

CERT-In Security Guideline CISG-2003-08

CERT-In

Indian Computer Emergency Response Team
Handling Computer Security Incidents

Cisco Router Security Guidelines

**Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India**

Issue Date: October 21, 2003

TABLE OF CONTENTS

1. Introduction.....	3
2. Principles and Aim of router security.....	3
2.1. Router fortification.....	3
2.1.1. Physical security:	3
2.1.2. Appropriate operating system:	4
2.1.3. Proper hardening of configuration:.....	4
2.2 Network protection with Router.....	4
2.2.1 Roles in networks and its security	4
2.2.2 TCP/IP Packet filtering.....	5
2.3 Managing the router.....	7
2.3.1 Managing access for router.....	7
2.3.2 Router updates	7
2.3.3 Logging	8
3. Implementing Routers security.....	8
3.1. Router Configuration and Commands (IOS)	8
3.2. Secure Interface configuration.....	9
3.3. Secure Global Services Configurations	10
3.3.1 Privileges.....	11
3.4. Password security.....	11
3.5. Access Control Lists for security and filtering	12
3.5.1. General Recommendations.....	13
3.5.2. Filtering the traffic through Router.....	13
3.5.3. IP Address Spoofing Protection	14
3.5.4. Protection from different attacks	15
3.6. Remote Access security	18
3.7 Securing IP Routing	19
3.7.1. Authenticating Routing Protocol Updates.....	19
3.8. Audit and Management.....	22
3.8.1. Concepts and Mechanisms	22
3.8.2. Logging	23
4. Testing and security validation.....	25
4.1. Guidelines for Router Security Testing.....	25
4.2 Tools for testing	25
5. References.....	27
5.1 Books.....	27
5.2 Web Sites.....	27

1. INTRODUCTION

In most of the networks, routers are the first line of defense and play a very important role in the network. We all understand that routers are used at the edge of the perimeter of network as well as inside the network for routing the packets. Securing the routers within the network is very critical for the security of that network. Compromise of a router can lead to various security problems on the network served by that router, or even other networks with which that router is communicating.

Compromise of routing tables in a router may lead to reduced performance, Denial of network communication services, and exposure of sensitive data. Compromise of a router's access control can result in exposure of details of network configuration or exposure to denial of service, and can facilitate attacks against other network components. A poor router filtering configuration can reduce the overall security of an entire network. On the other hand, proper use of router and its security features can help in protecting the sensitive data, ensure data integrity, and facilitate secure cooperation between autonomous networks.

The main focus of this document is to provide guidelines for the security of Cisco routers both at the perimeter and in the internal network. The security recommendations and considerations in this paper are specific to IPv4. Although many of the issues and recommendations are quite similar for IPv6, they are not explicitly discussed here.

2. PRINCIPLES AND AIM OF ROUTER SECURITY

Routers can play an important role in security of network. This section describes principle of securing the router and accessing router securely. It also describes how to secure the network with router.

2.1. Router fortification

2.1.1. Physical security.

The first and foremost aspect of the security for any device is the physical security. Once an individual has physical access to a piece of networking equipment there is no way to stop him from modifying the system. There are various ways for the physical security of router. The placement of router should be isolated from electrostatic and magnetic interference. It should have online UPS and must also have on hand spare components, which should be tested online at regular intervals. Router should have redundant power supply (SMPS). It must have controls for humidity and temperature. Router should be configured with maximum amount of memory to safeguard against denial of service attacks. If possible, this area should only be accessible by personnel with administrative responsibilities for the router. This area should be under some sort of supervision 24 hours a day and 7 days a week. This can be accomplished through the use of guards, system personnel, or electronic monitoring. It should be locked in a cabinet/rack

2.1.2. Appropriate operating system

The Internetwork Operating System (IOS) is extremely important component for a router. Cisco issues new IOS versions and upgrades fairly frequently; making it a significant administrative burden to keep all the routers on a large network up to date. Newer versions of IOS fix bugs and vulnerabilities that existed in the older versions, and add new security features. Decide the features and needs of the network and use the feature list to select the version of IOS. However the very latest version of operating system is not considered to be the most reliable because of its limited exposure to the wide range of network environments. Latest stable operating system should be used, which supports all the required security features.

2.1.3. Proper hardening of configuration:

A router is also a computer which has a specific defined function that has many services enabled by default. Many of the services are unnecessary and may be used by an attacker for information gathering and exploitation. All the services which are not required should be disabled in router configuration. Apart from this router should also be patched with latest patches and proper ACL's.

2.2 Network protection with Router

2.2.1 Roles in networks and its security

In modern networks router play various roles. Three major roles of the router, which are common in most of the networks, are explained below.

Interior Routers. An interior router is used for forwarding the traffic between different networks or different subnet of the same organization. The networks/subnets which are connected by interior routers share the same common security policy and usually have the high level of trust. The routers within an organization have static routes or Interior Gateway Protocol for routing.

Backbone Routers. A backbone router is one which forwards traffic between different enterprises or between different Autonomous System. The level of trust between the networks connected by backbone router is negligible. Typically backbone routers are configured to forward the traffic with imposing any kind of restriction. The primary security goals for a backbone router is to ensure that the management and operation of the router are conducted only by authorized parties, and to protect the integrity of the routing information it uses to forward traffic. Backbone routers use Exterior Gateway Protocol (EGP) to manage the routes.

Border Routers. The Border router is used to forward the traffic between internal network and exterior network (i.e. Internet). It forms a boundary between internal network and the Internet. It can help to secure the perimeter of an enterprise network by enforcing restrictions on the traffic that it controls. The border router can use both routing protocol and static route according to the requirements.

2.2.2 TCP/IP Packet filtering.

A TCP/IP packet filtering service provides control on the data transfer between different networks or subnet based on the addresses and protocols. Router can apply filters on the traffic passing through it in different ways. Routers can apply restriction both on inbound and outbound traffic and it can apply restriction in one direction depending on router capabilities. Most routers can filter one or more of the following: source IP address, source port, destination IP address, destination port, and protocol type.

Packet filters are especially important for routers that act as the border router or the gateway between trusted and non trusted networks. In that role, the router can enforce security policy, Rejecting protocols and restricting ports according to the policies of the trusted network.

