Cisco IOS

Router Checklist Procedure Guide

02 December 2005

Supplement to the Network Infrastructure Checklist V6R1

DISA
FIELD SECURITY OPERATIONS

This page is intentionally left blank.

TABLE OF CONTENTS

NET0400 5
NET0410 7
NET0425 8
NET0430 9
NET0440 10
NET0465 11
NET0645 12
NET0650 13
NET0655 14
NET0665 15
NET0670 16
NET0680 17
NET0681 18
NET0682 19
NET0685 20
NET0690 21
NET0740 22
NET0800 23
NET0810 24
NET0820 25
NET0890 26
NET0894 27
NET0910 28
NET0920 29
NET0940 30
NET0950 31
NET0960 33
NET0980 34
NET0990 35
NET1000 36
NET1020 37
NET1021 38
NET1070 39

This page is intentionally left blank.

NET0400

Requirement: *The router administrator will ensure neighbor authentication with MD5 is implemented for all routing protocols with all peer routers within the same or between autonomous systems (AS).*

Procedure: Determine what routing protocols have been implemented on the edge with external peers as well as internally. With the exception of external NIPRNet or SIPRNet peers, neighbor authentication must be implemented using MD5. The following routing protocols support MD5: BGP, OSPF, IS-IS, EIGRP, and RIP V2. Following are some sample configurations for BGP, OSPF, and EIGRP neighbor authentication.

BGP

router bgp 100
 neighbor external-peers peer-group
 neighbor 171.69.232.90 remote-as 200
 neighbor 171.69.232.90 peer-group external-peers
 neighbor 171.69.232.100 remote-as 300
 neighbor 171.69.232.100 peer-group external-peers
 neighbor 171.69.232.90 **password** xxxxxxxxxx
 neighbor 171.69.232.100 **password** xxxxxxxxxx

Note: The neighbor/password statement can be applied to either the peer-group or the neighbor definition.

OSPF

interface Ethernet0
 ip address 10.10.10.10 255.255.255.0
 ip ospf **message-digest-key** 10 **md5 mypassword**

router ospf 10
 network 10.10.0.0 0.0.255.255 area 0
 area 0 **authentication message-digest**

Note: Authentication has to be enabled for each area. In OSPF, an interface belongs to only one area; hence, there would always be a network statement under the OSPF process ID for each interface that has OSPF traffic. The network statement defines the area in which the network belongs.

The MD5 key-id and password is defined under each interface connected to an OSPF neighbor.

EIGRP

interface Ethernet0
ip address 10.10.10.10 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp **1 mypassword**
.
.
.
key chain mypassword
key 12345
key-string abcdefg
accept-lifetime infinite
.
.
.
router eigrp **1**
network 10.0.0.0
no auto-summary

NET0410

Requirement: *The router administrator will restrict BGP connections to known IP addresses of neighbor routers from a trusted AS.*

Procedure: Review the running configuration to ensure that BGP connections are only from known neighbors in a trusted AS by restricting TCP port 179 to specific IP addresses.

Using an Ingress ACL

interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group **101 in**
.
.
.
access-list 101 permit tcp host 192.168.1.1 host 192.168.1.2 **eq 179**
.
.
.
access-list 101 deny ip any any

Using an IP Receive ACL

The IP Receive ACL feature can also be used to filter traffic that is destined for the router. The filtering occurs after any ingress ACL on the interface in which the traffic enters. Following is an example using an IP Receive ACL:

ip receive access-list 100
access-list 100 deny icmp any any fragments
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 permit tcp host 192.168.1.1 any eq **bgp**
access-list 100 deny ip any any

Note: This feature is currently only supported on 7500 and 12000 series routers with 12.0 (24)S and 12.0(22)S respectively.

NET0425

Requirement: *The IAO/NSO will ensure the lifetime of a MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.*

NOTE: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains. This check is in place to ensure keys do not expire creating a DOS due to adjacencies being dropped and routes being aged out. The recommendation is to use two rotating six month keys with a third key set as infinite lifetime. The lifetime key should be changed 7 days after the rotating keys have expired and redefined.

Procedure: Review the running configuration to determine if key authentication has been defined with an infinite lifetime.

