging console* command with the associated parameter of the name of the level of logging you wanted to log. Example below:

```
Router (Config)# logging console errors
Router (Config)# logging on
```

In order to turn on buffer logging you would enter the command *logging buffered* followed by the parameters to set the buffer size and the name of the log level you wanted to log. Example below:

```
Router (Config)# logging buffered 16000 errors
```

Terminal line logging is needed if you are connected to the router over a virtual terminal line and want to see the log messages. In order to enable terminal line logging you need to declare what level of logs you want to be displayed and enable the logging messages to be shown during that vty sessions. You do this by entering the commands *logging monitor* and *terminal monitor*. Example below:

```
Router (Config)# logging monitor errors
Router (Config)# exit
Router# terminal  monitor
```

Cisco routers are able to send their log files to other devices on the network for the purpose of maintaining a central location for storing log files. This central device is a syslog server. A syslog server is a host on the network that has the ability to receive log files from remote host. Having the router send its logs to a syslog server is beneficial because it provides a safe place for permanently storing the log files and is another device that has the logs in case an intruder manages to erase the logs on the router or the router becomes unusable. Syslog is installed by default on most Unix and Linux operating systems. If you only have windows operating systems there are third party applications that you can purchase and run on your windows box to act as a syslog server. This paper will not discuss how to setup or configure a syslog

server. Instead we will concentrate on the router side. In order to configure a Cisco router to send log messages to a syslog server you have to configure four items. These four items consist of defining the destination host, log level, syslog facility, and source interface.

The first step to configure the router to use a syslog server is to define the syslog destination host. In order to do this you enter the *logging* command with the IP addrees or host name of the target host.

Second, you need to declare what levels of log messages you want sent to the syslog server. This is accomplished using the *logging trap* command followed by the level name of logging.

The third step is to set the syslog facility in order to set up storage for your messages on the syslog server. Router facilities are usually local0 through local7. To configure the facility enter the command *logging facility* with the additional local parameter.

Finally, the last item to configure is the interface of which the log messages will be sent out. The router needs to be told which interface to send the logs out. You should ensure you define the interface that resides on the same network as the syslog server or that is the fewest amount of hops from it. Below is an example of how to set up logging to a syslog server from a Cisco router.

```
Router (Config)# logging 192.168.1.2
Router (Config)# logging trap errors
Router (Config)# logging facility local6
Router (Config)# logging source-interface ethernet 0/1
```

Securing Remote Administration

It is very common for router administrators to configure the router remotely over the network rather than through the console port. It is because of this remote administration that we must also look at securing the communications pathway that the data between the router and the administrator's host machine travels. Typically, an administrator can connect to the router for remote administration using the telnet protocol. Telnet does allow us to perform the configurations necessary on the router. However, telnet is an insecure protocol that sends all data over the network, including passwords, in clear text. Because data is sent in clear text any intruder running a packet sniffer could capture the data between the host machine and router thus possible compromising router passwords and configuration settings. Cisco's solution to this insecurity is the use of the Secure Shell (SSH) protocol. Cisco began implementing SSH server software in its IOS images starting with IOS 12.0.5.S and introduced SSH client software in IOS 12.1.3.T. SSH terminal-line access support in Cisco routers began with IOS 12.2.2.T. Currently there are two versions of SSH. Cisco routers only support SSHv1 with no future plans of implementing SSHv2 according to Cisco's web site at http://www.cisco.com/warp/public/707/ssh.shtml. SSH enables us to perform remote administration on the router in a secure manner. SSH uses RSA public Key cryptography to setup a secure connection between

hosts. This SSH connection is encrypted preventing sensitive information from being exposed while traversing the network.

Now that we know about SSH and its advantages over telnet lets look at how to configure the router to use SSH. Before we can configure SSH on the router we must ensure all the prerequisites are meet.

First, we need to ensure a hostname is configured on the router. If no hostname is configured on the router you can configure one with the *hostname* command while in global configuration mode.

