

## Executive Summary

This card is a supplement to the NSA/SNAC Router Security Configuration Guide. It describes quick but effective ways to tighten the security of a Cisco router, along with some important general principles for maintaining good router security. For more information, consult the sections of the main guide listed with each recommendation.

### General Recommendations

1. Create and maintain a router security policy. The policy should identify who is allowed to log in to the router, who is allowed to configure and update it, and should outline the logging and management practices for it. [Section 3.4]
2. Comment and organize the offline edition of router configuration file! This sounds fluffy despite being a big security win. Also, keep the offline copy of all router configurations in sync with the actual configuration running on the routers. This is invaluable for diagnosing suspected attacks and recovering from them. [Section 4.1]
3. Implement access list filters by permitting only those protocols and services that the network users really need, and denying everything else. [Section 3.2, 4.3]
4. Run the latest available General Deployment (GD) IOS version. [Sections 4.5.5, 8.3]
5. Test the security of your routers regularly, especially after any major configuration changes. [Section 6]

### Specific Recommendations: Router Access

1. Shut down unneeded servers on the router. Servers that are not running cannot break. Also, more memory and processor slots are available. Start by running the `show proc` command on the router, then turn off clearly unneeded facilities and services. Some servers that should almost always be turned off and the corresponding commands to disable them are listed below. [Section 4.2, 4.5.3]
  - Small services (echo, discard, chargen, etc.)
    - `no service tcp-small-servers`
    - `no service udp-small-servers`
  - BOOTP - `no ip bootp server`
  - Finger - `no service finger`
  - HTTP - `no ip http server`
  - Identd - `no ip identd` (some IOS versions)
  - SNMP - `no snmp-server`
2. Shut down unneeded services on the routers. These services allow certain packets to pass through the router, or send special packets, or are used for remote router configuration. Some services that should almost always be turned off and the corresponding commands to disable them are listed below. [Section 4.1, 4.2]
  - CDP - `no cdp run`
  - Remote config. - `no service config`
  - Source routing - `no ip source-route`
  - Zero subnet - `no ip subnet-zero`
3. The interfaces on the router can be made more secure by using certain commands in the Configure Interface mode. These commands should be applied to every interface. [Section 4.1, Section 4.2]
  - Unused interfaces - `shutdown`
  - No Smurf attacks - `no ip directed-broadcast`
  - Ad-hoc routing - `no ip proxy-arp`
4. The console line, the auxiliary line and the virtual terminal lines on the router can be made more secure in the Configure Line mode. The console line and the virtual terminal lines should be secured as shown below. The Aux line should be disabled, as shown below, if it is not being used. [Section 4.1]

- Console Line - `line con 0`  
`exec-timeout 5 0`  
`login`  
`transport input telnet`
- Auxiliary Line - `line aux 0`  
`no exec`  
`exec-timeout 0 10`  
`transport input none`
- VTY lines - `line vty 0 4`  
`exec-timeout 5 0`  
`login`  
`transport input telnet`

5. Passwords can be configured more securely as well. Configure the Enable Secret password, which is protected with an MD5-based algorithm. Also, configure passwords for the console line, the auxiliary line and the virtual terminal lines. Provide a basic protection for the passwords for these lines by using the `service password-encryption` command. See examples below. [Section 4.1]
  - Enable secret - `enable secret 0 2manyRt3s`
  - Console Line - `line con 0`  
`password Soda-4-jimmy`
  - Auxiliary Line - `line aux 0`  
`password Popcorn-4-sara`
  - VTY Lines - `line vty 0 4`  
`password Dots-4-georg3`
  - Basic protection - `service password-encryption`
6. Do not disclose the contents of your router configuration file to unauthorized individuals.

### Specific Recommendations: Access Lists

1. Always start an access-list definition with the privileged command `no access-list nnn` to clear out any previous versions of access list `nnn`. [Section 4.3]

```
East(config)# no access-list 51
East(config)# access-list 51 permit host 14.2.9.6
East(config)# access-list 51 deny any log
```
2. Log access list port messages properly. For reasons of efficiency, Cisco IOS doesn't look at an entire packet header unless it has to. To ensure that logs contain correct port number information, use the special port range arguments shown below.

```
no access-list 106
access-list 106 deny udp any range 1 65535
any range 1 65535 log
access-list 106 deny tcp any range 1 65535
any range 1 65535 log
access-list 106 deny ip any any log
```

The last line is necessary to ensure that rejected packets of protocols other than TCP and UDP are properly logged. [Section 4.3]
3. Allow only internal addresses to enter the router from the internal interfaces, enforce this using access-lists. Block illegal addresses at the outgoing interfaces. Besides preventing an attacker from using the router to attack other sites, it helps identify poorly configured internal hosts and networks. This approach may not be feasible for very complicated networks. [Section 4.3]

```
East(config)# no access-list 101
East(config)# access-list 101 permit ip
10.1.1.0 0.0.0.255 any
East(config)# access-list 101 deny udp any
range 1 65535 any log
East(config)# access-list 101 deny tcp any
range 1 65535 any log
East(config)# access-list 101 deny ip any any log
East(config)# interface eth 1
East(config-if)# ip access-group 101 in
East(config-if)# exit
East(config)# interface eth 0
East(config-if)# ip access-group 101 out
```