Length and ordering are the two characteristics of TCP/IP packet filtering. A filter consists of one or multiple rules for either accepting or denying a certain set of packets. Generally, as the length grows the filter becomes more complex and more difficult to troubleshoot. The order of the rules in a packet filter is critical. When the router analyzes a packet against a filter the packet is compared to each filter rule in a sequential order. If a match is found then the packet is either permitted or denied and the rest of the filter is ignored. If no match is found then the packet is denied due to the implicit deny rule at the end of the filter. You must carefully create filter rules in the proper order so that all packets are treated according to the intended security policy. One method of ordering involves placing those rules that will handle the bulk of the traffic as close to the beginning of the filter as possible. Consequently, the length and ordering of a packet filter rule set can affect the router's performance.

Consider carefully what network services (inbound and outbound) are allowed through the router. The following guidelines are recommended for creating filters: those services that are not explicitly permitted are prohibited. This guideline is especially important for border routers and can also be implemented at interior routers. A list should be made for the services and protocol that pass through the router, and the services that are required by the router itself. Create a set of filtering rules that permit the traffic identified on the list, and prohibits all other traffic. In cases where only certain hosts or networks need access to particular services, add a filtering rule that permits that service but only for the specific host addresses or address ranges.

In case it's not possible to follow the security guidelines given above, restrict the services that are not required and can be exploited for compromise. The following table 2-2 lists the services that need to be restricted. Unless there is a specific operational need to support the service, the protocol listed in table 2-2 should not be allowed across the router in either direction.

Table 2-2 List of Services to be blocked at Router for both incoming and outgoing.

Services	Port Type	Port Number
tcpmux	TCP & UDP	1
echo	TCP & UDP	7
discard	TCP & UDP	9
systat	TCP	11
daytime	TCP & UDP	13

netstat	TCP	15
chargen	TCP & UDP	19
time	TCP & UDP	37
whois	TCP	43
bootp	UDP	67
tftp	UDP	69
supdup	TCP	93
sunrpc	TCP & UDP	111
loc-srv	TCP & UDP	135
netbios-ns	TCP & UDP	137
netbios-dgm	TCP & UDP	138
netbios-ssn	TCP & UDP	139
xdmcp	UDP	177
netbios (ds)	TCP	445
rexec	TCP	512
lpr	TCP	515
talk	UDP	517
ntalk	UDP	518
uucp	TCP	540
Microsoft upnp sssdp	TCP & UDP	1900, 5000
nfs	UDP	2049
X window system	TCP	6000 – 6063
irc	TCP	6667
netbus	TCP	12345
netbus	TCP	12346
back orifice	TCP & UDP	31337

Table 2-3 List of services to be blocked at Router for incoming traffic

Service s	Port Type	Port Number
finger	TCP	79
snmp	TCP & UDP	161
snmp trap	TCP & UDP	162
rlogin	TCP	513
who	UDP	513
rsh, rcp, rdist, rdump	TCP	514
syslog	UDP	514
new who	TCP & UDP	550

Standard Ports and Protocols approach and Address filtering. Many organizations maintain a list of standard ports and protocols which should be allowed in the network. Various organizations in the US like DOD maintain such lists. For networks that are subject to such lists, it is best to take the first approach, allowing only those ports and protocols which are mandatory in the standard list, and rejecting all others.

Router filters should also be used to protect against IP address spoofing, especially on border routers. In most cases filtering rules should apply both ingress and egress filtering, including blocking reserved addresses. The principles to apply on the routers are given below:

- The inbound packets on the internal interface having a source address of the internal network or 127.0.0.x or reserved address spaces are dropped and logged.
- The outbound packets on the internal interface have a source address of only the internal network or 127.0.0.x or a reserved address are dropped and logged.

2.3 Managing the router

2.3.1 Managing access for router

Controlling administrative access to router is an important issue. Router can be accessed locally or remotely. Local access means accessing the router using console port by connecting computer to it. Remote access typically involves allowing telnet or SNMP connections to the router from some computer on the same subnet or a different subnet. It is recommended to only allow local access because during remote access all telnet passwords or SNMP community strings are sent in the clear text to the router. However, there are some options if remote access is required.

- Establish a dedicated management network. The management network should include only identified administration hosts.
- Another method is to encrypt all traffic between the administrator's computer and the router.
- Packet filters should be configured to permit only the identified administration hosts for the management of routers.

In addition to how administrators access the router, it is also advisable to have more than one level of administrator, or more than one administrative role. Capability of each level or role should be clearly defined in the router security policy.

2.3.2 Router updates

Router should be updated periodically for both the operating system and the configuration file. The reasons for updates are fixing for known security vulnerability, to improve the performance, and support new features. Before updating, the administrator should complete the following checks. Determine the memory required for the update, and if necessary install additional memory. Set up and test file transfer capability between the administrator's host and the router. Schedule the proper down times as appropriate. Before applying any update or patch, back up the current operating system and the current configuration file. Perform tests to confirm

that the update works properly. If the tests are successful then restore or reconnect the interfaces on the router. If the tests are not successful then back out the update.

2.3.3 Logging

Logging must be enabled on the routers as it has many benefits. Using the information in a log, the administrator can tell if the router is working properly or if it has been compromised. It can also show what types of probes or attacks are being attempted against the router or the protected network. Send the router logs to a designated log host, which is a separate computer whose only job is to accept and store logs. Harden the log host by removing all unnecessary services and accounts. The most important thing is to monitor the log regularly. By checking over the logs periodically, you can gain a feeling for the normal behavior of your network. A sound understanding of normal operation and its reflection in the logs will help you to identify abnormal or attack conditions.

Accurate time's stamps are also very important to logging. All routers are capable of maintaining their own time-of-day, but this is usually not sufficient. Instead, direct the router to at least two different reliable time servers to ensure accuracy and availability of time information.

3. IMPLEMENTING ROUTERS SECURITY

This section discusses the various mechanisms used to protect the router. The physical access and software protection are covered in section 2.1. Remote administrations, password security, and other configurations are covered in this section.

3.1. Router Configuration and Commands (IOS)

After connecting to a router and initially logging in, the system is in user mode also known as EXEC mode. EXEC mode gives limited access to the command set of the router. Access to all the router commands, including the ability to change the configuration, is reserved for the privileged EXEC mode. Typing the enable command at an EXEC mode prompt will give access to the privileged EXEC mode. Privileged EXEC mode is sometimes called 'enable mode'. There are several configuration modes on a Cisco router. To enter the global configuration mode (config t) type the command configure terminal, commonly abbreviated "config t". In the global configuration mode a wide variety of overall router features and settings can be changed: banners, authentication systems, access lists, logging, routing protocols, and much more. There are sub-modes which are used to configure specific settings for interfaces, lines, routing protocols, etc. The list below describes some of the sub-modes.

