Detailed Instructions

Part 1: Validate network connectivity and note initial state of routers.

Your network is configured using OSPF, BGP and static routing to provide network connectivity between the remote site and the hub site as depicted in **Figure 1** below. The goal of this part of the lab is to validate connectivity to each of the routers from the Windows 2000 server connected to the *Remote_J23* router. You should also observe the initial state of each router. i.e. CPU, configuration, interface statistics, IGP and BGP neighbors, etc…

Note: Each of the routers are configured with the **username=xxx and password=xxx**.

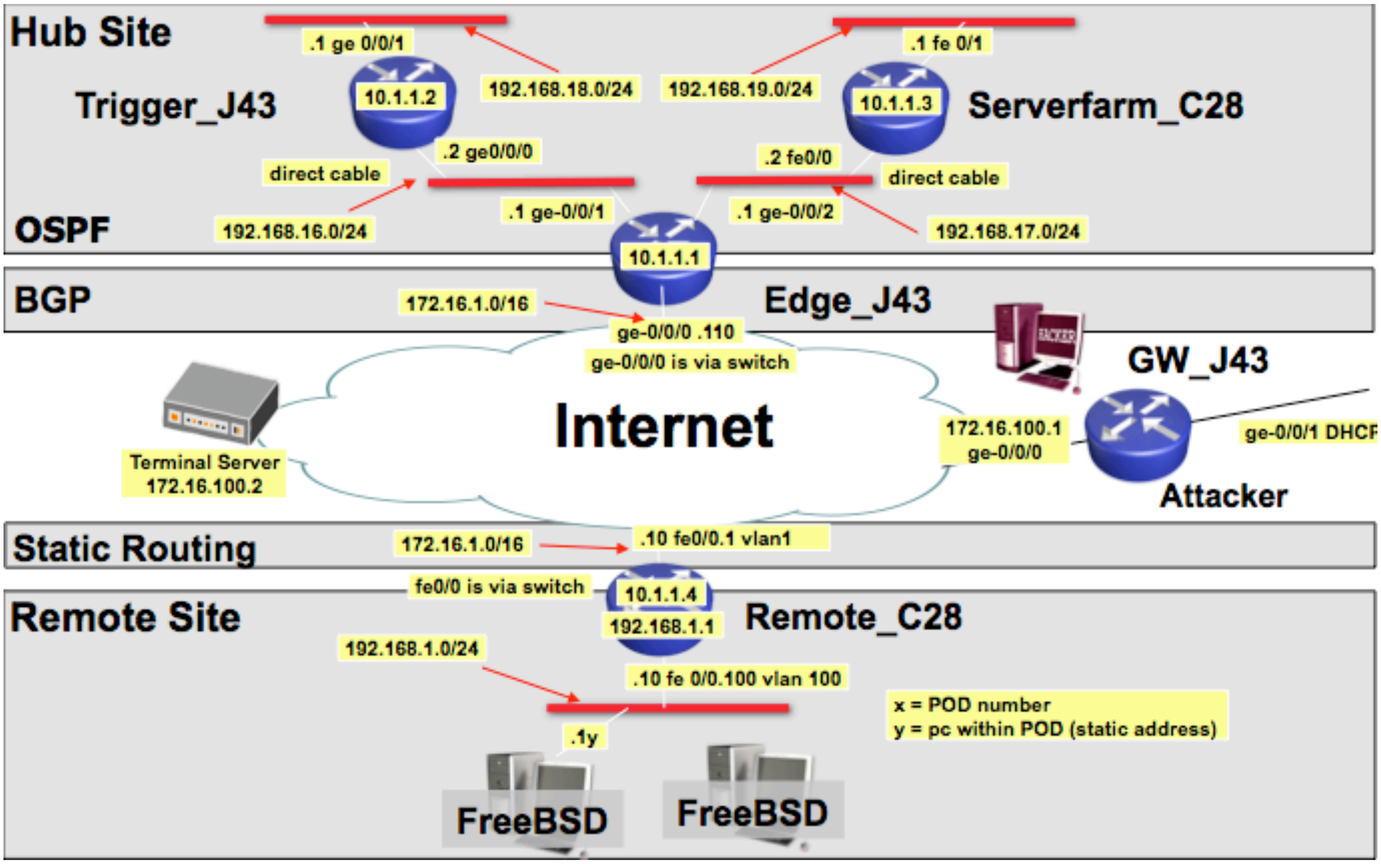


Figure 1: Lab Network topology, addressing and routing

Step 1 Access the Ubuntu station that is available on your lab pod.

Step 2 From the FreeBSD station, open a command prompt and telnet to the loopback address of each of the routers in your network to ensure network connectivity. NOTE: each of the routers are configured with **username=xxx and password=xxx**.

