Building a Secure Network

Abstract

I built a secure network using Cisco Packet Tracer. This is a simple network designed for a small company. It includes a Human Resources (HR) department and a Finance department. This secure network was created using the NIST Cybersecurity Framework (CSF) as a guideline. I've implemented VLANs, which ensure network segmentation and isolation. Additionally, I've implemented a firewall to protect against unauthorized access and contribute to secure network management. In conjunction with the firewall, I've implemented Access Control Lists (ACLs) to control access at both network perimeter and internal segments. Furthermore I have enabled SSH for secure remote access so that the network aligns with the Zero Trust model to make sure remote access is authenticated and encrypted. Also, password protections have been implemented to ensure only authorized users have access to critical network systems. After implementing all of these security controls, I tested each one to make sure they are running properly. This project is for my own education and to demonstrate my ability to understand and build a network in a cybersecurity context.

Step by Step Project Walkthrough

Step 1: Create a Basic Network Topology

1) Add Devices
    a) Place the router into the workspace
        i) We will use the **Cisco 1841 Router** as we are creating a basic network, and this router will allow us to implement firewalls and ACLs.

    b) Place two switches into the workspace
        i) We are going to use **2960 Switch** because it allows us to create a basic security network with everything we need
    c) Place 2 PCs next to Switch0 (this will be the Human Resources Department) and 2 PCs next to Switch1 (This will be the Finance Department)
2) Connect Devices
    a) Connect the switches to the PCs with **copper straight-through cables**
        i) Connect the cable from **FastEthernet0/1** in the **Switch0** to **FastEthernet0** in **PC0**
        ii) Connect the cable from **FastEthernet0/2** in the **Switch0** to **FastEthernet0** in **PC1**
        iii) Connect the cable from **FastEthernet0/3** in the **Switch1** to **FastEthernet0** in **PC2**
        iv) Connect the cable from **FastEthernet0/4** in the **Switch1** to **FastEthernet0** in **PC2**
    b) Connect the router to the switches with **copper straight-through cables**
        i) Connect the cable from **FastEthernet0/0** in the router **FastEthernet0/5** in **Switch0**
        ii) Connect the cable from **FastEthernet0/1** in the router **FastEthernet0/6** in **Switch1**

Step 2: Configure IP Addressing

1) Assign IP Addresses
    a) Set the router’s IP Address, and make sure the Port Status in each interface is turned on
        i) For **FastEthernet0/0** set the IPv4 address to 192.168.1.10
        ii) For **FastEthernet0/1** set the IPv4 address to 192.168.2.10

b) Set the PCs IP Addresses (Open the PC and click Desktop tab then IP Configuration)

i) For **PC0** set the static IPv4 address to 192.168.1.20

ii) For **PC1** set the static IPv4 address to 192.168.1.30

iii) For **PC2** set the static IPv4 address to 192.168.2.20

iv) For **PC4** set the static IPv4 address to 192.168.2.30

c) Set the **default gateway** to the same IP address as the router (for **PC0** and **PC1** use the router's **FastEthernet0/0** address and for **PC2** and **PC3** use the router's **FastEthernet0/1** address)

Step 3: Implement Basic Security with VLANs

1) Create VLANs on the switches

a) Create a VLAN named **VLAN 10** on **Switch0**

i)
```
Switch0> enable
Switch0# configure terminal
Switch0(config)# vlan 10
Switch0(config-vlan)# name HR
Switch0(config-vlan)# exit
```

b) Create a VLAN named **VLAN 20** on **Switch1**

i)
```
Switch1> enable
Switch1# configure terminal
Switch1(config)# vlan 20
Switch1(config-vlan)# name Finance
Switch1(config-vlan)# exit
```