- Interface (config-if). It is used to configure aspects of a particular interface like FastEthernet0, Ethernet 0/1, or Vlan2.
- line (config-line). It is used to set up the console port, auxiliary port and virtual terminal lines.

- Access-list. There are two types of IP named access lists, extended (config-ext-n) and standard (config-std-n), which can be used instead of numbered lists. Access-list mode is used for building named access lists.
- Route (config-route). In this sub-mode specific parameters can be set and modified for a selected routing protocol.

3.2. Secure Interface configuration

The very first point is that routers and other network devices communicates using various management protocols, such as routing protocols, SNMP, NTP, and TFTP. When the router initiates a network connection, that connection must have some source address; typically a router will select a source address from one of the addresses bound to one of its network interfaces. So it is considered best practice, in configuring Cisco routers, to define one loopback interface, and designate it as the source interface for most traffic generated by the router itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. When a router is configured to use the loopback interface for services, it is possible to configure the security of other devices in the network more tightly. (When a service is configured to use the loopback interface as its source, we say that the service is bound to that interface. It means that IP packets generated by the router will have the loopback interface's address as their source address. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of your network from potential attackers is usually good practice. To create a loopback interface, simply assign it an IP address.

```
Router #config t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# interface loopback0
Router (config-if)# description Main loopback interface
Router (config-if)# ip address xxx.yyy.zzz.x 255.255.255.255
Router (config-if)# end
```

Apart from loopback interface review the configuration in the router and put these commands under each interface. Some routers may have 2 interfaces and some may have more than 2. Repeat this step for each separate interface. Shutdown any interface that is not used! This needs to be done on the all the Routers.

```
# no ip proxy-arp – under each interface or sub-interface – disables the use of
ip proxy-arp
# no ip directed-broadcast - under each interface or sub-interface – disables the
forwarding of broadcasts
# no ip unreachable – does not send icmp reply when denied by acl
# no ip redirect – disables ip redirects (unless you have an application that
relies on it)
# no ip mask-reply – eliminates IP from giving out IP Addressing Info
# ip verify unicast reverse-path – ensures that the source address is valid and
not spoofed
# no cdp enable – configure on interface where cdp is not needed
```

3.3. Secure Global Services Configurations

These are the commands which are required to be given in global configuration mode after giving # config t.

```
# no service finger – does not allow finger software to get usernames, etc
# no boot network – disables loading startup configuration from the network
# no service config. – disables loading startup configuration from the network
# no service pad – shuts down unnecessary services
# no service tcp-small-servers – shuts down unnecessary services
# no service udp-small-servers – shuts down unnecessary services
# no ip bootp server – does not allow the use of bootp
# no ip http server – shuts down the http server on a device
# no ip source-route – disables ip based source routing
# no cdp run – disables Cisco Discovery Protocol entirely on router
# no cdp enable – disables Cisco Discovery Protocol on interfaces
#no ip name-server – disables router sending DNS queries to broadcast
addresses
# no ip domain-lookup – disables router using domain names in IOS commands
# service tcp-keepalives-in – limits tcp inbound open connections
# service tcp-keepalives-out – limits tcp outbound connections
# service timestamp log datetime msec localtime show-timezone – timestamps
log entries
# logging console notification – notifies any alerts except acl matches
# logging on – enables the use of syslog
# logging ip address – ip address of syslog server
# logging trap information – sets the level of syslog information to be used
# logging source-interface... – sources the logging traffic from the ip address of
the interface
# aaa logging – sends AAA log information
# log-input – logging information
# banner motd ^C – configures a Message of the Day banner

*****WARNING*****

Legal notice as per company policy

*****WARNING*****

^C

# enable secret XYZ – choose a password with both letters and numbers

# line con 0
# exec-timeout 3 0 – 3 minute timeout for inactivity
# transport input none – prevents remote access to the console port via
reverse-telnet
# login local – requires tacacs login
# password XYZ

# line aux 0
# exec-timeout 3 0 – 3 minute timeout for inactivity
# transport input none – disables login on the aux port
# no exec
```

```
# password XYZ

# line vty 0 4
# exec-timeout 3 0 – 3 minute timeout for inactivity
# access-class XX in – access list for limiting telnet or ssh access
```

3.3.1 Privileges

Cisco IOS provides 16 different privilege levels ranging from 0 to 15. Cisco IOS comes with 2 predefined user levels. User EXEC mode runs at privilege level 1 and “enabled” mode (privileged EXEC mode) runs at level 15. Every IOS command is pre-assigned to either level 1 or level 15.

By default Cisco provides EXEC (level 1) with a few commands which may, in terms of security, make more sense being at a higher privilege level. The next example shows how to move the commands to the privileged mode, which in most configurations should be protected better.

```
# privilege exec level 15 connect
# privilege exec level 15 telnet
# privilege exec level 15 rlogin
# privilege exec level 15 show ip access-lists
# privilege exec level 15 show access-lists
# privilege exec level 15 show logging
# privilege exec level 1 show ip
```

The last line is required to move the show command back down to level 1. It is also possible to set up intermediate privilege levels. For example, an organization might want to set up more than the two levels of administrative access on their routers. This could be done by assigning a password to an intermediate level, like 5 or 10, and then assigning particular commands to that privilege level.

3.4. Password security

There are two password protection schemes in Cisco IOS i.e. Type 7 and Type 5. Type 7 uses the Cisco defined encryption algorithm which is known to the commercial security community. Hence it is a weak password scheme. Type 5 uses an iterated MD5 hash which is much stronger. Cisco recommends that Type 5 encryption be used instead of Type 7 where possible. Type 7 encryption is used by the enable password, username, and line password commands.

- To protect the privileged EXEC level as much as possible, do not use the enable password command; only use the enable secret command. Even if the enable secret is set do not set the enable password, it will not be used and may give away a system password.

```
# config t
# enable secret 2-mAny-rOUtEs
# no enable password
# end
```

- Because it is not possible to use Type 5 encryption on the default EXEC login or the username command, no user account should be created above privilege level 1. But user accounts should be created for auditing purposes. The username command should be used to create individual user accounts at the EXEC level and then the higher privilege levels should be protected with enable secret passwords. Then users with a need to work at higher levels would be given the higher privilege level password.
- If the login command is used to protect a line then the line password command is the only way to set a password on a line. But if the login local command is used to protect a line then the specified user name/password pair is used. For access and logging reasons the login local method should be used. In addition to the above password access mechanisms, AAA mechanisms may be used to authenticate, authorize, and audit users. Good security practice dictates some other rule for passwords.
- The privileged EXEC secret password should not match any other user password or any other enable secret password. Do not set any user or line password to the same value as any enable secret password.
- Enable service password-encryption ; this will keep passersby from reading your passwords when they are displayed on your screen.
- Be aware that there are some secret values that service password encryption does not protect. Never set any of these secret values to the same string as any other password.
- Avoid dictionary words, names, phone numbers, and dates.
- Always include at least one of each of the following: lowercase letters, uppercase letters, digits, and special characters.
- Make all passwords at least eight characters long.
- Avoid more than 4 digits or same-case letters in a row. Note: enable secret and username passwords may be up to 25 characters long including spaces.