Step 3 Observe the initial state of each of the routers:

- CPU
- Interface statistics

- Routes
- Configuration
- IGP neighbors
- BGP neighbors
- Etc…

Step 4 Once you have validated network connectivity and made note of the initial state of the routers, close all telnet sessions to your routers.

Step 5 Use ping to monitor connectivity to the *Trigger_J63* router by opening another command prompt on the FreeBSD station and starting a continuous ping to the 10.1.1.2 address.

```
Ping –t 10.1.1.2
```

Note: You will use this ping as your management tool indicating the health of your network. If pings are successful, then your network is operating normally. However, if your pings begin to fail, then this is an indication that your network may be experiencing a security incident – an attack, worm manifestation, etc…

Part 2: Detection and Mitigation of Attack 1

Note: Before proceeding with this part of the lab, please inform the Lab Proctor.

During this part of the lab, you will experience an attack on your network. Your goal is to determine where the attack is coming from, what routers are being affected, how are the routers being affected and then mitigate the attack. After mitigating the attack, you should have full connectivity within your network and your routing protocols should be stable.

Note: Use your continuous ping that you started in the previous section, as an indication of network stability in your network.

Step 6 You receive a call from Joe User stating that response time and connectivity is poor giving you an indication that something is happening on the network.

Step 7 Observe the output of your ping that is running on your FreeBSD station. Are all responses successful?

Step 8 From the FreeBSD station, open up a command prompt and telnet to the loopback of each of your routers and make note of the following:

- Can you still access all of your routers from the FreeBSD station?
- Do you have good response time to all of the routers?
- Is your routing protocol stable and are neighbors staying up?

Hint: If you are not able to access all routers via telnet to perform the investigation in the next step, you may need to access the routers via console access using the device access window from LabOps.

Hint: You may find it helpful to open up a telnet window to each of the routers and reflect on the Lab topology to help with troubleshooting the security event.

Step 9 Investigate and identify what kind of attack is occurring on the network. Determine the following:

- What routers are being affected?
- How are the routers affected?
- What type of attack is happening?
- Where is the attack coming from? Where is it entering the network?
- What is the source address of the attack?
- What addresses/ports are being targeted?

Hint: Would flow information help with your investigation. Check out the following URL: Cisco IOS Netflow and Security

Step 10 After determining the characteristics of the attack and where the attack is entering the network, mitigate the attack without using access-lists.

Note: Do not use the Access Control Lists to mitigate the attack.

Hint: What is the source address(es) of the attack? Do you have routes to these addresses in your router?

Step 11 Once the attack has been mitigated, validate the following:

- Ping responses from your continuous ping on your FreeBSD station are all successful.
- Telnet to the loopback of each of your routers to make sure you have connectivity to all of your routers and make note of the following
  - You should have good response time to each of your routers.
  - OSPF neighbors and routing should be stable.
  - CPU should be at a reasonable rate

Questions:

What feature did you use to identify the attack?

What other features could you have used to identify the attack?

Did the feature you used to identify the attack affect your router CPU? Is this what you expected?

What feature did you use to mitigate/drop the attack packets and why?

Where in your topology should the attack be mitigated? Should you apply the same command elsewhere in the network?

What command can you use to show attack packets are being mitigated/dropped?

What other features could have been used to mitigate the attack?

Once the attack has been mitigated and your network connectivity is restored and stable, you have successfully completed this part of the lab.

Part 3: Preparing your routers for future attacks.

Note: Before proceeding with this part of the lab, please inform the Lab Proctor.

An important part of maintaining a stable network is to follow the Six Phase Methodology of securing your router. The Six phase methodology consists of the following phases:

Preparation – Minimize your exposure to attacks by configuring the various Infrastructure Security features before an attack occurs. i.e. be prepared for attacks before they occur. This is the phase where you should also create and train your security response team, setup your communication process, create your tools and practice.

