Executive Summary

This card is a supplement to the NSA/SNAC Router Security Configuration Guide version 1.1. 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 written 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 offline master editions of your router configuration files! This sounds fluffy despite being a big security win. Also, keep the offline copies of all router configurations in sync with the actual configurations running on the routers. This is invaluable for diagnosing suspected attacks and recovering from them. [Section 4.1]
3. Implement access lists that allow only those protocols, ports and IP addresses that are required by network users and services, and that deny 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 services 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`
   - 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`
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`
   - Mask replies `- no ip mask-reply`
   - 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
     ```
   - 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 ssh
     ```
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 basic protection for the user and line passwords 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. Consider adopting SSH, if your router supports it, for all remote administration. [Section 5.3]
7. Protect your router configuration file from unauthorized disclosure.

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 number *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. To ensure that logs contain correct port number information, use the port range arguments shown below at the end of an access list.
   ```
       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. Enforce traffic address restrictions using access lists. On a border router, allow only internal addresses to enter the router from the internal interfaces, and allow only traffic destined for internal addresses to enter the router from the outside (external interfaces). 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 or networks. This approach may not be feasible for complicated networks. [Section 4.3, also RFC 2827]
   ```
   East(config)# no access-list 101
   East(config)# access-list 101 permit ip
           14.2.6.0 0.0.0.255 any
   East(config)# access-list 101 deny ip any any log
   East(config)# no access-list 102
   East(config)# access-list 102 permit ip
           any  14.2.6.0 0.0.0.255
   East(config)# access-list 102 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
   East(config-if)# ip access-group 102 in
   ```

4. Block packets coming from the outside (untrusted network) that are obviously fake or have source or destination addresses that are reserved, for example networks 0.0.0.0/8, 10.0.0.0/8, 169.254.0.0/16, 172.16.0.0/12, 192.168.0.0/16. This protection should be part of the overall traffic filtering at the interface attached to the external, untrusted network. [Section 4.3, see also RFC 1918]

5. Block incoming packets that claim to have a source address of any internal (trusted) networks. This impedes TCP sequence number guessing and other attacks. Incorporate this protection into the access lists applied to interfaces facing any untrusted networks. [Section 4.3]

6. Drop incoming packets with loopback addresses, network 127.0.0.0/8. These packets cannot be real. [Section 4.3]

7. If the network doesn't 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 and certainly shouldn't cross border routers.)

9. A number of remote probes and attacks use ICMP echo, redirect, and mask request messages, 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 our 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 special/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
    0.0.0.0 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
    169.254.0.0 0.0.255.255 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 15.255.255.255 any
North(config)# ! block some ICMP message types
North(config)# access-list 107 deny icmp
    any any redirect log
North(config)# access-list 107 deny icmp
    any any echo log
North(config)# access-list 107 deny icmp
    any any mask-request log
North(config)# access-list 107 permit ip
    any 14.2.0.0 0.0.255.255
North(config)# access-list 107 permit ip
    any 14.1.0.0 0.0.255.255
North(config)# interface Eth 0/0
North(config-if)# description External interface
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]

```
access-list 102 deny ip host 14.1.1.250
    host 14.1.1.250 log
interface Eth 0/1
ip address  14.1.1.250 255.255.0.0
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)# no access-list 92
South(config)# access-list 92 permit 14.2.10.1
South(config)# access-list 92 permit 14.2.9.1
South(config)# line vty 0 4
South(config-line)# access-class 92 in
```

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 14.2.9.1
Central(config)# logging buffered 16000
Central(config)# logging console critical
Central(config)# logging trap informational
Central(config)# logging facility local1
```

2. Configure the router to include time information in the logging. Configure at least 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]

```
East(config)# service timestamps log datetime
               localtime show-timezone msec
East(config)# clock timezone GMT 0
East(config)# ntp server 14.1.1.250
East(config)# ntp server 14.2.9.1
```

3. If your network requires SNMP, then configure an SNMP ACL and 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, with an ACL. [Section 4.5]

```
East(config)# no snmp community public ro
East(config)# no snmp community private rw
East(config)# no access-list 51
East(config)# access-list 51 permit 14.2.9.1
East(config)# snmp community BTRl8+never ro 51
```

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.

□ 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.

□ Password encryption in use, enable secret in use.

□ Enable secret difficult to guess, knowledge of it strictly limited.
(if not, change the enable secret immediately)

□ Access restrictions imposed on Console, Aux, VTYs.

□ Unneeded network servers and facilities disabled.

□ Necessary network services configured correctly (e.g. DNS)

□ Unused interfaces and VTYs shut down or 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 consistent time information.

□ Logs checked, reviewed, archived in accordance with local policy.

□ SNMP disabled or enabled with good community strings and ACLs.