IT NE 2005
Implementing Firewall Technologies Part 2

LAB 8

WEEK - 11

CONTENTS

Week 6 Implementing Firewall Technologies

Objective: Configuring Zone-Based Policy Firewalls

Copyright © 2016 VIT, All Rights Reserved. VIT and its logo are trademarks of Victorian Institute of Technolog

Note: ISR G1 devices have Fast Ethernet interfaces instead of Gigabit Ethernet Interfaces.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default	Switch Port
R1-S0000	F0/1	192.168.1.1	255.255.255.0	**Gateway**N/A	S1-S0000 F0/1
	S0/0 (DEC)	10.1.1.1	255.255.255.252	N/A	N/A
R2-S0000	S0/0	10.1.1.2	255.255.255.252	N/A	N/A

	S0/1 (DCE)	10.2.2.2	255.255.255.252	N/A	N/A
R3-S0000	F0/0	192.168.33.1	255.255.255.0	N/A	N/A
	F0/1	192.168.3.1	255.255.255.0	N/A	S3-S0000 F0/1
	S0/1	10.2.2.1	255.255.255.252	N/A	N/A
PC-A-S0000	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1-S0000 F0/2
PC-B-S0000	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3-S0000 F0/2
PC-C-S0000	NIC	192.168.33.3	255.255.255.0	192.168.33.1	N/A

In this lab, you will perform the following tasks:

Part 1: Configure Basic Device Settings

- Configure basic settings such as host name, interface IP addresses, and access passwords.
- Configure static routing to enable end-to-end connectivity.

Part 2: Configuring a Zone-Based Policy Firewall (ZPF)

- Use the CLI to configure a Zone-Based Policy Firewall.
- Use the CLI to verify the configuration.

BACKGROUND

The most basic form of a Cisco IOS firewall uses access control lists (ACLs) to filter IP traffic and monitorest ablished traffic patterns. A traditional Cisco IOS firewall is an ACL-based firewall.

The newer Cisco IOS Firewall implementation uses a zone-based approach that operates as a function of interfaces instead of access control lists. A Zone-Based Policy Firewall (ZPF) allows different inspection policies to be applied to multiple host groups connected to the same router interface. It can be configured for extremely advanced, protocol specific, granular control. It prohibits traffic via a default deny-all policy between different firewall zones. ZPF is suited for multiple interfaces that have similar or varying security requirements.

In this lab, you build a multi-router network, configure the routers and PC hosts, and configure a Zone-Based Policy Firewall using the Cisco IOS command line interface (CLI).

Note: The router commands and output in this lab are from a Cisco 1941 with Cisco IOS Release 15.4(3)M2 (UniversalK9-M). Other routers and Cisco IOS versions can be used. See the Router Interface Summary Table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the router model and Cisco IOS version, the commands available and output produced might vary from what is shown in this lab.

Note: Before beginning, ensure that the routers and switches have been erased and have no startup configurations.

Task 1: Configure Basic Device Settings

The desktop system assigned to you serves as an end-user terminal. You access and manage the lab environment from the student desktop system using GNS3 Software.

Students should perform the steps in this task individually.

In Part 1 of this lab, you set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

All steps should be performed on routers R1-S0000 and R3-S0000. The procedures are shown for only one of the routers.

The procedure for R1 is shown here as an example.

Step 1: Deploy router in GNS3 network.

Attach the devices, as shown in the topology diagram, and connection as necessary.

Step 2: Configure basic settings for each router.

a. Configure host names as shown in the topology plus your student ID.

b. Configure interface IP addresses as shown in the IP Addressing Table.
R1 Config

R1-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1-S0000(config)#interface f0/1
R1-S0000(config-if)#ip address 192.168.1.1 255.255.255.0
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#interface s0/0
R1-S0000(config-if)#ip address 10.1.1.1 255.255.255.252
R1-S0000(config-if)#no shutdown
R1-S0000(config-if)#exit
R1-S0000(config)#exit
R1-S0000#copy running-config startup-config Destination
filename [startup-config]?

```
R1-Si40951#
R1-Si40951#
R1-Si40951#
R1-Si40951#in
R1-Si40951#int
R1-Si40951#conf
R1-Si40951#configure t
R1-Si40951#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Si40951(config)#int
R1-Si40951(config)#interface f0/1
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#exit
R1-Si40951(config)#int
R1-Si40951(config)#interface f
R1-Si40951(config)#interface fastEthernet 0/1
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#ip address 192.168.1.1 255.255.255.0
R1-Si40951(config-if)#no shu
R1-Si40951(config-if)#no shutdown
R1-Si40951(config-if)#exit
*Mar  1 00:02:49.711: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:02:50.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1-Si40951(config-if)#exit
R1-Si40951(config)#int
R1-Si40951(config)#interface ser
R1-Si40951(config)#interface serial 0/0
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#ip address 10.1.1.1 255.255.255.252
R1-Si40951(config-if)#no shu
R1-Si40951(config-if)#no shutdown
R1-Si40951(config-if)#exit
R1-Si40951(config)#
*Mar  1 00:03:24.231: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
R1-Si40951(config)#
*Mar  1 00:03:25.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
R1-Si40951(config)#exit
R1-Si40951#
*Mar  1 00:03:32.123: %SYS-5-CONFIG_I: Configured from console by console
R1-Si40951#co
R1-Si40951#cop
R1-Si40951#copy runn
R1-Si40951#copy running-config sr
R1-Si40951#copy running-config st
R1-Si40951#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1-Si40951#
*Mar  1 00:03:54.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
R1-Si40951#
```

```
R1-Si40951
R1-Si40951(config)#interface f
R1-Si40951(config)#interface fastEthernet 0/1
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#ip address 192.168.1.1 255.255.255.0
R1-Si40951(config-if)#no shu
R1-Si40951(config-if)#no shutdown
R1-Si40951(config-if)#exit
*Mar  1 00:02:49.711: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:02:50.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1-Si40951(config-if)#exit
R1-Si40951(config)#int
1-Si40951(config)#interface ser
1-Si40951(config)#interface serial 0/0
1-Si40951(config-if)#ip add
1-Si40951(config-if)#ip address 10.1.1.1 255.255.255.252
1-Si40951(config-if)#no shu
1-Si40951(config-if)#no shutdown
1-Si40951(config-if)#exit
1-Si40951(config)#
Mar  1 00:03:24.231: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up
1-Si40951(config)#
Mar  1 00:03:25.235: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
1-Si40951(config)#exit
1-Si40951#
Mar  1 00:03:32.123: %SYS-5-CONFIG_I: Configured from console by console
1-Si40951#co
1-Si40951#cop
1-Si40951#copy runn
1-Si40951#copy running-config sr
1-Si40951#copy running-config st
1-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
1-Si40951#
Mar  1 00:03:54.063: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to down
1-Si40951#
1-Si40951#
solarwinds | Solar-PuTTY free tool
```

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

R3 Config:

```
R3-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3-S0000(config)#interface f0/1
R3-S0000(config-if)#ip address 192.168.3.1 255.255.255.0
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#interface f0/0
R3-S0000(config-if)#ip address 192.168.33.1 255.255.255.0
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#interface s0/1
R3-S0000(config-if)#ip address 10.2.2.1 255.255.255.252
R3-S0000(config-if)#no shutdown
R3-S0000(config-if)#exit
R3-S0000(config)#exit
R3-S0000#copy running-config startup-config Destination
filename [startup-config]?
```

```
R3-Si40951#
R3-Si40951#
R3-Si40951#
R3-Si40951#conf
R3-Si40951#configure t
R3-Si40951#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3-Si40951(config)#inte
R3-Si40951(config)#interface fa
R3-Si40951(config)#interface fastEthernet 0/1
R3-Si40951(config-if)#ip add
R3-Si40951(config-if)#ip address 192.168.3.1 255.255.255.0
R3-Si40951(config-if)#no shu
R3-Si40951(config-if)#no shutdown
R3-Si40951(config-if)#exit
R3-Si40951(config)#
*Mar  1 00:05:47.895: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:05:48.895: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R3-Si40951(config)#int
R3-Si40951(config)#interface f
R3-Si40951(config)#interface fastEthernet 0/0
R3-Si40951(config-if)#ip add
R3-Si40951(config-if)#ip address 192.168.33.1 255.255.255.0
R3-Si40951(config-if)#no sh
R3-Si40951(config-if)#no shutdown
R3-Si40951(config-if)#ex
*Mar  1 00:06:53.687: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:06:54.687: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R3-Si40951(config-if)#exit
R3-Si40951(config)#exit
R3-Si40951#
*Mar  1 00:07:03.183: %SYS-5-CONFIG_I: Configured from console by console
R3-Si40951#cop
R3-Si40951#copy run
R3-Si40951#copy running-config sta
R3-Si40951#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R3-Si40951#
```

R2 Config:

R2-S0000#conf t
Enter configuration commands, one per line. End with CNTL/Z. R2-S0000(config)#interface s0/0
R2-S0000(config-if)#ip address 10.1.1.2 255.255.255.252
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#interface s0/1

R2-S0000(config-if)#ip address 10.2.2.2 255.255.255.252
R2-S0000(config-if)#no shutdown
R2-S0000(config-if)#exit
R2-S0000(config)#exit
R2-S0000#copy running-config startup-config Destination filename [startup-config]?

```
R2-Si40951#

R2-Si40951#

R2-Si40951#

R2-Si40951#in

R2-Si40951#con

R2-Si40951#conf

R2-Si40951#configure r

R2-Si40951#configure t

R2-Si40951#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

R2-Si40951(config)#int

R2-Si40951(config)#interface f

R2-Si40951(config)#interface se

R2-Si40951(config)#interface serial 0/0

R2-Si40951(config-if)#ip add

R2-Si40951(config-if)#ip address 10.1.1.2 255.255.255.252

R2-Si40951(config-if)#no sh

R2-Si40951(config-if)#no shutdown

R2-Si40951(config-if)#exit

R2-Si40951(config)#

*Mar  1 00:09:26.303: %LINK-3-UPDOWN: Interface Serial0/0, changed state to up

R2-Si40951(config)#

*Mar  1 00:09:27.335: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
```

```
R2-Si40951(config)#int

R2-Si40951(config)#interface se

R2-Si40951(config)#interface serial 0/1

R2-Si40951(config-if)#ip add

R2-Si40951(config-if)#ip address 10.2.2.2 255.255.255.252

R2-Si40951(config-if)#no sh

R2-Si40951(config-if)#no shutdown

R2-Si40951(config-if)#exit

R2-Si40951(config)#e

*Mar  1 00:10:10.631: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up

R2-Si40951(config)#ex

*Mar  1 00:10:11.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up

R2-Si40951(config)#exit

R2-Si40951#

*Mar  1 00:10:15.287: %SYS-5-CONFIG_I: Configured from console by console

R2-Si40951#cop

R2-Si40951#copy runn

R2-Si40951#copy running-config st

R2-Si40951#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

R2-Si40951#

*Mar  1 00:10:34.267: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down

R2-Si40951#
```

Configure a clock rate for routers with a DCE serial cable attached to their serial interface. R1-STUDENTID is shown here as an example.

R1-S0000# Conf t

R1-S0000(config)# interface S0/0

R1-S0000(config-if)# clock rate 64000

R1-S0000# Exit

R1-S0000# Exit

```
R1-Si40951#conf
R1-Si40951#configure t
R1-Si40951#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1-Si40951(config)#int
R1-Si40951(config)#interface ser
R1-Si40951(config)#interface serial 0/0
R1-Si40951(config-if)#cl
R1-Si40951(config-if)#clo
R1-Si40951(config-if)#clock r
R1-Si40951(config-if)#clock rate 64000
R1-Si40951(config-if)#exit
R1-Si40951(config)#exit
R1-Si40951#
*Mar  1 00:15:26.983: %SYS-5-CONFIG_I: Configured from console by console
R1-Si40951#
```

R3:

R3-S000 # Conf t

R3-S0000(config)# interface S0/1

R3-S0000(config-if)# clock rate 64000

R1-S0000# Exit

R1-S0000# Exit

```
R3-Si40951#
R3-Si40951#conf
R3-Si40951#configure t
R3-Si40951#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R3-Si40951(config)#int
R3-Si40951(config)#interface ser
R3-Si40951(config)#interface serial s0/1
                    ^
% Invalid input detected at '^' marker.

R3-Si40951(config)#interface serial 0/1
R3-Si40951(config-if)#clo
```

```
R3-Si40951(config-if)#clock r
R3-Si40951(config-if)#clock rate 64000
R3-Si40951(config-if)#exit
R3-Si40951(config)#exit
R3-Si40951#
*Mar  1 00:16:17.939: %SYS-5-CONFIG_I: Configured from console by console
R3-Si40951#
```

R2:

R2-S000 # Conf t

R2-S0000(config)# interface S0/0

R2-S0000(config-if)# clock rate 64000

R2-S0000(config-if)# exit

R1-S0000(config)# interface S0/1

R1-S0000(config-if)# clock rate 64000

R1-S0000# Exit

```
R2-Si40951(config)#interface serial 0/0
R2-Si40951(config-if)#cl
R2-Si40951(config-if)#cloc
R2-Si40951(config-if)#clock r
R2-Si40951(config-if)#clock rate 64000
R2-Si40951(config-if)#exit
R2-Si40951(config)#int
R2-Si40951(config)#interface ser
R2-Si40951(config)#interface serial 0/1
R2-Si40951(config-if)#cl
R2-Si40951(config-if)#clock rate 64000
R2-Si40951(config-if)#exit
R2-Si40951(config)#exit
R2-Si40951#
*Mar  1 00:18:21.979: %SYS-5-CONFIG_I: Configured from console by console
R2-Si40951#
```

d. To prevent the router from attempting to translate incorrectly entered commands as though they were host names, disable DNS lookup. R1-STUDENTID is shown here as an example.

R1-STUDENTID(config)# no ip domain-lookup

R2-STUDENTID(config)# no ip domain-lookup

R3-STUDENTID(config)# no ip domain-lookup

Step 3: Configure static routing on the routers.

a. Configure a static default route from R1 to R2 and from R3 to R2.

R1:

R1-S0000#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1-S0000(config)#ip route 0.0.0.0 0.0.0.0 **10.1.1.2**

R1-S0000(config)#end

R3:

R3-S0000#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R3-S0000(config)#ip route 0.0.0.0 0.0.0.0 **10.2.2.2**

R3-S0000(config)#end

c. Configure a static route from R2 to the R1 LAN and from R2 to the R3 LAN.

R2:

R2-S0000#conf t

Enter configuration commands, one per line. End with CNTL/Z.

R2-S0000(config)#ip route 192.168.1.0 255.255.255.0 **10.1.1.1**

R2-S0000(config)#ip route 192.168.3.0 255.255.255.0 **10.2.2.1**

R2-S0000(config)#ip route 192.168.33.0 255.255.255.0 **10.2.2.1**

R2-S0000(config)#end

```
R2-Si40951
R2-Si40951(config)#interface serial 0/0
R2-Si40951(config-if)#cl
R2-Si40951(config-if)#cloc
R2-Si40951(config-if)#clock r
R2-Si40951(config-if)#clock rate 64000
R2-Si40951(config-if)#exit
R2-Si40951(config)#int
R2-Si40951(config)#interface ser
R2-Si40951(config)#interface serial 0/1
R2-Si40951(config-if)#cl
R2-Si40951(config-if)#clock rate 64000
R2-Si40951(config-if)#exit
R2-Si40951(config)#exit
R2-Si40951#
Mar  1 00:18:21.979: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#
2-Si40951#conf
2-Si40951#configure t
2-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
2-Si40951(config)#no ip dom
2-Si40951(config)#no ip domain-lo
2-Si40951(config)#no ip domain-look
2-Si40951(config)#no ip domain-lookup
2-Si40951(config)#exit
2-Si40951#
Mar  1 00:20:54.379: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#conf
2-Si40951#configure t
2-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
2-Si40951(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
2-Si40951(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
2-Si40951(config)#ip route 192.168.33.0 255.255.255.0 10.2.2.1
2-Si40951(config)#end
2-Si40951#
Mar  1 00:27:47.531: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#
solarwinds | Solar-PuTTY free tool   © 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

Step 4: Disable DNS lookup.

To prevent the router from attempting to translate incorrectly entered commands, disable DNS lookup.

R2(config)# no ip domain-lookup

```
R2-Si40951
R2-Si40951(config-if)#exit
R2-Si40951(config)#exit
R2-Si40951#
*Mar  1 00:18:21.979: %SYS-5-CONFIG_I: Configured from console by console
R2-Si40951#
R2-Si40951#conf
R2-Si40951#configure t
R2-Si40951#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2-Si40951(config)#no ip dom
R2-Si40951(config)#no ip domain-lo
R2-Si40951(config)#no ip domain-look
R2-Si40951(config)#no ip domain-lookup
2-Si40951(config)#exit
2-Si40951#
Mar  1 00:20:54.379: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#conf
2-Si40951#configure t
2-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
2-Si40951(config)#ip route 192.168.1.0 255.255.255.0 10.1.1.1
2-Si40951(config)#ip route 192.168.3.0 255.255.255.0 10.2.2.1
2-Si40951(config)#ip route 192.168.33.0 255.255.255.0 10.2.2.1
2-Si40951(config)#end
2-Si40951#
Mar  1 00:27:47.531: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#
2-Si40951#no ip dom
2-Si40951#no ip domain
2-Si40951#conf
2-Si40951#configure t
2-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
2-Si40951(config)#no ip-do
2-Si40951(config)#no ip dom
2-Si40951(config)#no ip domain-loo
2-Si40951(config)#no ip domain-lookup
2-Si40951(config)#
solarwinds | Solar-PuTTY free tool   © 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

Step 5: Configure PC host IP settings.

Configure a static IP address, subnet mask, and default gateway for PC-A and PC-C, as shown in the IP addressing table.

Deploy VPCS A: Connect Switch Port 1 to R1 f0/1

PC-A> ip 192.168.1.3/24 192.168.1.1

PC-A> Save

Deploy VPCS B: Connect Switch Port 1 to R3 f0/1

PC-B> ip 192.168.3.3/24 192.168.3.1

PC-B> Save

Deploy VPCS C: Connect to R3 f0/0

PC-C> ip 192.168.33.3/24 192.168.33.1

PC-C> Save

Step 6: Verify connectivity between PC-A and R3.

a. Ping from R1 to R3.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

```
R1-Si40951#
*Mar  1 01:46:50.611: %SYS-5-CONFIG_I: Configured from console by console
R1-Si40951#ping 10.2.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
R1-Si40951#
```

b. Ping from PC-A on the R1 LAN to PC-C on the R3 LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

```
PC-A-Si40951> ping 192.168.33.3
192.168.33.3 icmp_seq=1 timeout
192.168.33.3 icmp_seq=2 timeout
84 bytes from 192.168.33.3 icmp_seq=3 ttl=61 time=17.326 ms
84 bytes from 192.168.33.3 icmp_seq=4 ttl=61 time=21.460 ms
84 bytes from 192.168.33.3 icmp_seq=5 ttl=61 time=22.218 ms
```

Note: If you can ping from PC-A to PC-C, you have demonstrated that static routing is configured and functioning correctly. If you cannot ping but the device interfaces are up and IP addresses are correct, use the show run and show ip route commands to help identify routing protocol-related problems.

Step 7: Save the basic running configuration for each router.

```
R1-Si40951
R1-Si40951(config)#interface fastEthernet 0/1
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#ip address 192.168.1.1 255.255.255.255.0
                                                             ^
% Invalid input detected at '^' marker.

R1-Si40951(config-if)#ip address 192.168.1.1 255.255.255.0
R1-Si40951(config-if)#no shu
R1-Si40951(config-if)#no shutdown
R1-Si40951(config-if)#exit
R1-Si40951(config)#int
R1-Si40951(config)#interface ser
R1-Si40951(config)#interface serial 0/0
R1-Si40951(config-if)#ip add
R1-Si40951(config-if)#ip address 10.1.1.1 255.255.255.252
1-Si40951(config-if)#no shu
1-Si40951(config-if)#no shutdown
1-Si40951(config-if)#exit
1-Si40951(config)#exit
1-Si40951#
Mar  1 01:46:50.611: %SYS-5-CONFIG_I: Configured from console by console
1-Si40951#ping 10.2.2.1

ype escape sequence to abort.
ending 5, 100-byte ICMP Echos to 10.2.2.1, timeout is 2 seconds:
!!!!
uccess rate is 100 percent (5/5), round-trip min/avg/max = 1/3/12 ms
1-Si40951#
1-Si40951#sav
1-Si40951#c
1-Si40951#cop
1-Si40951#copy run
1-Si40951#copy running-config st
1-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
1-Si40951#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

```
R2-Si40951
R2-Si40951(config-if)#exit
R2-Si40951(config)#int
R2-Si40951(config)#interface s0/1
R2-Si40951(config-if)#ip add
R2-Si40951(config-if)#ip address 10.2.2.2 255.255.255.252
R2-Si40951(config-if)#no shu
R2-Si40951(config-if)#no shutdown
R2-Si40951(config-if)#exit
R2-Si40951(config)#exit
R2-Si40951#
Mar  1 01:45:29.039: %SYS-5-CONFIG_I: Configured from console by console
2-Si40951#sho
2-Si40951#show ip rou
2-Si40951#show ip route
odes: C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
      ia - IS-IS inter area, * - candidate default, U - per-user static route
      o - ODR, P - periodic downloaded static route

ateway of last resort is not set

    10.0.0.0/30 is subnetted, 2 subnets
      10.2.2.0 is directly connected, Serial0/1
      10.1.1.0 is directly connected, Serial0/0
    192.168.1.0/24 [1/0] via 10.1.1.1
    192.168.3.0/24 [1/0] via 10.2.2.1
    192.168.33.0/24 [1/0] via 10.2.2.1
2-Si40951#cop
2-Si40951#copy ru
2-Si40951#copy running-config st
2-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
2-Si40951#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

```
R3-Si40951
R3-Si40951(config-if)#exit
R3-Si40951(config)#int
R3-Si40951(config)#interface f
R3-Si40951(config)#interface fastEthernet 0/0
R3-Si40951(config-if)#ip add
R3-Si40951(config-if)#ip address 192.168.33.1 255.255.255.0
R3-Si40951(config-if)#no shi
R3-Si40951(config-if)#no shu
R3-Si40951(config-if)#no shutdown
R3-Si40951(config-if)#exit
R3-Si40951(config)#ip add
3-Si40951(config)#int
3-Si40951(config)#interface ser
3-Si40951(config)#interface serial 0/1
3-Si40951(config-if)#ip add
3-Si40951(config-if)#ip address 10.2.2.1 255.255.255.252
3-Si40951(config-if)#no shu
3-Si40951(config-if)#no shutdown
3-Si40951(config-if)#exit
3-Si40951(config)#
Mar  1 01:42:47.315: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up
3-Si40951(config)#
Mar  1 01:42:48.319: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to up
3-Si40951(config)#cop
3-Si40951(config)#copy
3-Si40951(config)#copy run
3-Si40951(config)#copy run
3-Si40951(config)#exit
3-Si40951#c
Mar  1 02:23:57.075: %SYS-5-CONFIG_I: Configured from console by console
3-Si40951#cop
3-Si40951#copy run
3-Si40951#copy running-config st
3-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
3-Si40951#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

Step 8: Configure a user account, encrypted passwords and crypto keys for SSH.

Note: Passwords in this task are set to a minimum of 10 characters but are relatively simple for the benefit of performing the lab. More complex passwords are recommended in a production network.

For this step, configure the same settings for R1-S0000 and R3. Router R1-S0000 is shown here as an example. a.

Configure a minimum password length.

Use the security passwords command to set a minimum password length of 10 characters.

R1-S0000(config)# security passwords min-length 10

R3-S0000(config)# security passwords min-length 10

b. Configure a domain name.

R1-S0000(config)# ip domain-name ccnasecurity.com

R3-S0000(config)# ip domain-name ccnasecurity.com

c. Configure crypto keys for SSH

R1-S0000(config)# crypto key generate rsa general-keys modulus 1024

R3-S0000(config)# crypto key generate rsa general-keys modulus 1024

Configure an admin01 user account using algorithm-type scrypt for encryption and a password of cisco12345.

R1(config)# username admin01 secret cisco12345

d. Configure the enable secret password on both routers. Use the type 9 (SCRYPT) hashing algorithm.

R1-S0000(config)# enable secret cisco12345

R3-S0000(config)# enable secret cisco12345

e. Configure line console 0 to use the local user database for logins. For additional security, the exectimeout command causes the line to log out after 5 minutes of inactivity. The logging synchronous command prevents console messages from interrupting command entry.

Note: To avoid repetitive logins during this lab, the exec timeout can be set to 0 0, which prevents it from expiring. However, this is not considered a good security practice.

R1-S0000(config)# line console 0

R1-S0000(config-line)# login local

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# logging synchronous

R1-S0000# exit

```
R1-Si40951(config)#ip domain-name ccnasecurity.com
R1-Si40951(config)#cry
R1-Si40951(config)#crypto k
R1-Si40951(config)#crypto key ge
R1-Si40951(config)#crypto key generate r
R1-Si40951(config)#crypto key generate rsa gen
R1-Si40951(config)#crypto key generate rsa general-keys mod
R1-Si40951(config)#crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1-Si40951.ccnasecurity.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*Mar  1 00:06:09.647: %SYS-3-CPUHOG: Task is running for (2024)msecs, more than (2000)msecs (0/0),process = crypto sw pk pro
c.
-Traceback= 0x62F8AAA4 0x62FB71A0 0x62FB7CBC 0x62FB548C 0x62FB686C 0x62B1E28C 0x62B1E270 [OK]

R1-Si40951(config)#
*Mar  1 00:06:10.839: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1-Si40951(config)#user
R1-Si40951(config)#username admin01 sec
R1-Si40951(config)#username admin01 secret cisco12345
R1-Si40951(config)#en
R1-Si40951(config)#enn
R1-Si40951(config)#ena
R1-Si40951(config)#enable sec
R1-Si40951(config)#enable secret cisco12345
R1-Si40951(config)#line con
R1-Si40951(config)#line console 0
R1-Si40951(config-line)#login loc
R1-Si40951(config-line)#login local
R1-Si40951(config-line)#exec
R1-Si40951(config-line)#exec-tim
R1-Si40951(config-line)#exec-timeout 5 0
R1-Si40951(config-line)#logg
R1-Si40951(config-line)#logging syn
R1-Si40951(config-line)#logging synchronous
R1-Si40951(config-line)#exit
R1-Si40951(config)#
```

© 2019 SolarWinds Worldwide, LLC. All rights reserved.

b. Configure a password for the aux port for router R1.

R1-S0000(config)# line aux 0

R1-S0000(config-line)# login local

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# exit

```
R1-Si40951
c.
-Traceback= 0x62F8AAA4 0x62FB71A0 0x62FB7CBC 0x62FB548C 0x62FB686C 0x62B1E28C 0x62B1E270 [OK]

R1-Si40951(config)#
*Mar  1 00:06:10.839: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1-Si40951(config)#user
R1-Si40951(config)#username admin01 sec
R1-Si40951(config)#username admin01 secret cisco12345
R1-Si40951(config)#en
R1-Si40951(config)#enn
1-Si40951(config)#ena
1-Si40951(config)#enable sec
1-Si40951(config)#enable secret cisco12345
1-Si40951(config)#line con
1-Si40951(config)#line console 0
1-Si40951(config-line)#login loc
1-Si40951(config-line)#login local
1-Si40951(config-line)#exec
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#logg
1-Si40951(config-line)#logging syn
1-Si40951(config-line)#logging synchronous
1-Si40951(config-line)#exit
1-Si40951(config)#line au
1-Si40951(config)#line aux 0
1-Si40951(config-line)#log
1-Si40951(config-line)#loging loc
1-Si40951(config-line)#loging local
                         ^
% Invalid input detected at '^' marker.

1-Si40951(config-line)#login local
1-Si40951(config-line)#exe
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#exit
1-Si40951(config)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

c. Configure the password on the vty lines for router

R1. R1-S0000(config)# line vty 0 4

R1-S0000(config-line)# login local

R1-S0000(config-line)# transport input ssh

R1-S0000(config-line)# exec-timeout 5 0

R1-S0000(config-line)# exit

```
R1-Si40951
R1-Si40951(config)#line con
R1-Si40951(config)#line console 0
R1-Si40951(config-line)#login loc
R1-Si40951(config-line)#login local
R1-Si40951(config-line)#exec
R1-Si40951(config-line)#exec-tim
R1-Si40951(config-line)#exec-timeout 5 0
R1-Si40951(config-line)#logg
R1-Si40951(config-line)#logging syn
R1-Si40951(config-line)#logging synchronous
1-Si40951(config-line)#exit
1-Si40951(config)#line au
1-Si40951(config)#line aux 0
1-Si40951(config-line)#log
1-Si40951(config-line)#loging loc
1-Si40951(config-line)#loging local
                         ^
% Invalid input detected at '^' marker.

1-Si40951(config-line)#login local
1-Si40951(config-line)#exe
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#exit
1-Si40951(config)#line
1-Si40951(config)#line vt
1-Si40951(config)#line vty 0 4
1-Si40951(config-line)#log
1-Si40951(config-line)#login loca
1-Si40951(config-line)#login local
1-Si40951(config-line)#trans
1-Si40951(config-line)#transport in
1-Si40951(config-line)#transport input ssh
1-Si40951(config-line)#exec
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#exit
1-Si40951(config)#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

d. Encrypt the console, aux, and vty passwords.

R1-S0000(config)# enable secret class12345

R1-S0000(config)# exit

```
R1-Si40951
R1-Si40951(config-line)#logging syn
R1-Si40951(config-line)#logging synchronous
R1-Si40951(config-line)#exit
R1-Si40951(config)#line au
R1-Si40951(config)#line aux 0
R1-Si40951(config-line)#log
R1-Si40951(config-line)#loging loc
R1-Si40951(config-line)#loging local
                         ^
% Invalid input detected at '^' marker.

R1-Si40951(config-line)#login local
1-Si40951(config-line)#exe
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#exit
1-Si40951(config)#line
1-Si40951(config)#line vt
1-Si40951(config)#line vty 0 4
1-Si40951(config-line)#log
1-Si40951(config-line)#login loca
1-Si40951(config-line)#login local
1-Si40951(config-line)#trans
1-Si40951(config-line)#transport in
1-Si40951(config-line)#transport input ssh
1-Si40951(config-line)#exec
1-Si40951(config-line)#exec-tim
1-Si40951(config-line)#exec-timeout 5 0
1-Si40951(config-line)#exit
1-Si40951(config)#en
1-Si40951(config)#ena
1-Si40951(config)#enable sec
1-Si40951(config)#enable secret clas
1-Si40951(config)#enable secret class12345
1-Si40951(config)#exit
1-Si40951#
Mar  1 00:15:35.379: %SYS-5-CONFIG_I: Configured from console by console
1-Si40951#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

Step 9: Save the basic configurations on all routers.

Save the running configuration to the startup configuration from the privileged EXEC

prompt.

R1-S0000# copy running-config startup-config

R3-S0000# copy running-config startup-config

R2-S0000# copy running-config startup-config

Part 2: Configuring a Zone-Based Policy Firewall (ZPF)

In Part 2 of this lab, you configure a zone-based policy firewall (ZPF) on R3 using the command line interface (CLI).

Task 1: Verify Current Router Configurations.

In this task, you will verify end-to-end network connectivity before implementing ZPF.

Step 1: Verify end-to-end network connectivity.

a. Ping from R1 to R3 Using both of R3's FastEthernet interface IP addresses.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

b. Ping from PC-A on the R1 LAN to PC-C on the R3 conference room LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

c. Ping from PC-A on the R1 LAN to PC-B on the R3 internal LAN.

If the pings are not successful, troubleshoot the basic device configurations before continuing.

Step 2: Display the R3 running configurations.

a. Issue the show ip interface brief command on R3 to verify the correct IP addresses were assigned. Use the IP Address Table to verify the addresses.

b. Issue the show ip route command on R3 to verify it has a static default route pointing to R2's serial 0/1 interface.

c. Issue the show run command to review the current basic configuration on R3.

d. Verify the R3 basic configuration as performed in Part 1 of the lab. Are there any security commands related to access control?

_____

Task 2: Create a Zone-Based Policy Firewall

In this task, you will create a zone-based policy firewall on R3, making it act not only as a router but also as a firewall. R3 is currently responsible for routing packets for the three networks connected to it. R3's interface roles are configured as follows:

Serial 0/1 is connected to the Internet. Because this is a public network, it is considered an untrusted network and should have the lowest security level.

F0/1 is connected to the internal network. Only authorized users have access to this network. In addition, vital institution resources also reside in this network. The internal network is to be considered a trusted network and should have the highest security level.

F0/0 is connected to a conference room. The conference room is used to host meetings with people who are not part of the organization.

The security policy to be enforced by R3 when it is acting as a firewall dictates that:

- No traffic initiated from the Internet should be allowed into the internal or conference room networks.
- Returning Internet traffic (return packets coming from the Internet into the R3 site, in response to requests originating from any of the R3 networks) should be allowed.

- Computers in the R3 internal network are considered trusted and are allowed to initiate any type traffic (TCP, UDP or ICMP based traffic).
- Computers in the R3 conference room network are considered untrusted and are allowed to initiate only web traffic (HTTP or HTTPS) to the Internet.
- No traffic is allowed between the internal network and the conference room network. There is no guarantee regarding the condition of guest computers in the conference room network. Such machines could be infected with malware and might attempt to send out spam or other malicious traffic.

Step 1: Creating the security zones.

A security zone is a group of interfaces with similar security properties and requirements. For example, if a router has three interfaces connected to internal networks, all three interfaces can be placed under the same zone named "internal". Because all security properties are configured to the zone instead of to the individual router interfaces, the firewall design is much more scalable.

In this lab, the R3 site has three interfaces; one connected to an internal trusted network, one connected to the conference room network and another connected to the Internet. Because all three networks have different security requirements and properties, we will create three different security zones.

a. Security zones are created in global configuration mode, and the command allows for zone name definition. In R3, create three zones named INSIDE, CONFROOM and INTERNET:

```
R3-S0000(config)# zone security INSIDE

R3-S0000(config)# zone security CONFROOM

R3-S0000(config)# zone security INTERNET
```

Step 2: Creating Security Policies

Before ZPF can decide if some specific traffic should be allowed or denied, it must be told what traffic is to be considered. Cisco IOS uses class-maps to select traffic. Interesting traffic is a common denomination for traffic that has been selected by a class-map.

While class-maps select traffic, it is not their job to decide what happens to the selected traffic; Policymaps decide the fate of the selected traffic.

ZPF traffic policies are defined as policy-maps and use class-maps to select traffic. In other words, classmaps define what traffic is to be policed while policy-maps define the action to be taken upon the selected traffic.

Policy-maps can drop, pass or inspect traffic. Because we want the firewall to watch traffic moving in the direction of zone-pairs, we will create inspect policy-maps. Inspect policy-maps allow for dynamic handling of the return traffic.

First, you will create class-maps. After the class-maps are created, you will create policy-maps and attach the class-maps to the policy-maps.

a. Create an inspect class-map to match traffic to be allowed from the INSIDE zone to the INTERNET zone. Because we trust the INSIDE zone, we allow all the main protocols.

In the commands below, the first line creates an inspect class-map. The match-any keyword instructs the router that any of the match protocol statements will qualify as a successful match resulting in a policy being applied. The result is a match for TCP or UDP or ICMP packets.

The match commands refer to specific Cisco NBAR supported protocols. For more information on Cisco NBAR visit Cisco Network-Based Application Recognition.

R3-S0000(config)# class-map type inspect match-any INSIDE_PROTOCOLS

R3-S0000(config-cmap)# match protocol tcp

R3-S0000(config-cmap)# match protocol udp

R3-S0000(config-cmap)# match protocol icmp

b. Similarly, create a class-map to match the traffic to be allowed from the CONFROOM zone to the INTERNET zone. Because we do not fully trust the CONFROOM zone, we must limit what the server can send out to the Internet:

R3-S0000(config)# class-map type inspect match-any CONFROOM_PROTOCOLS

R3-S0000(config-cmap)# match protocol http

R3-S0000(config-cmap)# match protocol https

R3-S0000(config-cmap)# match protocol dns

```
R3-Si40951(config)#zone security CONFROOM
R3-Si40951(config-sec-zone)#exit
R3-Si40951(config)#zone security INTERNET
R3-Si40951(config-sec-zone)#exit
R3-Si40951(config)#conf
R3-Si40951(config)#config t
R3-Si40951(config)#config term
R3-Si40951(config)#config term
R3-Si40951(config)#class-ma
R3-Si40951(config)#class-map typ
R3-Si40951(config)#class-map type insp
R3-Si40951(config)#class-map type inspect matc
R3-Si40951(config)#class-map type inspect match-any INSIDE_PROTOCOLS
R3-Si40951(config-cmap)#matc
3-Si40951(config-cmap)#match prot
3-Si40951(config-cmap)#match protocol tcp
3-Si40951(config-cmap)#matc
3-Si40951(config-cmap)#match pro
3-Si40951(config-cmap)#match protocol udp
3-Si40951(config-cmap)#ma
3-Si40951(config-cmap)#match pro
3-Si40951(config-cmap)#match protocol icmp
3-Si40951(config-cmap)#exit
3-Si40951(config)#clas
3-Si40951(config)#class-map typ
3-Si40951(config)#class-map type insp
3-Si40951(config)#class-map type inspect matc
3-Si40951(config)#class-map type inspect match-any CONFROOM_PROTOCOLS
3-Si40951(config-cmap)#mat
3-Si40951(config-cmap)#match prot
3-Si40951(config-cmap)#match protocol http
3-Si40951(config-cmap)#matc
3-Si40951(config-cmap)#match prot
3-Si40951(config-cmap)#match protocol https
3-Si40951(config-cmap)#matc
3-Si40951(config-cmap)#match prot
3-Si40951(config-cmap)#match protocol dns
3-Si40951(config-cmap)#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

c. Now that the class-maps are created, you can create the policy-maps.

In the commands below, the first line creates an inspect policy-map named INSIDE_TO_INTERNET. The second line binds the previously created INSIDE_PROTOCOLS class-map to the policy-map. All packets matched by the INSIDE_PROTOCOLS class-map will be subjected to the action taken by the INSIDE_TO_INTERNET policy-map. Finally, the third line defines the actual action this policy-map will apply to the matched packets. In this case, the matched packets will be inspected.

The next three lines creates a similar policy-map named CONFROOM_TO_INTERNET and attaches the CONFROOM_PROTOCOLS class-map.

The commands are as follows:

R3-S0000(config)# policy-map type inspect INSIDE_TO_INTERNET

R3-S0000(config-pmap)# class type inspect INSIDE_PROTOCOLS

R3-S0000(config-pmap-c)# inspect

R3-S0000(config)# policy-map type inspect CONFROOM_TO_INTERNET

```
R3-Si40951(config-cmap)#match pro
R3-Si40951(config-cmap)#match protocol udp
R3-Si40951(config-cmap)#ma
R3-Si40951(config-cmap)#match pro
R3-Si40951(config-cmap)#match protocol icmp
R3-Si40951(config-cmap)#exit
R3-Si40951(config)#clas
R3-Si40951(config)#class-map typ
R3-Si40951(config)#class-map type insp
R3-Si40951(config)#class-map type inspect matc
R3-Si40951(config)#class-map type inspect match-any CONFROOM_PROTOCOLS
R3-Si40951(config-cmap)#mat
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol http
R3-Si40951(config-cmap)#matc
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol https
R3-Si40951(config-cmap)#matc
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol dns
R3-Si40951(config-cmap)#exit
R3-Si40951(config)#pol
R3-Si40951(config)#policy-map ty
R3-Si40951(config)#policy-map type insp
R3-Si40951(config)#policy-map type inspect INSIDE_TO_INTERNET
R3-Si40951(config-pmap)#class
R3-Si40951(config-pmap)#class typ
R3-Si40951(config-pmap)#class type insp
R3-Si40951(config-pmap)#class type inspect INSIDE_PROTOCOLS
R3-Si40951(config-pmap-c)#insp
R3-Si40951(config-pmap-c)#inspect
R3-Si40951(config-pmap-c)#exit
R3-Si40951(config-pmap)#exit
R3-Si40951(config)#poli
R3-Si40951(config)#policy-map ty
R3-Si40951(config)#policy-map type insp
R3-Si40951(config)#policy-map type inspect CONFROOM_TO_INTERNET
R3-Si40951(config-pmap)#
```

R3-S0000(config-pmap)# class type inspect CONFROOM_PROTOCOLS

R3-S0000(config-pmap-c)# inspect

```
R3-Si40951(config-cmap)#exit
R3-Si40951(config)#clas
R3-Si40951(config)#class-map typ
R3-Si40951(config)#class-map type insp
R3-Si40951(config)#class-map type inspect matc
R3-Si40951(config)#class-map type inspect match-any CONFROOM_PROTOCOLS
R3-Si40951(config-cmap)#mat
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol http
R3-Si40951(config-cmap)#matc
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol https
R3-Si40951(config-cmap)#matc
R3-Si40951(config-cmap)#match prot
R3-Si40951(config-cmap)#match protocol dns
R3-Si40951(config-cmap)#exit
R3-Si40951(config)#pol
R3-Si40951(config)#policy-map ty
R3-Si40951(config)#policy-map type insp
R3-Si40951(config)#policy-map type inspect INSIDE_TO_INTERNET
R3-Si40951(config-pmap)#class
R3-Si40951(config-pmap)#class typ
R3-Si40951(config-pmap)#class type insp
R3-Si40951(config-pmap)#class type inspect INSIDE_PROTOCOLS
R3-Si40951(config-pmap-c)#insp
R3-Si40951(config-pmap-c)#inspect
R3-Si40951(config-pmap-c)#exit
R3-Si40951(config-pmap)#exit
R3-Si40951(config)#poli
R3-Si40951(config)#policy-map ty
R3-Si40951(config)#policy-map type insp
R3-Si40951(config)#policy-map type inspect CONFROOM_TO_INTERNET
R3-Si40951(config-pmap)#clas
R3-Si40951(config-pmap)#class typ
R3-Si40951(config-pmap)#class type insp
R3-Si40951(config-pmap)#class type inspect CONFROOM_PROTOCOLS
R3-Si40951(config-pmap-c)#inspect
R3-Si40951(config-pmap-c)#
```

Step 3: Create the Zone Pairs

A zone pair allows you to specify a unidirectional firewall policy between two security zones.

For example, a commonly used security policy dictates that the internal network can initiate any traffic towards the Internet but no traffic originating from the Internet should be allowed to reach the internal network.

This traffic policy requires only one zone pair, INTERNAL to INTERNET. Because zone-pairs define unidirectional traffic flow, another zone-pair must be created if Internet-initiated traffic must flow in the INTERNET to INTERNAL direction.

Notice that Cisco ZPF can be configured to inspect traffic that moves in the direction defined by the zone pair. In that situation, the firewall watches the traffic and dynamically creates rules allowing the return or related traffic to flow back through the router.

To define a zone pair, use the zone-pair security command. The direction of the traffic is specified by the source and destination zones.

For this lab, you will create two zone-pairs:

INSIDE_TO_INTERNET: Allows traffic leaving the internal network towards the Internet.

CONFROOM_TO_INTERNET: Allows Internet access from the ConfRoom network. a.

Creating the zone-pairs:

R3-S0000(config)# zone-pair security INSIDE_TO_INTERNET source INSIDE destination INTERNET

R3-S0000(config)# zone-pair security CONFROOM_TO_INTERNET source CONFROOM destination INTERNET

b. Verify the zone-pairs were correctly created by issuing the show zone-pair security command. Notice that no policies are associated with the zone-pairs yet. The security policies will be applied to zone-pairs in the next step.

R3-S0000# show zone-pair security

Copy and paste the output below

```
R3-Si40951#show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
   Source-Zone INSIDE  Destination-Zone INTERNET
   service-policy not configured
Zone-pair name CONFROOM_TO_INTERNET
   Source-Zone CONFROOM  Destination-Zone INTERNET
   service-policy not configured

R3-Si40951#
```

Step 4: Applying Security Policies

a. As the last configuration step, apply the policy-maps to the zone-pairs:

R3-S0000(config)# zone-pair security INSIDE_TO_INTERNET

R3-S0000(config-sec-zone-pair)# service-policy type inspect INSIDE_TO_INTERNET

R3-S0000(config)# zone-pair security CONFROOM_TO_INTERNET

R3-S0000(config-sec-zone-pair)# service-policy type inspect CONFROOM_TO_INTERNET

b. Issue the show zone-pair security command once again to verify the zone-pair configuration. Notice that the service-polices are now displayed:

R3-S0000#show zone-pair security

Zone-pair name INSIDE_TO_INTERNET

Source-Zone INSIDE Destination-Zone INTERNET service-

policy INSIDE_TO_INTERNET

Zone-pair name CONFROOM_TO_INTERNET

Source-Zone CONFROOM Destination-Zone INTERNET service-

policy CONFROOM_TO_INTERNET

```
R3-Si40951
*Mar  1 00:21:31.107: %SYS-5-CONFIG_I: Configured from console by console
R3-Si40951#sh
R3-Si40951#show zo
R3-Si40951#show zone-pa
R3-Si40951#show zone-pair sec
R3-Si40951#show zone-pair security
Zone-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy not configured
Zone-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy not configured

R3-Si40951#conf
3-Si40951#configure t
3-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
3-Si40951(config)#zone-pair security INSIDE_TO_INTERNET
3-Si40951(config-sec-zone-pair)#$icy type inspect INSIDE_TO_INTERNET
3-Si40951(config-sec-zone-pair)#exit
3-Si40951(config)#zone-pair security CONFROOM_TO_INTERNET
3-Si40951(config-sec-zone-pair)#$icy type inspect CONFROOM_TO_INTERNET
3-Si40951(config-sec-zone-pair)#exit
3-Si40951(config)#exit
3-Si40951#s
Mar  1 00:25:42.563: %SYS-5-CONFIG_I: Configured from console by console
3-Si40951#sh
3-Si40951#show zon
3-Si40951#show zone-pair sec
3-Si40951#show zone-pair security
one-pair name INSIDE_TO_INTERNET
    Source-Zone INSIDE  Destination-Zone INTERNET
    service-policy INSIDE_TO_INTERNET
one-pair name CONFROOM_TO_INTERNET
    Source-Zone CONFROOM  Destination-Zone INTERNET
    service-policy CONFROOM_TO_INTERNET

3-Si40951#
solarwinds | Solar-PuTTY free tool
© 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

To obtain more information about the zone-pairs, their policy-maps, the class-maps and match counters, use the show policy-map type inspect zone-pair command:

R3-S0000#show policy-map type inspect zone-pair

Copy and paste the output below

```
R3-Si40951#show policy-map type inspect zone-pair
 Zone-pair: INSIDE_TO_INTERNET

  Service-policy inspect : INSIDE_TO_INTERNET

    Class-map: INSIDE_PROTOCOLS (match-any)
      Match: protocol tcp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Maxever session creation rate 0
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
Zone-pair: CONFROOM_TO_INTERNET
```

```
Service-policy inspect : CONFROOM_TO_INTERNET

  Class-map: CONFROOM_PROTOCOLS (match-any)
    Match: protocol http
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol https
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol dns
      0 packets, 0 bytes
      30 second rate 0 bps
    Inspect
      Session creations since subsystem startup or last reset 0
      Current session counts (estab/half-open/terminating) [0:0:0]
      Maxever session counts (estab/half-open/terminating) [0:0:0]
      Last session created never
      Last statistic reset never
      Last session creation rate 0
      Maxever session creation rate 0
      Last half-open session total 0

  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      0 packets, 0 bytes
R3-Si40951#
```

Step 5: Assign Interfaces to the Proper Security Zones

Interfaces (physical and logical) are assigned to security zones with the zone-member security interface command.

a. Assign R3's f0/0 to the CONFROOM security zone:

R3-S0000(config)# interface f0/0

R3-S0000(config-if)# zone-member security CONFROOM

b. Assign R3's f0/1 to the INSIDE security zone:

R3-S0000(config)# interface f0/1

R3-S0000(config-if)# zone-member security INSIDE

```
R3-Si40951
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol dns
      0 packets, 0 bytes
      30 second rate 0 bps
    Inspect
      Session creations since subsystem startup or last reset 0
      Current session counts (estab/half-open/terminating) [0:0:0]
      Maxever session counts (estab/half-open/terminating) [0:0:0]
      Last session created never
      Last statistic reset never
      Last session creation rate 0
      Maxever session creation rate 0
      Last half-open session total 0

  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      0 packets, 0 bytes
3-Si40951#
3-Si40951#conf
3-Si40951#configure t
3-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
3-Si40951(config)#inte
3-Si40951(config)#interface fas
3-Si40951(config)#interface fastEthernet 0/0
3-Si40951(config-if)#zone-mem
3-Si40951(config-if)#zone-member secu
3-Si40951(config-if)#zone-member security CONFROOM
3-Si40951(config-if)#exit
3-Si40951(config)#int
3-Si40951(config)#interface fas
3-Si40951(config)#interface fastEthernet 0/1
3-Si40951(config-if)#zon
3-Si40951(config-if)#zone-member sec
3-Si40951(config-if)#zone-member security INSIDE
3-Si40951(config-if)#
solarwinds | Solar-PuTTY free tool   © 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

c. Assign R3's S0/1 to the INTERNET security zone:

R3-S0000(config)# interface s0/1

R3-S0000(config-if)# zone-member security INTERNET

```
R3-Si40951
      Current session counts (estab/half-open/terminating) [0:0:0]
      Maxever session counts (estab/half-open/terminating) [0:0:0]
      Last session created never
      Last statistic reset never
      Last session creation rate 0
      Maxever session creation rate 0
      Last half-open session total 0

  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      0 packets, 0 bytes
R3-Si40951#
3-Si40951#conf
3-Si40951#configure t
3-Si40951#configure terminal
nter configuration commands, one per line.  End with CNTL/Z.
3-Si40951(config)#inte
3-Si40951(config)#interface fas
3-Si40951(config)#interface fastEthernet 0/0
3-Si40951(config-if)#zone-mem
3-Si40951(config-if)#zone-member secu
3-Si40951(config-if)#zone-member security CONFROOM
3-Si40951(config-if)#exit
3-Si40951(config)#int
3-Si40951(config)#interface fas
3-Si40951(config)#interface fastEthernet 0/1
3-Si40951(config-if)#zon
3-Si40951(config-if)#zone-member sec
3-Si40951(config-if)#zone-member security INSIDE
3-Si40951(config-if)#exit
3-Si40951(config)#int
3-Si40951(config)#interface ser
3-Si40951(config)#interface serial 0/1
3-Si40951(config-if)#z
3-Si40951(config-if)#zone-member sec
3-Si40951(config-if)#zone-member security INTERNET
3-Si40951(config-if)#
solarwinds | Solar-PuTTY free tool   © 2019 SolarWinds Worldwide, LLC. All rights reserved.
```

Step 6: Verify Zone Assignment

a. Issue the show zone security command to ensure the zones were properly created, and the interfaces were correctly assigned:

R3-S0000# show zone security

zone self

Description: System defined zone

zone CONFROOM

Member Interfaces:

GigEthernet0/0

zone INSIDE

Member Interfaces:

GigEthernet0/1

zone INTERNET

Member Interfaces:

Serial0/0/1

```
R3-Si40951#show zone security
zone self
  Description: System defined zone


zone INSIDE
  Member Interfaces:
    FastEthernet0/1


zone CONFROOM
  Member Interfaces:
    FastEthernet0/0


zone INTERNET
  Member Interfaces:
    Serial0/1


R3-Si40951#
```

```
R3-Si40951(config-if)#zone-member security INSIDE
R3-Si40951(config-if)#exit
R3-Si40951(config)#int
R3-Si40951(config)#interface ser
R3-Si40951(config)#interface serial 0/1
R3-Si40951(config-if)#z
R3-Si40951(config-if)#zone-member sec
R3-Si40951(config-if)#zone-member security INTERNET
R3-Si40951(config-if)#exit
R3-Si40951(config)#sh
R3-Si40951(config)#exit
R3-Si40951#s
*Mar  1 00:31:56.967: %SYS-5-CONFIG_I: Configured from console by console
R3-Si40951#sh
R3-Si40951#show zon
R3-Si40951#show zone sec
R3-Si40951#show zone security
zone self
 Description: System defined zone


zone INSIDE
 Member Interfaces:
   FastEthernet0/1


zone CONFROOM
 Member Interfaces:
   FastEthernet0/0


zone INTERNET
 Member Interfaces:
   Serial0/1


R3-Si40951#
R3-Si40951#
```

solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All rights reserved.

b. **Even though no commands were issued to create a "self" zone, the output above still displays it. Why is R3 displaying a zone named "self"? What is the significance of this zone?**

The "self" zone is a special default security zone. This zone relates to traffic that originates in or is destined to the control plane of the router itself (e.g. routing protocols, SSH, SNMP, etc.). By default, all traffic is allowed into the "self" zone.

Part 3: ZPF Verification

Task 1: Verify ZPF Firewall Functionality **Step**

1: Traffic originating on the Internet

a. To test the firewall's effectiveness, ping PC-B from PC-A. In PC-A, open a command prompt and

issue: PC-A> ping 192.168.3.3

Was the ping successful? Explain.

No. The ICMP packets sent by PC-A enter R3 through its Serial0/0/1 interface. Because R3's serial 0/0/1 was assigned to the INTERNET zone, R3 correctly sees these ICMP packets as Internet originating packets. PC-B has an IP address of 192.168.3.3 which belongs to the IP range assigned to R3's G0/1 interface. Because R3's G0/1 was assigned to the INSIDE zone, R3 correctly assumes PC-B is a member of the INSIDE zone. Based on the security policy in place in R3, Internet originating packets should not be allowed to reach the internal network, and the ICMP packets generated by PC-A's ping are dropped.

b. **Ping PC-C from PC-A. In PC-A, open a command window and**

issue PC-A> ping 192.168.33.3

Was the ping successful? Explain.

No. The ICMP packets sent by PC-A enter R3 through its Serial0/0/1 interface. Because R3's serial 0/0/1 was assigned to the INTERNET zone, R3 correctly sees these ICMP packets as Internet originating packets.

c. Ping PC-A from PC-B. In PC-B, open a command window and issue

PC-B> ping 192.168.1.3

d. Was the ping successful? Explain.

Yes. The ICMP packets sent by PC-B enter R3 through its G0/1 interface. Because R3's G0/1 was assigned to the INSIDE zone, R3 correctly sees these ICMP packets as INSIDE originating packets. PCA has an IP address of 192.168.1.3 which doesn't belong any of R3's networks; R3 must use its default route through R2 to reach this destination.

f. **Ping PC-A from PC-C. In PC-C, open a command window and**

issue PC-C> ping 192.168.1.3

g. Was the ping successful? Explain.

No. The ICMP packets sent by PC-C enter R3 through its G0/0 interface. Because R3's G0/0 was assigned to the CONFROOM zone, R3 correctly sees these ICMP packets as ConfRoom originating packets. PC-A has an IP address of 192.168.1.3 which does not belong to any of R3's networks; R3 must use its default route through R2 to reach this destination. Because the packets will exit R3 via R3's s0/0/1 towards R2, R3 correctly concludes the ICMP packets are originating in the CONFROOM zone towards the INTERNET zone. Based on the security policy in place in R3, ConfRoom originating packets moving towards the INTERNET zone should only be allowed if they are HTTP or HTTPS or DNS packets. Since the ping generates ICMP packets, they are dropped and not able to reach PC-A.

Step 2: The Self Zone Verification

a. From PC-A ping R3's G0/1 interface:

PC-A> ping 192.168.3.1

Was the ping successful? Is this the correct behaviour? Explain.

Yes, the ping is successful and yes, the behaviour is correct. The policy is implemented in the place in R3 blocks internet going outside or inside conform zones. While R3 sees the ICMP packets generated by PC-A as Internet originating traffic, the ICMP packets are targeting R3's own IP assigned to G0/1. All of R3's own IP addresses (10.2.2.1, 192.168.33.1 and 192.168.3.1) are considered part of the Self zone. Because no policies were explicitly configured for the Self Zone, R3 follows the default behaviour and allows the packets.

b. From PC-C ping R3's G0/1 interface:

PC-C> ping 192.168.3.1

Was the ping successful? Is this the correct behaviour? Explain.

Yes, the ping is successful and yes, the behaviour is correct. The security policy in place in R3 blocks ConfRoom originating traffic going to the INSIDE zone. While R3 sees the ICMP packets generated by PC-C as ConfRoom originating traffic, the ICMP packets are targeting R3's own IP assigned to G0/1.

Save running configuration on all routers

R1-Si40951 | R2-Si40951 | R3-Si40951 | PC-A-Si40951 | PC-B-Si40951 | PC-C-Si40951

```
*Mar  1 00:00:07.715: %LINK-3-UPDOWN: Interface FastEthernet2/10, changed state to up
*Mar  1 00:00:07.719: %LINK-3-UPDOWN: Interface FastEthernet2/9, changed state to up
*Mar  1 00:00:07.719: %LINK-3-UPDOWN: Interface FastEthernet2/8, changed state to up
*Mar  1 00:00:07.723: %LINK-3-UPDOWN: Interface FastEthernet2/7, changed state to up
*Mar  1 00:00:07.723: %LINK-3-UPDOWN: Interface FastEthernet2/6, changed state to up
*Mar  1 00:00:07.727: %LINK-3-UPDOWN: Interface FastEthernet2/5, changed state to up
*Mar  1 00:00:07.727: %LINK-3-UPDOWN: Interface FastEthernet2/4, changed state to up
*Mar  1 00:00:07.731: %LINK-3-UPDOWN: Interface FastEthernet2/3, changed state to up
*Mar  1 00:00:07.731: %LINK-3-UPDOWN: Interface FastEthernet2/2, changed state to up
*Mar  1 00:00:07.739: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
 Mar  1 00:00:07.739: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
 Mar  1 00:00:08.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/15, changed state to down
 Mar  1 00:00:08.707: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/14, changed state to down
 Mar  1 00:00:08.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/13, changed state to down
 Mar  1 00:00:08.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/12, changed state to down
 Mar  1 00:00:08.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/11, changed state to down
 Mar  1 00:00:08.715: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/10, changed state to down
 Mar  1 00:00:08.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/9, changed state to down
 Mar  1 00:00:08.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/8, changed state to down
 Mar  1 00:00:08.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/7, changed state to down
 Mar  1 00:00:08.727: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/6, changed state to down
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#
2-Si40951#s
2-Si40951#cop
2-Si40951#copy ru
2-Si40951#copy running-config st
2-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
2-Si40951#
```

solarwinds | Solar-PuTTY *free tool* © 2019 SolarWinds Worldwide, LLC. All rights reserved.

R3-Si40951

```
R3-Si40951(config)#sh
R3-Si40951(config)#exit
R3-Si40951#s
*Mar  1 00:31:56.967: %SYS-5-CONFIG_I: Configured from console by console
R3-Si40951#sh
R3-Si40951#show zon
R3-Si40951#show zone sec
R3-Si40951#show zone security
zone self
  Description: System defined zone


one INSIDE
  Member Interfaces:
    FastEthernet0/1


one CONFROOM
  Member Interfaces:
    FastEthernet0/0


one INTERNET
  Member Interfaces:
    Serial0/1


3-Si40951#
3-Si40951#co
3-Si40951#cop
3-Si40951#copy sta
3-Si40951#copy runn
3-Si40951#copy running-config star
3-Si40951#copy running-config startup-config
estination filename [startup-config]?
uilding configuration...
OK]
3-Si40951#
```

solarwinds | Solar-PuTTY *free tool* © 2019 SolarWinds Worldwide, LLC. All rights reserved.