CMSGu2011-05

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Securing Cisco Routers

CERT-MU

National Computer Board
Mauritius

Version 1.1

August 2011

Issue No. 5

Table of Contents

Tables and Figures

Tables

Figures

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This guide provides the technical guidance intended to help network administrators and security officers improve the security of their networks. Using the information presented in this document, they can configure their routers to control access, resist attacks, shield other network components, and protect the integrity and confidentiality of network traffic.

1.2 Audience

Network administrators and network security officers are the primary audience for this configuration guide. Most network administrators are responsible for managing the connections within their networks, and between their network and various other networks. Network security officers are usually responsible for selecting and deploying the assurance measures applied to their networks. For this audience, this guide provides security goals and guidance, along with specific examples of configuring Cisco routers to meet those goals.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an outline of the document's content, the targeted audience and the document's structure.

Section 2 presents a generic background on routers.

Section 3 provides the general security guidelines.

Section 4 shows how to set up the Cisco Router.

Section 5 details how to set strong password controls and secure account policies.

Section 6 gives details on logging, monitoring and update.

Section 7 concludes the document.

Section 8 comprises a list of references that have been used in this document.

2.0 Background

2.1 The Role of Routers in Modern Networks

On a very small computer network, it is feasible to use simple broadcast or sequential mechanisms for moving data from point to point. An Ethernet local area network (LAN) is essentially a broadcast network. In larger, more complex networks, data must be directed specifically to the intended destination. Routers direct network data messages, or packets, based on internal addresses and tables of routes, or known destinations that serve certain addresses. Directing data between portions of a network is the primary purpose of a router.

Most large computer networks use the TCP/IP protocol suite. Figure 1, below, illustrates the primary function of a router in a small IP network.

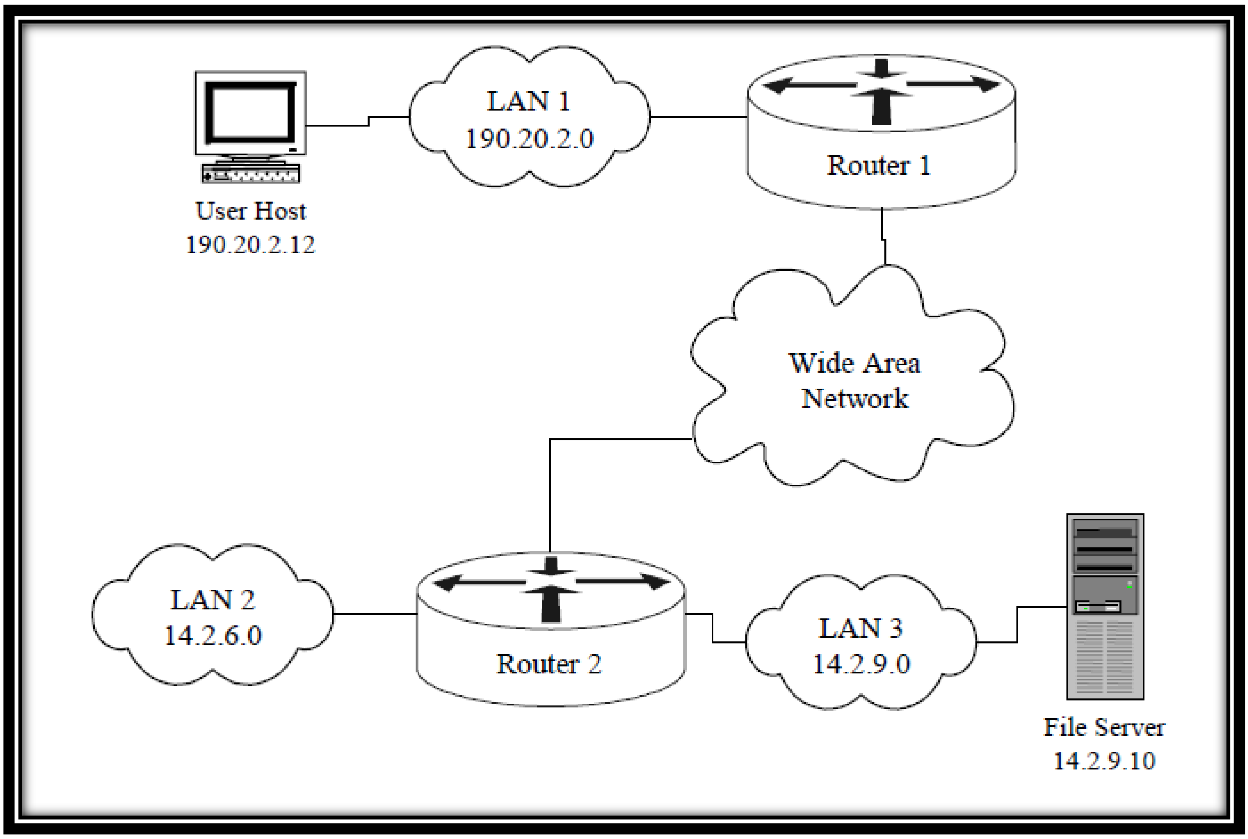


Figure 1 A Simple Network with Two Routers

If the user host (top left) needs to send a message to the file server (bottom right), it creates a packet with address 14.2.9.10, and sends the packet over LAN 1 to its gateway, Router 1. Consulting its internal route table, Router 1 forwards the packet to Router 2. Consulting its own route table, Router 2 sends the packet over LAN 3 to the File Server. In practice, the operation of any large network depends on the route tables in all of its constituent routers. Without robust routing, most modern networks cannot function. Therefore, the security of routers and their configuration settings is vital to network operation.

In addition to directing packets, a router may be responsible for filtering traffic, allowing some data packets to pass and rejecting others. Filtering is a very important responsibility for routers; it allows them to protect computers and other network components from illegitimate or hostile traffic.

2.2 Main Router Categories

There are three main categories of routers in use at companies today. These include Internet Gateway routers, Corporate Internal routers and *"B2B*[1]*"* routers. These three categories of routers should all be given consideration from a security perspective, because they each pose unique security problems that should be addressed.

Internet Gateway routers should be hardened to protect the corporation from external persons who might wish to gain access to internal corporate resources. These external persons might be script kiddies, malicious crackers or paid hackers intending to steal data.

