CERT-In

Indian Computer Emergency Response Team

Handling Computer Security Incidents

Cisco Router Security Best Practices

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

Issue Date: June 10, 2004

Table of Contents

1. Introduction

This document provides Guideline for securing a typical enterprise perimeter (Gateway) router.

** Security issues related to routing protocols (BGP, OSPF, RIP, VRRP etc) are beyond the scope of this document.

****** Latest IOS version available from CISCO (www.cisco.com) should be used.

2. Access Management

I. Console –

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router (config)# line con 0
Router (config-line)# login local  //Enforce local user login; Local user must be created
Router (config-line)# exec-timeout 5 0 //Set automatic session timeout
```

IOS - Create local users -Create at least one local user with password to enable console login

```
Router(config)# username user_name password <Password>
```

II. Auxiliary port-

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

III. VTY -

Disable access through VTY (Telnet)

```
Router(config)# no access-list 90
Router(config)# access-list 90 deny any log
Router(config)# line vty 0 4
Router(config-line)# access-class 90 in
Router(config-line)# transport input none
Router(config-line)# login local
Router(config-line)# exec-timeout 0 1
```

Securing VTY (Telnet) if required

Allow only specific IP to telnet the Router

```
Router(config)# ip telnet source-interface loopback0
Router(config)# access-list 99 permit IP_allowed log
Router(config)# access-list 99 deny any log
Router(config)# line vty 0 4
Router(config-line)# access-class 99 in
Router(config-line)# exec-timeout 5 0
Router(config-line)# transport input telnet
Router(config-line)# transport output none    ---Disable telnet outside
Router(config-line)# login local
Router(config)# service tcp-keepalives-in
```

Disable unnecessary VTY lines

```
Router(config)# no line vty 5
```

IV. Enable Secret

```
Router(config)#enable secret <My_Secret_Password>
```

3. Disable unnecessary Services

```
Router(config)# no service finger
Router(config)# no ip identd
Router(config)# no ip finger
Router(config)# no ip http server
Router(config)# no service tcp-small-servers
Router(config)# no service udp-small-servers
Router(config)# no ip bootp server
Router(config)# no cdp run
Router(config)# no service config   -- Disable loading of remote configs.
Router(config)# no tftp-server INSTANCE
Router(config)# no boot network
Router(config)# no ip domain-lookup
```

4. SNMP Security

Disable SNMP if not in use.

Router(config)# no snmp-server

If the network requires SNMP, then configure an SNMP ACL and hard-to-guess SNMP community strings.

```
Router(config)# no snmp community public ro
Router(config)# no snmp community private rw

Router(config)# access-list 51 permit Permited_IP_Address
Router(config)# snmp community Your_Password ro 51
```

5. Routing Rules

I. Turn off opportunities for crafted spoof attacks & probes

Router(config-if)# no ip directed-broadcast *// Disable IP directed broadcast on each interface*
Router(config-if)# no ip proxyarp *// Disable proxy ARP*

```
Router(config-if)# no ip directed-broadcast // Disable directed broadcast
Router(config-if)# no ip unreachables  // Disable host unreachable reply
Router(config-if)# no ip mask-reply  // Disable mask reply message
Router(config-if)# no ip redirects  //Disable ip redirects
Router(config)# no ip source-route // Disable source routing.
Router(config)# service tcp-keepalives-in  // Use tcp keepalives to kill sessions
where the remote side has died.
```

II. Unicast reverse path forwarding

```
Router(config)# ip cef
Router(config-if)# ip verify unicast reverse-path
```

// Unicast Reverse Path Forwarding (RPF) helps to mitigate problems caused by malformed or forged IP source addresses passing through a router.
Reference
http://www.cisco.com/univercd/cc/td/doc/product/software/ios111/cc111/uni_rpf.htm

6. Access control lists

The ACLs mentioned here are designed for restricting inbound traffic of a perimeter router.

******The access_list number (101) given is user defined. User can change it as per their requirement
******The access list has to be applied to inbound traffic on external interface.

I. Filter all RFC 1918,3330 address space and special/reserved addresses

```
Router(config)# access-list 101 deny ip 10.0.0.0  0.255.255.255 any log
Router(config)# access-list 101 deny ip 172.16.0.0  0.15.255.255 any log
Router(config)# access-list 101 deny ip 192.168.0.0  0.0.255.255 any log
Router(config)# access-list 101 deny ip 127.0.0.0  0.255.255.255 any log
Router(config)#access-list 110 deny ip 192.0.2.0 0.0.0.255 any log
Router(config)# access-list 101 deny ip 255.0.0.0 0.255.255.255 any log
Router(config)# access-list 101 deny ip 224.0.0.0 7.255.255.255 any log
Router(config)# access-list 101 deny ip host 0.0.0.0 any log
Router(config)#access-list 110 deny ip host 255.255.255.255 any log
Router(config)# access-list 101 deny ip 169.254.0.0  0.0.255.255 any log
```

II. Apply ingress filtering (RFC 2827)

Stop spoofing Deny anything source address as own address

```
Router(config)#access-list 101 deny ip my_network_id any log
```

III. Permit the required services for the required IP Addresses only

!! Incoming Requests

! Permit access to Public web, Mail

```
access-list 101 permit tcp any host web_server_ip  eq www
access-list 101 permit tcp any host mail_server_ip  eq smtp
```

! Allow DNS request to DNS Servers

```
access-list 101 permit tcp any host dns_server_ip eq domain
access-list 101 permit tcp any host dns_server_ip eq domain
access-list 101 permit udp any host dns_server_ip eq domain
access-list 101 permit udp any host dns_server_ip eq domain
```

!! Return traffic

! Allow only ACKed tcp packets to your network or only to specific IP's accessing Internet

```
access-list 101 permit tcp any my_network gt 1023 established
```

! Allow DNS query return traffic

```
access-list 110 permit udp any eq 53  host DNS_Client_IP gt 1023
```

! Allow FTP Clients return traffic

```
access-list 110 permit tcp any eq 20 my_network gt 1023
```

! Permit limited ICMP message types

```
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 echo-reply
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 net-unreachable
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 host-unreachable
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 port-unreachable
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 packet-too-big
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 administratively-prohibited
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 source-quench
access-list 101 permit icmp any 100.100.100.0  0.0.0.15 ttl-exceeded
```

IV. Block everything else

```
Router(config)# access-list 101 deny ip any any log
```

V. Apply the following on the External Interface as in

```
Router(config-if)# ip access-group 101 in
```

VI. OutBound ACLs

Include all ACLs of section 6.1

Permit packets only from own network only

```
access-list 102 permit ip My_network any
```

Deny and log everything else

7. Logging

Turn on the Router's logging capability, send all log errors and blocked packets to an trusted syslog server.

```
Router(config)# logging buffered
Router(config)# logging syslog_server_ip
```

8. Benchmark

Use Benchmarking tools to verify the configuration. Suggested benchmarking tool-

http://www.cisecurity.org/

9. Reference

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml

NSA Cisco Router Guide - http://nsa2.www.conxion.com/