4. Block packets coming from the outside (untrusted network) that are obviously fake or are commonly used for attacks. This protection should be part of the overall design for traffic filtering at the router interface attached to the external, untrusted network. [Section 4.3, see also RFC 1918]
5. Block packets that claim to have a source address of any internal (trusted) networks. This impedes some TCP sequence number guessing attacks and related attacks. Incorporate this protection into the access lists applied to interfaces connected to any untrusted networks. [Section 4.3]
6. Block incoming loopback packets (network 127.0.0.0). These packets cannot be real. Block reserved IP addresses (network 10.0.0.0, 172.16.0.0-172.31.0.0, 192.168.0.0). [Section 4.3 and RFC 1918]
7. If the network does not need IP multicast, then block multicast packets.
8. Block broadcast packets. (Note that this may block DHCP and BOOTP services, but these services should not be used on external interfaces.)
9. A number of remote attacks use ICMP redirects, block them. (A superior but more difficult approach is to permit only necessary ICMP packet types.)

The example below shows one way to implement these recommendations.

```
North(config)# no access-list 107
North(config)# ! block internal addresses
North(config)# access-list 107 deny ip
14.2.0.0 0.0.255.255 any log
North(config)# access-list 107 deny ip
14.1.0.0 0.0.255.255 any log
North(config)# ! block loopback/reserved addresses
North(config)# access-list 107 deny ip
127.0.0.0 0.255.255.255 any log
North(config)# access-list 107 deny ip
10.0.0.0 0.255.255.255 any log
North(config)# access-list 107 deny ip
172.16.0.0 0.15.255.255 any log
North(config)# access-list 107 deny ip
192.168.0.0 0.0.255.255 any log
North(config)# ! block multicast (if not used)
North(config)# access-list 107 deny ip
224.0.0.0 0.0.255.255 any
North(config)# ! block broadcast
North(config)# access-list 107 deny ip
host 0.0.0.0 any log
North(config)# ! block ICMP redirects
North(config)# access-list 107 deny icmp
any any redirect log
North(config)# interface eth 0/0
North(config-if)# ip access-group 107 in
```

10. Block incoming packets that claim to have the same destination and source address (i.e. a 'Land' attack on the router itself). Incorporate this protection into the access list used to restrict incoming traffic into each interface, using a rule like the one shown below. [Section 4.3]

```
no access-list 102
access-list 102 deny ip host 10.2.6.250
host 10.2.6.250 log
access-list 102 permit ip any any

interface Eth 0/0
ip address 10.2.6.250 255.255.255.0
ip access-group 102 in
```

11. Configure an access list for the virtual terminal lines to control telnet access. See example commands below. [Section 4.1, Section 4.6]

```
South(config)# line vty 0 4
South(config-line)# access-class 92 in
South(config-line)# exit
South(config)# no access-list 92
South(config)# access-list 92 permit 10.1.1.1
South(config)# access-list 92 permit 10.1.1.2
```

## Specific Recommendations: Logging & Debugging

1. Turn on the router's logging capability, and use it to log errors and blocked packets to an internal (trusted) syslog host. Make sure that the router blocks syslog traffic from untrusted networks. See example commands below. [Section 4.5]

```
Central(config)# logging on
Central(config)# logging 10.1.1.200
Central(config)# logging buffered
Central(config)# logging console critical
Central(config)# logging trap debugging
Central(config)# logging facility local1
```

2. Configure the router to include time information in the logging. Point to two different NTP servers to ensure availability of good time information. This will allow an administrator to trace network attacks more accurately. See example commands below. [Sections 4.2, 4.5]

```
service timestamps log datetime
localtime show-timezone
clock timezone EST -5
clock summer-time EDT recurring
ntp source Ethernet0/1
ntp server 192.5.41.40
ntp server 192.5.41.41
```

3. If you are using SNMP, then select and configure hard-to-guess SNMP community strings. The example commands below show how to remove the default community strings and set a better read-only community string. [Section 4.5]

```
East(config)# no snmp community public
East(config)# no snmp community private
East(config)# snmp community BTR-18+never
```

## 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.

- Router security policy written, approved, distributed.
- Router IOS version checked and up to date.
- Router configuration kept off-line, backed up, access to it limited.
- Router configuration is well-documented, commented.
- Router users and passwords configured and maintained.
- Enable password difficult to guess, knowledge of it strictly limited. (if not, change the password immediately)
- Access restrictions imposed on Console, Aux, VTYs.
- Unneeded network services disabled.
- Unused interfaces disabled.
- Risky interface services disabled.
- Port and protocol needs of the network identified and checked.
- Access lists limit traffic to identified ports and protocols.
- Access lists block reserved and inappropriate addresses.
- Static routes configured where necessary.
- Routing protocols configured to use integrity mechanisms.
- Logging enabled and log recipient hosts identified and configured.
- Router's time of day set accurately, maintained with NTP.
- Logging set to include time information.
- Logs checked, reviewed, archived in accordance with local policy.
- SNMP disabled or enabled with hard-to-guess community strings.