3.5. Access Control Lists for security and filtering

Cisco IOS uses access lists to separate data traffic into that, which it will process (permitted packets) and that which it will not process (denied packets). Secure configuration of Cisco routers makes very heavy use of access lists, for restricting access to services on the router itself, and for filtering traffic passing through the router, and for other packet identification tasks.

Syntax

The two syntax of IP access list is given below.

Standard IP access-list
access-list list-number {deny | permit} source [source-wildcard] [log]

Extended IP access-list

*access-list list-number {deny | permit} protocol source source-wildcard
source-qualifiers destination destination-wildcard destination-qualifiers [log |
log-input]*

The optional keyword `log` may be applied to log matches to the rule. Note that logging for IP standard access lists is supported only in IOS 12.0 and later. The access list number tells Cisco IOS which access list the rule should be a part of, and what kind of access list it is. The condition field, which is different for each kind of access list, specifies which packets match the rule. Conditions typically involve protocol information and addresses, but do not involve application-level information.

3.5.1. General Recommendations

Refer to the tables in Section 2.2.2 that present common services to restrict because they can be used to gather information about an internal network or they have weaknesses that can be exploited. In each access list there must be at least one permit statement. Otherwise, an access list with no permit statements will block all network traffic wherever it is applied. Note that an access list is applied to packets traveling in one direction only. For any connection that requires two-way interaction (e.g., all TCP traffic, some UDP traffic) the access list will only affect approximately half the packets. It is possible however to apply two access lists (one for each direction) for router interfaces, vty lines and routing protocols.

Use the `log` keyword at the end of each deny statement in each extended access list, as shown in the example below. This feature will provide valuable information about what types of packets are being denied. Logs of denied packets can be useful for detection and analysis of probes and attacks against a network. Access list log messages always include the access list number, which is usually sufficient to identify the provenance of the traffic. If you might apply the same access list to more than one interface, then use the qualifier `log-input` instead of `log`.

Add the following statements at the end of each extended IP access list to deny and to log any packets that are not permitted. These statements include the entire port ranges for TCP and UDP explicitly. This will guarantee that the router will log the values for the source and destination ports for TCP and UDP traffic.

```
# access-list 101 deny tcp any range 0 65535  
any range 0 65535 log  
# access-list 101 deny udp any range 0 65535  
any range 0 65535 log  
# access-list 101 deny ip any any log
```

3.5.2. Filtering the traffic through Router

The access lists can be used in different ways to control access to the services running on router. Though access control to these services can be done in many ways but it is very easy and reliable to do it with specialized feature of Cisco IOS which is ACL's.

Telnet service: The vty lines are used for remote access to the router. Typically, a router administrator telnets to one of the vty lines. The following example shows the

configuration of an extended IP access list that is applied to the vty lines. This simple IP access list allows the hosts with IP addresses 10.10.10.2 and 10.10.10.15 to connect to the router via Telnet. The list denies all other connections. It also logs all successful and unsuccessful connections.

```
# access-list 102 permit tcp host xxx.yyy.zzz.xxx any eq 23 log
# access-list 102 permit tcp host xxx.yyy.zzz.xxx any eq 23 log
# access-list 102 deny ip any any log
# line vty 0 4
# access-class 102 in
```

SNMP Service. When SNMP service is enabled on a router, network management tools can use it to gather information about the router configuration. Versions 1 and 2 of SNMP are not considered secure due to the lack of strong authentication. Thus, SNMP should be used only on internal or protected networks. The following example shows the configuration of a standard IP access list that is applied to a snmp server.

```
# access-list 1 permit host
# access-list 1 deny any log
# snmp-server community ActAS40DewaAR ro 1
```

Routing service. Access lists can be used to restrict what routes the router will accept (in) or advertise (out) via some routing protocols. The distribute-list acl-num out command is used to restrict routes that get distributed in routing updates, while the distribute-list acl-num in command may be used to filter routes that will be accepted from incoming routing updates.

3.5.3. IP Address Spoofing Protection.

The filtering suggested in this section is applicable to all the router roles except for backbone routers because inbound and outbound access can not be defined on backbone routers.

Inbound Traffic: Do not allow any inbound IP packet that contains an IP address from the internal network, or any reserved private addresses. If your network does not need multicast traffic, then block the IP multicast address range (224.0.0.0) and apply this access list to the external interface of the router.

```
# access-list 103 deny ip (Internal network) any log
# access-list 103 deny ip 127.0.0.0 0.255.255.255 any log
# access-list 103 deny ip 10.0.0.0 0.255.255.255 any log
# access-list 103 deny ip 0.0.0.0 0.255.255.255 any log
# access-list 103 deny ip 172.16.0.0 0.15.255.255 any log
# access-list 103 deny ip 192.168.0.0 0.0.255.255 any log
# access-list 103 deny ip 192.0.2.0 0.0.0.255 any log
# access-list 103 deny ip 224.0.0.0 15.255.255.255 any log
# access-list 103 deny ip host 255.255.255.255 any log
# access-list 103 permit ip any IP (Internal network)
```

Outbound Traffic: Do not allow any outbound IP packet that contains an IP address other than a valid internal one in the source field. Apply this access list to the internal interface of the router. See the following example with the network address (10.10.10.0).

```
# access-list 103 permit ip 10.10.10.0 0.0.0.255 any
# access-list 103 deny ip any any log
```

3.5.4. Protection from attacks.

This sub-section will describe how to use access lists to defeat several common attacks using IOS traffic filtering capabilities.

TCP SYN Attack. The TCP SYN Attack involves transmitting a volume of half open connections that cannot be completed at any destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users. The following discussion shows two different approaches.