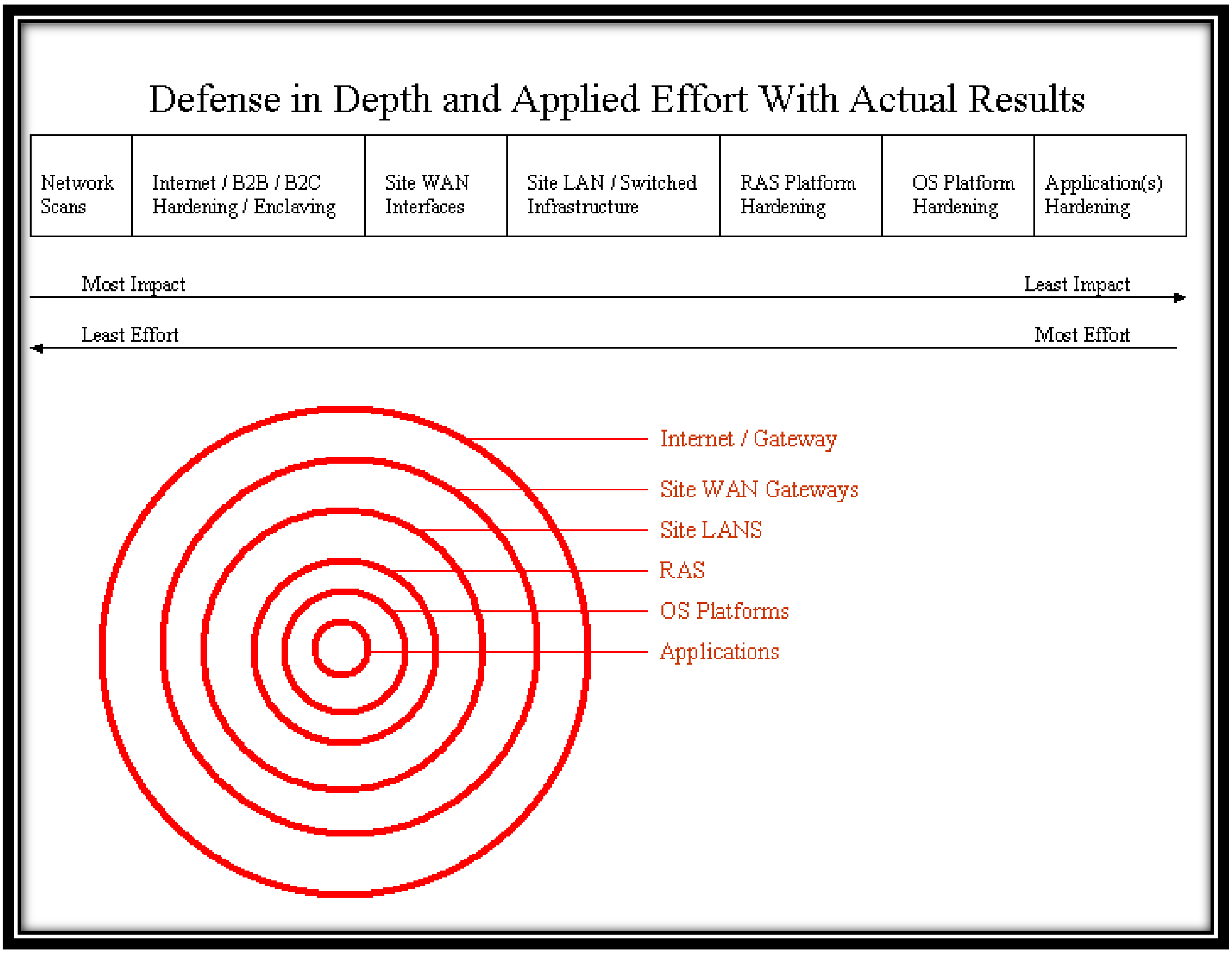
Corporate internal routers should be hardened to protect the corporation from internal threats. Internal threats can be uninformed users who unintentionally cause harm or disgruntled employees who are intent on malicious behavior. Internal routers should also be hardened using tools such as access lists to protect especially sensitive corporate resources such as financial data, research data or employee data. *"B2B"* routers need to be hardened because they pose the same threats as Internet gateway routers and corporate internal routers to the internal network. In addition they expose the company to a certain level of risk because the partner network could be compromised if security measures are not in place. Protecting business partners from risks from the internal network is good for security and for business relations.

[1] **B2B**: Business-to-business (B2B) describes commerce transactions between businesses.

Cisco Systems is the leading manufacturer of WAN equipment. For all the reasons, a set of standard practices for hardening a router becomes a necessity. Certain variations will always need to be addressed based on the topology of the network, the protocols used and the business needs. Those variations should be exceptions to the written security policy and should be noted because they could expose the company to certain risks.

3.0 General Security Guidelines

3.1 Tradeoff - Defense Benefit vs. Required Effort



Network Scans	Internet / B2B / B2C Hardening / Enclaving	Site WAN Interfaces	Site LAN / Switched Infrastructure	RAS Platform Hardening	OS Platform Hardening	Application(s) Hardening

Figure 2 Defense in Depth and Applied Effort with Actual Results

The above chart is one viewpoint on defense in depth. The idea behind the chart is that network security tasks can be seen on a sliding scale from least effort to most effort while moving inversely from high impact to low impact. Routers are included in three of the top four categories that have high impact on network security. Hardened routers, however, are only part of the solution. Additional measures must be taken to achieve organisational objectives of mitigated computer risk. For example, it is easy to implement an access list on a router to block all HTTP traffic. However, filtering certain websites while allowing others is not a task for which a router is designed. Another area where routers are not the best solution is in filtering email attachments. For these reasons, defense in depth is an important security philosophy.

3.1.1 Network Scans

The task with the least effort and the highest impact is the network security scan. A network security scan generates a list of vulnerabilities to present to the appropriate stakeholders. The scan report should be used to make management aware of the extent of security problems. Tools that can be used to perform a security scan are include without charge scanner Nessus (http://www.nessus.org) and with charge scanner ISS (http://www.iss.net).

Note: Security scans should ONLY be performed when there is clear written permission from a person or multiple persons in authority.

3.1.2 Internet/B2B/B2C/Hardening/Isolation

The next task is defined as "Internet". This task includes hardening Internet gateway routers, B2B routers, isolating servers and services for B2B and B2C communications behind a firewall infrastructure, and using an intrusion detection system. The isolated servers should be hardened using industry best practices.

3.1.3 Site WAN Interfaces

WAN applies to site-based routers. These routers should also be hardened according to industry standards to only allow needed services in and out. WAN routers are part of corporate internal router category.

3.1.4 Site LAN/Switched Infrastructure

LAN applies to the internetwork infrastructure that supports the local network. That infrastructure includes routers, route modules, switches and hubs. Examples of hardening methods include "*ACLs*[2]" on the routers and VLANs on the switches. Routers and route modules on the LAN are part of the corporate internal router category.

[2] **ACL**: An access control list (ACL), is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

3.1.5 Remote Access Service (RAS) Platform Hardening

A number of methods of hardening are available for *"RAS[3]"*. Those techniques can include apply proper authentication, use unlisted numbers in a range different than your company's public telephone lines, monitor access, limit dial up times and limit access to systems.

3.1.6 OS Platform Hardening

OS Platforms refers to internal systems. They vary widely and all require different hardening techniques. Those techniques include apply patches, disable routing, remove unneeded servers, disable unused services, apply *"TCPWrappers[4]"*, install *"TripWire[5]"* and apply reverse DNS lookups.

3.1.7 Application(s) Hardening

Applications have two varieties – purchased applications and in-house developed applications. Security measures for purchased applications can include apply vendor patches and limit services per server (i.e. the *"PDC[6]"* is not also the public web server). In-house developed applications should have security included as part of the initial software design. If not included, future releases should address security issues.

3.2 Enforce the least privilege principle

Enforcing the least privilege principle means that users and administrators get the commands they need and ONLY the commands they need. Having additional privileges allows employees to move beyond the scope of their assigned duties, which can be positive from a

[3] **RAS**: Remote Access Services (RAS) refers to any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices.

[4] **TCP Wrapper**: is a host-based Networking ACL system, used to filter network access to Internet Protocol servers on (Unix-like) operating systems such as Linux or BSD. It allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens on which to filter for access control purposes.

[5] **TripWire**: Tripwire for Routers and Switches is a data and networking integrity product that provides real-time detection of incorrect configurations and attacks on Cisco routers and switches running IOS version 11.3, 12.0, or 12.1. The software performs restoration subsequent to detection.

[6] **PDC**: A Primary Domain Controller (PDC) is a server computer in a Windows domain. A domain is a group of computers (technically named a "forest"), where access to a variety of computer resources is controlled by the PDC.

business perspective. However from a security point of view, users should have the privileges assigned to them in a manner to limit their ability to go outside their specified tasks.

This can pose problems because an administrator may have an assigned area of duty and privileges, but may need additional privileges in order to facilitate cross training on another administrator’s duties. A written security policy and a set of operational policies and procedures should outline how this problem is resolved. Cisco routers allow for assignment of up to 15 levels of privilege.

