1. Overview

In this **lab project**, I designed, configured, and implemented a robust and secure multi-vendor network infrastructure. We utilized a **Cisco Catalyst Switch (C3750)**, a **FortiGate 100E Next-Generation Firewall**, and a **Cisco C2800 Router (PE/CPE)**. It's important to note that the appliances used in this project are **older models and considered End-of-Life (EOL)**, but they served as excellent platforms for hands-on learning and demonstrating core networking and security principles. Our primary goal was to establish efficient internal network communication, secure internet access, and apply traffic control. Key functionalities I configured include **VLANs for network segmentation**, **EtherChannel for link aggregation and redundancy**, **Source Network Address Translation (SNAT)** for internet access, comprehensive **firewall policies**, and **web content filtering**.

2. Objectives

The main objectives I aimed to achieve in this project were to:

• **Establish a segmented internal network** using VLANs (VLAN 10 and VLAN 20) with specific IP subnets (10.0.10.0/24 and 10.0.20.0/24 respectively).

• **Implement high-availability and increased bandwidth** between the Cisco Switch and the FortiGate firewall using an EtherChannel configured with LACP.

• **Configure the FortiGate firewall** to act as a central security and routing device, defining zones, address groups, and managing inter-VLAN and internet-bound traffic.

• **Provide secure internet access** for internal networks through the FortiGate and a Cisco Router, utilizing Source NAT (SNAT) on both the FortiGate and the Cisco Router.

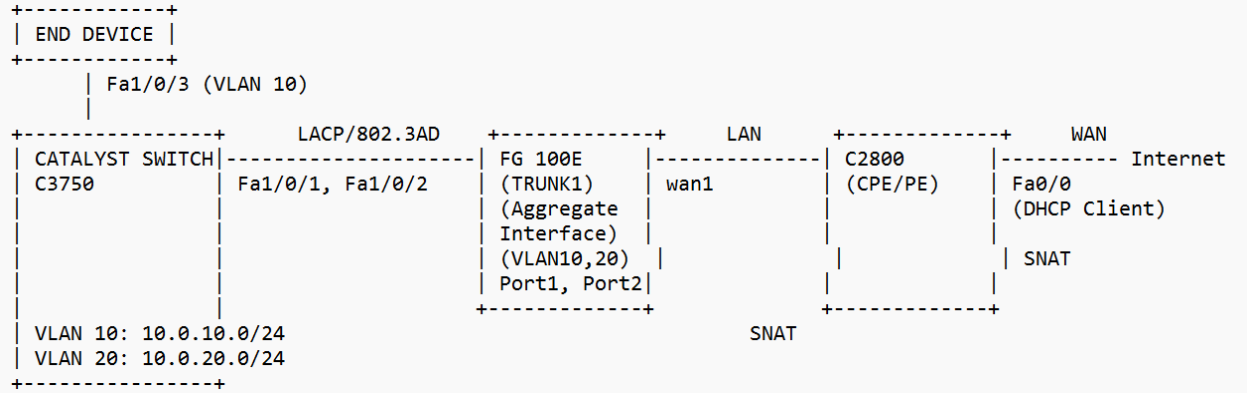
• **Implement web content filtering** on the FortiGate to control access to specific categories or URLs.

• **Configure the Cisco Router (PE)** as a WAN edge device, obtaining an IP address via DHCP and performing SNAT for outbound internet traffic.

• **Ensure network stability and prevent loops** on access ports by enabling Spanning-Tree PortFast on the Cisco Switch.

3. Network Diagram

The designed network topology is as follows, illustrating the layered approach:



This diagram depicts:

• An **End Device** connecting to the Cisco Catalyst Switch via FastEthernet1/0/3.

• The **Cisco Catalyst Switch C3750** serving as the access layer, connecting end devices and aggregating traffic from VLANs 10 (10.0.10.0/24) and 20 (10.0.20.0/24). It connects to the FortiGate via an **EtherChannel (TRUNK1)** formed by FastEthernet1/0/1 and FastEthernet1/0/2, utilizing **LACP (Link Aggregation Control Protocol)** for link aggregation and redundancy.

• The **FortiGate 100E Firewall** acting as the distribution/core layer, providing inter-VLAN routing, firewall security, and connecting the internal network (LAN) to the external network (WAN) via the Cisco C2800 Router. VLANs 10 and 20 are terminated on sub-interfaces of the aggregate link (TRUNK1).

• The **Cisco C2800 Router (PE)** functioning as the WAN edge router, connecting the FortiGate to the internet. It obtains its WAN IP via DHCP and performs Source NAT (SNAT) before forwarding traffic to the internet. SNAT is also performed on the FortiGate for traffic exiting to the WAN.