- External Access Blocked. The access list rules shown below will block packets from an external network that have only the SYN flag set. Thus, it allows traffic from TCP connections that were established from the internal network (10.10.10.0 in this case), and it denies anyone coming from any external network from starting any TCP connection.

```
# access-list 104 permit tcp any 10.10.10.0 0.0.0.255 established
# access-list 104 deny ip any any log
# interface s 0/0
# description "external interface"
# ip access-group 104 in
```

- Limiting External Access with TCP Intercept. The access list rules shown below will block packets from unreachable hosts using the TCP intercept feature thus, it only allows reachable external hosts to initiate connections to a host on the internal network. In intercept mode the router intercepts each TCP connection establishment, and decides if the address from which the connection is being initiated is reachable. If the host is reachable, the router allows the connection to be established; otherwise, it prevents the connection.

```
# ip tcp intercept list 105
# access-list 105 permit tcp any xxx.yyy.zzz.x0.0.0.255
# access-list 105 deny ip any any log
# interface s 0/0
# description "External interface"
# ip access-group 105 in
```

TCP intercept is a very effective mechanism for protecting hosts on a network from outside TCP SYN attacks; consult the Cisco IOS 12 Security Configuration Guide. Note that TCP intercept, while it can be very useful, can also impose significant overhead on router operations. Examine and test the performance burden imposed by TCP intercept before using it on an operational network.

Smurf Attack. The Smurf Attack involves sending a large amount of ICMP Echo packets to a subnet's broadcast address with a spoofed source IP address from that subnet. If a router is positioned to forward broadcast requests to other routers on the protected network, then the router should be configured to prevent this forwarding

from occurring. This blocking can be achieved by denying any packets destined for broadcast addresses. The example statements below block all IP traffic from any outside host to the possible broadcast addresses (10.10.10.255 and 10.10.10.0) for the 10.10.10.0/24 subnet.

```
# access-list 107 deny ip any host 10.10.10.255 log
# access-list 107 deny ip any host 10.10.10.0 log
# interface interface eth0/0
# ip access-group 107 in
```

ICMP Message Types and Traceroute . There are different types of ICMP messages. Some these are associated with programs. Also, others are used for network management and are automatically generated and interpreted by network devices. For inbound ICMP traffic, block the message types Echo and Redirect. With Echo packets an attacker can create a map of the subnets and hosts behind the router. Also, he can perform a denial of service attack by flooding the router or internal network with Echo packets. With ICMP Redirect packets the attacker can cause changes to a host's routing tables. Otherwise, the other ICMP message types should be allowed inbound. See the example below for inbound ICMP traffic.

```
# access-list 100 deny icmp any any echo log
# access-list 100 deny icmp any any redirect log
# access-list 100 deny icmp any any mask-request log
# access-list 100 permit icmp any xxx.yyy.zzz.x 0.0.0.255
```

For outbound ICMP traffic, one should allow the message types Echo, Source Quench, Parameter Problem, and Packet Too Big and block all other message types. With Echo packets users will be able to ping external hosts. Parameter Problem packets and Source Quench packets improve connections by informing about problems with packet headers and by slowing down traffic when it is necessary. Packet Too Big is necessary for Path MTU discovery. The example below shows a set of filter rules for outbound ICMP traffic that permits these message types.

```
# access-list 108 permit icmp any any echo
# access-list 108 permit icmp any any packet-too-big
# access-list 108 permit icmp any any parameter-problem
# access-list 108 permit icmp any any source-quench
# access-list 108 deny icmp any any log
```

Traceroute is the program that also deals with certain ICMP message types. Traceroute is a utility that tells the IP addresses of the routers that handle a packet as the packet hops along the network from source to destination. On Unix and Linux operating systems, traceroute uses UDP packets and causes routers along the path to generate ICMP message types 'Time Exceeded' and 'Unreachable'. An attacker can use traceroute response to create a map of the subnets and hosts behind the router, just as they could do with ping's ICMP Echo Reply messages. Therefore, block tricky inbound traceroute by including a rule in the inbound interface access list, as shown in the example below (ports 33400 through 34400 are the UDP ports usually used for traceroute).

```
# access-list 110 deny udp any any range 33400 34400 log
```

A router may be configured to allow outbound traceroute by adding a rule to the outbound interface access list, as shown in the example below.

```
# access-list 110 permit udp any any range 33400 34400 log
```

Land Attack. The Land Attack involves sending a packet to the router with the same IP address in the destination and source address fields and with the same port number in the destination port and source port fields. This attack may cause denial of service or degrade the performance of the router. The example below shows how to prevent this attack, which can be blocked by following access-list.

```
# access-list 100 deny ip host xxx.yyy.zzz.x host xxx.yyy.zzz.x log
# access-list 100 permit ip any any
# interface s0/0
# description External interface
# ip address xxx.yyy.z.x 255.255.0.0
# ip access-group 100 in
```

Denial of service (DoS) Attacks. DoS *attack*, a type of attack on a network that is designed to bring the network down by flooding it with useless traffic and denying the service to legitimate users. The latest example of dos attack is Cisco IOS Interface Blocked by IPv4 Packets. Multiple IPv4 packets with specific protocol fields sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. Therefore, you may choose to apply the following access-list rules as a work

```
#access-list 101 permit tcp any any
#access-list 101 permit udp any any
#access-list 101 deny 53 any any
#access-list 101 deny 55 any any
#access-list 101 deny 77 any any
#access-list 101 deny 103 any any
```

Distributed Denial of Service (DDoS) Attacks. Routers cannot prevent DDoS attacks in general, but it is usually sound security practice to discourage the activities of specific DDoS agents by adding access list rules that block their particular ports. The given example shows access list rules for blocking several popular DDoS attack tools. [Note that some of these rules may also impose a slight impact on normal users, because they block high-numbered ports that legitimate network clients may randomly select. Therefore, you may choose to apply these rules only when an attack has been detected. Otherwise, these rules would normally be applied to traffic in both directions between an internal or trusted network and an untrusted network.]

! the Subseven DDoS system and some variants

```
access-list 170 deny tcp any any range 6711 6712 log
access-list 170 deny tcp any any eq 6776 log
access-list 170 deny tcp any any eq 6669 log
access-list 170 deny tcp any any eq 2222 log
access-list 170 deny tcp any any eq 7000 log
```

! the Stache ldraht DDoS system

```
access-list 170 deny tcp any any eq 16660 log
access-list 170 deny tcp any any eq 65000 log
```

! the TRINOO DDoS systems

```
access-list 170 deny tcp any any eq 27665 log
access-list 170 deny udp any any eq 31335 log
access-list 170 deny udp any any eq 27444 log
```

! the TrinityV3 system

```
access-list 170 deny tcp any any eq 33270 log
access-list 170 deny tcp any any eq 39168 log
```

The Tribe Flood Network (TFN) DDoS system uses ICMP Echo Reply messages, which are problematic to block because they are the heart of the ping program. Follow the directions in the ICMP sub-section, above, to prevent at least one direction of TFN communication.

