Network Security Fundamentals & FortiGate Integration

Fortinet Course Project

Presented by:

Ziad Saad, Ahmed Abdelnaser, Nada Amna, Rawan Ashraf, Nour Kholeif

Instructor:

Ahmed Mahmoud

Presentation Outline

Presentation Outline

Project Overview

Our primary goal is to establish a secure and functional network using FortiGate, demonstrating practical application of network security principles.

Network Setup

Configuring basic network infrastructure and device connectivity.

Firewall & Interfaces

Implementing FortiGate as the central firewall and setting up its various interfaces.

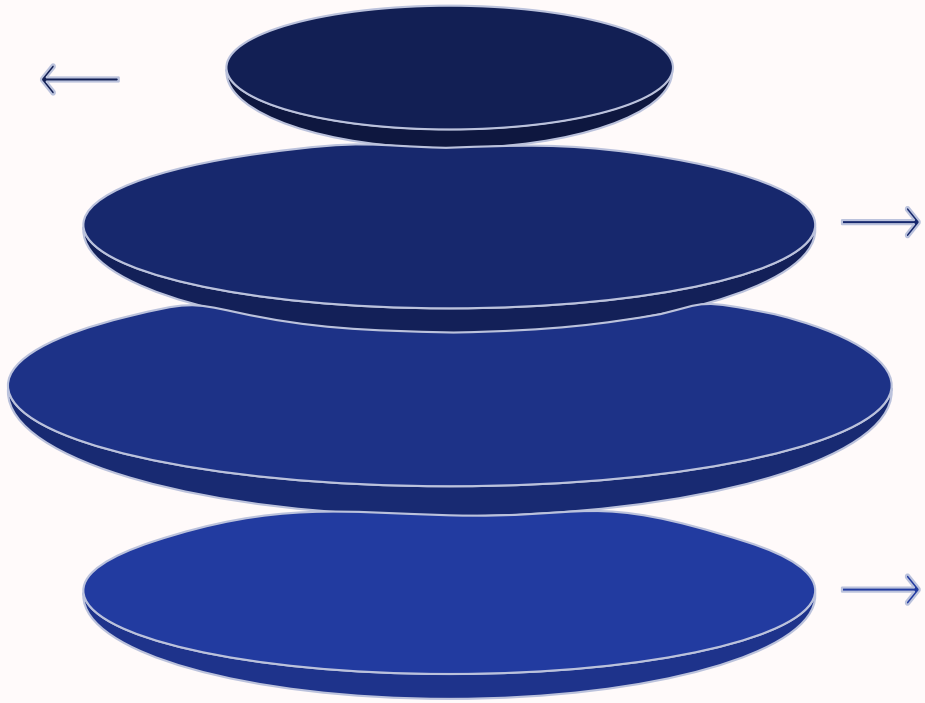
Security Policies

Defining and applying granular access control policies.

NAT & Routing

Configuring Network Address Translation and essential routing for Internet access.

Network Topology: Our FortiGate Setup



LAN1

Two PCs on 10.0.0.0/24 via switch

LAN2

Two PCs on 10.0.1.0/24 via switch

FortiGate

Central firewall connecting both switches

Internet

Cloud connection for outbound traffic

- **LAN1:** 10.0.0.0/24 subnet with two connected PCs.
- **LAN2:** 10.0.1.0/24 subnet with two connected PCs.
- Two network switches facilitating connections within each LAN segment.
- A central FortiGate Firewall acting as the security gateway.
- Connection to the Internet for external communication.

FortiGate Initial Configuration

The initial setup involved configuring the FortiGate unit to establish basic connectivity and administrative access.

- Enabled DHCP on **port1** to dynamically obtain an IP address from the upstream network.
- Accessed the FortiGate Graphical User Interface (GUI) via the obtained IP address from a connected management PC.