2) Assign PCs to the correct VLAN within the switches

a) Assign **PC0** and **PC1** to **VLAN 10** (HR)

i)
```
Switch0(config)# interface range FastEthernet0/1-2
Switch0(config-if-range)# switchport mode access
Switch0(config-if-range)# switchport access vlan 10
Switch0(config-if-range)# exit
```

b) Assign **PC2** and **PC3** to **VLAN 20** (Finance)

i)
```
Switch1(config)# interface range FastEthernet0/3-4
```

```
Switch1(config-if-range)# switchport mode access
Switch1(config-if-range)# switchport access vlan 20
Switch1(config-if-range)# exit
```

3) Assign VLANs to the switch interface that connects to the router

   a) Assign **FastEthernet0/5** in **Switch0** to **VLAN 10** (HR)

      i)
      ```
      Switch0(config)# interface range FastEthernet0/5
      Switch0(config-if-range)# switchport mode access
      Switch0(config-if-range)# switchport access vlan 10
      Switch0(config-if-range)# exit
      ```

   b) Assign **FastEthernet0/6** in **Switch1** to **VLAN 20** (Finance)

      i)
      ```
      Switch1(config)# interface range FastEthernet0/6
      Switch1(config-if-range)# switchport mode access
      Switch1(config-if-range)# switchport access vlan 20
      Switch1(config-if-range)# exit
      ```

4) Test VLAN segmentation

   a) Use the “ping” command within a PC’s command prompt to see if it is able to connect to a PC in the same VLAN

   b) From **PC0** try to “ping” **PC1** (Since this PC is within the same VLAN the connection should be successful)

      i)
      ```
      C:\>ping 192.168.1.30
      ```

   c) From **PC0** and **FastEthernet0/0** ping the router interface IP (Since this PC is connected to this router interface the connection should be successful)

      i)
      ```
      C:\>ping 192.168.1.10
      ```

5) There is no need to create subinterfaces or do trunking because we have two separate physical interfaces (**Switch0** and **Switch1**) for both **VLAN 10** and **VLAN 20** (subinterfaces and trunking is only necessary when there are multiple VLANs on one physical device)

Step 4: Implement Access Control Lists (ACLs)

1) Create ACLs to restrict network traffic and to make sure there is proper network segmentation

a) Access Control Lists allow you to control the traffic entering and leaving the network.

b) On the router create an ACL to block access between the VLANS, but still allow essential services (use the two IPs for each router interface combined with a wildcard mask, which will include all possible IPs within that subnet)

   i)
   ```
   Router(config)# access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
   Router(config)# access-list 100 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
   Router(config)# access-list 100 permit ip any any
   ```

2) Apply the ACL to the router interfaces to filter traffic as it enters and leaves the VLANS

   a) Apply an ACL to **VLAN 10**

      i)
      ```
      Router(config)# interface FastEthernet0/0
      Router(config-subif)# ip access-group 100 in
      Router(config-subif)# exit
      ```

   b) Apply an ACL to **VLAN 20**

      i)
      ```
      Router(config)# interface FastEthernet0/1
      Router(config-subif)# ip access-group 100 in
      Router(config-subif)# exit
      ```

3) Verify the ACL configuration

   a) Check the configuration in the router’s CLI

      i)
      ```
      Router# show access-lists
      ```

   b) The result should look like this

      i)
      ```
      Extended IP access list 100
      10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 (8 match(es))
      20 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
      30 permit ip any any (4 match(es))
      ```

4) Verify the ACLs and VLANs are setup correctly

   a) Perform the same ping tests we performed in **Step 3** to ensure that the PCs are still able to connect to PCs and router interfaces within their VLAN

b) From **PC0** try to “ping” **FastEthernet0/1** (Since this PC is in **VLAN 10** and **FastEthernet0/1** is the gateway for **VLAN 20** the connection should be unsuccessful)

i)
```
C:\>ping 192.168.2.10
```

c) From **PC0** try to “ping” **PC2** (Since this **PC0** is in **VLAN 10** and **PC2** is in **VLAN 20** the connection should be unsuccessful)

i)
```
C:\>ping 192.168.2.20
```

d) You can try different variations of the ping test to make absolutely sure the ACLs and VLANs are configured properly

e) Ultimately all devices and interfaces within **VLAN 10** should only be able to ping each other and all devices and interfaces within **VLAN 20** should only be able to ping each other

