Module 22 – Infrastructure Security Lab

Objective: This lab covers various infrastructure security features and best practices for securing a Cisco router against unwanted attacks. Attack Mitigation Techniques will also be covered in this lab module.

Prerequisite: Module 2 and 3

Topology :

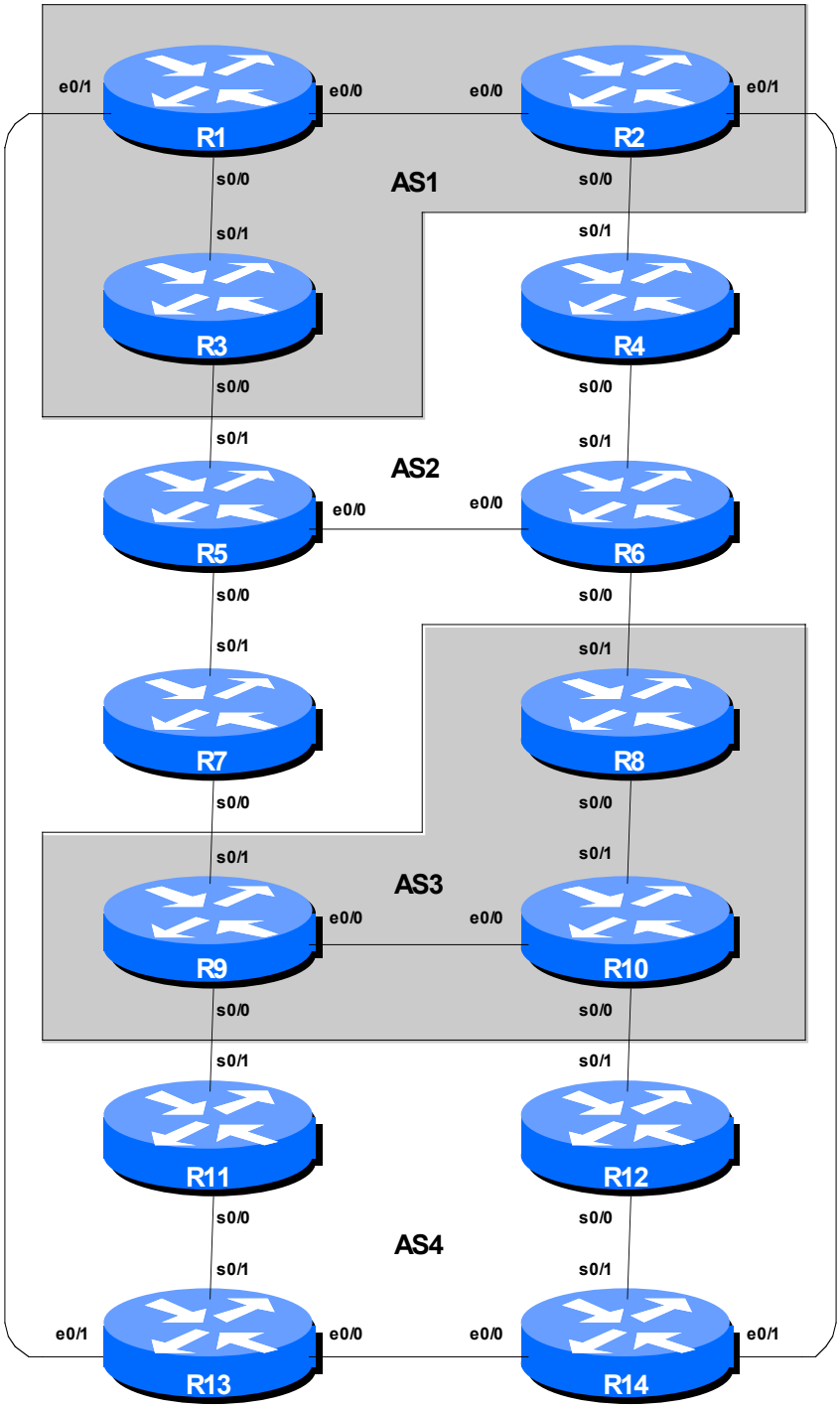


Figure 1 – BGP AS Numbers

Lab Notes

This lab will walk you through various IOS infrasttructure security features for securing a Cisco Router against unwanted attacks. This lab will cover features such as Unicast RPF (uRPF) and Remotely Triggered Black Hole (RTBH) filtering. Students will learn router security Best Practices and attack mitigation techniques via hands-on configuration and attack simulations.