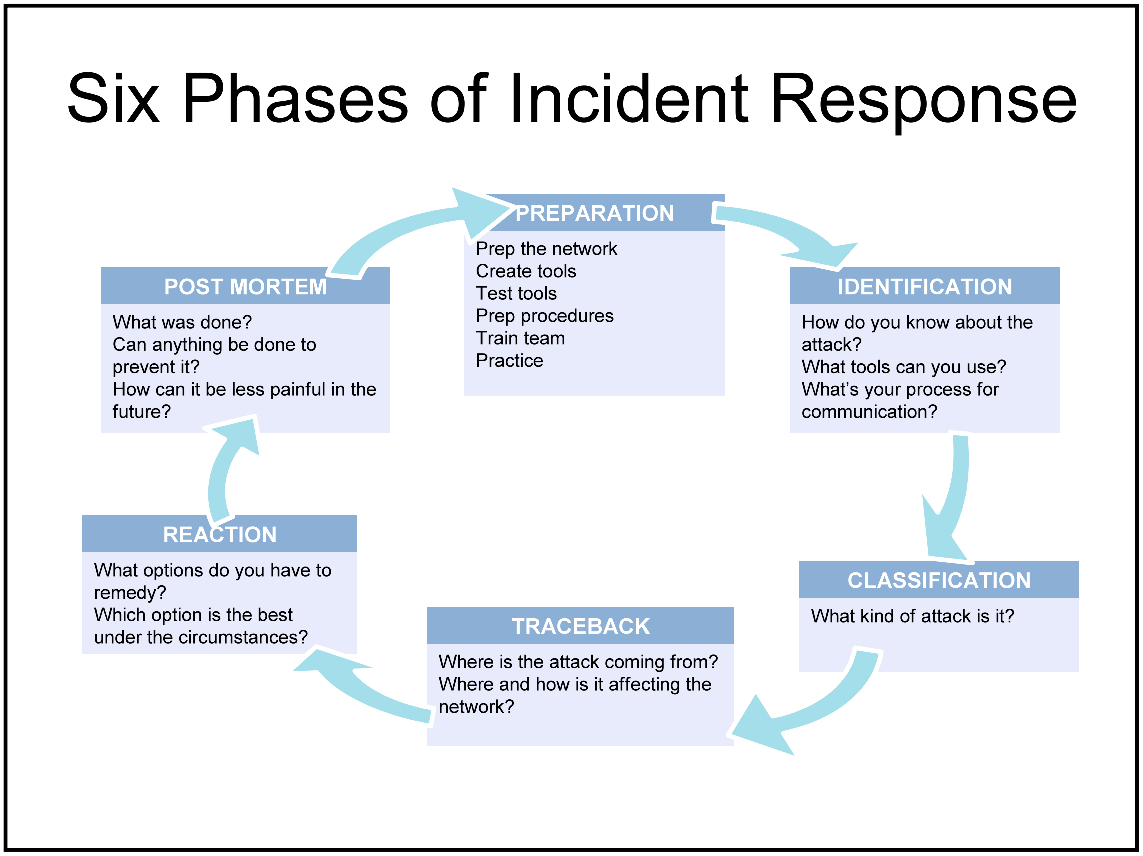
Identification – Ability to identify an attack and know when an attack is occurring.

Classification – Ability to classify an attack when they occur.

Traceback – Ability to traceback an attack to determine where it is coming from.

Reaction – Ability to react to an attack to mitigate an attack.

Post Mortem – Once an attack is mitigated, discuss what went well and learn from it to determine if changes need to be made to the process.



Six Phases of Incident Response

PREPARATION
Prep the network
Create tools
Test tools
Prep procedures
Train team
Practice

IDENTIFICATION
How do you know about the attack?
What tools can you use?
What's your process for communication?

CLASSIFICATION
What kind of attack is it?

TRACEBACK
Where is the attack coming from?
Where and how is it affecting the network?

REACTION
What options do you have to remedy?
Which option is the best under the circumstances?

POST MORTEM
What was done?
Can anything be done to prevent it?
How can it be less painful in the future?

Figure 2: Six Phases of Incident Response

For more information on the Six Phase Methodology, please refer to the following URL:

New techniques and best practices help service providers counter increase in cyber attacks.

This part of the lab will focus on the preparation phase of the Six Phase Methodology. During this part of the lab, you will configure various Infrastructure security features to minimize the effect of any future attacks.

During the next part of the lab, you will experience an attack on the network. During that part of the lab, you use the other phases to identify and mitigate the attack.

Task 1: Configuring Unicast Reverse Path Forwarding (uRPF)

Unicast RPF is a feature that helps mitigate attacks based on source address spoofing. Unicast RPF drops the packets with spoofed IP source address as they enter into a network as it can verify the source IP address. Spoofed source addresses can indicate denial-of-service (DoS) attacks. When Unicast RPF is enabled on an interface, the router examines all packets received as input on that interface to make sure that the source address and source interface appear in the routing table or match the interface on which the packet was received.

For more information on uRPF, please refer to the following URLs:

uRPF Enhancements for the ISP - ISP Network Edge
Unicast Reverse Path Forwarding Loose Mode Feature Module

For this part of the lab, you will configure uRPF on the *Trigger_J63* router to protect it against future attacks using spoofed IP source addresses.

Step 12 Access the *Trigger_J63* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 13 Configure uRPF strict mode on the FastEthernet0/0 interface. (Use the new command syntax for configuring uRPF. i.e. 'ip verify unicast source reachable-via' command)

Note: There are two modes for uRPF, Strict mode and Loose mode

Task 2: Configuring Control Plane Policing (CoPP)

For this part of the lab, you will configure Control Plane Policing on the *Edge_C38* router in order to rate-limit and/or drop packets destined to the control-plane of the router. This exercise will step you thru setting up a sample template for this lab's environment. Please refer to the below reference documents for guidance on setting up CoPP for production networks and tailoring it for different network needs based on actual traffic in the network.