Step 5: Secure the Router and Switches with Passwords

1) Create console passwords to prevent unauthorized users from accessing physical devices

a) First, the router

i)
```
Router(config)# line con 0
Router(config-subif)# password C0mp1exx
Router(config-subif)# login
Router(config-subif)# exit
```

f) Then, **Switch 0**

i)
```
Switch0(config)# line con 0
Switch0(config-subif)# password F1ying_Pi3
Switch0(config-subif)# login
Switch0(config-subif)# exit
```

g) Next, **Switch 1**

i)
```
Switch1(config)# line con 0
Switch1(config-subif)# password MaN1k!Ham
Switch1(config-subif)# login
Switch1(config-subif)# exit
```

2) Create password for VTY (Virtual Terminal), which allows remote access through Telnet or SSH, so that there is secure remote access

a) First, the router

  i)
    ```
    Router(config)# line vty 0 4
    Router(config-line)# password Big.beaR99
    Router(config-line)# login
    Router(config-line)# exit
    ```

b) Then, **Switch 0**

  i)
    ```
    Switch0(config)# line vty 0 4
    Switch0(config-line)# password hairee55LEAVEz
    Switch0(config-line)# login
    Switch0(config-line)# exit
    ```

c) Next, **Switch 1**

  i)
    ```
    Switch1(config)# line vty 0 4
    Switch1(config-line)# password barnacle!SQuar333
    Switch1(config-line)# login
    Switch1(config-line)# exit
    ```

3) Create the enable password to allow certain users to access privileged EXEC mode

a) First, the router

  i)
    ```
    Router(config)# enable secret red.graPe!!7
    ```

b) Then, **Switch 0**

  i)
    ```
    Switch0(config)# enable secret Pan.daF33t
    ```

c) Next, **Switch 1**

  i)
    ```
    Switch1(config)# enable secret F0revrPirate980
    ```

Step 6: Configure SSH for Secure Remote Access

1) There are two ways to access the switches and router remotely, Telnet and SSH, and SSH is the more secure of the two

a) For SSH a hostname and domain name must be set, and first start with the router

  i)
    ```
    Router(config)# hostname Good Company
    GoodCompany(config)# ip domain-name goodcompany.com
    ```

b) Generate RSA keys for SSH

        - i) GoodCompany(config)# crypto key generate rsa
    - c) Then you will be prompted to choose the size of the key modulus
        - i) How many bits in the modulus [512]: 1024
    - d) Enable Version 2 of SSH
        - i) GoodCompany(config)# ip ssh version 2
    - e) Configure the VTY lines to use SSH
        - i) GoodCompany(config)# line vty 0 4
          GoodCompany(config-line)# transport input ssh
          GoodCompany(config-line)# login local
          GoodCompany(config-line)# exit
    - f) Create a local username and password
        - i) GoodCompany(config)# username admin secret tipsy.turvy!1839
- 2) Now enable SSH for **Switch 0**
    - a) For SSH a hostname and domain name must be set
        - i) Switch0(config)# hostname HR-Switch0
          HR-Switch0(config)# ip domain-name goodcompany.com
    - b) Generate RSA keys for SSH
        - i) HR-Switch0(config)# crypto key generate rsa
    - c) Then you will be prompted to choose the size of the key modulus
        - i) How many bits in the modulus [512]: 1024
    - d) Enable Version 2 of SSH
        - i) HR-Switch0(config)# ip ssh version 2
    - e) Configure the VTY lines to use SSH
        - i) HR-Switch0(config)# line vty 0 4
          HR-Switch0(config-line)# transport input ssh
          HR-Switch0(config-line)# login local
          HR-Switch0(config-line)# exit
    - f) Create a local username and password
        - i) HR-Switch0(config)# username admin secret Maybee432!Man
- 3) Now enable SSH for **Switch 1**
    - a) For SSH a hostname and domain name must be set