3.3 Identify the Groups

3.3.1 Administrators

Large corporations have many assets and need many administrators. Small companies may have one employee who administers all the systems. In either case it is a good idea to break out all the various roles and determine what privileges each of them should have. This table should be included in the written security policy. For example:

Title	Privileges	Number of Devices per Administrator (optional)
Router Administrator	Level 15 access to all routers	
Access Server Administrator	Level 15 access to all access servers	
Firewall Administrator	Root privilege to all firewalls and management stations	
IDS Administrator	Root privilege to all IDS systems and syslog servers	

Table 1 Identify the Groups - Administrators and Privileges

The above is a limited example of the roles available and levels of privilege available to administrators. In the above scenario, the router and access-server administrator may be the same person while two additional fulltime personnel will handle the duties of firewall administrator and IDS administrator. Or all of the above administrators may be one person. Or all there may be a team of three router administrators, three access-server administrators, three firewall administrators and three IDS administrators. Additionally the table could have information about how many devices a single administrator is expected to administer. That will allow for personnel planning based on the number of devices. This is good because certain devices require much more hands-on administration than others. This is especially important because as companies acquire other companies, they can determine what staffing level is appropriate for operations personnel.

3.3.2 Users

Identifying users is an important step in securing the network. Users can be classified in many different ways. In multi-protocol networks users can be classified as IP users, IPX users, Appletalk users, etc. For example, IP users could be further broken down according to whether they are Unix users, Linux users and Windows users. Users can also be classified according to their business function. Examples include finance, administration, sales, graphics, training, information technology, and research. Under sales, the users could be subdivided into sales managers, outside salespeople, inside salespeople, sales technical support and sales administrators. The way that each company classifies its users depends on the structure of the organisation. Understanding the organisation and understanding the needs of the users within that organisation allows for judicious assignment of privileges. A smart way to classify users is to develop a matrix based on the criteria best suited to classifying the organisation.

3.4 Limit Trust

3.4.1 Administrators

To be useful for any company, the matrix of roles should be developed and then the personnel should be assigned to each role. This table, with the personnel assigned, should be part of the operations documentation. It should NOT be in the written security policy as it may change.

Title	Privileges	Number of Devices per Administrator (optional)	Name	Backup (optional)
Router Administrator	Level 15 access to all routers		Ted	Alice
Access Server Administrator	Level 15 access to all access servers		Alice	Bob
Firewall Administrator	Root privilege to all firewalls and management		Bob	Alice

	stations			
IDS Administrator	Root privilege to all IDS systems and syslog servers		Alice	Ted

Table 2 Limit Trust - Administrators and Privileges

If administrators transfer to another department, procedures need to be in place to remove the old permissions. When they leave the company, procedures should be in place about removing the employee from the devices for which they have permissions.

3.4.2 Users

Policies and procedures need to put into place to ensure the users do not gain more privileges then they need and are allowed. The structure of the organisation and the matrix of users will highlight what should be done. For example, account creation and deletion should be coordinated if users belong to both a Windows NT domain and have terminal access to a mainframe. Users should be prevented from accessing areas other than the ones that have been set up for them. As users transfer from department to another, procedures need to be in place to remove the old permissions and set up new permissions. When employees leave a company, procedures should be in place about removing the employee from the groups for which they have permissions. If the company employs a centralised directory, that could serve as a focal point.

4.0 Setting up the Router

4.1 Physically secure the router

Physical security is the foundation of internetworking security. If an attacker can gain physical access to your device, all the patches, *"ACLs"*, and firewall feature sets in the world cannot protect them. The attacker can cause either overt or covert damage to your network is physical access is compromised. Overt damage is classified as immediate shutdown of the services provided by the router. Examples include stealing the router or turning it off. Covert damage is much harder to find and correct. It consists of the intentional introduction of malicious information that affects the router's services. For example, a malicious attacker could change one line in a multi-line *"ACL"* that will cause routing issues. That change could lead to hours, days or weeks spent tracking down the routing problem.

4.2 Choosing a Cisco Internetwork Operating System (IOS®)

4.2.1 Cisco IOS® Background and History

The operating system for Cisco routers is the Cisco Internetwork Operating System (IOS®). The original function of a router is just what is seems it should be – to route packets. Over time this function has expanded greatly with the advent and adoption of new technologies such as voice, video, and virtual private networking. Additional functions will surely be added over time to this cornerstone of the network.

Cisco IOS® Software supports every major protocol and type of physical medium, for end to end connectivity across IP and legacy networks. Cisco IOS® WAN and dial connectivity software offers support for ATM, Frame Relay, X.25, ISDN, digital subscriber line (xDSL), cable, wireless, dial, Point-to-Point Protocol (PPP), VPN, and virtual private dialup network (VPDN) services. The functionality and multi-protocol support of the Cisco IOS® Software allow it to be a very useful security measure in any internetwork. Access Control Lists (ACL), Authentication, Authorisation, and Accounting (aaa), and Cisco IOS® Firewall are some of the major tools used in the Cisco IOS® Software to ensure security. Security professionals need to become experts in the use of those tools to mitigate security risks to their network.

The emergence of e-commerce as a viable means to do business has required that networks become more secure so that customers will feel comfortable conducting transactions over the

Internet. Part of that security consists of “hardening” the routers. Having hardened routers, in conjunction with hardened switches, servers and applications, assists in having another layer to a “defense in depth” scheme.

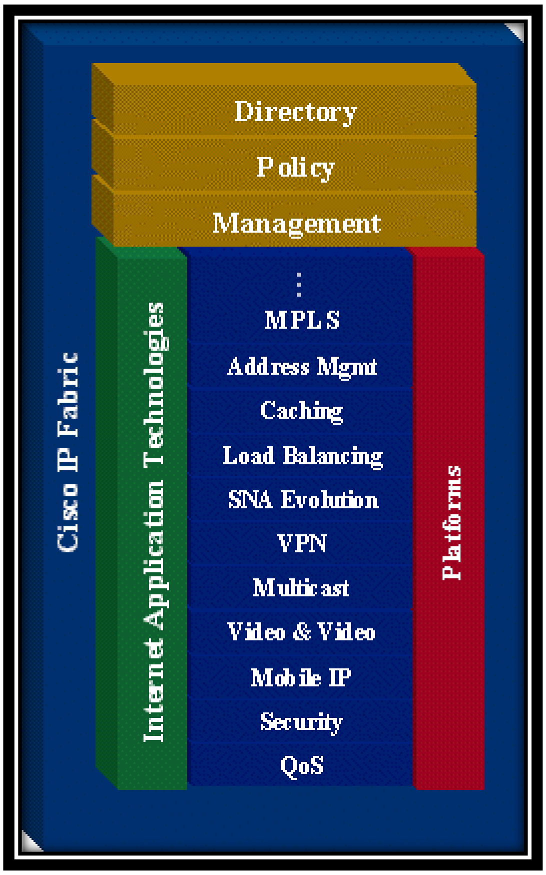


Figure 3 Cisco IOS Software Intelligent Network Services

Cisco uses the terms release and feature set. A release is analogous to a version number and works on many, if not all, of the various Cisco platforms. Feature sets (also known as software images) are subsets of releases and are also supported across different platforms. Not all feature sets are available on all platforms. Based on the number of releases, number of features and number of platforms there are a large number of IOS® packages available.

Examples of feature-set categories include:

Feature Set	Description
Basic	A basic feature set for the hardwareplatform; for example IP, IP/FW
Plus	A basic feature set plus additional features such as IP Plus, IP/FW Plus, and Enterprise Plus

Plus - Encryption	The addition of the 56-bit (Example: Plus 56) data encryption feature sets to either a basic or plus feature set; example include IP/ATM PLUS IPSEC 56 or Enterprise Plus 56

Table 3 Feature Set Categories

From Cisco IOS® Release 12.2 onwards, the encryption designators are k8/k9:

1. k8: less than or equal to 64-bit encryption (on 12.2 and up)
2. k9: greater than 64-bit encryption (on 12.2 and up)

Release	Description
Early-deployment (ED)	Indicates timely introduction of innovation internetworking technologies.
Major Release	Takes the new functions introduced in several ED releases and extends them to more platforms and ensures that reliability is achieved over a long period of time, 12.0 and 12.1 are major releases.
Maintenance Level	12.0 is the number of the major release and 7 is its maintenance level. The complete release number is 12.0(7).
T (Technology) Release	Uses the current major release as its foundation to provide new features and platform support. An example is Cisco IOS® Release 12.1T
X Release	Supports only a limited number of platforms and is based on a T release. An example is 12.1(1)XB.
General-Deployment (GD) Release	A major release that has had extensive market release, testing and bug analysis in a wide range of network environments. GD is achieved by a particular maintenance version. Subsequent maintenance updates for that release are also GD releases. For example, 12.0 got the GD certification at 12.0(8). Thus, 12.0(9), 12.0(10), and so on are GD releases.