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. Thus, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

For more information in CoPP, please refer to the following URLs:

Control Plane Policing Feature Guide
Deploying Control Plane Policing - Whitepaper

Here is an outline of the four steps required to configure CoPP. You will follow these steps to configure CoPP in this part of the lab.

1. **Define a packet classification criteria**

```
router(config)#class-map <traffic_class_name>
router(config-cmap)#match <access-group | protocol  | ip prec | ip dscp>
```

2. **Define a service policy**

```
router(config)#policy-map <service_policy_name>
router(config-pmap)#class <traffic_class_name>
router(config-pmap-c)# police <cir | rate> conform-action <transmit | drop > exceed-action <transmit | drop>
      cir             Committed information rate (Bits per second)
      rate            Specify policy rate in packets per second (pps)
```

3. **Enter control-plane configuration mode**

```
router(config)#control-plane
```

4. **Apply QoS Policy**

```
service-policy <input | output> <service_policy_name>
    input    Assign policy-map to the input of an interface
    output   Assign policy-map to the output of an interface
```

Step 14 Access the *Edge_C38* router via the device access window from LabOps. (**username=nfp, password=infrasec)**

Step 15 Create a named ACL called cppacl-igp to classify your OSPF traffic

Step 16 Create a named ACL called cppacl-management to classify your management traffic and include the following traffic/protocols:

- Permit telnet traffic from the 192.168.1.0/24 subnet
- Permit ssh traffic from the 192.168.1.0/24 subnet
- Permit snmp traffic from host 192.168.1.100
- Permit ntp traffic from 10.1.1.0/24 subnet

Step 17 Create a named ACL called cppacl-monitoring to classify your monitoring traffic and include the following traffic/protocols:

- Permit pings to the router (icmp – echo) from addresses within your network
  - 192.168.1.0/24 subnet
  - 192.168.2.0/24 subnet
  - 192.168.16.0/24 subnet
  - 192.168.17.0/24 subnet
  - 192.168.18.0/24 subnet
  - 192.168.19.0/24 subnet
  - 10.1.1.0/24 subnet
  - 172.16.1.0/24 subnet
  - 172.16.2.0/24 subnet

- Permit router to receive responses from pings it originates (icmp – echo-reply)

Step 18 Create a named ACL called cppacl-undesirable for undesirable traffic. At this point you are just creating a placeholder for classifying undesirable traffic. You would use this ACL to classify undesirable attack traffic in the future as they occur or for known attacks that have occurred in the past. You would use this classification to create a policy that explicitly dropped the undesirable traffic. At this point, you are in the preparation stage and no attacks are occurring. i.e. you are preparing the groundwork for future attack mitigation. So, you do not need to create any permits under this ACL.

Note: Why are named ACLs are better choice? They allow targeted removal and insertion within the ACL unlike numbered ACLs.

Step 19 Create a class-map called cppclass-igp and use the cppacl-igp ACL as the classification criteria.

Step 20 Create a class-map called cppclass-management and use the cppacl-management ACL as the classification criteria

Step 21 Create a class-map called cppclass-monitoring and use the cppacl-monitoring ACL as the classification criteria.

Step 22 Create a class-map called cppclass-undesirable and use the cppacl-undesirable ACL as the classification criteria

Step 23 Create a Service Policy called cpp-policy

Step 24 Define your cppclass-igp class under the service policy. Since IGP traffic is critical to maintaining network connectivity in your network, do not define a rate limit or drop policy for this class. Allow all IGP traffic unrestricted access to your route processor.

Note: In the future, you could tighten down this class by monitoring how much traffic is generated by your IGP process under normal operating conditions and specify the rate limit as appropriate making sure to leave extra room to ensure IGP packets are not dropped. This would allow you to further protect yourself against attacks.

Step 25 Define your cppclass-management class under the cpp-policy service policy and police it at a rate of 50 pps and drop all packets exceeding this rate. (i.e. police rate 50 pps conform-action transmit exceed-action drop)

Note: Rate-limiting at a PPS rate is better as the packet size vary on the network. Understanding your network's baseline from a PPS perspective is important as well as the bandwidth requirement in bits-per-second (bps).

Step 26 Define your cppclass-monitoring class under your service policy and police it at a rate of 30 pps and drop all packets exceeding this rate.

Step 27 Define your cppclass-undesirable class under your service policy and drop all packets for this class. (conforming and non-conforming traffic.)

Step 28 Define your class-default class under your service policy and police it at a rate of 10 pps and drop all packets that exceed this rate.

Step 29 Apply the cpp-policy service policy as an input policy to your control-plane.

Step 30 Verify your Service Policy is working by telneting and pinging your router to ensure packets are being properly classified in the correct classes.