RIP 2 **Example**

```
interface ethernet 0
  ip rip authentication key-chain trees
  ip rip authentication mode md5

router rip
 network 172.19.0.0
 version 2

key chain trees
key 1
  key-string willow
  accept-lifetime 22:45:00 Feb 10 2005 22:45:00 Aug 10 2005
  send-lifetime 23:00:00 Feb 10 2005 22:45:00 Aug 10 2005
key 2
  key-string birch
  accept-lifetime 22:45:00 Aug 9 2005 22:45:00 Feb 10 2006
  send-lifetime 23:00:00 Aug 9 2005 22:45:00 Feb 10 2006
key 9999
  key-string maple
  accept-lifetime 22:45:00 Feb 9 2005 infinite
  send-lifetime 23:00:00 Feb 9 2005 infinite
```

EIGRP **Example**

```
interface ethernet 0
 ip authentication mode eigrp 1 md5
 ip authentication key-chain eigrp 1 trees

router eigrp 1
network 172.19.0.0

key chain trees
key 1
key-string willow
accept-lifetime 22:45:00 Feb 10 2005 22:45:00 Aug 10 2005
send-lifetime 23:00:00 Feb 10 2005 22:45:00 Aug 10 2005
key 2
key-string birch
 accept-lifetime 22:45:00 Dec 10 2005 22:45:00 Feb 10 2006
 send-lifetime 23:00:00 Dec 10 2005 22:45:00 Jan 10 2006
 key 9999
 key-string maple
 accept-lifetime 22:45:00 Feb 9 2005 infinite
 send-lifetime 23:00:00 Feb 9 2005 infinite
```

NOTE: When using MD5 authentication keys, it is imperative the site is in compliance with the NTP policies. The router has to know the time!

NOTE: Must make this a high number to ensure you have plenty of room to put keys in before it. All subsequent keys will be decremented by one (9998, 9997…)

NET0430

Requirement: *The IAO/NSO will ensure that an authentication server is used to gain administrative access to all routers.*

Procedure: Verify that an authentication server is required to access the router by reviewing the running configuration. You should find an authentication statement similar to the example below:

aaa new-model
aaa authentication login ***list-name*** **tacacs+** local
.
.
tacacs-server host x.x.x.x
tacacs-server key xxxx
.
.
line vty 0 4
login authentication ***list-name***

The *aaa new-model* statement must be present as it enables AAA. The authentication *list-name* defined in the *aaa authentication* statement must be specified for console and vty access via the login statement as shown above. The authentication server must be defined to the router (i.e., tacacs-server, radius-server) and must be reachable; otherwise, the next available authentication method specified in the *list-name* will be used (i.e. local).

NET0440

Requirement: *The IAO/NSO will ensure that when an authentication server is used for administrative access to the router, only one account is defined locally on the router for use in an emergency (i.e., authentication server or connection to the server is down).*

Procedure: Review the running configuration and verify that only one local account has been defined. An example of a local account is shown in the example below:

username xxxxxxx password 7 xxxxxxxxxxx

NET0465

Requirement: *The router administrator will ensure that all user accounts are assigned the lowest privilege level that allows them to perform their duties.*

Procedure: There are 16 possible privilege levels that can be specified for users in the router configuration. The levels can map to commands, which have set privilege levels--or you can reassign levels to commands. Usernames with corresponding passwords can be set to a specific level. There would be several username *name* password *password* followed by username *name* privilege *level*. The user will automatically be granted that privilege level upon logging in. Below is an example of assigning a privilege level to a local user account and changing the default privilege levels of the configure terminal command.

username junior-engineer1 **privilege 7** password xxxxxx
username senior-engineer1 **privilege 15** password xxxxxx
privilege exec level 7 configure terminal

Note The above example only covers local accounts, you will still need to check the accounts and their associated privilege levels configured in the authentication server. You can also use TACACS for even more granularity at the command level.

Below is an example of CiscoSecure TACACS+ server

```
user = junior-engineer1 {
      password = clear "xxxxx"
      service = shell  {
           set priv-lvl = 7
      }
}
```

NET0645

Requirement: *The IAO/NSO will ensure that all OOB management connections to the router require passwords*

Procedure: Review each router's configuration to ensure that the console port and the vty ports used by the OOBM network require a login prompt. The configuration should look similar to the following:

line con 0
login authentication admin_only
exec-timeout 10 0
line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh

NET0650

Requirement: *The router administrator will ensure the router console port is configured to time out after 10 minutes or less of inactivity.*

Procedure: Review each Cisco router configuration to ensure that the console is disabled after 15 minutes of inactivity. The configuration should look similar to the following:

line con 0
login authentication admin_only
exec-timeout 10 0

Note: the default is 10 minutes.