4. Components Used

The following network devices were utilized in this project:

• **FortiGate-100E (Next-Generation Firewall)**:

  ◦ **Model**: FortiGate-100E.

  ◦ **Firmware Version**: 05000008 (dated 12:19-01.31.2017).

  ◦ **Serial Number**: FG100ETK18011980.

  ◦ **CPU**: 1000MHz.

  ◦ **Total RAM**: 4 GB.

  ◦ **Role**: Security gateway, routing, NAT, web filtering.

◦ **Note**: This appliance is an **older model and is considered End-of-Life (EOL)**.

• **Cisco Catalyst Switch C3750 (Layer 2/3 Switch)**:

◦ **Role**: Network access, VLAN segmentation, EtherChannel.

◦ **Note**: This appliance is an **older model and is considered End-of-Life (EOL)**.

• **Cisco C2800 Router (PE/CPE)**:

◦ **Role**: WAN connectivity, DHCP client, Source Network Address Translation (SNAT).

◦ **Note**: This appliance is an **older model and is considered End-of-Life (EOL)**.

5. Configuration Steps

5.1. Cisco Router (PE) Configuration

I configured the Cisco C2800 Router to handle WAN connectivity and Source Network Address Translation (SNAT).

1. **Interface IP Address Configuration**:

◦ **FastEthernet0/1 (Internal Interface)**: I configured this interface with a static IP address of **172.16.1.2 255.255.255.252**. I then designated it as the ip nat inside interface.

◦ **FastEthernet0/0 (WAN Interface)**: I configured this interface as a **DHCP client** to automatically obtain its IP address and other network parameters from an upstream DHCP server. It successfully acquired the IP address **10.0.100.184** with a subnet mask of **255.255.252.0**. I designated this interface as the ip nat outside interface.

2. **Source NAT (SNAT) Configuration**:

◦ I created a standard numbered **Access Control List (ACL)** to permit all internal traffic (access-list 1 permit any) that should be translated.

◦ I applied the NAT rule ***ip nat inside source list 1 interface FastEthernet0/0 overload***. This command enables **Port Address Translation (PAT)**, allowing multiple internal devices to share the single public IP address of FastEthernet0/0 when accessing external networks.

3. **Default Gateway**: The router automatically learned a default route (S* 0.0.0.0/0 [254/0] via 10.0.100.1) with the gateway of last resort being **10.0.100.1**, which was received via DHCP.

5.2. Cisco Catalyst Switch Configuration

I configured the Cisco Catalyst C3750 Switch for VLAN segmentation, trunking, and EtherChannel.

1. **VLAN Access Port Configuration with Spanning-Tree PortFast**:

◦ I configured **FastEthernet1/0/3** as an **access port** and assigned it to **VLAN 10** (switchport mode access, switchport access vlan 10).

◦ I enabled **Spanning-Tree PortFast** on FastEthernet1/0/3 (*spanning-tree portfast enable*). A warning was generated, emphasizing that PortFast should only be used on ports connected to a single host to prevent potential bridging loops and that it only takes effect in a non-trunking mode.

2. **VLAN Trunk Ports and EtherChannel (LACP) Configuration**:

◦ I selected an **interface range** for **FastEthernet1/0/1** and **FastEthernet1/0/2**.

◦ These interfaces were configured for **802.1Q trunk encapsulation** (*switchport trunk encapsulation dot1q*) and set to **trunking mode** (*switchport mode trunk*).

◦ **VLANs 10 and 20** were explicitly allowed on this trunk link (switchport trunk allowed vlan 10,20).

◦ I created a **Layer 2 EtherChannel** using these two interfaces by configuring **channel-group 1 mode active**. The active mode enabled **LACP (Link Aggregation Control Protocol)**, allowing the switch to actively negotiate the EtherChannel with the FortiGate.

5.3. FortiGate 100E Configuration

I configured the FortiGate 100E for initial setup, internal VLAN management, network zoning, address groups, firewall policies, and web filtering.

1. **Initial Setup**:

◦ During initial attempts, multiple incorrect login attempts for the admin user were observed.

◦ I performed a **factory reset** (*execute factoryreset*) to restore the device to its default configuration, followed by a system reboot.

◦ The default mgmt interface had an IP address of **192.168.1.99 255.255.255.0** and allowed ping, https, and ssh access.