Task 3: Configuring the groundwork for Remotely Triggered Blackhole (RTBH) Filtering

Remotely triggered blackhole (RTBH) filtering is a technique that provides the ability to drop undesirable traffic at the ingress into the network. RTBH filtering provides a method for quickly dropping undesirable traffic at the edge of the network, based on either source addresses or destination addresses by forwarding it to a null0 interface. A typical deployment scenario for RTBH filtering would require running internal Border Gateway Protocol (iBGP) at the access and aggregation points and configuring a separate device in the network operations center (NOC) to act as a trigger. For destination-based drops, the triggering device sends iBGP updates to the edge that sets the next-hop of the victim's IP address to the null0 interface. Source-based drops are similar but it relies on the pre-existing deployment of uRPF which drops a packet if its source is "invalid"; invalid includes routes to Null0. Using the same mechanism for destination-based drops, a BGP update is sent, and this update sets the next hop for a source to Null0. Now all traffic entering an interface with uRPF enabled drops traffic from that source.

For this part of the lab, you will configure the groundwork for RTBH filtering by configuring iBGP between the *Edge_C38* router and the *Serverfarm_C26* router and the *Serverfarm_C26* router will act as the trigger.

For more information on RTBH filtering, please refer to the following URL:

Remotely Triggered Black Hole Filtering: Destination Based and Source Based

Step 31 Access the *Edge_C38* router using the device access window in LabOps (**username=nfp, password=infrasec**)

Step 32 Create a Null0 interface and configure 'no ip unreachables' under this interface.

Note: How many Null interfaces can you have on a router?

Step 33 Configure a static route for host address 192.0.2.1 pointing to Null0. Note. The IP address 192.0.2.1 is reserved for use in test networks and is not used as a deployed IP address in production networks.

Step 34 Configure uRPF loose mode on the FastEthernet1/0 interface.

Note: uRPF Loose mode can only be configured with the new syntax.

Step 35 Under your router BGP process, configure an iBGP neighbor to the Loopback 0 address of the *Serverfarm_C26* router.

Step 36 Configure BGP to use Loopback 0 as the update-source for that neighbor

Step 37 Access the *Serverfarm_C26* router using the device access window in LabOps (**username=nfp, password=infrasec**)

Step 38 Create a Null0 interface and configure 'no ip unreachables' under this interface

---

Note: Try a 'Show' command for your Null0 interface. Can you track an attack packets being directed to the Null0 interface in order to determine if attack is still occurring?

Step 39 Configure a static route for host address 192.0.2.1 pointing to Null0.

Step 40 Configure a route-map called black-hole-trigger and configure the following under your route-map permit (i.e. route-map black-hole-trigger permit 10):

- Match on a tag value of 66
- Set the next-hop to 192.0.2.1
- Set the local preference to 200
- Set the origin to IGP
- Set the community to no-export

Step 41 Configure a route-map deny (i.e. route-map black-hole-trigger deny 20) and do not configure anything under this part of the route-map

Step 42 Under your router BGP process, configure the following:

- Redistribute static routes and filter the redistribution using the black-hole-trigger route-map
- Configure an iBGP neighbor to the Loopback 0 address of the *Edge_C38* router
- Configure BGP to use Loopback 0 as the update source for that neighbor.
- Configure BGP to send the community attributes to that neighbor

Step 43 Ensure the iBGP neighbor relationship is established between the *Serverfarm_C26* router and the *Edge_C38* router.

Once this is done, you have successfully created the groundwork for RTBH filtering. This will now allow you to use the *Serverfarm_C26* router as a remote triggering device for dropping packets based on source or destination addresses on the *Edge_C38* router. This is done by adding a static route to Null0 with a Tag 66 on the *Serverfarm_C26* router for packets that you want dropped on the *Edge_C38* router.

Task 4: Configuring Role Based Command-Line Interface (CLI) Access also known as CLI Views.

The Role-Based CLI Access feature allows the network administrator to define "views," which are a set of operational commands and configuration capabilities that provide selective or partial access to Cisco IOS EXEC and configuration (Config) mode commands. Views restrict user access to Cisco IOS command-line interface (CLI) and configuration information; that is, a view can define what commands are accepted and what configuration information is visible. Thus, network administrators can exercise better control over access to Cisco networking devices

For more information on the Role based CLI access, please refer to the below URL:

Role-Based CLI Access

For this part of the lab, you will create Role-Based CLI access views for different Network operational users on the *Edge_C38* router. You will configure the following views as detailed below:

Network Ops Administrator

- Some EXEC
- Some Router Config
- No Security Config

Security OPS Administrator

- Show Everything
- EXEC Copy Run only
- EXEC Crypto
- Security Config

Operator

- Ping
- Show Controller
- Show Hardware
- Show Interfaces
- Show Version

WAN Engineer

- Access Everything

Step 44 Access the *Edge_38* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 45 Enable AAA using the 'aaa new-model' global config command

Step 46 Configure the AAA default list to use the router's local database for authentication and authorization

Step 47 Configure AAA console authorization

Step 48 Configure the operator view as follows:

Step 49 Access the root view (Note. In order to access the root view, you must have a secret or enable password configured on the router. Before accessing the root view, configure the secret password to be 'Nfp!nfr4sec' and use this to access the root view.)