NET0655

Requirement: *The router administrator will ensure that the router's auxiliary port is disabled.*

Procedure: View each Cisco router's configuration to ensure that the auxiliary port is disabled with a configuration similar to the following:

line aux 0
no exec
transport input none

NET0665

Requirement: *The IAO/NSO will ensure that all in-band management connections to the router require passwords.*

Procedure: Review each router's configuration to ensure that the VTY ports require a login prompt. The configuration should look similar to the following:

line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh

NET0670

Requirement: *The router administrator will ensure that the router only allows in-band management sessions from authorized IP addresses from the internal network.*

Procedure: Review all Cisco router configurations and verify that only authorized internal connections are allowed on VTY ports. The configuration should look similar to the following:

```
access-list 3 permit 192.168.1.10 log
access-list 3 permit 192.168.1.11 log
access-list 3 deny any
        .
.
line vty 0 4
access-class 3 in
```

NET0680

Requirement: *The router administrator will ensure in-band management access to the router is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.*

Procedure: Review all Cisco router configurations and verify that only ssh is allowed on the VTY ports. The configuration should look similar to the following:

line vty 0 4
transport input **ssh**

NET0681

Requirement: *The router administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shutdown after 60 seconds or less.*

Procedure: Review the global configuration or have the router administrator execute the *show ssh* command to verify the timeout is set for 60 seconds or less. The default is 120 seconds. The configuration should look similar to the following:

ip ssh time-out 60

NET0682

Requirement: *The router administrator the maximum number of unsuccessful SSH login attempts iss set to three, locking access to the router.*

Procedure: Review the global configuration or have the router administrator execute the *show ssh* command to verify the authentication retry is set for 3. The default is 3.

ip ssh authentication-retries 3

NET0685

Requirement: *The router administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.*

Procedure: Review each router's configuration to ensure that the VTY ports are disabled after 15 minutes of inactivity. The configuration should look similar to the following:

line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh

Note: default is 10 minutes

NET0690

Requirement: *The router administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.*

Procedure: Review each Cisco router configuration to ensure that all connection attempts to the VTY ports are logged.

access-list 3 permit 192.168.1.10 **log**
access-list 3 permit 192.168.1.11 **log**
access-list 3 deny any **log**
.
line vty 0 4
access-class 3 in

NET0740

Requirement: *The router administrator will ensure HTTP, FTP, and all BSD r-command servers are disabled.*

Procedure: Review all Cisco router configurations to verify that the IOS command *no ip http server* is present

Note: HTTP server is not available with IOS releases prior to 11.0. Also, *http-server* is disabled by default in IOS version 12.0; hence the *no ip http-server* command will not appear in the running configuration.

FTP, RCP, and RSH are disabled by default. Review all Cisco router configurations to verify that none of the following statements are present:

ftp-server enable
ip rcmd rcp-enable
ip rcmd rsh-enable
.
.
.
line vty 0 4
transport input rlogin telnet

Note: Rlogin is not actually supported by IOS other than via Kerberos. However, the rlogin keyword must be specified on the vty transport statement to allow any r-command to the Cisco router.

NET0800

Requirement: *The router administrator will ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.*

Procedure: For IOS version 12.0 and later review the running configuration of the premise router and ensure the following commands are not present on all external interfaces: *ip unreachables, ip redirects,* and *ip mask-reply.* For versions prior to 12.0, ensure the following commands are present: *no ip unreachable, no ip redirects,* and *no ip mask-reply.* The configuration should look similar to the following:

interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group 101 in
no ip redirects
no ip unreachables
no ip mask-reply

In addition, host unreachable messages will be sent in reply to black-hole routes. Be sure that the Null0 interface also has *no ip unreachable* defined if there are static routes destined for this interface.

interface null0
no ip unreachables

NET0810

Requirement: *The IAO/NSO will ensure that two Network Time Protocol (NTP) servers are defined on the premise router to synchronize its time.*

Procedure: Review the router configurations and verify that NTP servers have been defined similar to the following example:

ntp update-calendar
ntp server 129.237.32.2
ntp server 142.181.31.6

If the software clock is synchronized to an outside time source via NTP, it is a good practice to periodically update the hardware clock with the time learned from NTP. Otherwise, the hardware clock will tend to gradually drift, and the software clock and hardware clock will become out of synch with each other. The *ntp update-calendar* command will enable the hardware clock to be periodically updated with the time specified by the NTP source.