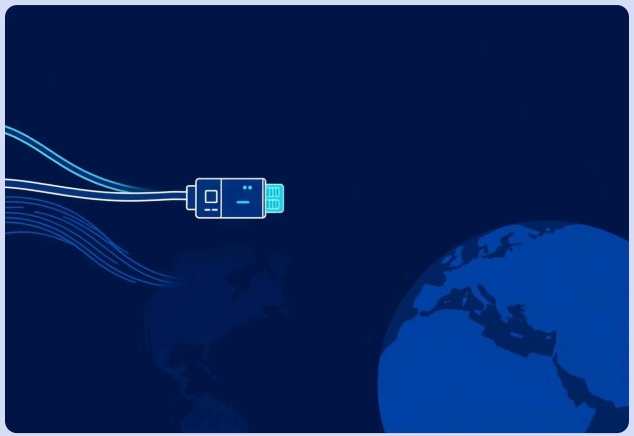
- Created a new administrative profile named "Trainee" with carefully defined permissions.
- Added a new administrator account with **limited privileges**, assigned to the "Trainee" profile, enhancing security by enforcing least privilege.

Interface Configuration Overview

Each FortiGate interface was set up carefully to organize the network, separate the LANs, and make sure traffic is routed properly to and from the internet.

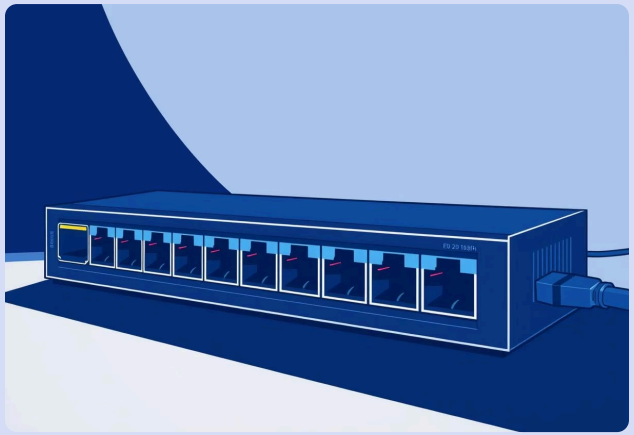
Port1: WAN & Management

Configured with a **static IP** address, serving as both the Wide Area Network (WAN) uplink and the primary management interface for the FortiGate device.



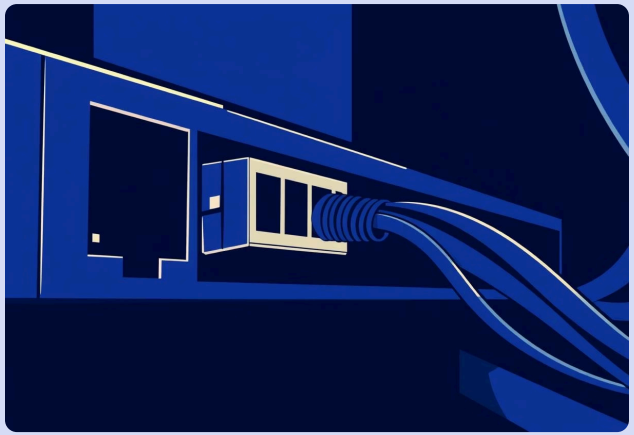
Port2: LAN1 Assignment

Designated for **LAN1** (10.0.0.0/24 subnet), with DHCP enabled to automatically assign IP addresses to devices within this segment.



Port3: LAN2 Assignment

Dedicated to **LAN2** (10.0.1.0/24 subnet), also configured with DHCP to streamline IP address distribution for its connected PCs.



All connected PCs successfully received their respective IP addresses from the DHCP pools configured on **Port2** and **Port3**.