Step 50 Create the Operator view

Step 51 Configure a password for this view

Step 52 Assign the commands allowed for this view as follows:

- Ping
- Show controllers
- Show hardware
- Show interfaces
- Show version

Step 53 Access the Operator view and verify its capability

Step 54 Configure the Network Ops View as follows:

Step 55 Access the root view (secret password = Nfp!nfr4sec)

Step 56 Create the NetOps view

Step 57 Configure a password for this view

Step 58 Assign the commands allowed for this view as follows:

- Clear
- Clock
- Connect
- Copy
- Login
- Logout
- Ping
- Show (all show related commands)
- Telnet
- Traceroute
- Write
- Configure
- Configure access-list
- Configure banner
- Configure clock
- Configure hostname
- Configure interface (all interfaces)
- Configure IP
- Configure line

Step 59 Access the NetOps view and verify its capability

Step 60 Configure the Security Ops View as follows:

Step 61 Access the root view (secret password = Nfp!nfr4sec)

Step 62 Create the SecOps view

Step 63 Configure a password for this view

Step 64 Assign the commands allowed for this view as follows:

- Copy running-config
- Login
- Show crypto (this command should be exclusive to this view)
- Show key (this command should be exclusive to this view)
- Show (all show related commands)
- Write
- Configure Terminal
- Configure access-lists
- Configure aaa
- Configure password
- Configure username
- Configure crypto (this command should be exclusive to this view)
- Configure key (this command should be exclusive to this view)
- Configure login

Step 65 Access the SecOps view and verify its capability

Step 66 Also note that the ‘show crypto’ and ‘show key’ are no longer allowed to be issued from the NetOps view since they are exclusive to the SecOps view.

Since the WAN Engineer has access to everything, it is easier just to assign them a username with Privilege level fifteen rather than configuring a view to allow everything.

Step 67 Create a username called ‘engineer’ and assign it to privilege level 15 and assign it a password.

Step 68 Create a username called ‘opadmin’ and specify the Operator view to be used once they successfully authenticate.

Step 69 Create a username called ‘netadmin’ and specify the NetOps view to be used once they successfully authenticate

Step 70 Create a username called ‘secadmin’ and specify the SecOps view to be used once they successfully authenticate

Step 71 Verify the above usernames are assigned the correct view and verify they are restricted to the commands you assigned.

Task 5: Configuring Cisco IOS Login enhancements

The Cisco IOS Login Enhancements feature allows users to better secure their Cisco IOS devices when creating a virtual connection, such as Telnet, secure shell (SSH), or HTTP. Thus, users can help slow down dictionary attacks and help protect their router from a possible denial-of-service (DoS) attack.

For more information on Cisco IOS Login Enhancements, please refer to the following URL:

Cisco IOS Login Enhancements

For this part of the lab, you will be configuring login parameters on the *Serverfarm_C26* router that will help detect suspected DOS attacks and slow down dictionary attacks.

Step 72 Access the *Serverfarm_C26* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 73 Configure a 2 second login delay between successive Login attempts made on the router.

Step 74 Configure the router to stop accepting logins (quiet mode) for 180 seconds when 5 unsuccessful attempts are made within 60 seconds.

Step 75 Configure an access-list to allow your FreeBSD station access to the router during quiet-mode.

Step 76 Configure your router to log failed login attempts after every 5th failed login

Step 77 Configure your router to log successful login attempts made on the router.

Step 78 Verify your login parameters are working. Validate that your router stops accepting logins for 180 seconds after 5 failed attempts and make sure that you can still login from the FreeBSD station during the quiet-mode.

Task 6: Configuring CPU Thresholding Notifications

The CPU Thresholding Notification feature notifies users when a predefined threshold of CPU usage is crossed by generating a Simple Network Management Protocol (SNMP) trap message for the top users of the CPU. The CPU Thresholding Notification feature allows you to configure CPU utilization thresholds that, when crossed, triggers a notification. The notification can be triggered on both a rising threshold and a falling threshold.

For more information on CPU Thresholding Notification feature, please refer to the following URL:

CPU Thresholding Notification

For this part of the lab, you will configure a CPU Thresholding Notification to be triggered on a rising CPU threshold and a falling CPU threshold on the *Edge_C38 and Serverfarm_C26* router.