3.6. Remote Access security

This section describes five connection schemes which can be used for router administration.

1. No Remote – administration is performed on the console only.
2. Remote Internal only with AAA – administration can be performed on the router from a trusted internal network only, and AAA is used for access control.
3. Remote Internal only – administration can be performed on the router from the internal network only.
4. Remote External with AAA – administration can be performed with both internal and external connections and uses AAA for access control.
5. Remote External – administration can be performed with both internal and external connections.

Remote administration is inherently dangerous. When you use remote administration, anyone with a network sniffer and access to the right LAN segment can acquire the router account and password information. This is why remote administration security issues center around protecting the paths which the session will use to access the router. The five regimes listed above are listed in the order that best protects the router and allows for accounting of router activities. Remote access over untrusted networks (e.g. the Internet) should not be used, with or without AAA, unless the traffic is adequately protected, because the user's password will travel the network in clear text form. The security of remote administration can be enhanced by using a security protocol, such as IPSec or SSH.. Cisco has added support for the Secure Shell (SSH) protocol to many versions of IOS 12.0 and later. Section 5.3 describes how to use SSH for secure remote administration.

Prior to establishing an IPSec configuration on the router, certain network and current router configuration checks should be made to eliminate any router connectivity problems. Since IPSec utilizes IP protocols 50 and 51, and the User Datagram Protocol (UDP) port 500 in its communications, any access list restrictions on these ports or protocols should be removed or changed to allow the IPSec packets to be transmitted and received by the participating routers. The example below illustrates the ACL rule syntax for permitting incoming IPSec traffic.

```
access-list 100 permit 50 host xxx.yyy.zzz.x host yyy.zzz.xxx.y
access-list 100 permit 51 host xxx.yyy.zzz.x host yyy.zzz.xxx.y
```

access-list 100 permit udp host xxx.yyy.zzz.x host yyy.zzz.xxx.y eq 500

An alternative to setting up IPSec for secure remote administration is to configure your router to use the secure shell service, commonly called SSH. SSH was originally intended to be a secure replacement for classic telnet, rlogin, rsh, and rcp services. It utilizes RSA public key cryptography to establish a secure connection between a client and a server. Because the connection is encrypted, passwords and other sensitive information are not exposed in the clear between the administrator's host and the router. SSH also prevents session hijacking and many other kinds of network attacks. Only certain Cisco IOS versions are shipped with the SSH feature set. Versions after and including 12.0(5)S with IPSec include support for SSH. IOS versions that do not support IPSec do not support SSH either. There are two main versions of the SSH protocol in widespread use, SSH versions 1 and 2. Cisco IOS 12.0 through 12.2 are currently capable of supporting only SSH version 1.

Before you can configure SSH, there are two important prerequisites to address. First, make sure that the router has a local hostname and domain name set. With SSH, you must establish usernames for people that will be attempting to connect to the router.

3.7 Securing IP Routing

The routing process is the most important part of your network: If it is exploited, network will not function. Also, it gives a lot of information away to people have access to the routing-tables. This section discusses some basic security measures related to the way in which the router forwards IP packets.

Cisco IOS has several tools to help protect the routing protocols from intentional or unintentional attacks. The first and primary mechanism to protect route protocol updates is through configuring router authentication. MD5 is a valuable tool that will validate the authentication of a routing update. The second tool is the extended ACL. ACL's should be used strategically through out the network to validate the source / destination address of packets headed for the IGP (Interior Gateway Protocol) and EGP (Exterior Gateway Protocol) ports. ACL's make it more difficult for DOS/DDOS attacks from targeting the routing protocol. Finally, there are specific commands and in the routing protocols that help protect them from attack. For example, BGP's (Border Gateway Protocol) maximum-prefix command alerts the operators and optionally shuts down the BGP session whenever the maximum prefix limit is reached. This protects the router from being overwhelmed by the number of updates or having its memory completely consumed – potentially crashing the router. This section will review these tools and techniques to have a better understanding of how to protect their routing protocols.

3.7.1. Authenticating Routing Protocol Updates

Neighbour router authentication is part of an IP routing security plan. This section describes what neighbour router authentication is, how it works, and why it should be used to increase overall network security. Documentation details can be found at: http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secure/scprt5/scrouter.htm

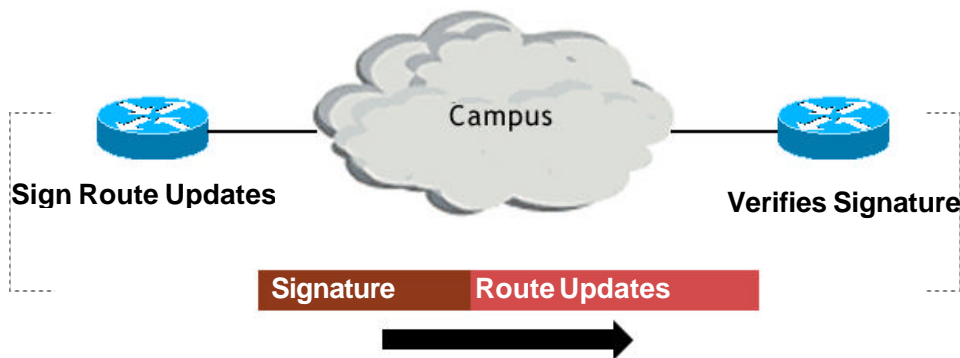
Benefits of Neighbour Authentication: When configured, neighbour authentication occurs whenever routing updates are exchanged between neighbour routers. This

authentication ensures that a router receives reliable routing information from a trusted source. Without neighbour authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly party diverts or analyses your network traffic. For example, an unauthorized router could send a fictitious routing update to convince your router to send traffic to an incorrect destination. This diverted traffic could be analyzed to learn confidential information of your organization, or merely used to disrupt your organization's ability to effectively communicate using the network. Neighbour Authentication prevents any such fraudulent route updates from being received by your router.

Protocols That Use Neighbour Authentication

- Border Gateway Protocol (BGP)
- DRP Server Agent
- Intermediate System-to-Intermediate System (IS-IS)
- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol version 2 (RIPv2)

Configure Router Authentication



Certifies authenticity of neighbour and integrity of route updates

Figure: 3 -1

When to Configure Neighbour Authentication

You should configure any router for neighbour authentication if that router meets all of these conditions:

- The router uses any of the routing protocols previously mentioned.