CAVEAT: Since IOS uses the software clock for logging, synching the hardware clock is not a requirement—only a best practice. Lower end models such as 2500/2600 series do not have hardware clocks, so this command is not available on those platforms.

NET0820

Requirement: *The IAO/NSO will ensure that the DNS servers are defined if the router is configured as a client resolver.*

Procedure: Review the running configuration to ensure that DNS servers have been defined if the router had been configured as a client resolver. The configuration should look similar to one of the following examples:

```
 ! configure as client resolver and specify DNS server
ip domain-lookup
ip name-server 192.168.1.253
```

or

```
! disable client resolver
no ip domain-lookup
```

Note: ip domain-lookup is enabled by default.

NET0890

Requirement: *The router administrator will restrict SNMP access to the router from only authorized internal IP addresses.*

Procedure: Review all router configurations to ensure ACLs are in place to limit SNMP access to specific NMS hosts using a configuration similar to the following:

access-list **10** permit host **7.7.7.5**
snmp-server community <clear text string> ro **10**

NET0894

Requirement: *The router administrator will ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.*

Procedure: Review all Cisco router configurations to ensure SNMP access from the network management stations is read only. The configuration look similar to the following:

access-list 10 permit host 7.7.7.5
snmp-server **community** xxxxxxxxx **ro** 10

NET0910

Requirement: *The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in DOD Instruction 8551.1 for all ports and protocols required for operational commitments.*

Procedure:

1. Determine Boundary- Determined by Connectivity, not Destination. ACLs use source and destination addresses. PPS defines boundary by physical connectivity. All Federal Agencies are not DOD!

2. NOTE on Enclave to Enclave: If data traffic between Enclaves transverses a router not owned by the Enclave's DAA then it falls into the "Boundary 7&8 DoD Network to Enclave or other applicable category for that particular connectivity.

3. Block by specifying ports on permit statements when in deny-by-default **or** explicitly block all known red ports.

4. All ports and protocols allowed into the enclave should be registered in the PPS database.

Review the CISCO premise router configuration to ensure ACLs are in place to restrict inbound IP addresses are filtered to permit only green or yellow ports. Red and yellow ports are permitted with conditions noted on the Category Assignment List (CAL). A DSAWG 2 year expiration date listed on the PPS CAL will indicate expiration of permits for particular red ports. The router configuration should look similar to following highlighted:

interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group 100 in
.
.
access-list 100 deny ip <internal network range> <wildcard mask> any log
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log
access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.0.2.0 0.0.0.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
access-list 100 deny ip 240.0.0.0 7.255.255.255 any log
access-list 100 permit tcp [external network] [wildcard mask] any eq ##
access-list 100 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 100 deny ip any any log

NET0920

The router administrator will bind the ingress ACL filtering packets entering the network to the external interface, and bind the egress ACL filtering packets leaving the network to the internal interface—both on an inbound direction.

Note: All filters must be applied to the appropriate interfaces on an inbound direction. Ingress filtering is applied to all traffic entering the enclave; hence, this filter would be bound to all external interfaces. Since egress filtering is applied to all traffic leaving the enclave, this filter would be bound to all internal interfaces.

Procedure: Review the running configuration of the premise router and verify that all interfaces, with the exception of loopback interfaces, have the appropriate ingress or egress ACL applied to with an inbound direction. An example configuration is depicted below:

interface FastEthernet 0/0
description **NIPRNet link**
ip address 199.36.92.1 255.255.255.252
ip access-group 100 **in**

interface FastEthernet 1/0
description **downstream link to our network**
ip address 199.36.90.1 255.255.255.0
ip access-group 102 **in**

Note: The default direction for the *ip access-group* command is *out*.

NET0940

Requirement: *The router administrators will restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network, any local host loop back address (127.0.0.0/8), the link-local IP address range (169.254.0.0/16), IANA unallocated addresses or any reserved private addresses in the source field*.