Table 4 Cisco IOS Releases

Since the different releases of the Cisco IOS® work on different platforms and support different features, one must carefully examine the Release notes to find the most stable, most secure version of IOS® that supports the features that the internetwork needs.

4.2.2 Known Vulnerabilities

Cisco has several major vulnerabilities detailed on its website. A short description of each one, quoted directly from the Cisco website, is included below.

Security Advisories	First Published	Last Updated	Additional Information
Cisco Security Advisory: Apache HTTPd Range Header Denial of Service Vulnerability	30-Aug-2011 16:00 GMT	02-Sep-2011 16:00 GMT	Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Apache HTTP Server Overlapping Ranges Denial of Service Vulnerability
Cisco Security Advisory: Denial of Service Vulnerability in Cisco TelePresence Codecs	31-Aug-2011 16:00 GMT	01-Sep-2011 21:00 GMT	Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerability in Cisco TelePresence Codecs
Cisco Security Advisory: Open Query Interface in Cisco Unified Communications Manager and Cisco Unified Presence Server	24-Aug-2011 16:00 GMT	26-Aug-2011 22:00 GMT	Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Open Query Interface in Cisco Unified Communications Manager and Presence Server
Cisco Security Advisory: Cisco Unified Communications Manager Denial of Service Vulnerabilities	24-Aug-2011 16:00 GMT		Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco Intercompany Media Engine
Cisco Security Advisory: Denial of Service Vulnerabilities in Cisco Intercompany Media Engine	24-Aug-2011 16:00 GMT		Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Denial of Service Vulnerabilities in Cisco Unified Communications Manager and Cisco Intercompany Media Engine
Cisco Security Advisory: Cisco TelePresence Recording Server Default Credentials for Root	29-Jul-2011		Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco TelePresence Recording Server

Account Vulnerability	16:00 GMT		Default Credentials for Root Account Vulnerability
Cisco Security Advisory: Cisco SA 500 Series Security Appliances Web Management Interface Vulnerabilities	20-Jul-2011 16:00 GMT		
Cisco Security Advisory: Cisco ASR 9000 Series Routers Line Card IP Version 4 Denial of Service Vulnerability	20-Jul-2011 16:00 GMT		
Cisco Security Advisory: Multiple Vulnerabilities in Cisco AnyConnect Secure Mobility Client	01-Jun-2011 16:00 GMT	11-Jul-2011 15:00 GMT	
Cisco Security Advisory: Cisco Content Services Gateway Denial of Service Vulnerability	06-Jul-2011 16:00 GMT		Cisco Applied Mitigation Bulletin: Identifying and Mitigating Exploitation of the Cisco Content Services Gateway Denial of Service Vulnerability
Cisco Security Advisory: Cisco RVS4000 and WRVS4400N Web Management Interface Vulnerabilities	25-May-2011 16:00 GMT	17-Jun-2011 17:00 GMT	
Cisco Security Advisory: Multiple Vulnerabilities in Cisco Unified IP Phones 7900 Series	01-Jun-2011 16:00 GMT		

Table 5 Cisco IOS Vulnerabilies

In an environment where uptime and responsiveness are paramount and resources are at a premium, policies and procedures need to be put in place to ensure that all routers have an

IOS version installed to avoid exploits and vulnerabilities. Security procedures should require that IT staff visit on a regular basis and sign up for email distributions from the various exploit and vulnerability alert centers.

4.3 Choose a Routing Protocol

Unless this is an installation of a new network, a routing protocol is likely to be already in use. However, the routing protocol in use may not be the most secure protocol. Migrating from the current insecure protocol to a more secure protocol is recommended. Routing protocols provide security through the use of peer authentication. A major concern with any routing protocol is the possibility of a router accepting invalid routing updates. The routing protocols listed in the table are protocols that route IP, IPX and Appletalk only. If additional protocols are being routed the authentication available should be investigated.

Protocol Name	Authentication	Clear-Text	MD5 Hash	Protocol RFCs
RIPv1	No			RFC 1058
IGRP	No			Proprietary
RIPv2	Yes	Yes	Yes	RFC 1723
EIGRP	Yes		Yes	Proprietary
OSPFv2	Yes	Yes	Yes	RFC 2328
IS-IS	Yes	Yes		RFC 1142 (ISO 10589), 1195
BGPv4	Yes		Yes	RFC 1771
IPX RIP	No			
NLSP	No			
IPX EIGRP	No			
RTMP	No			
Appletalk EIGRP	No			
AURP	No			

Table 6 Authentication per routing protocol

4.4 Cisco IPv6 Configuration Commands

4.4.1 Basic Commands

To enable routing of IPv6 packets – required to enable IPv6 on a router:

```
Router(config)# ipv6 unicast-routing
```

To enable IPv6 on an interface:

```
Router(config-if)# ipv6 enable
```

To add an IPv6 address to an interface:

```
ipv6 address <address>/<prefix> [link-local] [eui-64]
```

To leave the interface unnumbered:

```
ipv6 unnumbered eth 0/0
```

4.4.1.1 IPv6 Enabled Commands

```
ping ipv6 <ipv6adr>
traceroute ipv6 <ipv6adr>
telnet <ipv6adr>
ssh [-l <userid>] [-c <des|3des>] [-o numberofpasswdprompts <#>] [-
p <port#>] <ipv6addr> [command]
show ip ssh
ip http server
dns lookup
tftp
```

4.4.2 Neighbor Discovery

To adjust the Router Advertisement intervals:

```
ipv6 nc reachable-time <#>
ipv6 nd ra-interval <#>          default is 200 seconds
ipv6 nd ra-lifetime <#>          default   is   1800   seconds   (30
minutes)
ipv6 nd ns-interval <#>          default is 1000 milliseconds
ipv6 nd suppress-ra
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
```

To adjust the lifetimes for the prefix:

```
ipv6  nd  prefix-advertisement  <routing-prefix>/<length>  <valid-
lifetime> <preferred-lifetime> [onlink] [auto-config]
ipv6 nd prefix-advertisement FEC0::C0A8:20C0/123 0 0 autoconfig
```

Valid lifetime = how long the node's address remains in the valid state – after that it is invalid

Preferred lifetime = how long the stateless autoconfig address remains preferred – less than or equal to the valid lifetime - If preferred-lifetime = 0 then this router is not preferred

Off-link = sets the L-bit to OFF – default setting is to have the L-bit set to ON

No-autoconfig = sets the A-bit to OFF – default setting is to have the A-bit set to ON

No-advertise = the specified prefix cannot be used for stateless autoconfiguration – the prefix is not included in RA messages – default is to have this flag turned OFF

To remove an advertised prefix:

```
no ipv6 nd prefix <ipv6-prefix>
```

To turn off Router Advertisements:

```
no suppress-ra
```

Duplicate Address Detection (DAD):

```
ipv6 nd dad attempts <#>         disabled with a setting of “0”
```

Router Redirection:

```
ipv6 redirects
ipv6 icmp error-interval msec
```

4.4.3 Other Commands

```
ip domain lookup
ip name-server <ipv6addr>
ipv6 host <NAME> [<port>] <ipv6addr1> <ipv6addr2> . . .
ipv6 neighbor <ipv6addr> Ethernet 0 <macaddr>
```

4.4.4 Basic Show Commands

```
show ipv6 ?
show ipv6 interface <interface-name-number> [prefix]
show interface
show ipv6 neighbors [ <ipv6addr-or-name> | <interfacetype-number> ]
show ipv6 mtu
show ipv6 protocols
show ipv6 interface [brief]
show ipv6 traffic
show ipv6 route
show ipv6 routers
show bgp
show bgp summary
show bgp ipv6 unicast 25eighbour <addr> routes
show bgp ipv6 unicast 25eighbour <addr> advertised
```