        i) Switch1(config)# hostname Finance-Switch1
           Finance-Switch1(config)# ip domain-name goodcompany.com

    b) Generate RSA keys for SSH
        i) Finance-Switch1(config)# crypto key generate rsa
    c) Then you will be prompted to choose the size of the key modulus
        i) How many bits in the modulus [512]: 1024
    d) Enable Version 2 of SSH
        i) Finance-Switch1(config)# ip ssh version 2
    e) Configure the VTY lines to use SSH
        i) Finance-Switch1(config)# line vty 0 4
           Finance-Switch1(config-line)# transport input ssh
           Finance-Switch1(config-line)# login local
           Finance-Switch1(config-line)# exit
    f) Create a local username and password
        i) Finance-Switch1(config)# username admin secret forty3_0France

Step 7: Enable Firewall and Security Features

1) Implement a firewall using CBAC (this is a Cisco firewall feature that contributes to an effective firewall that monitors outbound traffic and allows related inbound traffic, so that unauthorized traffic is blocked)
2) Implement a set of CBAC inspection rules, to inspect TCP and UDP traffic
    a) In the router, implement an inspection rule for TCP and UDP, so that the router inspects and tracks outgoing TCP and UDP traffic to allow related inbound responses
        i) GoodCompany(config)# ip inspect name Firewall tcp
           GoodCompany(config)# ip inspect name Firewall udp
3) Now, apply firewall rules to to the interfaces that connect to **VLAN 10** (HR) and **VLAN 20** (Finance), so these are **FastEthernet0/0** and **FastEthernet0/1** respectively

a) First, apply the firewall inspection to **VLAN 10**, which will allow traffic entering this interface to be inspected

   i)
   ```
   GoodCompany(config)# interface FastEthernet0/0
   GoodCompany(config-if)# ip inspect Firewall in
   GoodCompany(config-if)#exit
   ```

b) Next, apply the firewall inspection to **VLAN 20**, which will allow traffic entering this interface to be inspected

   i)
   ```
   GoodCompany(config)#interface FastEthernet0/1
   GoodCompany(config-if)#ip inspect Firewall in
   GoodCompany(config-if)#exit
   ```

Step 8: Test Network Security

1) Now that all of the security controls have been implemented we will test the connection between the PCs, SSH access, ACL functionality, and firewall effectiveness

   a) Perform a ping test between a PC in **VLAN 10** (HR) (**PC0** / 192.168.1.20) and a PC in **VLAN 20** (Finance) (**PC2** / 192.168.2.20), and if the ACLs and Firewalls are properly implement, the ping test should fail

      i)
      ```
      C:\>ping 192.168.2.20
      Pinging 192.168.2.20 with 32 bytes of data:
      Reply from 192.168.1.10: Destination host unreachable.
      Reply from 192.168.1.10: Destination host unreachable.
      Reply from 192.168.1.10: Destination host unreachable.
      Reply from 192.168.1.10: Destination host unreachable.
      Ping statistics for 192.168.2.20:
      Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
      ```

   b) Perform a ping test between a PC in **VLAN 10** (HR) (**PC0** / 192.168.1.20) and a PC in **VLAN 10** (HR) (**PC1** / 192.168.1.30), and the ping test should be successful

      i)
      ```
      C:\>ping 192.168.1.30
      Pinging 192.168.1.30 with 32 bytes of data:
      Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
      ```

```
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Reply from 192.168.1.30: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.30:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

c) On a PC (**PC 0**) see if it’s possible to SSH into the router using the router's admin username (admin) and IP address (192.168.1.10) for the interface (**FastEthernet0/0**) the PC and Switch are connected to, to see if secure remote access is set up correctly

   i)
   ```
   C:\> ssh -l admin 192.168.1.10
   Password: tipsy.turvy!1839
   GoodCompany>
   ```