2. **Aggregate Interface and VLANs**:

◦ As indicated in the diagram, an aggregate interface named **"TRUNK1"** was formed using **Port1** and **Port2** on the FortiGate to connect to the Cisco Switch.

◦ VLAN interfaces **Trunk1VLAN10** and **Trunk1VLAN20** were configured as sub-interfaces on this aggregate link to handle traffic for VLAN 10 and VLAN 20, respectively.

3. **Zone Configuration**:

◦ I created a **security zone named "VLANS"**.

◦ This zone was configured with ***set intrazone allow***, permitting traffic to flow between interfaces within this zone (e.g., between Trunk1VLAN10 and Trunk1VLAN20).

◦ The VLAN interfaces **"Trunk1VLAN10"** and **"Trunk1VLAN20"** were added as members of the "VLANS" zone.

4. **Address Group Configuration**:

◦ I created an address group named **"VLANS"**, including **"Trunk1VLAN10 address"** and **"Trunk1VLAN20 address"**. This group simplifies policy creation by referencing both internal VLAN networks collectively.

◦ I also configured additional address groups, such as **"G Suite"** (including "gmail.com" and "wildcard.google.com") and **"Microsoft Office 365"** (including "login.microsoftonline.com", "login.microsoft.com", and "login.windows.net"), likely for targeted policy enforcement.

5. **WAN Interface Configuration**:

◦ I configured the **"wan1"** interface with the static IP address **172.16.1.1 255.255.255.252**.

◦ It was assigned a wan role and allowed ping access. This interface connects to the Cisco C2800 Router's FastEthernet0/1 interface.

6. **Firewall Policy Configuration**:

◦ I established a firewall policy named **"LAN2INTERNET" (ID 1)** to permit outbound traffic.

◦ **Source Interface**: "VLANS" zone.

◦ **Source Address**: "VLANS" address group.

◦ **Destination Interface**: "wan1".

◦ **Destination Address**: "all" (internet).

◦ **Action**: accept.

◦ **Services**: "PING" and "Web Access" were specifically allowed.

◦ **UTM (Unified Threat Management)**: Enabled, using both "certificate-inspection" for SSL/SSH and “deep inspection” (to verify the differences) and a webfilter profile to block a website.

◦ **Logging**: All traffic matching this policy was configured to be logged (set logtraffic all).

◦ **NAT**: Enabled for this policy (set nat enable), indicating the FortiGate performs NAT for traffic leaving the "VLANS" zone towards "wan1".

7. **Web Filtering Profile**:

◦ I configured a web filtering profile named **"Blocking BADWEBSITE"** and applied it to the "LAN2INTERNET" policy. This profile was specifically set up for **URL filtering only**.

6. Verification and Testing

I performed several verification steps to ensure connectivity and correct configuration:

• **Cisco Router (PE)**:

◦ **IP Address and Status**: *show ip int brief* confirmed FastEthernet0/0 obtained **10.0.100.184** via DHCP and FastEthernet0/1 was configured with **172.16.1.2**, both interfaces showing up/up status.

◦ **Routing**: *show ip route* confirmed the default gateway via DHCP and directly connected routes.

◦ **Connectivity to FortiGate**: I successfully pinged **172.16.1.1** (FortiGate's wan1 interface) with an 80% then 100% success rate. (**ARP resolution delayed first ping packet)**

◦ **Internet Connectivity with NAT**: I successfully pinged **1.1.1.1** with a 100% success rate, verifying internet access through the NAT configuration.

◦ **NAT Configuration**: *show run | s ip nat* and *show access-list* confirmed the ip nat inside/outside interface assignments, the *access-list 1 permit any*, and *the ip nat inside source list 1 interface FastEthernet0/0 overload* rule.

• **Cisco Catalyst Switch**:

◦ **VLAN Configuration**: do show vlan brief confirmed VLANs 10 and 20 were active.

◦ **EtherChannel Status**: show etherchannel summary confirmed **Port-channel 1 (Po1)** was created, operating in **LACP (SU)** mode, bundling **Fa1/0/1(P)** and **Fa1/0/2(P)**.

• **FortiGate 100E**:

◦ The show system zone, show system interface wan1, show firewall policy, and show firewall addrgrp commands confirmed the configuration of zones, interfaces, policies, and address groups. Implicit verification of policies and web filtering would involve attempting to access allowed and blocked websites from a device in VLAN 10 or 20, and checking firewall logs. The configuration explicitly shows logtraffic all for the "LAN2INTERNET" policy, indicating detailed

logging for monitoring and verification. The successful ping from the PE router to the FortiGate's WAN interface also confirmed basic connectivity to the firewall.