Testing Connectivity Before Policy Implementation

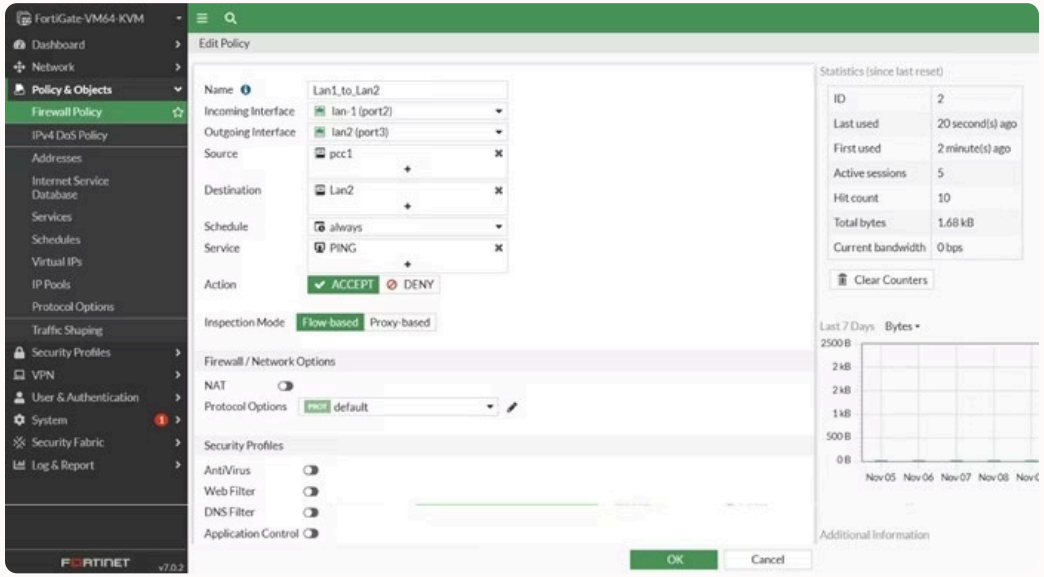
Before applying any security policies or advanced routing, initial connectivity tests were performed to verify basic network functionality.

- **LAN-to-LAN Communication:** Devices within LAN1 could successfully communicate with devices in LAN2, confirming internal network segment connectivity.
- **Internet Access:** As expected, no devices within either LAN could access the Internet, due to the absence of outbound policies and NAT configurations.

This crucial step confirms the network's physical and logical baseline before introducing security controls.

Firewall Policy #1: LAN1 to LAN2 Restriction

Our first firewall rule was created to control how devices in LAN1 can communicate with devices in LAN2, showing how we can manage access in detail.



- **Allowed Traffic:** Only **PC1** from LAN1 was explicitly permitted to establish connections and communicate with devices within LAN2.
- **Denied Traffic:** All other devices in LAN1, specifically **PC2**, were denied access to LAN2, effectively demonstrating basic access control based on source IP.
- This policy showcased the FortiGate's ability to create segmentation and enforce least privilege within the internal network.

Internet Access Challenges Before Routing

Despite successful internal LAN communication, accessing the Internet remained impossible, highlighting critical missing configurations.

- **No Internet Access:** PCs in both LAN segments were unable to reach external websites or services.
- **Missing Default Route:** The FortiGate lacked a default route to forward unknown traffic (i.e., Internet-bound traffic) out to the gateway.
- **Absent Internet Policy:** No firewall policy was yet configured to permit outbound traffic from the internal networks to the WAN interface.
- **NAT Not Applied:** Network Address Translation (NAT) was not enabled, preventing internal private IP addresses from being translated to a public IP for Internet communication.

Firewall Policy #2 (Internet Access + SNAT)

LAN1 Traffic to Internet

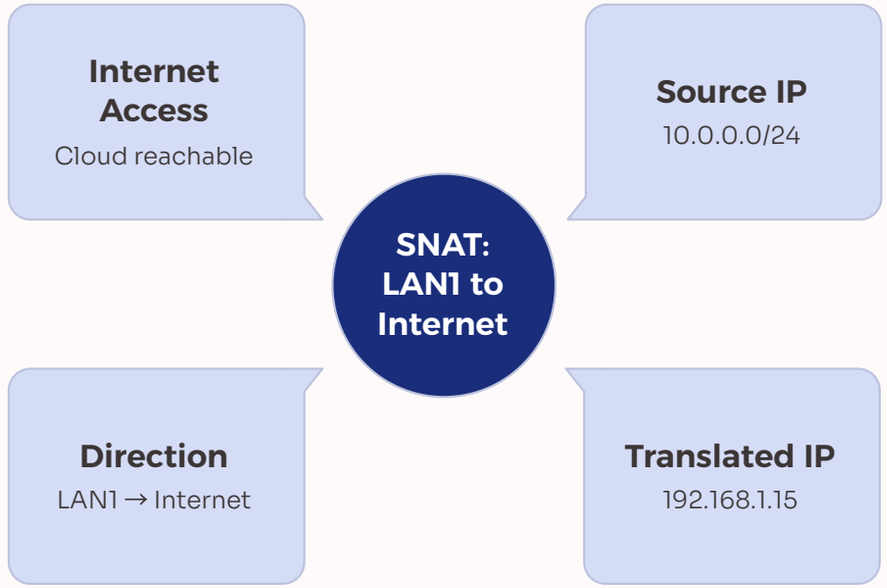
This policy specifically permits traffic originating from the LAN1 network segment to reach the Internet. It's crucial for enabling internal users to browse websites, access cloud services, and perform other external communications.

