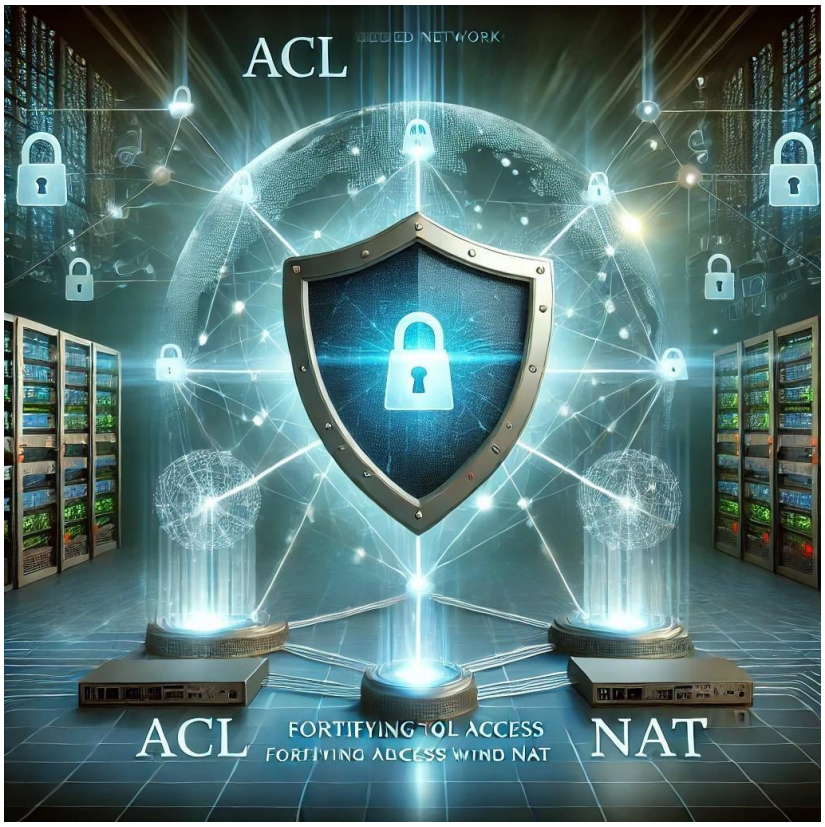
رواد مصر الرقمية



THE SHIELDED NETWORK

Fortifying Access with ACLs and NAT

Eng / Al Hussein Ahmed

TEAM MEMBERS:

Manar Nasser

Malak Abdelaziz

Yassin Tamer

AbdallahMohamed

Zaid Ali

رواد مصر الرقمية

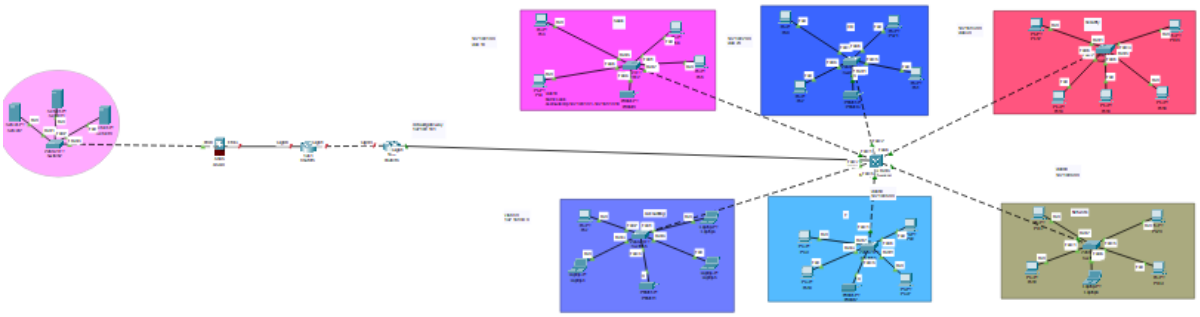
The Shielded Network

<< Fortifying Access with ACLs and NAT >>

Project Overview:

- **Objective:** Secure network traffic using ACLs and manage IP address usage using NAT. ○ **Tools:** Cisco Packet Tracer ○ **Scope:**
- Filter network traffic using ACLs ○ Enable secure internet access using NAT
- Ensure internal network devices are protected from unauthorized access

Network Topology Design:



Configuration:

Steps to Configure DHCP on a Multilayer Switch

1. Set Up VLANs

- Ensure VLANs are configured on the switch for each subnet that needs a DHCP service.

2. Assign IP Addresses to VLAN Interfaces

- Each VLAN must have an interface configured with an IP address to serve as the default gateway.

3. Enable Routing on the Switch

- Enable IP routing to allow inter-VLAN communication.

4.Configure DHCP Pools

- Create DHCP pools for each VLAN to provide dynamic IP addresses.

```
Switch(config)#interface f0/7
Switch(config-if)#switchport trunk encapsulation dotlq
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#interface f0/5
Switch(config-if)#switchport trunk encapsulation dotlq
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
Switch(config)#interface f0/6
Switch(config-if)#switchport trunk encapsulation dotlq
Switch(config-if)#switchport mode trunk
Switch(config-if)#ex
```

5. Verify the DHCP Configuration

- After completing the configuration, verify that the DHCP server is operational.

7. Configure DHCP Snooping for Security (To protect against rogue DHCP servers, enable DHCP snooping.)

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gig0/1, Gig0/2
40   accounting                       active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

1. Create VLANs on the Layer 2 Switch

Ensure the same VLANs as those on the MLS are created**.**

2. Assign VLANs to Switch Ports

Assign specific ports to the respective VLANs**.**

3. Configure the Trunk Link to the Multilayer Switch

Set the port connecting to the MLS as a trunk port to carry multiple VLANs.

```
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#switchport trunk allowed vlan 60
Switch(config-if)#no shutdown
Switch(config-if)#
Switch(config-if)#ex
Switch(config)#int fa0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up

Switch(config-if)#switchport trunk allowed vlan 50
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/5 (1),
with Switch FastEthernet0/1 (50).

Switch(config-if)#switchport trunk allowed vlan 50
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#no shutdown
Switch(config-if)#ex
Switch(config)#
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int fa0/8
Switch(config-if)#no shutdown
Switch(config-if)#e
Switch(config)#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (50), with Switch FastEthernet0/5 (1).

Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (50), with Switch FastEthernet0/5 (1).

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 50
Switch(config-vlan)#name it
Switch(config-vlan)#ex
Switch(config)#interface range fa0/20
Switch(config-if-range)#ex
Switch(config)#interface range fa0/1-20
Switch(config-if-range)#switchport mode access
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on FastEthernet0/1 (50), with Switch FastEthernet0/5 (1).

Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#ex
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk
```

```
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan 50
Switch(config-if-range)#ex
Switch(config)#int fa0/1
Switch(config-if)#switchport mode trunk

Switch(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

Switch(config-if)#switchport trunk allowed vlan 50
Switch(config-if)#ex
Switch(config)#spanning-tree mode rapid-pvst
Switch(config)#ex
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gig0/1, Gig0/2
50   it                               active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                Fa0/18, Fa0/19, Fa0/20
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
```

Enable Spanning Tree Protocol

Prevent network loops with STP. Enable Rapid Spanning Tree Protocol (RSTP) for better performance.