

Infrastructure Security: *Securing Network Foundation from DoS Attacks using Cisco IOS Features Lab Overview*

Objective

This lab will walk you through various IOS Infrastructure Security features for securing a Cisco router against unwanted attacks. This lab will cover features such as Control Plane Policing (CoPP), Unicast RPF, (uRPF), Remotely Triggered Blackhole (RTBH) filtering, Role Based Command-Line Interface (CLI) access (CLI Views), IOS Login Enhancements and others. Students will learn router Security Best Practices and attack mitigation techniques via hands-on configuration and attack simulations.

Your network is connected in a typical hub-and-spoke type configuration as depicted below:

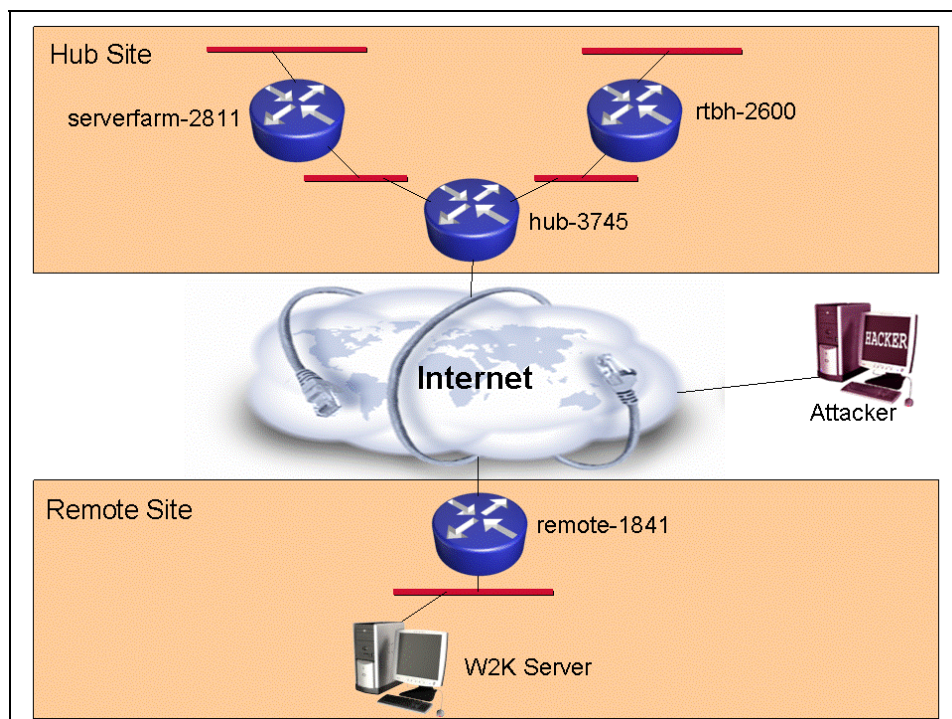


Figure 1 - Network Topology

The network is pre-configured with basic IP connectivity using EIGRP, BGP and static routing.

Note Please refer to the *Topology* section for more details on physical connectivity and to the *Addressing* section for detailed IP addressing and routing information.

During the first part of this lab, you will validate network connectivity and make note of the initial state of the routers. You will validate connectivity to each of the routers from the Windows 2000 server connected to the *remote-1841* router. You will also make note of the initial state of each router. i.e. CPU, configuration, interface statistics, IGP and BGP neighbors, etc... This will give you an idea of the router state during 'normal' conditions.

During the next part of the lab, you will experience an initial attack on the network that disrupts connectivity between the remote site and the hub site. You will experience this attack prior to configuring any Infrastructure Security features. 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.

The third part of the lab will introduce the Six Phase Methodology for securing your routers. An important part of maintaining a stable network is to follow the Six Phase Methodology. 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. Create your tools, prepare your procedures, train your operations team and practice.

Identification – Identify an attack and know when an attack is occurring. Know what tools to use and know the process to communicate.

Classification – Classify an attack when they occur. What kind of an attack is it?

Traceback – Trace an attack to determine where it is coming from and how it is affecting the network.

Reaction – React to an attack to mitigate it. Know what options you have to mitigate the attack. What option is best under the given circumstance.

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

Six Phases of Incident Response

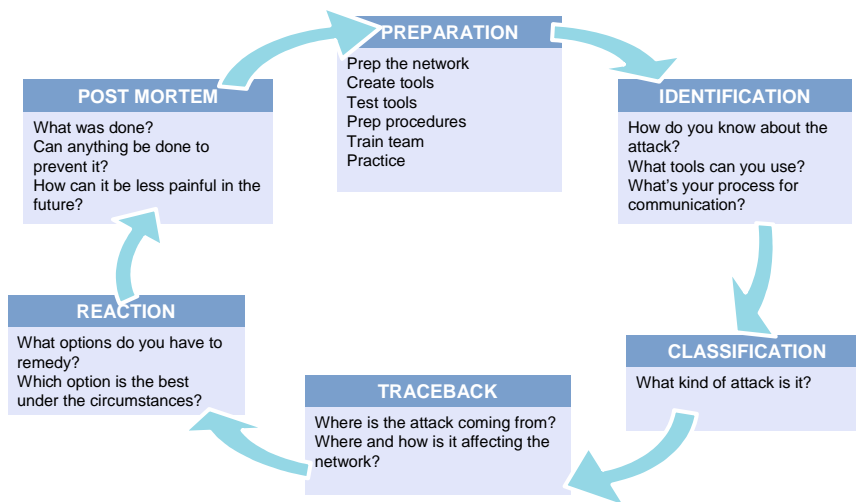


Figure 2 - Six Phases of Incident Response

This part of the lab will focus on the 'Preparation' phase of the Six Phase Methodology where it will walk you through configuring various Infrastructure Security features in order to prepare you for future attacks on your network. These features include the following:

- Unicast RPF (uRPF)
- Control Plane Policing (CoPP)
- Remotely Triggered Blackhole (RTBH) filtering
- Role Based Command-Line Interface Access (CLI Views)
- Cisco IOS Login Enhancements
- CPU Thresholding Notifications
- Memory Thresholding Notifications
- IOS Resilient Configuration
- Autosecure

During the last part of the lab, you will experience another attack on your network. Again, your goal will be to determine where the attack is coming from, what routers are being affected, how are the routers 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. This time the attack will occur after you have completed the 'Preparation' phase of the Six Phase Methodology. You should make note of whether your router acted any differently during this attack.

There is an additional optional section at the end. If time permits, you can test your skills at identifying and mitigating an additional attack on your network.