Before starting this module, retain the topology and configurations as used in Module 2. This requires the removal of **all** the filtering and community configurations examined in Module 3, and ensuring that all BGP peerings are up and running.

Recommendation: Remember, if any configuration on a router is not in use, **it should be removed**. Surplus configuration usually gives rise to delayed error detection and debugging of configurations in cases of routing problems or other network failures.

Lab Exercise – Part I

1. **Validate Network Connectivity and note initial state of routers.**

   Observe the initial state of each of the routers:
   - CPU
   - Interface statistics
   - Routes
   - Configuration
   - IGP neighbors
   - BGP neighbors
   - Etc…

The router configuration may need to be tidied up substantially before this module is attempted.

Checkpoint #1*: Call your lab instructor and display the following:*

> ***i]*** *Output of a "**show proc cpu | excl 0.00", "show ip route**" and "**show ip bgp sum**" and "**show ip bgp**"*
> ***ii]*** *Outputs of the '**ping**' and '**trace**' to various destinations within the network*

2. **Detection and Mitigation of Attack**. 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.

3. **You receive a call from Joe User stating that the response time and connectivity is poor giving you an indication that something is happening on the network.** Observe the output of your ping commands to your routers, and also check that you still have good response time to all of the routers. Are your routing protocols stable and neighbors are staying up?

Cisco Systems Inc
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

4. **Investigate and Identify what kind of attack is occuring 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? Where would you need to configure this if you think it is necessary?

5. **Mitigate the Attack**. 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 access-lists to mitigate the attacks.

   Hint: What is the source addresses of these attacks? Do you have routes to these addresses in your router?

6. Once the attack has been mitigated, validate that you have good connectivity to all of your routers and make note of the following:
   - You should have good response time to each of your routers.
   - IGP and BGP routing should be stable.
   - CPU should be at a reasonble 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.

Lab Exercise – Part II

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.

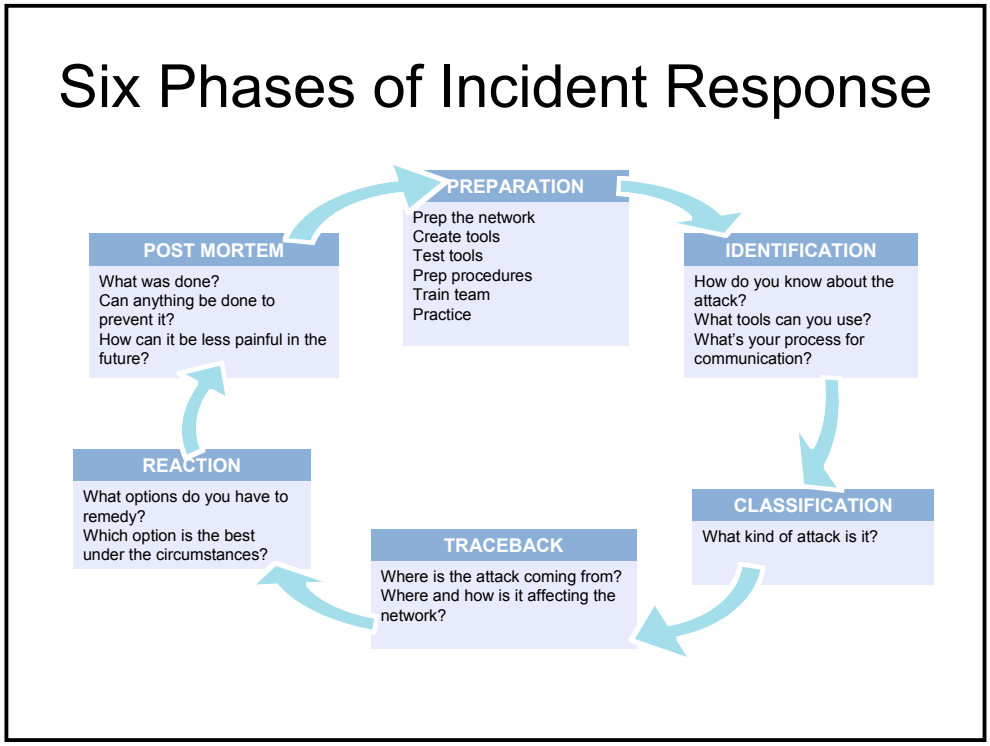
Identification – Ability to identify an attack and know when an attack is occurring.