Procedure: Review the Cisco premise router configuration to ensure ACLs are in place to restrict inbound IP addresses. The router configuration should look similar to following:

interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group **100 in**
.
.
.
access-list 100 deny ip <**internal network range**> <wildcard mask> any log
access-list 100 deny ip 0.0.0.0 0.255.255.255 any log

access-list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.0.2.0 0.0.0.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 224.0.0.0 15.255.255.255 any log
access-list 100 deny ip 240.0.0.0 7.255.255.255 any log

NET0950

Requirement: *The router administrator will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Reverse Path Forwarding.*

Procedure for egress ACL: Review the premise router configuration to ensure egress ACLs are in place on all internal interfaces to restrict the router from accepting outbound IP packets that contain an external IP address in the source field. In order to comply with the deny-by-default policy, permit statements for those ports that are allowed will have to be defined followed by the deny any statement. The permit statements must qualify the source address with the internal network address range. Following is an example configuration:

interface FastEthernet 0/0
description **downstream link to our network**
ip address 199.36.90.1 255.255.255.0
ip access-group 102 **in**
.
.
.
access-list 102 permit tcp any any established
access-list 102 permit udp host [external DNS] any eq domain
access-list 102 permit udp host [external DNS] any gt 1023
access-list 102 permit tcp [**internal network**] [wildcard mask] any eq ftp-data
access-list 102 permit tcp [**internal network**] [wildcard mask] any eq ftp
access-list 102 permit tcp [**internal network**] [wildcard mask] any eq http
access-list 102 permit . . . . . .
access-list 102 deny any

Procedure for Unicast Reverse Path Forwarding: Review the premise router configuration to ensure RPF has been configured on all internal interfaces. Following is an example configuration:

interface FastEthernet 0/0
description **downstream link to our network**
ip address 199.36.90.1 255.255.255.0
ip verify unicast reverse-path 197
!
access-list 197 deny ip any any log

Note: If no ACL is specified in the Unicast RPF command, the router drops the forged or malformed packet immediately and no ACL logging occurs.

A unicast RPF check performs a route table lookup on an IP packet's source address, and checks the incoming interface. The router determines whether the packet is arriving from a path that the

sender would use to reach the destination. If the packet is from a valid path, the router forwards the packet to the destination address. If it is not from a valid path, the router discards the packet.

Best practice is to implement Unicast RPF downstream from the premise router, preferably at the distribution layer or at the edges of the network. The further downstream Unicast RPF is applied, the finer the granularity you have in mitigating address spoofing and in identifying the sources of spoofed addresses. Applying Unicast RPF on the premise router helps mitigate attacks from many downstream networks and it is easier to administer, but it makes it harder to identify the source of the attack.

NET0960

Requirement: *The IAO/NSO will implement features provided by the router to protect servers from any TCP SYN flood attacks from an outside network.*

Procedure: Review the premise or edge router configuration to ensure the TCP intercept command is in place to intercept any TCP SYN connection requests. The configuration should like similar to the following:

ip tcp intercept list 107
access-list 107 permit tcp any <internal network> < wildcard mask>

NET0980

Requirement: *The router administrator will block all inbound ICMP messages with the exception of Echo Reply (type 0), and Time Exceeded (type 11). ICMP message number 3, code 4, are permitted inbound with the following exception: Must be denied from external AG addresses, otherwise permitted.*

Procedure: Review the Cisco premise router configuration to ensure that the ingress ACL blocks all inbound ICMP traffic message types with the exception of Echo Reply (type 0), Time Exceeded (type 11), and Destination Unreachable (type 3). The ACL should look similar to the following:

interface FastEthernet 0/0
description to NIPRNet core router
ip address 199.36.92.1 255.255.255.252
ip access-group **100 in**
.
.
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any time-exceeded
access-list 100 permit icmp 199.36.90.0 0.0.255.255 any packet-too-big
access-list 100 **deny icmp any any** log

Note: The above ACL could also look similar to the following using the icmp type codes instead of the icmp message type:

access-list 100 permit icmp any any 0
access-list 100 permit icmp any any 11
access-list 100 permit icmp any any 3
access-list 100 deny icmp any any log

NET0990

Requirement: *The router administrator will block outbound ICMP traffic message types except Echo Request (type 8), Parameter Problem (type 12), and Source Quench (type 4) Destination Unreachable - Fragmentation Needed and Don't Fragment was Set (type3, code 4).*

Procedure: Review the Cisco premise router configuration to ensure egress ACLs are bound to the proper interfaces to block all outbound ICMP traffic message types except Echo, Parameter Problem, Source Quench, and Destination Unreachable - Fragmentation Needed and Don't Fragment was Set. The configuration should look similar to the following:

interface FastEthernet 0/0
description **link to our network**
ip address 199.36.90.1 255.255.255.0
ip access-group 102 in
.
.
.
access-list 102 permit icmp 199.36.90.0 0.0.255.255 any echo
access-list 102 permit icmp 199.36.90.0 0.0.255.255 any parameter-problem
access-list 102 permit icmp 199.36.90.0 0.0.255.255 any source-quench
access-list 102 permit icmp 199.36.90.0 0.0.255.255 any packet-too-big
access-list 102 **deny icmp any any** log