- It is conceivable that the router might receive a false route update.
- If the router were to receive a false route update, your network might be compromised.
- If you configure a router for neighbour authentication, you also need to configure the neighbour router for neighbour authentication.

How Neighbour Authentication Works: When neighbour authentication has been configured on a router, the router authenticates the source of each routing update packet that it receives. This is accomplished by the exchange of an authenticating key (sometimes referred to as a password) that is known to both the sending and the receiving router. There are two types of neighbour authentication used: plain text authentication and Message Digest Algorithm Version 5 (MD5) authentication. Both forms work in the same way, with the exception that MD5 sends a “message digest” instead of the authenticating key itself. The message digest is created using the key and a message, but the key itself is not sent, preventing it from being read while it is being transmitted. Plain text authentication sends the authenticating key itself over the wire.

Note: Plain text authentication is not recommended for use as part of your security strategy. Its primary use is to avoid accidental changes to the routing infrastructure. Using MD5 authentication, however, is a recommended security practice.

CAUTION: As with all keys, passwords, and other security secrets, it is imperative that you closely guard the keys used in neighbour authentication. The security benefits of this feature are reliant upon your keeping all authenticating keys confidential. Also, when performing router management tasks via Simple Network Management Protocol (SNMP), do not ignore the risk associated with sending keys using non-encrypted SNMP.

Plain Text Authentication. Each participating neighbour router must share an authenticating key. This key is specified on each router during configuration. Multiple keys can be specified with some protocols; each key must be identified by a key number. In general, when a routing update is sent, the following authentication sequence occurs:

Step 1: A router sends a routing update with a key and the corresponding key number to the neighbour router. For protocols that can have only one key, the key number is always zero.

Step 2: The receiving (neighbour) router checks the received key against the same key stored in its own memory.

Step 3: If the two keys match, the receiving router accepts the routing update packet. If the two keys did not match, the routing update packet is rejected.

MD5 Authentication. MD5 authentication works similarly to plain text authentication, except that the key is never sent over the wire. Instead, the router uses the MD5 algorithm to produce a “message digest” of the key (also called a “hash”). The message digest is then sent instead of the key itself. This ensures that nobody can eavesdrop on the line and learn keys during transmission. These protocols use MD5 authentication:

- OSPF
- RIP version 2
- BGP

- EIGRP
- ISIS

Routing Protocol Authentication Summary: The following are some examples of how router authentication is configured in OSPF, ISIS, and BGP:

OSPF

```
interface ethernet1
ip address yyy.zzz.xxx.y 255.255.255.0
ip ospf message-digest-key 100 md5 cisco
!
router ospf 1
network yyy.zzz.xxx.y 0.0.0.255 area 0
area 0 authentication message-digest
```

ISIS

```
interface ethernet0
ip address yyy.zzz.xxx.y 255.255.255.0
ip router isis
isis password cisco level-2
```

BGP

```
router bgp 200
no synchronization
neighbor 4.1.2.1 remote-as 300
neighbor 4.1.2.1 description Link to Excalibur
neighbor 4.1.2.1 send-community
neighbor 4.1.2.1 version 4
neighbor 4.1.2.1 soft-reconfiguration inbound
neighbor 4.1.2.1 route-map Community1 out
neighbor 4.1.2.1 password cisco
```

3.8. Audit and Management

3.8.1. Concepts and Mechanisms

Routers are a critical part of network operations and network security. Careful management and diligent audit of router operations can reduce network downtime, improve security, and aid in the analysis of suspected security breaches. Cisco routers and Cisco IOS are designed to support centralized audit and management. This section describes the logging, management, monitoring, and update facilities offered in Cisco IOS 11.3, 12.0, and later.

- Logging – Cisco routers support both on-board and remote logs.
- Time – Accurate time is important for good audit and management; Cisco routers support the standard time synchronization protocol, NTP.

The sub-sections below describe recommended configurations for good security. Complete details on the commands and features discussed may be found in the Cisco IOS documentation, especially the Cisco IOS Configuration Fundamentals Command Reference documents for IOS 12.0.

3.8.2. Logging

Cisco routers can record information about a variety of events, many of which have security significance. Logs can be invaluable in characterizing and responding to security incidents. The main types of logging used by Cisco routers are:

- AAA logging, this collects information about user dial-in connections, logins, logouts, HTTP accesses, privilege level changes, commands executed, and similar events. AAA log entries are sent to authentication servers using the TACACS+ and/or RADIUS protocols, and are recorded locally by those servers, typically in disk files. If you are using a TACACS+ or RADIUS server, you may wish to enable AAA logging of various sorts; this is done using AAA configuration commands such as `aaa accounting`. Detailed description AAA configuration is beyond the scope of this document.
- SNMP trap logging, which sends notifications of significant changes in system status to SNMP management stations. You will probably want to use SNMP traps only if you have a preexisting SNMP management infrastructure.
- System logging, which records a large variety of events, depending on the system configuration. System logging events may be reported to a variety of destinations, including the following:
 - The system console port (logging console).
 - Servers using the UNIX "syslog" protocol (logging ip-address, logging trap).
 - Remote sessions on VTYS and local sessions on TTYs (logging monitor, terminal monitor).
 - A local logging buffer in router RAM (logging buffered).

From a security point of view, the most important events usually recorded by system logging are interface status changes, changes to the system configuration, access list matches, and events detected by the optional firewall and intrusion detection features.

Each system logging event is tagged with an urgency level. The levels range from debugging information (at the lowest urgency), to major system emergencies. Each logging destination may be configured with a "threshold" urgency, and will receive logging events only at or above that threshold.

Saving Log Information: By default, system logging information is sent only to the asynchronous console port. Since many console ports are unmonitored, or are connected to terminals without historical memory and with relatively small displays, this information may not be available when it's needed, especially when a problem is being debugged over the network.

Almost every router should save system logging information to a local RAM buffer. The logging buffer is of a fixed size, and retains only the newest information. The contents of the buffer are lost whenever the router is reloaded. Even so, even a moderately-sized logging buffer is often of great value. On low-end routers, a reasonable buffer size might be 16384 or 32768 bytes; on high-end routers with lots of memory (and many logged events), even 262144 bytes might be appropriate. You can use the `show memory` command to make sure that your router has enough free memory to support a logging buffer. Create the buffer using the `logging buffered` buffer-size configuration command.