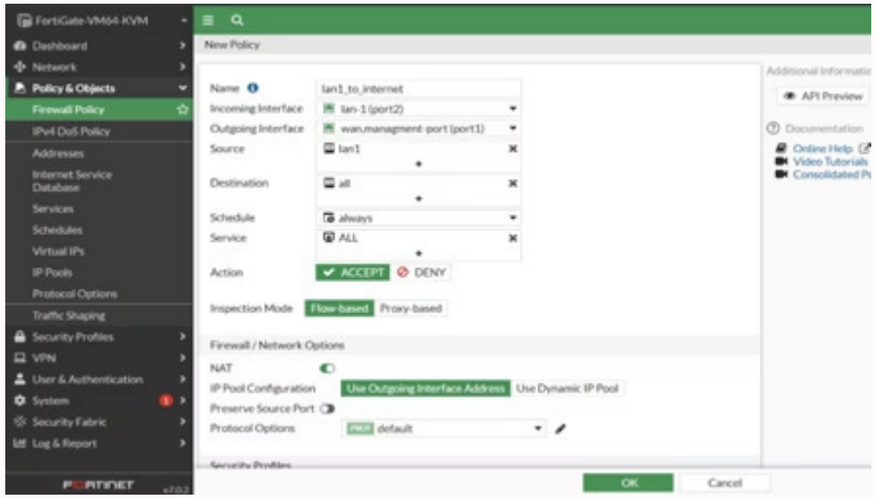
Source NAT using WAN IP

Source Network Address Translation (SNAT) is applied, translating the private IP addresses of devices on LAN1 to the FortiGate's public WAN IP address. This ensures that outbound traffic appears to come from a single, authorized public IP, protecting the internal network's structure.

Result: Internet Access for PC1 & PC2

With this policy active, both PC1 and PC2, located within the LAN1 segment, gain full and controlled access to the Internet. The FortiGate manages the translation and ensures secure communication.





Static Routing: Enabling Internet Connectivity

Default Static Route

A default static route acts as the last resort for traffic that doesn't match any other specific routes. It's essential for guiding all non-local traffic towards the Internet.

Destination: 0.0.0.0/0

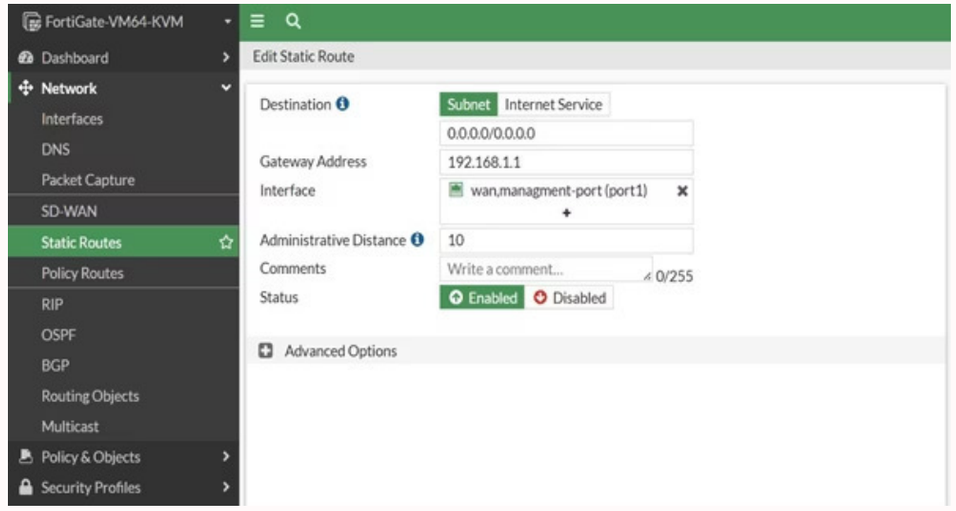
This destination address signifies "any network" or "all networks." By setting it, we instruct the FortiGate to send any traffic destined for an unknown network segment via the specified gateway.