7. Security Considerations

While this lab project implemented several security measures, it's crucial to acknowledge areas where the current design presents **limitations in terms of redundancy, impacting overall security and availability**.

• **Single Points of Failure**: A significant security consideration in the current design is the **lack of redundancy for key network components**. There is a **single Cisco C2800 Router (CPE)** and a **single FortiGate 100E firewall**. This means that a failure in either of these devices would result in a complete loss of internet connectivity and security services for the internal network. This **reduces the overall resilience and availability** of the network, making it vulnerable to outages caused by hardware failure, software bugs, or even misconfiguration.

• **Network Segmentation**: My use of **VLANs 10 and 20** isolates different traffic types or user groups, limiting the scope of potential breaches.

• **Next-Generation Firewall (FortiGate)**: The FortiGate 100E acts as a central enforcement point, providing granular control over traffic flow between internal networks and the internet.

• **Firewall Policies**: The "LAN2INTERNET" policy I configured explicitly defines what traffic (source, destination, service) is allowed, adhering to the principle of least privilege.

• **Source NAT (SNAT)**: Both the FortiGate and Cisco Router utilize SNAT, hiding the internal IP addressing scheme from external networks, which adds a layer of privacy and security.

• **Web Filtering**: The "Blocking BADWEBSITE" webfilter profile, applied with SSL/SSH inspection, helps prevent access to malicious or inappropriate websites, protecting users from web-based threats.

• **Password Enforcement**: The forced password change on the FortiGate after a factory reset ensures that default or weak credentials are not left exposed.

• **Spanning-Tree PortFast**: By enabling PortFast on access ports, I ensured the switch prevents temporary bridging loops that could occur when a new device is connected, enhancing network stability and preventing denial-of-service attacks that exploit loop conditions.

• **Traffic Logging**: The "LAN2INTERNET" policy includes set logtraffic all, ensuring that all traffic flowing through this policy is recorded for auditing, security monitoring, and incident response.

8. Future Improvements

While the current lab setup provides a solid foundation for demonstrating core networking concepts, I recognize that significant improvements focusing on **redundancy, modern security, and operational efficiency** would be essential for a production environment:

• **Implement High Availability for Critical Devices**:

◦ **Dual FortiGate Firewalls in HA**: To address the single point of failure with the current single FortiGate, deploying a **second FortiGate firewall in a High Availability (HA) cluster** is crucial. This would ensure continuous security and network operation by providing automatic failover if one unit fails.

◦ **Dual Cisco CPE Routers with HSRP/VRRP**: Introducing a **second Cisco C2800 Router (CPE)** at the WAN edge, configured with **HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol)**, would provide redundancy for internet access. This ensures that if one router fails, the other can seamlessly take over the gateway role, addressing the single point of failure of the current CPE.

• **Upgrade to Modern, Supported Appliances**: As noted, the current appliances are **old and End-of-Life (EOL)**. Upgrading to newer, vendor-supported models for the Cisco Switch, FortiGate firewall, and Cisco Router would provide:

◦ Access to the latest security features and threat intelligence.

◦ Performance improvements (faster CPUs, higher throughput).

◦ Vendor support and regular security patches.

◦ Improved manageability and automation capabilities.

• **Intrusion Prevention System (IPS)/Antivirus**: Currently, only web filtering is explicitly mentioned. Integrating and configuring **IPS and Antivirus profiles** on the FortiGate would add another critical layer of defense against known exploits and malware, inspecting traffic for malicious payloads and activities.

• **Centralized Logging and Monitoring**: Implementing a **FortiAnalyzer** or a similar SIEM (Security Information and Event Management) solution would provide centralized logging, real-time threat intelligence, correlation of events, and enhanced reporting capabilities for the FortiGate.

• **Wireless Network Integration**: If not already present, integrating a secure wireless network with appropriate VLANs and firewall policies would extend connectivity securely to mobile devices.

• **Quality of Service (QoS)**: Implementing QoS policies on the FortiGate and Cisco devices could prioritize critical business applications (e.g., VoIP, video conferencing) over less critical traffic, especially during periods of high network utilization.

• **Configuration Backup and Restore**: Establishing automated routines for backing up configurations of all network devices would be crucial for disaster recovery and efficient restoration in case of unexpected failures.

• **Network Access Control (NAC)**: Implementing a NAC solution could enforce granular access policies for devices connecting to the switch, ensuring only authorized and compliant devices can access the network resources.

• **IPv6 Implementation**: As IPv6 adoption grows, configuring and securing IPv6 connectivity and services would future-proof the network.