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.



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)

Cisco Systems Inc
170 West Tasman Drive.
San Jose, CA 95134-1706
Phone: +1 408 526-4000
Fax: +1 408 536-4100

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. (Use the new command syntax for configuring uRPF, i.e. 'ip verify unicast source reachable-via' command).

Configure uRPF loose mode for all router interfaces facing your EBGP peers, or facing networks external to your Autonomous System.

E.g. for AS 3, we configure uRPF on Router8 serial 3/1, Router9 on serial 1/1 and serial 1/0, and Router 10 on serial s1/0.

E.g. On Router 8

```
Router8#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router8(config)#interface serial 3/1
Router8(config-if)#ip verify unicast source reachable-via any
Router8(config-if)#^Z
```

Task 2: Configuring Control Plane Policing (CoPP) - Optional

For this part of the lab, you will configure Control Plane Policing on your infrastructure routers 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.

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.

On ALL routers in your Autonomous system:

1. Configure a static route for host address 192.0.2.1 pointing to null0 on ALL your BGP routers in the Autonomous System.

   E.g. On Router 8

```
Router8#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router8(config)#ip route 192.0.2.1 255.255.255.255 null0
Router8(config-if)#^Z
```

On a selected Trigger Router in your Autonomous System only:

2. Select one of the router in your Autonomous System to be used as a trigger router. 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

   E.g. In AS 3, we have selected Router 10 as the trigger router.

```
Router10#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router10(config)#route-map black-hole-trigger permit 10
Router10(config-route-map)#match tag 66
Router10(config-route-map)#set ip next-hop 192.0.2.1
Router10(config-route-map)#set local-preference 200
Router10(config-route-map)#set origin igp
Router10(config-route-map)#set community no-export
Router10(config-route-map)#^Z
```

3. 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.

```
Router10(config)#route-map black-hole-trigger deny 20
```

4. Under the router BGP process (for the trigger router), configure the following:
   Redistribute static routes and filter the redistribution using the black-hole-trigger route-map.

```
Router10#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router10(config)#router bgp 3
Router10(config-router)#redistribute static route-map black-hole-trigger
Router10(config-router)#^Z
```

Important: You need to ensure the following:

- BGP is sending the community attribute to all the neighbors in your Autonomous System.
- The black holed prefix that is redistributed into BGP will not be sent to routers outside of our Autonomous System (How do we achieve that?).

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

E.g. If I want to drop traffic at the edge with a **source or destination** address of 210.210.11.225. I would configure at the trigger router only,

```
ip route 210.210.11.225 255.255.255.255 null0 tag 66
```

You may want to test that your RTBH mechanism is working, in cooperation with your eBGP neighbors (e.g. Router in AS 1 performing an extended ping to a router in AS 3), and using RTBH to drop traffic originated by AS 1's router. Make sure that you remove the RTBH after testing.

Checkpoint #2*: Call your lab instructor and display the following:*

i] *Output of a "**show ip route x.x.x.x**" for the prefix that you are trying to drop using RTBH on both the trigger router, and the rest of the BGP routers in your ASN.*

Lab Exercise – Part III (Detection and Mitigation of Attack 2)

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.

7. **Detection and Mitigation of Attack**. 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.

8. **You receive a call from Joe User stating that the response time and connectivity is poor giving you an indication that something is happening on the network.** Observe the output of your ping commands to your routers, and also check that you still have good response time to all of the routers. Are your routing protocols stable and neighbors are staying up?

9. **Investigate and Identify what kind of attack is occuring 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? Where would you need to configure this if you think it is necessary?

10. **Mitigate the Attack**. 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 access-lists to mitigate the attacks.

    Hint: Use RTBH to mitigate the attacks that are destined towards your Autonomous System.

11. Once the attack has been mitigated, validate that you have good connectivity to all of your routers and make note of the following:
    - You should have good response time to each of your routers.
    - IGP and BGP routing should be stable.
    - CPU should be at a reasonble rate.

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 your IGP remain stable and up during this attack? Why?

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