4.4.5 Basic Debug Commands

```
debug ipv6 ?
debug ipv6 packet
debug ipv6 icmp
debug ipv6 nd

ping ipv6 <ipv6addr>
traceroute ipv6 <ipv6addr>

clear ipv6 ?
clear ipv6 neighbors
```

4.4.6 Cisco Express Forwarding

```
ipv6 cef
ipv6 cef distributed
show ipv6 cef . . .
show cef
debug ipv6 cef [drops | events | hash | receive | table]
```

4.4.7 Routing Commands

```
ipv6 route <ipv6prefix>/<prefix-length> [ <next-hop-IPv6-addr> |
<interface-type-#> ] [AD#]
show ipv6 route [connected | local | static | rip | bgp | isis |
ospf]
show ipv6 route <ipv6prefix>/<prefix-length>
```

4.4.8 RIPng

To enable RIPng:

```
Router(config)# ipv6 router rip <TAG>
```

To enable RIPng on an interface:

```
Router(config-if)# ipv6 rip <TAG> enable
```

To originate the default router (::/0) out an interface:

```
Router(config-if)# ipv6 rip <TAG> default-information originate
Router(config-rtr)# distance <#>
Router(config-rtr)# distribute-list prefix-list <prefixlistNAME>
[in | out] <interface>
Router(config-rtr)# metric-offset <#>
Router(config-rtr)# poison-reverse
Router(config-rtr)# split-horizon
Router(config-rtr)# port <UDP-port> multicast-group <mcastaddr>
Router(config-rtr)# timers <update> <expire> <holddown> <garbage-
collect>
Router(config-rtr)# redistribute [ connected | isis | ospf | static
| bgp | rip <TAG> ] [metric <metric>] [level-1 | level-1-2 | level-
2] [route-map <NAME>]
```

4.4.8.1RIPng Show Commands

```
show ipv6 route
show ipv6 rip [database] [next-hops]
show ipv6 protocols
```

4.4.8.2 RIPng Debug Commands

```
debug ipv6 rip <interface>
debug ipv6 routing
clear ipv6 rip <TAG>
```

4.4.9 OSPF Commands

```
Router(config)# ipv6 router ospf <process-ID>
Router(config-rtr)# router-ID <ipv4addr>
Router(config-rtr)# area <v4areaID> range <ipv6addr/length>
Router(config)# interface 27thernet 0
Router(config-if)# ipv6 ospf <process-ID> area <v4areaID>
Router(config-rtr)# redistribute [bgp | isis | rip | static]
```

4.4.9.1 OSPF Show Commands

```
show ipv6 ospf <27rocessed>
show ipv6 ospf database
show ipv6 ospf <27rocessed> database link
show ipv6 ospf <27rocessed> database prefix
show ipv6 ospf route ospf
```

4.4.9.2 OSPF Debug Commands

```
clear ipv6 ospf <processed>
```

4.4.9.3 OSPF Example

```
interface Ethernet 0
 ipv6 address 2001:100:1::1/64
 ipv6 enable
 ipv6 ospf 100 area 0
interface Ethernet 1
 ipv6 address 2001:200:2::1/64
 ipv6 enable
 ipv6 ospf 100 area 1
ipv6 router ospf 100
 router-id 10.1.1.1
 area 1 range 2001:200:FFFF:1::1/64
```

4.4.10 EIGRP Commands

```
interface FastEthernet 0/0
 ipv6 enable
 ipv6 eigrp 10
ipv6 bandwidth-percent eigrp <as-number> <percent>
ipv6  summary-address  eigrp  <as-number>  <ipv6-address>  [admin-
distance]
ipv6 authentication mode eigrp <as-number> md5
ipv6 authentication key-chain eigrp <as-number> <key-chain>
!
ipv6 router eigrp 10
 router-id 10.1.1.1
 stub [receive-only | connected | static | summary | redistributed]
 log-neighbor-changes
 log-neighbor-warnings [seconds]
 metric weights tos k1 k2 k3 k4 k5
!
show ipv6 eigrp interfaces
show ipv6 eigrp neighbors detail
show ipv6 eigrp topology
show ipv6 eigrp traffic

clear  ipv6  eigrp  [as-number]  [neighbor  [ipv6-address  |  interface-
type interface-number]]

debug eigrp fsm
debug eigrp neighbor [siatimer] [static]
debug eigrp packet
debug  eigrp  transmit  [ack]  [build]  [detail]  [link]  [packetize]
[peerdown] [sia] [startup] [strange]
debug ipv6 eigrp [as-number] [neighbor ipv6-address | notification
| summary]
```

4.4.11 BGP4+ Commands

Enable BGP-4 on the router:

```
router bgp <ASN>
```

Turns off BGP IPv4 peering:

```
no bgp default ipv4 unicast
```

Establish a BGP4+ neighbor:

```
neighbor <ipv6addr> remote-as <ASN>
neighbor <ipv6addr> update-source <interface>
neighbor <ipv6addr> soft-reconfiguration inbound
neighbor <ipv6addr> password 5 <password>
```

Address Families:

```
address-family ipv6 unicast …
neighbor <ipv6addr> activate
exit-address-family
```

To enable a prefix-list for a BGP-peer:

```
neighbor <ipv6addr> prefix-list <NAME> [in | out]
ipv6 prefix-list <NAME> [ seq [#] ] [ permit | deny ]
<IPv6prefix/length> [ ge <min-value> ] [ le <max-value> ]
```

Route Maps:

```
neighbor <ipv6addr> route-map <NAME> [in|out]
route-map <NAME> [ permit | deny ] <seq#>
 match ipv6 [<ipv6addr> | next-hop | route-source] prefix-list
<prefixlistNAME>
 set ipv6 next-hop <ipv6addr> <link-local-addr>
 set local-pref 120
```

Redistribution:

```
redistribute [bgp | connected | isis | ospf | rip | static] [metric
<metric>] [route-map <routemapNAME>]
```

4.4.11.1 BGP4+ Show Commands

```
show ipv6 route bgp
show ipv6 neighbors
show bgp neighbors
show bgp ipv6 [summary]
show bgp ipv6 [<ipv6prefix/length> | community | community-list |
dampened-paths | regexp <regexp> | summary ]
show ipv6 prefix-list [summary | detail] <prefixlistNAME>
```

4.4.11.2 BGP4+ Debug Commands

```
debug bgp ipv6
clear bgp ipv6 [ * | ASN | <ipv6addr> | dampening | external |
flap-statistics | <peer-group-name> ]
```

4.4.11.3 BGP4+ Example

```
interface Ethernet0
ipv6 address 5f00:0100:0:0:1::1 80
!
router bgp 100
no bgp default ipv4-unicast
30eighbour 5f00:0100:0:0:2::1 remote-as 101
aggregate-address 2001:420:2000::/42 summary-only
!
address-family ipv6
30eighbour 5f00:0100:0:0:2::1 activate
30eighbour 5f00:0100:0:0:2::1 prefix-list bgp-in in
30eighbour 5f00:0100:0:0:2::1 prefix-list aggregate out
network 5f00:0100:0:0:1::/40
exit-address-family
ipv6 prefix-list aggregate seq 5 deny 3FFE:C00::/24 ge 25
ipv6 prefix-list aggregate seq 10 permit ::/0 le 48
!
ipv6 prefix-list bgp-in seq 5 deny 5F00::/8 le 128
ipv6 prefix-list bgp-in seq 10 deny ::/0
ipv6 prefix-list bgp-in seq 15 deny ::/1
ipv6 prefix-list bgp-in seq 20 deny ::/2
```

```
ipv6 prefix-list bgp-in seq 25 deny ::/3 ge 4
ipv6 prefix-list bgp-in seq 30 permit ::/0 le 128
```