Second, the DNS domain name must be set on the router. This can be set using the *ip domain-name* command in global configuration mode.

Next, a username must be configured to authenticate the connection. You can setup a local database of usernames on the router using the *username [name] password [password]* command. If the local database on the router is how you want to authenticate remote connection ensure you enter the *login local* command from specific configuration mode for all the vty lines.

Now, to configure the router for SSH you first have the router generate a key pair. To generate a key you enter the command *crypto key generate rsa*. Once you enter this command and the key has been created the SSH service is enabled and running on the router. However, the router will not accept SSH connections until the following three additional parameters are set. The *ip ssh timeout [number in minutes]* command sets the timeout value for SSH connections. The *ip ssh authentication-retries [number]* command sets the amount of failed logins attempts that will be accepted. Finally, you must enable the ssh protocol on the vty lines. This is done using the transport input ssh command on all vty lines. Below is an example of all the above commands mentioned for configuring SSH.

```
Router (Config)# hostname SanDiegoRouter
Router (Config)# ip domain-name abc.mycompany.com
Router (Config)# username Joe password  cisco
Router (Config)# line vty 0 4
Router (Config-line)# login local
Router (Config-line)#exit
Router (Config)# crypto key generate rsa
Router (Config)# ip ssh timeout 60
Router (Config)# ip ssh authentication-retries 3
Router (Config)# line vty 0 4
Router (Config-line)# transport input ssh
```

After adding the SSH configuration, you should be able to test accessing the router from your host machine. You can also verify ssh is enabled by using the command *show ip ssh* from privilege exec mode. Of course, to be able to use the ssh capabilities you have just configured on the router your workstation must have SSH client software loaded. If you do not currently have SSH software you can obtain SSH client software from various places. Two SSH clients that are

freely available for download are OpenSSH for Unix and Linux host and PuTTY for Windows host.

Conclusion

Cisco routers provide a vital service to networks. Routers are the backbone to any network and can often be the first device an intruder would try to compromise in order to gain control of a network or to bring the network down. In this paper I have mentioned many topics that need to be addressed in establishing a good router security policy. A good security policy can do wonders in preventing unauthorized users from accessing your router. Perhaps the most important points I would like to stress in this paper are the disabling of unnecessary services, protocols, and processes running on the router as well as the importance of keeping logs. Every item mentioned in this paper is a crucial step in implementing router security. However, failure to keep logs will not enable you to see why something happened our how it happened and failure to disable unnecessary items places your network at greater risk for no reason. When you have a properly secured router you have a better more secured network.

References

Antoine, Vanessa, et al. Router Security Configuration Guide. Version 1.1. United States: National Security Agency, Sept. 27, 2002. < http://nsa2.www.conxion.com/cisco/guides/cis-2.pdf>

Benton, Chris. Mastering Cisco Routers. California: Sybex, 2000.

Cole, Eric, et al. SANS Security Essentials with CISSP CBK. Vol 1. United States: SANS Institute, 2003.

McClure, Stuart, Joel Scambray, and George Kurtz. Hacking Exposed. 3rd Edition. United States: Osborne/McGraw-Hill, 2001.

"Configuring Secure Shell on Routers and Switches Running Cisco IOS." Tech Notes. April 11, 2003. Cisco Systems. July 8, 2003. < http://www.cisco.com/warp/public/707/ssh.shtml>

"Improving Security on Cisco Routers." Tech Notes. June 25, 2003. Cisco Systems. June 25, 2003. < http://www.cisco.com/warp/public/707/21.html>

"Cisco Product Security Advisories and Notices." Security Advisories. July 23, 2003. Cisco Systems. June 20, 2003. <http://www.cisco.com/warp/public/707/advisory.html>

"The 60 Minute Network Security Guide." Version 1.0. United States: National Security Agency. October 16, 2001. July 21, 2003. <http://downloads.securityfocus.com/library/sd-7.pdf>