Step 79 Access the *Edge_C38 and Serverfarm_C26* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 80 Configure the CPU thresholding violation notification as SNMP traps

Step 81 Configure the router to send CPU SNMP traps to the FreeBSD station.

Step 82 Configure your router to send syslog messages to 192.168.1.100

Step 83 Configure a rising CPU threshold notification when total CPU utilization exceeds 60 percent for a period of 5 seconds or longer and a falling CPU threshold notification when total CPU utilization falls below 30 percent for a period of 5 seconds or longer.

Step 84 On the FreeBSD station, open up the Syslogd application.

Note: If syslogd and SNMP are not configured on the FreeBSD, please configure it now.

Step 85 Enable FreeBSD to receive SNMP traps..

Step 86 Ensure that the Kiwi SNMP and Syslog services are running.

Step 87 FreeBSD should now receive traps when the CPU notification threshold is triggered.

Note: We will check to ensure the notifications are being received later in the lab when we initiate another attack.

Note: If your router router CPU is running at 50% baseline, how would you setup the CPU thresholding?

Task 7: Configuring Memory Thresholding Notifications

The Memory Threshold Notifications feature allows you to reserve memory for critical notifications and to configure a router to issue notifications when available memory falls below a specified threshold. The Memory Threshold Notifications feature provides two ways to mitigate low-memory conditions on a router: notifications can be sent to indicate that free memory has fallen below a configured threshold, and memory can be reserved to ensure that sufficient memory is available to issue critical notifications.

For more information on the Memory Thresholding Notification feature, please refer to the below URL:

Memory Thresholding Notification

For this part of the lab, you will configure a Memory Thresholding Notification and memory reservation on the *Edge_C38 and Serverfarm_C26* router.

Step 88 Access the *Edge_C38 and Serverfarm_C26* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 89 Configure a Memory threshold value of 50MB for processor memory.

Step 90 Configure a Memory threshold value of 4MB for IO memory.

Step 91 Configure 1MB of memory to reserve for critical notifications.

Note: Can you name a kind of attack that would cause memory depletion?

Task 8: Configuring Cisco IOS Resilient Configuration.

The Cisco IOS Resilient Configuration feature enables a router to secure and maintain a working copy of the running image and configuration so that those files can withstand malicious attempts to erase the contents of persistent storage (NVRAM and flash). A great challenge of network operators is the total downtime experienced after a router has been compromised and its operating software and configuration data erased from its persistent storage. The operator must retrieve an archived copy (if any) of the configuration and a working image to restore the router. Recovery must then be performed for each affected router, adding to the total network downtime.

For more information on Cisco IOS Resilient Configuration, please refer to the below URL:

Cisco IOS Resilient Configuration

For this part of the lab, you will configure IOS Resilient Configuration on the *Trigger_J63* router.

Step 92 Access the *Serverfarm_C26* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 93 Securely archive a copy of your running config

Step 94 Secure a copy of your running IOS image on the router.

Step 95 Verify your image and config is secured by displaying the status of configuration resilience and the primary bootset filename.

Step 96 Restore a copy of the secured configuration to a file on flash.

In a case where your router configuration is inadvertently changed, you can use the Cisco IOS Resilient config feature to restore a copy of your secure configuration to file and flash and use that configuration to restore your router to the correct running configuration.

Note: With the newer ISR series routers, eToken can be used to securely bootstrap the router from the USB port. Combine that with resilient configuration and Cisco IOS routers have started to address 'Physical Security' aspects of network security – a first in the market.

Task 9: Configuring Auto Secure and Auto Secure Rollback

AutoSecure provides vital security requirements to Enterprise and Service Provider networks by incorporating a straightforward "one touch" device lockdown process. Cisco AutoSecure enables rapid implementation of security policies and procedures to simplify the security process, without having to understand all the Cisco IOS Software features and execute each of the many Command Line Interface (CLI) commands manually. This feature uses a single command that instantly configures the security posture of routers and disables non-essential system processes and services, thereby eliminating potential security threats.

For more information on AutoSecure, please refer to the following URLs:

Cisco AutoSecure Whitepaper

Cisco AutoSecure Feature Guide

For this part of the lab, you will configure AutoSecure on the *Serverfarn-2811* router. You will also perform a manual rollback of the AutoSecure Configuration to the pre-autosecure configuration.

Step 97 Access the *Trigger_J63* router via the device access window from LabOps. (**username=nfp, password=infrasec**)

Step 98 Initiate Auto Secure configuration by issuing the Auto Secure command

Step 99 Answer ‘no’ for the question asking whether this router is connected to the Internet.

Step 100 Answer ‘yes’ to the question asking whether SNMP is used to manage the router.