4.4.12 IPv6 Access Control Lists

```
ipv6 access-list <NAME> [permit|deny] <src-prefix[*]> | any | host
<hostip> … <dest-prefix[*]> | any | host <hostip> … [log | log-
input]
ipv6 access-list BLAH deny fec0:0:0:2::/64 * any
ipv6 access-list BLAH permit any
```

Apply ACL to an interface:

```
Router(config-if)# ipv6 traffic-filter <ACL-NAME> [in | out]
```

For 6Bone – minimum prefix to announce:

```
3ffe::/16
3ffe:0800::/28
2000::/3                - 6to4
```

For 6Bone – prohibits advertisements of these:

```
fe80::/10               - link local
fec0::/10               - site local
::1/128                 - loopback
::0/128                 - default route
ff00::/8                - multicast
::/96                   - ipv4 compatible addresses
::ffff/96               - ipv4 mapped addresses
```

View the ACLs:

```
show ipv6 access-list <ACL-MANE>
clear ipv6 access-list <ACL-NAME>
debug ipv6 packet [access-list <ACL-NAME>] [detail]
```

4.4. 13 Configured Tunnel Router Commands

Router 1:

```
interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::3/27
 tunnel source 192.168.1.1
 tunnel destination 192.168.2.1
 tunnel mode ipv6ip [auto-tunnel]
```

Auto-tunnel if used for automatic tunnels

Router 2:

```
interface tunnel 0
 ipv6 address 3ffe:b00:c18:1::2/27
 tunnel source 192.168.2.1
 tunnel destination 192.168.1.1
 tunnel mode ipv6ip [auto-tunnel]
```

4.5 In-Band and Out-of-Band Communications

4.5.1 In-Band communications

Two major forms of in-band communications are available. They are SNMP and Telnet.

4.5.1.1 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a vulnerable service to use on an internetwork and should be used with caution. Many devices have community strings (which are SNMP passwords) of public for read-only access and private for read-write access. An SNMP sweep should be done of the routers on the internetwork. If either public or private is found, they should be removed immediately and replaced with strong passwords.

Multiple versions of SNMP are available: SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 provides for several important security features: message integrity, authentication and encryption. SNMPv3 uses HMAC-MD5 or HMAC-SHA for authentication and 56-bit DES for encryption. If possible, use a different MD5 secret value for sections of the network or for each router. The minimum IOS® software revision must be Release 12.0(3)T to enable all of the SNMPv3 commands below. SNMPv3 operates in a manner similar to privilege levels. Each user belongs to a group that determines their privileges. The three user groups are auth, noauth, and priv. The table below is taken from the Cisco Systems website:

Model	Level	Authentication	Encryption	What Happens
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	MD5 or SHA	No	Provides authentication based on the HMAC-MD5 or HMACSHA algorithms.
v3	authPriv	MD5 or SHA	DES	Provides authentication based on the HMAC-MD5 or HMACSHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard.

Table 7 User Groups in SNMP v3

The commands to enable SNMPv3 are:

Command	Description
snmp-server engineID local *engineid-string* | remote *ip-address* udp-port *port-number engineid-string*	Configures names for both the local and remote SNMP engine (or copy of SNMP) on the router.
snmp-server group *groupname* v3{auth | noauth | priv} access *access-list*	Configures a new SNMP group and maps the users to an access list.
snmp-server host *host* traps version 3 {auth | noauth | priv} udp-port *port notificationtype*	Configures the recipient of an SNMP trap operation.
snmp-server user *username groupname* remote *ip-address* udp-port *port* v3 *encrypted auth* {md5 | sha} *auth-password* [*priv des56 priv password*] [*access accesslist*]	Configures a new user to an SNMP group.

Table 8 Commands to enable SNMPv3

Local asynchronous terminals and dialup modems use standard lines, known as "TTYs". Remote network connections, regardless of the protocol, use virtual TTYs, or "VTYs". The best way to protect a system is to make certain that appropriate controls are applied on all lines, including both VTY lines and TTY lines.

4.5.1.2 Telnet

Telnet access should be secured using SSH. There are multiple versions of SSH available, but Cisco only supports SSH version 1.

Command	Description
line *line-number ending-line-number*	Identifies a line for configuration and enters line configuration mode.
(config-line) transport input ssh	Enable SSH access on VTY ports
(config-line) exec-timeout *minutes* [*seconds*]	Prevents an idle session from consuming a VTY indefinitely. Attackers could use idle sessions as a denial-of-service attack.
(config-line) service tcp-keepalives-in	Can help to guard against both malicious attacks and "orphaned" sessions caused by remote system crashes.
(config-line) session-limit *session-number*	Sets the maximum number of sessions. A small number of sessions may be useful in limiting risk, but leads to the opportunity for denial-of-service.

Table 9 Telnet Access

4.5.2 Out-of-Band Communications

The console port of a router has special privileges. Using the “password recovery” procedures found on the Cisco website (http://www.cisco.com), an attacker can gain control over the router. If no modem or terminal server is attached, the console port is protected because the router has been physically secured. However, an attacker who can crash the router, and who has access to the console port via a hardwired terminal, a modem, a terminal server, or some other network device, can take control of the system, even if they do not have physical access to it or the ability to log in to it normally. If these other methods to access the console are available, passwords and privilege levels should be used to limit access.

4.6 Choose a log server

A log server should be chosen on the network. It should be physically and logically secured. The server should be secured and hardened so that the logs on it will have a high deal of accuracy.

5.0 Establish Strong Password Controls and Secure Account Policies

5.1 Passwords

Protect Passwords with “Enable Secret”

To provide a layer of security, particularly for passwords that cross the network or are stored on a TFTP server, use the enable secret command. It allows you to establish an encrypted password that users must enter to access enable mode (the default), or any privilege level you specify.

Command	Description
enable secret *password*	Establish a new password or change an existing password for the privileged command level.

Table 10 Protect Passwords with Enable Secret

There is another type called the Enable Password. Anyone who gets a copy of the configuration file can easily crack this type of password. Several tools are available to crack these passwords. They include Password Decryption in the Solarwinds suite (www.solarwinds.net) and GetPass.exe from Boson (www.boson.com). A way to spot a password that uses this weak form of encryption in a configuration file would be to find a line that looks like “enable password 7 023c445a05024f0b43460758”. The 7 before the string of letters and numbers shows that the password was encrypted using a simple *“Vigenère”* cipher that is easy to break. However, enable secret passwords are not completely invulnerable. They are subject to “dictionary attacks” so copies of the configuration file should be protected from people who should not have access to them.

5.2 Privilege Levels

Cisco employs privilege levels to tighten security. By default, the Cisco IOS® software has two modes of password security: user mode (EXEC) and privilege mode (enable). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands. For example, if you want the configure command to be available to a more restricted set of users than the clear line command, you can assign level 2 security to the clear line command and distribute the level 2 password fairly widely, and assign level 3 security to the configure command and distribute the password to level 3 commands to fewer users.

To set the privilege level for a command:

Command	Description
privilege *mode* level *level command*	Set the privilege level for a command.
enable password level *level [encryptiontype] password*	Specify the enable password for a privilege level.

Table 11 Set Privilege level for a command

To change the default privilege level for a given line or a group of lines:

Command	Description
(config-line) privilege level *level*	Specify a default privilege level for a line.

Table 12 Change default privilege level

5.3 Banners

Banners are an important security consideration. Banners should be written that meet local, law considerations. Banners should NOT include verbiage that implies or states directly "Welcome". Sample banners are included for an Internet Service Provider, a company and a university. These sample banners are only included as a starting point. Care should be taken to write an appropriate banner based on the sensitivity of the data and the perceived threat. For example, a company manufacturing bombs should have a more stringent banner than a university with an open access policy.

Sample ISP Banner

****

Use is restricted to X Company authorised users who must comply with the Acceptable User Policy (AUP). Usage is monitored; unauthorised use will be prosecuted.