NET1000

Requirement: *The router administrators will block all inbound traceroutes to prevent network discovery by unauthorized users.*

Procedure: Review the premise router configuration to ensure that an ingress ACL is in place to block inbound UDP 33400 through 34400, which are the ports commonly used by the traditional traceroute application. The ingress ACL should look similar to the following:

interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group **100 in**
.
access-list **100** deny **udp** any any range **33400 34400** log
access-list 100 deny ip any any

There are two methods that can be used to block the new inbound traceroute request by a Cisco router: IP Options Selective Drop Feature, which was introduced with IOS release 12.0(23), and ACL Support for Filtering IP Options Feature that is available with IOS Release 12.3(4)T or later. The IP Options Selective Drop Feature can be configured in one of two modes: drop or ignore. If the global command *ip options ignore* is configured, the router will still process the packet as normal while ignoring the IP Options field. The ACL Support for Filtering IP Options Feature can be used to selectively filter and drop packets based on specific option values.

The premise router must be configured to block any packet with the value of 82 in the IP Options fields either by configuring the global command *ip options drop* in addition to the ACL shown above to block the traditional traceroute or creating an extended named ACL for the ingress filter that would include ACL statements to block both traceroute methods. An example would look as follows:

interface FastEthernet 0/0
description NIPRNet link
ip address 199.36.92.1 255.255.255.252
ip access-group **ingress-filter** in
.
ip access-list extended **ingress-filter**
deny ip any any **option traceroute** log
deny **udp** any any range **33400 34400** log
.
deny ip any any

Note: Resource Reservation Protocol (RSVP) used by MPLS, Internet Group Management Protocol Version 2 (IGMPv2), and other protocols that use the IP options field may not function in either *drop* or *ignore* modes.

NET1020

Requirement: *The router administrator will ensure that all attempts to any port, protocol, or service that is denied are logged.*

Procedure: Review the running configuration of the premise router and verify that both the router's ingress and egress ACLs have a *log* keyword following every deny statement. An example configuration is depicted below:

access-list 100 permit tcp . . . . . .
access-list 100 permit tcp . . . . . .
access-list 100 permit tcp . . . . . .
.
.
.
access-list 100 deny any **log**

NET1021

Requirement: *The router administrator will configure all routers to log severity levels 0 through 6 and send log data to a syslog server.*

Procedure: Review all router configurations to ensure that all routers log messages for severity levels 0 through 6. By specifying *informational*, all severity levels above will be included.

Logging Level	**Severity Level**	**Description**
Emergencies	0	
Alerts	1	Immediate Action Required
Critical	2	Critical Conditions
Errors	3	Error Conditions
Warnings	4	Warning Conditions
Notifications	5	Normal but Significant Conditions
Informational	6	Informational Messages
Debugging	7	Debugging Messages

A sample configuration would look similar to the following:

logging on
logging host 192.168.1.22
logging console critical
logging trap informational
logging facility local7

Note: The command *logging on* is the default. If you see the command *no logging on*, then all logging except console logging will be disabled. The default trap level is *informational* so if a logging trap command were not present this would imply *logging trap informational*.

NET1070

Requirement: *The IAO/NSO will authorize and maintain justification for all tftp implementations.*

Procedure: Interview the router administrator to see how they transfer the router configuration files to and from the router. Verify that the running configuration for all Cisco routers have statements similar to the following:

ip ftp username xxxxxxxxx
ip ftp password 7 xxxxxxxxxxxxxxxxxx

Following are some alternative approaches that are actually more secured than using FTP:

1. If the router is equipped with PCMCIA Flash Memory Cards, you can copy IOS images as well as configurations to these cards (i.e., slot0, slot1).

2. Copy and paste from a *show run* while in a SSH session or HyperTerminal (i.e., Capture Text) console connection. The file can then be saved onto a floppy disk and stored in a secured location. Defaults will not be included since most of the IOS defaults are not displayed on a *show run* command.

3. Secure Copy Protocol (SCP)

Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the Cisco router. SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level. SCP allows a user who has appropriate authorization to copy any file that exists in the Cisco IOS File System (IFS) to and from a router by using the *copy* command. An authorized administrator may also perform this action from a workstation.

An example configuration would look as follows:

! AAA authentication and authorization must be configured for SCP to work.
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
.
.
.
! SSH must be configured.
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable