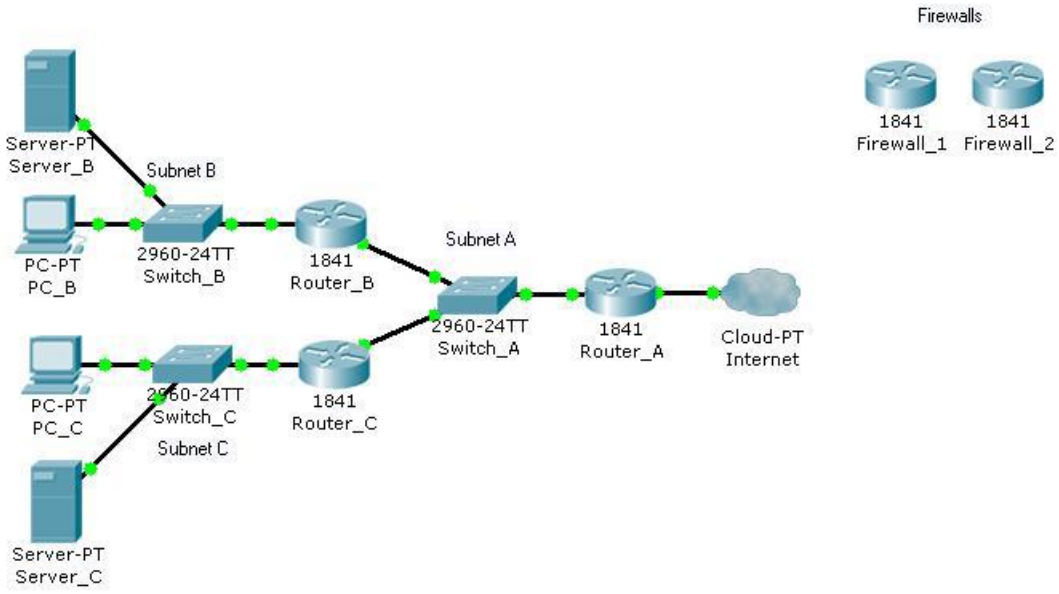
Planning Network-based Firewalls

Topology Diagram



Objectives

- Place firewalls in appropriate locations to satisfy security requirements.

Background / Preparation

You are a technician who provides network support for a medium-sized business. The business has grown and includes a research and development department working on a new, very confidential project. The livelihood of the project depends on protecting the data used by the research and development team.
Your job is to install firewalls to help protect the network, based on specific requirements. The Packet Tracer topology that you will use includes two preconfigured firewalls. In the two scenarios presented, you will replace the existing routers with the firewalls. The firewalls need to be configured with the appropriate IP address configurations, and the firewalls should be tested to ensure that they are installed and configured correctly.

Scenario 1: Protecting the Network from Hackers

Because the company is concerned about security, you recommend a firewall to protect the network from hackers on the Internet. It is very important that access to the network from the Internet is restricted. Firewall_1 has been preconfigured with the appropriate rules to provide the security required. You will install it on the network and confirm that it is functioning as expected.

Step 1: Replace Router_A with Firewall_1.

a. Remove Router_A and replace it with Firewall_1.
b. Connect the Fast Ethernet 0/0 interface on Firewall_1 to the Fast Ethernet 0/1 interface on Switch_A. Connect the Fast Ethernet 0/1 interface on Firewall_1 to the Ethernet 6 interface of the ISP cloud. (Use straight-through cables for both connections.)
c. Confirm that the host name of Firewall_1 is Firewall_1.
d. On Firewall_1, configure the WAN IP address and subnet mask for the FastEthernet 0/1 interface as 209.165.200.225 and 255.255.255.224.
e. Configure the LAN IP address and subnet mask for the Fast Ethernet 0/0 interface on Firewall_1

as 192.168.1.1 and 255.255.255.0.

Step 2: Verify the Firewall_1 configuration.

a. Use the **show run** command to verify your configuration. This is a partial example of the output.

```
Firewall_1#show run
Building configuration...
hostname Firewall_1
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 209.165.200.225 255.255.255.224
ip access-group 100 in
ip nat outside
duplex auto
speed auto
!
interface Vlan1
no ip address
shutdown
!
ip nat inside source list 1 interface FastEthernet0/0 overload
ip classless
ip route 192.168.2.0 255.255.255.0 192.168.1.2
ip route 192.168.3.0 255.255.255.0 192.168.1.3
!
access-list 1 permit 192.168.0.0 0.0.255.255
access-list 100 deny ip any host 209.165.200.225
<output omitted>
!
end
```

b. From PC_B, ping 209.165.200.225 to verify that the internal computer can access the Internet.

```
PC>ping 209.165.200.225
Pinging 209.165.200.225 with 32 bytes of data:
Reply from 209.165.200.225: bytes=32 time=107ms TTL=120
Reply from 209.165.200.225: bytes=32 time=98ms TTL=120
Reply from 209.165.200.225: bytes=32 time=104ms TTL=120
Reply from 209.165.200.225: bytes=32 time=95ms TTL=120
Ping statistics for 209.165.200.225:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 95ms, Maximum = 107ms, Average = 101ms
```

c. From privileged EXEC mode on Firewall_1, save the running configuration to the startup configuration using the **copy run start** command.

Scenario 2: Securing the Research and Development Network

Now that the entire network is secured from traffic originating from the Internet, secure the research and development network, Subnet C, from potential breaches from inside the network. The research and development team needs access to both the server on Subnet B and the Internet to conduct research. Computers on Subnet B should be denied access to the research and development subnet.

Firewall_2 has been preconfigured with the appropriate rules to provide the security required. You will install it on the network and confirm that it is functioning as expected.

Step 1: Replace Router_C with Firewall_2.

a. Remove Router_C and replace it with Firewall_2.
b. Connect the Fast Ethernet 0/1 interface on Firewall_2 to the Fast Ethernet 0/3 interface on Switch_A. Connect the Fast Ethernet 0/0 interface on Firewall_2 to the Fast Ethernet 0/1 interface on Switch_C. (Use straight-through cables for both connections.)
c. Confirm that the host name of Firewall_2 is Firewall_2.
d. On Firewall_2, configure the WAN IP address and subnet mask for the Fast Ethernet 0/1 interface as 192.168.1.3 and 255.255.255.0.
e. Configure the LAN IP address and subnet mask for the Fast Ethernet 0/0 interface of Firewall_2 as 192.168.3.1 and 255.255.255.0.

Step 2: Verify the Firewall_2 configuration.

a. Use the **show run** command to verify the configuration. This is a partial example of the output.

```
Firewall_2#show run
Building configuration...
...
!
interface FastEthernet0/0
ip address 192.168.3.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.1.3 255.255.255.0
ip access-group 100 in
ip nat outside
duplex auto
speed auto
!
access-list 1 permit 192.168.3.0 0.0.0.255
access-list 100 permit ip host 192.168.2.10 any
access-list 100 permit ip host 192.168.1.1 any
<output omitted>
!
end
```

b. From the command prompt on PC_B, use the **ping** command to verify that the computers on Subnet B cannot access the computers on Subnet C.

```
PC>ping 192.168.3.10
Pinging 192.168.3.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.3.10:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

c. From the command prompt on PC_C, use the **ping** command to verify that the computers on Subnet C can access the server on Subnet B.

```
PC>ping 192.168.2.10
Pinging 192.168.2.10 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.10: bytes=32 time=164ms TTL=120
Reply from 192.168.2.10: bytes=32 time=184ms TTL=120
Reply from 192.168.2.10: bytes=32 time=142ms TTL=120
Ping statistics for 192.168.2.10:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 142ms, Maximum = 184ms, Average = 163ms
```

d. From the command prompt on PC_C, use the **ping** command to verify that the computers on Subnet C can access the Internet.

PC>**ping 209.165.200.225**

Pinging 209.165.200.225 with 32 bytes of data:

Reply from 209.165.200.225: bytes=32 time=97ms TTL=120

Reply from 209.165.200.225: bytes=32 time=118ms TTL=120

Reply from 209.165.200.225: bytes=32 time=100ms TTL=120

Reply from 209.165.200.225: bytes=32 time=110ms TTL=120

Ping statistics for 209.165.200.225:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 97ms, Maximum = 118ms, Average = 106ms

e. From privileged EXEC mode on Firewall_2, save the running configuration to the startup configuration using the **copy run start** command.

f. Click the **Check Results** button at the bottom of this instruction window to check your work.

Reflection

a. Why would you install a firewall on the internal network?

b. How does a router that is configured to use NAT help protect computer systems on the inside of the NAT router?

c. Examine the location of Firewall_1 and Firewall_2 in the completed network topology. Which networks are considered trusted and untrusted for Firewall_1? Which networks are considered trusted and untrusted for Firewall_2?