****

Sample Company Banner

****

You have logged on to a X Company proprietary device. INFORMATION IN THIS DEVICE BELONGS TO X COMPANY AND/OR ONE OF ITS AUTHORISED CLIENTS AND MAY NOT BE COPIED (IN WHOLE OR IN PART) IN ANY MANNER WITHOUT EXPRESS WRITTEN AUTHORISATION. This device may be used only for the authorised business purposes of X Company and/or its clients. Anyone found using this device or its information for any unauthorised purpose or personal use may be subject to disciplinary action and/or prosecution.

****

Sample University Banner

****

Unauthorised use of this machine is prohibited.
This is a University machine intended for University purposes.
The University reserves the right to monitor its use as necessary to ensure its stability, availability, and security.

****

To enable banners on a router, use the following command.

Command	Description
Banner login *banner text*	To print a banner message

Table 13 Enable banners on a router

5.4 Router Management with CiscoSecure ACS

CiscoSecure ACS can be a valuable tool to enhance security because a structure can be developed to specify command authorisation, set administrative privilege levels, and monitor router access. CiscoSecure ACS uses either TACACS+ or RADIUS to support those functions. Configuration of the CiscoSecure ACS machine, command/control browser, NAS, external database, and optional token card server are outside the scope of this document. Only commands specific to the routers to be managed are included.

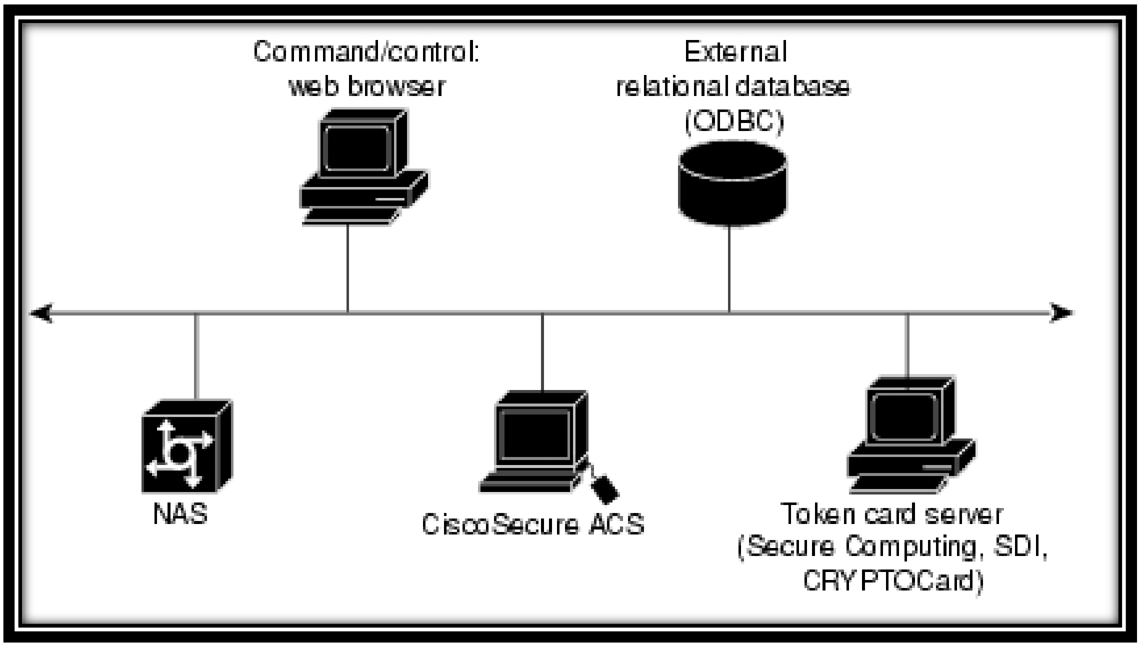


Figure 4 Overview of CiscoSecure ACS Configuration

The following command should be coded into router configuration.

Command	Description
tacacs-server host *IP address*	Identify the CiscoSecure TACACS+ server
tacacs-server key *key*	Identify the common key
aaa new-model	Global configuration command to enable aaa.
aaa authentication login default tacacs+	Enable aaa authentication with the TACACS+ as the method of authentication.
aaa authentication enable default tacacs+	Create a series of authentication methods that are used to determine whether a user can access the privileged EXEC command level.
aaa authorisation exec tacacs+ if authenticated	Contact the TACACS+ server to determine if users are permitted to start an EXEC shell when they login.
aaa authorisation commands 15 tacacs+ ifauthenticated	By default, privilege levels 0 and 15 are present in the Cisco IOS software. You can define other privilege levels on the router to further control authorisation. 15 is used here as an example.
aaa accounting commands 15 stop-only	Create an accounting method list and enable

tacacs+	accounting. The stop-only keyword instructs TACACS+ to send a stop record accounting notice at the end of the requested user process.

Table 14 Router Configuration with CiscoSecure ACS

5.5 Remove Unneeded Services

The following services should be disabled from security perspective. In global configuration mode, udp and tcp small services should be disabled. They are on by default in Cisco routers. The services are echo, chargen, daytime and discard. Finger is also on by default and should be disabled. Cisco Discovery Protocol (CDP) and Network Time Protocol (NTP) are on by default, and you should turn these off if you do not need them.

Command	Description
no service tcp-small-servers	When you disable the minor TCP/IP servers, access to the Echo, Discard, Chargen, and Daytime ports cause the Cisco IOS® software to send a TCP RESET packet to the sender and discard the original incoming packet.
no service udp-small-servers	When you disable the servers, access to Echo, Discard, and Chargen ports causes the Cisco IOS® software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
no ip bootp server	When you disable the BOOTP server, access to the BOOTP ports cause the Cisco IOS software to send an "ICMP port unreachable" message to the sender and discard the original incoming packet.
no service finger	To disallow Finger protocol requests (defined in RFC 742) to be made of the network server, use this global configuration command. This service is equivalent to issuing a remote show users command.
no ip source-route	To discard any IP datagram containing a source-route option use this command. It is not good practice to allow IP sourcerouting due to implicit tunneling attacks.
no ip identd	The ip identd command returns accurate information about the host TCP port; however, no attempt is made to protect against unauthorised queries.
no ip http server	To remove the ability to use http to manage Cisco routers. This is very important

	considering IOS® HTTP Authorisation vulnerability.
no cdp run	To prevent information gathering about routers.
ntp disable	If you must run NTP, configure NTP only on required interfaces, and configure NTP to listen only to certain specified peers.

Table 15 Remove unneeded services

5.6 Secure Interfaces

The following commands should be used on the interface level to make specific interfaces more secure.

Command	Description
(config-if) shutdown	All unused interfaces should be in the shutdown state.
(config-if) no ip proxy-arp	To prevent internal addresses from being revealed. (This is important to do if you do not already have NAT configured to prevent internal addresses from being revealed).
(config-if) no ip directed-broadcast	The command should be applied to every LAN interface that isn't known to forward legitimate directed broadcasts. It is the default is IOS version 12.0 and later.

Table 16 Secure interfaces

5.7 Cisco Access Control Lists

Access lists have several purposes. They are to serve as a security filter for traffic coming in from the Internet, to filter traffic to and from business partners, and for intra-company traffic to keep specific areas within the country secure. The first item, blocking traffic from the Internet is fairly well understood and documented. B2B connections are generally treated in the same manner as a connection to the Internet so access principles are the same. Securing traffic within a corporation is a less understood mechanism. For example, if human resources has sensitive information and is on a subnet with other departments, there is a higher risk of compromise than if human resources is on another subnet and has an access list that denies traffic.

There are two general stances on access lists. In the first stance, the access list specifically denies certain traffic and allows all else. The second stance is when the access list allows certain traffic and, by default, denies all else. The second stance is generally considered more secure and is the default that Cisco uses.

Cisco recommends the following access list to protect against spoofing.

Command	Description
ip access-group *list* in	Used on an incoming interface to apply the below access-list
access-list *number* deny icmp any any redirect	Blocks all ICMP redirects
access-list *number* deny ip 127.0.0.0 0.255.255.255 any	Blocks packets originating from a loopback address
access-list *number* deny ip 224.0.0.0 31.255.255.255 any	Blocks packets originating from a multicast address
access-list *number* deny ip host 0.0.0.0 any	Blocks packets originating from 0.0.0.0 address

Table 17 Access list to protect against spoofing

The final line could negatively impact BOOTP/DHCP clients and should be tested before wide implementation. The Common Sense Rules of Network Changes should be followed. A final note on access lists is that recording violations of access lists can be a useful tool in detecting attack patterns. By adding the log-input keyword, access list violations will be recorded along with the interface from which the packet was received and the MAC address of the host that sent it. That keyword should be used when an intrusion is suspected carefully because of the impact on system performance.

6.0 Logging, Monitoring and Updating the System

6.1 Turn on logging

Logging is a powerful tool when used on a regular basis. Servers are not the only equipment that should have logging turned on. Cisco router logs also provide useful information. Cisco allows granularity when specifying what actions should be logged. Cisco routers can provide an immense quantity of real time status information to support network management simply by enabling the system logging facility.

Command	Description
service timestamps log datetime msecs	Add the date and time to syslog messages.
logging *host*	Specify the host name or IP address of the host where you want to send syslog messages.
logging facility *facility*	Eight facilities LOCAL0(16) through LOCAL7(23); the default is LOCAL4(20). Hosts file the messages based on the facility number in the message.
logging trap *level*	(Optional) Use this command to limit messages logged to the syslog servers based on severity.

Table 18 Logging

There are seven logging levels. They are:

Level	Description
0 – emergencies	System unusable messages
1 – alerts	Take immediate action
2 – critical	Critical condition
3 – errors	Error message
4 – warnings	Warning message
5 – notifications	Normal but significant condition
6 – informational	Information message
7 – debugging	Debug messages and log FTP commands and WWW URLs

Table 19 Logging Levels

6.2 Monitor the Logs

Best practices indicate that logs are useless unless they are reviewed on a regular basis. To understand better what is happening on your system, it is recommended that you check your logs often and look for unusual entries. For instance, you have to see what is happening at 2AM when there is not supposed to be anyone on your system. If you see something, make sure you know what is and why it is running at 2AM.

Automating the analysis of router logs is essential to allow using the router logs as a proactive network management tool. Many tools are available to make reviewing log files easier. One example is SWATCH.

6.3 Change Management

According to Fred Nickols, there are two meanings to change management. One meaning of managing change refers to the making of changes in a planned and managed or systematic fashion. The aim is to more effectively implement new methods and systems in an ongoing organisation. The changes to be managed lie within and are controlled by the organisation. However, these internal changes might have been triggered by events originating outside the organisation, in what is usually termed "the environment." Hence, the second meaning of managing change, namely, the response to changes over which the organisation exercises little or no control (e.g., legislation, social and political upheaval, the actions of competitors, shifting economic tides and currents, etc).

These two meanings to change management apply to the types of routers defined above: Internet gateway routers, corporate internal routers and B2B routers. Corporate internal routers are generally considered to lie within and be controlled completely by the organisation. Internet gateway routers and B2B routers respond to changes external to the organisation and may require changes based on external stimuli. A change management process is invaluable for security. It assures that changes to devices are made in a logical, orderly manner and facilitates good security measures.

Example. A remote site has a router managed by the IT department that currently is only connected to the corporate WAN and they want to add a local connection to the Internet. If a proper change management program is in place, the remote site will need to submit a request to have the new link added. This change can then be reviewed against the corporate security policy to ensure that it does not violate the policy, reviewed by technical staff to ensure that the link is properly secured with ACLs and other measured specified according to security procedures developed to adhere to the security policy. Then the change can be scheduled and implemented with an understanding of how the new link will affect the security of the entire corporation. After the scheduled change has been implemented, tests should be conducted to verify that the changes have not invalidated security measures.

6.4 Common-Sense Rules of Network Changes

Having a method for network changes is an important step in a successful change. A method can include planning, configuring and documentation. It is a good idea to choose a method and use it faithfully in order to have successful network changes.

There are several items that make up a sensible plan for network changes:

1. Consult experts (internal and/or external)
2. Develop network change plan
3. Develop test plan
4. Develop backout plan
5. Validate plans against corporate security policy
6. Test the configuration in a lab
7. Backup current production configurations
8. Inform stakeholders about changes and change timing (via a Change Management process)
9. Implement changes off-peak in a pilot group, if possible
10. Implement changes off-peak for entire network
11. Test applications
12. Backout (if necessary)

These rules have been developed over time in response to many situations that have arisen based on changes made that were not planned. Based on the size of the network changes, it could require a full-time project manager and a number of staff for months or could require one person for a week.

6.5 Router Security Checklist

This security checklist is designed to help you review your router security configuration, and remind you of any security area you might have missed.

1. Router security policy written, approved, distributed.
2. Router IOS version checked and up to date.
3. Router configuration kept off-line, backed up, access to it limited.
4. Router configuration is well-documented, commented.
5. Router users and passwords configured and maintained.
6. Password encryption in use, enable secret in use.
7. Enable secret difficult to guess, knowledge of it strictly limited. (if not, change the enable secret immediately)
8. Access restrictions imposed on Console, Aux, VTYs.
9. Unneeded network servers and facilities disabled.
10. Necessary network services configured correctly (e.g. DNS)
11. Unused interfaces and VTYs shut down or disabled.
12. Risky interface services disabled.
13. Port and protocol needs of the network identified and checked.
14. Access lists limit traffic to identified ports and protocols.
15. Access lists block reserved and inappropriate addresses.
16. Static routes configured where necessary.
17. Routing protocols configured to use integrity mechanisms.
18. Logging enabled and log recipient hosts identified and configured.
19. Router's time of day set accurately, maintained with NTP.
20. Logging set to include consistent time information.
21. Logs checked, reviewed, archived in accordance with local policy.
22. SNMP disabled or enabled with good community strings and ACLs.

6.6 The Cost of Security

Securing the internetwork of a medium to large corporation is a monumental task. Security has many costs, some of which are obvious and some of which are hidden. These costs need to be known and understood.

6.6.1 Obvious Costs

Obvious costs include the cost of routers, servers, license upgrades, and personnel to run the systems. For example, new routers may need to be purchased in order to take advantage of new technologies. Costs for routers could also include maintenance costs for software upgrades. A new server may be required to take advantage of CiscoSecure. Personnel costs consist of the salaries of administrators as well as the cost of benefits such as health insurance and training. A cost benefit analysis should be conducted to ensure that the cost of the security measures is in line with the value of the corporate assets being protected.

6.6.2 Hidden Costs

According to Network Computing, ongoing tests have proved that there are significant performance penalties once you enable ACLs, especially long ones such as the 200-line list that we used in our tests, because an access list cannot always take advantage of the fastest switching technique that might otherwise be available on the router. Many security measures on a router use additional memory and CPU utilization. These measures can adversely affect performance. A decision needs to be made weighing the benefits of the security measures versus the costs related to performance.

5.0 Conclusion

Securing routers is an important part in hardening our networks, but it is only one step amongst many. This document gives you a broad overview of the methods that can be used in order to secure a Cisco IOS system device. If you secure the device, it increases the overall security of the networks that you manage. The protection of the management and control is discussed and recommendations for configuration are supplied. Where it is applicable, sufficient detail is provided for the configuration of associated features. However, those features are most effective when applied as part of a comprehensive security strategy.

6.0 References

- Router Security Configuration Guide, National Security Agency, United States of America
- Router Security Guidance Activity of the Systems and Network Attack Center (SNAC), National Security Agency, United States of America
- Cisco IPv6 Configuration Commands: www.hoggnet.com
- SANS Institute InfoSec Reading Room: Cisco Router Hardening Step-by-Step
- SANS Institute InfoSec Reading Room: Router Audit Tool: Securing Cisco Routers Made Easy!
- Cisco Website: www.cisco.com