Gateway: ISP/Cloud

The gateway is the next-hop router that connects the FortiGate to the Internet Service Provider (ISP) network. This route effectively directs all outbound Internet-bound traffic through the ISP's infrastructure.

Enables Internet Connectivity

Implementing this default static route is the fundamental step to ensure that all devices behind the FortiGate can successfully connect to and communicate with resources on the broader Internet.



A default route (0.0.0.0/0) is like a "catch-all" for your network. It tells your firewall where to send traffic if it doesn't know a more specific path. This is crucial for accessing the internet.

Destination NAT (DNAT) Overview: Hosting Internal Services

External Request

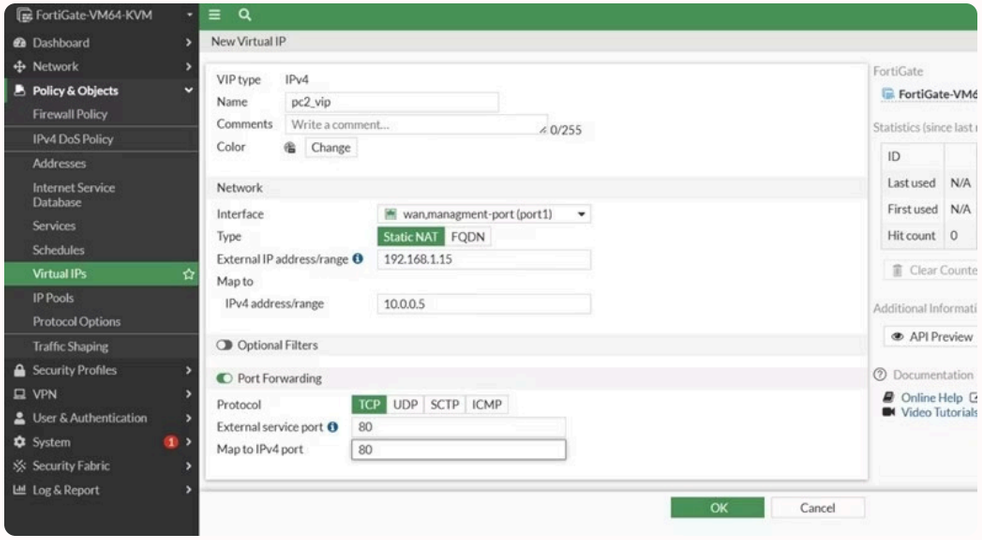
When an external user tries to access a service on a public IP address (e.g., your public website), the request first hits the FortiGate firewall at **192.168.1.15:80**.

IP Translation

The FortiGate performs Destination NAT, translating the public IP and port to the internal private IP address and port of the web server: **10.0.0.5:80 (PC2)**.

Internal Service Access

The request is then forwarded to the actual internal server (PC2), which processes the request. This allows external users to access internal resources securely.



Destination NAT is essential for hosting internal services, such as web servers, mail servers, or VPN gateways, that need to be accessible from the Internet while keeping the internal network protected.

DNAT Firewall Policy: Controlled Internet Access to Internal Services

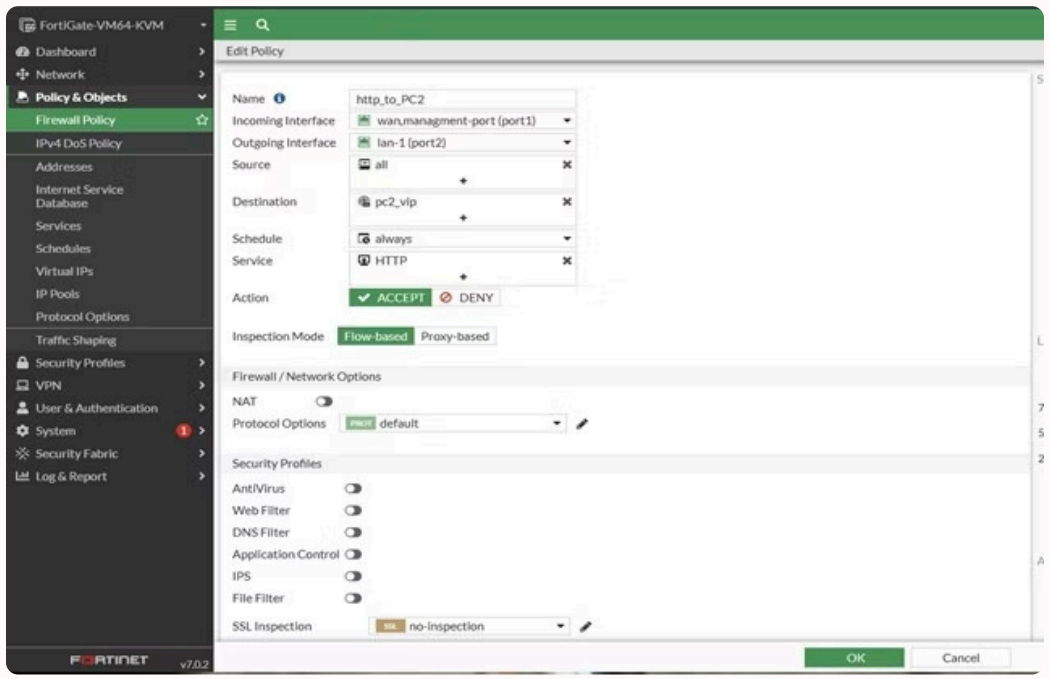
1. Source: Internet

This policy specifies that the incoming traffic can originate from any source on the Internet, allowing legitimate external users to reach the internal service.

2. Destination: Web-VIP

The destination is a Virtual IP (VIP) configured on the FortiGate, representing the public-facing IP address and port for the internal web server. This VIP handles the initial inbound connection.

This policy allows controlled and secure access from the Internet to PC2 (our internal web server). It effectively sets up a secured port forwarding mechanism, exposing only necessary services while protecting the rest of the internal network.



3. Service: HTTP

The policy is limited to the HTTP service (port 80), ensuring that only web traffic is allowed to pass through, enhancing security by restricting other protocols.

4. Action: Allow

This action explicitly permits the traffic that matches all the defined criteria (source, destination, service) to proceed into the internal network after the NAT translation.

Public–Private IP Resolution Summary

Understanding the flow of traffic between public and private IP addresses is foundational to network security and connectivity.

SNAT: Private → Public

Source NAT translates internal private IP addresses to a single public IP for outbound connections. This is how devices on your local network access the internet.

DNAT: Public → Private

Destination NAT translates external public IP requests to internal private IP addresses, allowing outside users to access services hosted within your network.

Both Source NAT and Destination NAT have been tested carefully to ensure the network runs smoothly.

Final Deliverables

Our project concludes with a comprehensive set of deliverables, ensuring a well-documented and fully functional network security solution.

Full Configuration Documentation

Detailed records of all FortiGate settings, including interfaces, routing, NAT rules, and firewall policies.

Testing Screenshots

Visual proof of successful connectivity, policy enforcement, and NAT operations from various test scenarios.

Working Topology

A clear diagram of the network setup, illustrating connections, IP addresses, and FortiGate placement.

NAT/Routing/Policies Implemented

Confirmation of all required Network Address Translation, static routing, and security policies being correctly in place.

Exported Backup Config

A complete backup of the FortiGate configuration for disaster recovery and future reference.

Conclusion: FortiGate Implementation Success

This project successfully concludes the deployment and configuration of the FortiGate firewall, demonstrating a robust and secure network environment.

→ Completed Full FortiGate Setup

The FortiGate appliance is fully operational, from initial installation to advanced policy configuration, serving as the central security gateway.

→ Implemented Multi-LAN Segmentation

We have successfully segmented the network into multiple LANs, enhancing security by isolating different user groups and resources.

→ Applied Access Control, Routing, NAT

Comprehensive access control policies, efficient routing mechanisms, and critical NAT services are all configured and functioning as intended.

→ Gained Practical Network Security Experience

Through this project, valuable hands-on experience in configuring and managing a leading enterprise-grade firewall has been acquired.

Questions & Answers

We welcome your questions and look forward to discussing any aspects of this FortiGate implementation in more detail.