Step 101 Answer ‘yes’ for the question asking whether to configure NTP authentication

Step 102 Enter ‘1’ for the NTP Trust-key number

Step 103 Type ‘cisco’ for the NTP authentication key

Step 104 Type ‘5’ for the ACL number for access control to all NTP services

Step 105 Type in a banner when prompted

Step 106 If asked to enter a new enable secret, type in ‘cisco123’

Step 107 If asked to enter a new enable password, type in ‘cisco1234’

Step 108 Type in ‘180’ for the question regarding the blocking period for when Login attacks are detected.

Step 109 Type in ‘5’ for question regarding Maximum login failures.

Step 110 Type in ‘60’ for question regarding time period for crossing the failed login attempts.

Step 111 Answer ‘yes’ to the question asking if you want to configure a SSH server.

Step 112 Answer ‘no’ for the question asking if you want to configure the CBAC firewall feature.

Step 113 Answer ‘no’ for the question asking if you want to configure TCP Intercept

Step 114 Scroll thru the suggested configuration changes made by AutoSecure

Step 115 Answer yes to the question regarding whether you want to apply this configuration to the running config

Step 116 The router has now committed the configuration changes to the running configuration.

Step 117 A copy of the router configuration before AutoSecure configurations were applied has been saved to flash called pre_autosec.cfg.

Step 118 Verify that AutoSecure has changed your running configuration with its suggested security config changes.

Step 119 (optional) Test the AutoSecure Rollback feature by issuing the following command:

- config replace flash:pre_autosec.cfg

Step 120 (optional) Verify that the AutoSecure Rollback feature returned your running configuration to the configuration prior to running AutoSecure.

You have now finished the preparation stage of the Six Phase Methodology. In the next part of the lab, you will use the other phases to identify, trace and mitigate an attack.

Note: Can you name those six phases again? -------- Just checking…….

Part 4: Detection and Mitigation of Attack 2

Note: Before proceeding with this part of the lab, please inform the Lab Proctor.

During this part of the lab, you will experience another attack on your network. You will use the 'identification', 'classification', 'traceback' and 'reaction' phases of the Six Phase Methodology in order to determine where the attack is coming from, what routers are being affected and then mitigate the attack. After mitigating the attack, you should have full connectivity within your network and your routing protocols should be stable.

Note: If you stopped your continuous ping on the FreeBSD station, please start it again (ping –t 10.1.1.2). You will use this as your management tool indicating the health of your network. If pings are successful, then your network is operating normally. However, if your pings begin to fail, then this is an indication that your network may be experiencing a security incident – an attack, worm manifestation, etc…

Step 121 You receive a call from Joe User stating that response time and connectivity is poor giving you an indication that something is happening on the network.

Step 122 Observe the output of your continuous ping. Are all responses successful?

Step 123 From the FreeBSD station, open up a command prompt and telnet to the loopback of each of your routers and make note of the following:

- Can you still access all of your routers from the FreeBSD station?
- Do you have good response time to all of the routers?
- Is your routing protocol stable and are neighbors staying up?

Note: Did you receive a notification on the Syslog server on the FreeBSD station indicating your CPU is rising?

Hint: If you are not able to access all routers via telnet to perform the investigation in the next step, you may need to access the routers via console access using the device access window from LabOps.

Hint: You may find it helpful to open up a telnet window to each of the routers and reflect on the Lab topology to help with troubleshooting the security event.

Step 124 Use Netflow to Investigate and identify what kind of attack is occurring on the network. Determine the following:

- What routers are being affected?
- How are the routers affected?
- What type of attack is happening?
- Where is the attack coming from? Where is it entering the network?

- What is the source address of the attack?
- What addresses/ports are being attacked?

Step 125 Check the status of your CoPP service policy on your *Edge_C38* router. Is all traffic being properly classified and dropped appropriately?

Step 126 After determining the characteristics of the attack and where the attack is entering the network, mitigate the attack without using access-lists.

Note: Do not use the Access Control Lists to mitigate the attack.

Hint: What is the source address of the attack? Did you setup a mitigation technique as part of the preparation stage in the previous part of the lab?

Step 127 Once the attack has been mitigated, validate the following:

- Ping responses from your FreeBSD station are all successful.
- From the FreeBSD station, telnet to the loopback address of each of your routers to make sure you have connectivity to all of your routers and make note of the following
    - You should be able to connect to all routers.
    - You should also have good response time to each of your routers.
    - OSPF neighbors and routing should be stable.
    - CPU should be at a reasonable rate
    - Pings sourced from Loopback 1 on the *Remote_J23* router to the *Trigger_J63* router should be successful.

Note: Did you receive a notification on the Kiwi Syslog server on the FreeBSD station indicating your CPU is rising?

Questions:

What feature did you use to mitigate/drop the attack packets?

Where should the attack be mitigated?

This time did the router being attacked behave any differently?

Did you have better response time via telnet during the attack? Why?

Did OSPF remain stable and up during this attack? Why?

Congratulations!!! You have now completed all parts of the lab.