Larger installations will have "syslog" servers. You can send logging information to a server with logging server-ip-address, and you can control the urgency threshold for logging to the server with logging trap urgency. Even if you have a syslog server, you should probably still enable local logging.

If your router has a real-time clock or is running NTP, you will probably want to timestamp log entries using service timestamps log datetime msec.

Recording Access List Violations: If you use access lists to filter traffic, you may want to log packets that violate your filtering criteria. Older Cisco IOS software versions support logging using the log keyword, which causes logging of the IP addresses and port numbers associated with packets matching an access list entry. Newer versions provide the log-input keyword, which adds information about the interface from which the packet was received, and the MAC address of the host that sent it.

It's not usually a good idea to configure logging for access list entries that will match very large numbers of packets. Doing so will cause log files to grow excessively large, and may cut into system performance. However, access list log messages are rate-limited, so the impact is not catastrophic.

Access list logging can also be used to characterize traffic associated with network attacks, by logging the suspect traffic.

3.8.3. Time Services, Network Time Synchronization and NTP

Successful audit of a large network can depend on synchronization of the various logs and records maintained for the hosts on that network. All Cisco routers have a clock that maintains the time and date, although some older Cisco models may lose time when turned off, and no router can keep accurate time by itself over weeks and months of operation. It is very important to set the time on a router when it is first installed, and then keep the time synchronized while the router is in operational use. It is possible to perform manual network time synchronization, adjusting the time on each router and host on a network manually on a regular basis. Manual time synchronization is tedious, error prone, and unreliable. Cisco routers fully support automated network time synchronization based on the standard Network Time Protocol (NTP). The sub-sections below give some background information on NTP, and explain how to configure it on Cisco IOS.

Setting the Time Manually. To set the time, follow these three steps: first, check the clock, second, set the timezone if necessary, and last set the time. Examine the clock using the show clock detail command. If the timezone is not correct, then set the time zone using the clock timezone configuration command. If the detail output reports a time source of NTP, then do not set the clock manually, see the descriptions of NTP below. Otherwise, set the time in privileged EXEC mode by using the clock set command, and turn off NTP on each interface using ntp disable .

```
# show clock detail  
16:25:21.747 UTC sun Mar 26 2000  
Time source is user configuration  
# config t  
# clock timezone EST -5  
# interface eth 0/0  
# ntp disable  
# end
```

```
# clock set 17:27:30 28 March 2000
# show clock
16:21:33.495 EST sun Mar 26 2000
```

If you manage routers spread across several time zones (e.g. US east and west coasts) then you should set the router time zone on all your routers to universal time or GMT.

```
## config t
# clock timezone GMT 0
```

4. TESTING AND SECURITY VALIDATION

4.1. Guidelines for Router Security Testing

The border or the edge router is often the perimeter defense when protecting against malicious network attack. Routers provide many services that can have severe security implications if improperly configured. Some of the services are enabled by default whereas other services are frequently enabled by users. Security testing provides a means of verifying that security functions are compatible with system operations and that they are configured in a secure manner. Ideally, testing should be performed at initial deployment of a router, and whenever major changes have been made to any part of the configuration of a router.

4.2 Tools for testing

There are a variety of tools available for testing purposes. Scanners such as Fyodor's nmap program are used to scan for open TCP and UDP ports on a router interface. Packet sniffer programs are used to monitor traffic passing through the network and steal unencrypted passwords and SNMP community strings; this information can then be used to formulate specific attacks against the router. Attack scripts are readily available on the Internet for numerous well-known exploits; several denial of service (DOS) attacks and the newer distributed denial of service (DDoS) attacks have been highly successful against some versions of IOS.

4.2.1 Other Tools are:

Ethereal

<http://www.ethereal.com/>

Ethereal is an effective "sniffer", a network traffic capture and analysis tool. Tools like Ethereal are valuable for diagnosing and testing router and network security.

Minicom

<http://www.pp.clinet.fi/~walker/minicom.html>

Minicom is a small, effective terminal emulation tool for Linux and Unix. While it has no fancy GUI, minicom is fast, efficient, flexible, and will serve well as a Cisco router console application on Linux.

NCAT/RAT

<http://ncat.sourceforge.net/>

NCAT is a general-purpose configuration-checking tool, RAT is a version specifically targeted to checking router configurations. The included rule sets may be used, or extended with rules that enforce your local security policy. Version 1.1 was the latest available at the time this guide was published.

NET-SNMP

<http://net-snmp.sourceforge.net/>

NET-SNMP is a free software toolkit for SNMP, originally created and distributed by the University of California at Davis. It was formerly called "ucd-snmp".

Nessus

<http://www.nessus.org/>

The Nessus security scanner is a handy tool for getting a quick idea of the security vulnerabilities present on a network. While Nessus is primarily oriented toward scanning host computers, it may also be used to scan routers.

Nmap

<http://www.insecure.org/nmap/>

<http://www.eeye.com/html/Databases/Software/nmapnt.html>

This is the most widely used port-scanning tool for Linux and UNIX systems. It can perform TCP, UDP, and address scans in a variety of ways, and is an invaluable tool for confirming filtering configurations. A version is also available for Windows NT/2000 systems.

OpenSSH

<http://www.openssh.com/>

The OpenSSH project offers a free, usable implementation of the SSH security protocol for a wide variety of platforms.

SAINT

<http://www.wwdsi.com/saint/index.html>

The Security Administrator's Integrated Network Tool (SAINT) is an advanced derivative of SATAN. It can provide valuable security scanning services for hosts, routers, and networks.

SATAN

<http://www.fish.com/~zen/satan/satan.html>

The Security Administrator's Tool for Analyzing Networks (SATAN) is primarily oriented toward network security assessment of traditional host computers, but it can also identify security vulnerabilities of routers and the network boundary protection they provide.

TeraTerm Pro

<http://hp.vector.co.jp/authors/VA002416/teraterm.html>

TeraTerm is a freely available terminal emulator and telnet application for Windows operating systems. It makes a most effective Cisco router console application.

5. REFERENCES

5.1 Books

1. CCIE Professional Development: Routing TCP/IP Volume I by Jeff Doyle

5.2 Web Sites

1. NSA Router security configuration guidelines: www.nsa.gov/snac/cisco/index.html
2. www.cisco.com
3. <http://www.cert.org/>
4. <http://www.cisco.com/univercd/home/home.htm>
5. <http://www.securityfocus.com/>
6. [nsa2.www.conxion.com/cisco/download.htm](http://www.conxion.com/cisco/download.htm)
7. www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/scprt5/scrouter.htm