# Implementing Enterprise VPN Solutions with FortiGate

| Team Members: |
|---|
| Mohamed Hany Samir |
| Seif Goda Adel |
| Ahmed Mohamed Mostafa |
| Amr Khaled Mohamed |
| Abdallah Ahmed Dighedy |

# What is a VPN in Our Project?

Creates a secure connection between HQ, Branch, and Remote Users.

Allows all sites to communicate as if on the same private network.

Ensures safety and privacy across the internet.

# Why We Use VPNs in This Project

- Secure communication between HQ and Branch.
- Safe remote access for users outside.
- Protects all data moving across the internet.
- Makes multi-site network behave like one connected system.

# VPN Types in Our Project

IPsec VPN – Connects HQ and Branch securely.

SSL-VPN – Allows remote users to access resources safely.

# How IPsec VPN Works (Simple)

HQ and Branch establish trusted connection.

A secure tunnel is created between both sites.

All traffic passes inside the protected tunnel.

# How SSL-VPN Works

User logs in through a secure portal.

A protected SSL tunnel is created.

User gains safe access to HQ and Branch.

# Why Our VPN Network Is Secure

All connections are encrypted.

Each site has its own network segment.

Firewalls control and filter access.

Remote users authenticate before entering.

# How Everything Connects Together

HQ ↔ Branch through IPsec Tunnel.

Remote User → SSL-VPN → HQ & Branch.

All sites operate together securely.

# IPSec VPN

# What is IPSec ?

- **Definition:** IPsec isn't just one protocol; it is a suite (a collection) of protocols that works at the Network Layer (Layer 3) to secure IP communications.

**Core Security Goals:**

It is designed to ensure four main things:

- Confidentiality: Keeps data secret so only authorized parties can read it.
- Integrity: Ensures the data hasn't been tampered with during transit.
- Authentication: Verifies that the data is coming from the person or device it claims to be from.
- Anti-replay: Prevents hackers from intercepting a data packet and resending it later to trick the system.

# Main Components & Modes

- **The Two Security Protocols:**
  - AH (Authentication Header):This acts like a digital signature. It proves who sent the data and that it hasn't changed, but it does not hide the data (no encryption).
  - ESP (Encapsulating Security Payload): This is the complete package. It provides everything AH does (integrity/auth) plus encryption. It is the industry standard for VPNs because it actually hides the data.

- **The Two Modes of Operation:**
  - Transport Mode: Connects two specific computers (hosts). It protects the payload (the data inside) but leaves the original IP header visible.
  - Tunnel Mode: Connects entire networks (like a Site-to-Site VPN). It wraps the entire original packet (header and all) inside a new packet. This is the most common mode for VPNs.

## IPSec operates in two main phases:

### 1. IKE Phase 1

In this phase creates a secure communication channel between the two peers using the ISAKMP protocol. During this step, the peers negotiate:

- The encryption algorithm
- The hashing algorithm
- The authentication method
- Encryption keys

### 2. IKE Phase 2 (IPSec SA Negotiation)

In this phase, the actual IPSec tunnel for data transmission is established. The peers agree on:

- Which protocol to use (ESP or AH)
- The encryption key
- Additional security parameters

## Key Concepts to Understand

- **1. Security Association (SA)**
  IPSec relies on Security Associations (SAs).
  An SA is an agreement between two peers that defines how to secure traffic (including encryption, hashing, and keys).
  Each SA is one-way, so you need one SA for sending and another for receiving.
- **2. Diffie-Hellman (DH) Group**
  This algorithm is used in IKE Phase 1 to exchange keys securely.
  There are multiple DH groups (e.g., 1, 2, 5, 14, 19…). A higher group number means stronger security.
- **3. Lifetime**
  Each SA has a defined lifetime (based on time or traffic volume).
  When an SA expires, peers must renegotiate to avoid using same key for prolonged periods.
- **4. Pre-shared Key vs Digital Certificates**
  Authentication can be achieved in two ways:
  **Pre-shared Key (PSK):** A shared password agreed upon by both parties.
  **Digital Certificates:** Issued by a trusted Certificate Authority (CA), commonly used in large organizations.
- **5. NAT Traversal (NAT-T)**
  When a NAT device (such as a home router performing private-to-public IP translation) is present, IPSec may fail.
  NAT-T solves this by encapsulating IPSec traffic inside UDP packets, allowing it to work even with NAT.

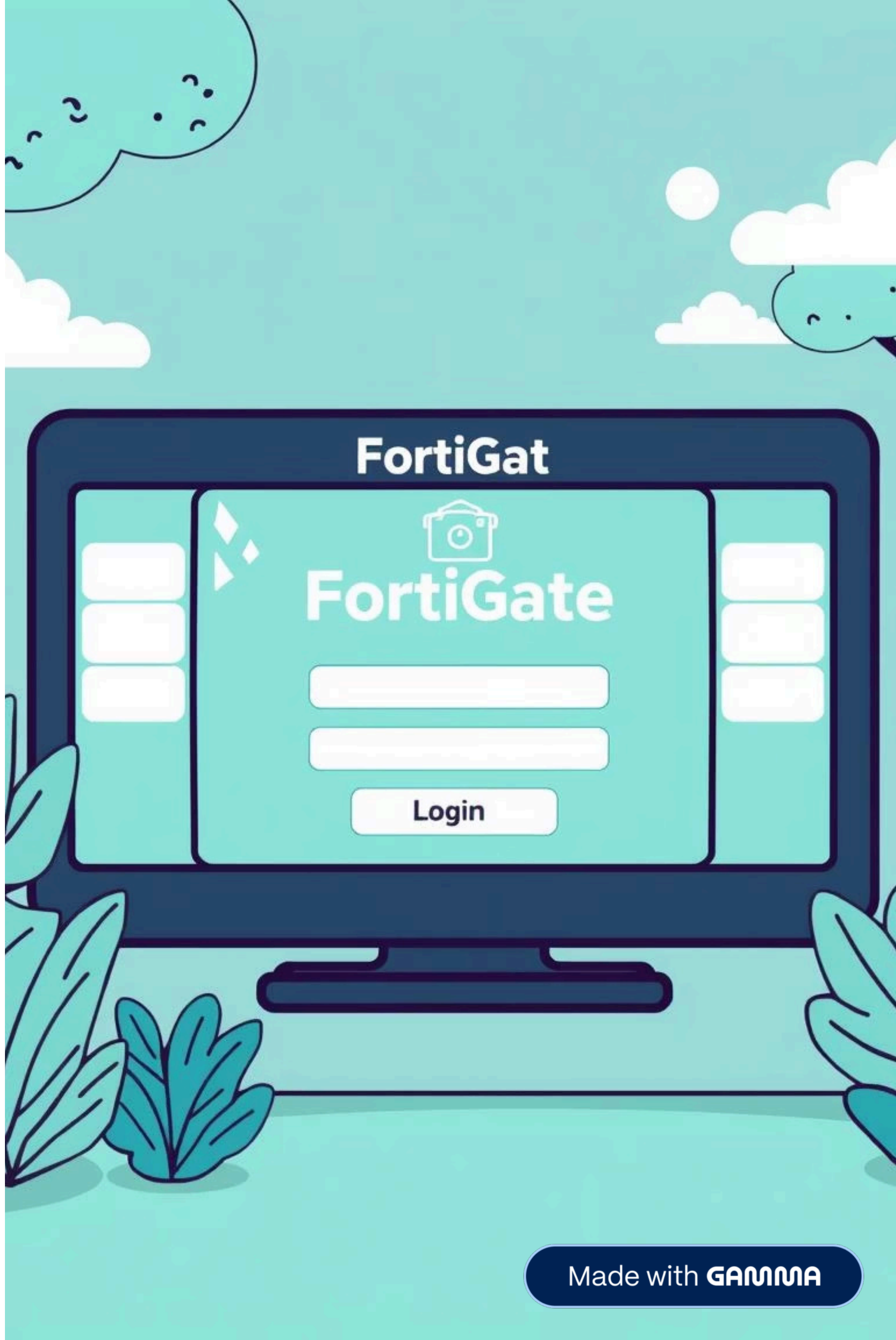
## Use Cases of IPSec

- **Site-to-Site VPNs**
  Used to securely connect two separate networks, such as linking two hospitals.
- **Remote Access VPNs**
  Allows employees to securely access the company network from home or other remote locations.

# SSL VPN Overview

Implementing VPN Solutions with FortiGate

Amr Khaled Mohamed



# What is SSL VPN?

## Secure Remote Access

Provides a secure method for users to connect to internal network resources from any location, primarily through a standard web browser.

## SSL/TLS Encryption

Leverages robust Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols to encrypt all data transmitted, ensuring confidentiality and integrity.

## Clientless Deployment

Unlike traditional VPNs, SSL VPNs often require no special client software installation, simplifying deployment and user onboarding.

## Public Network Compatibility

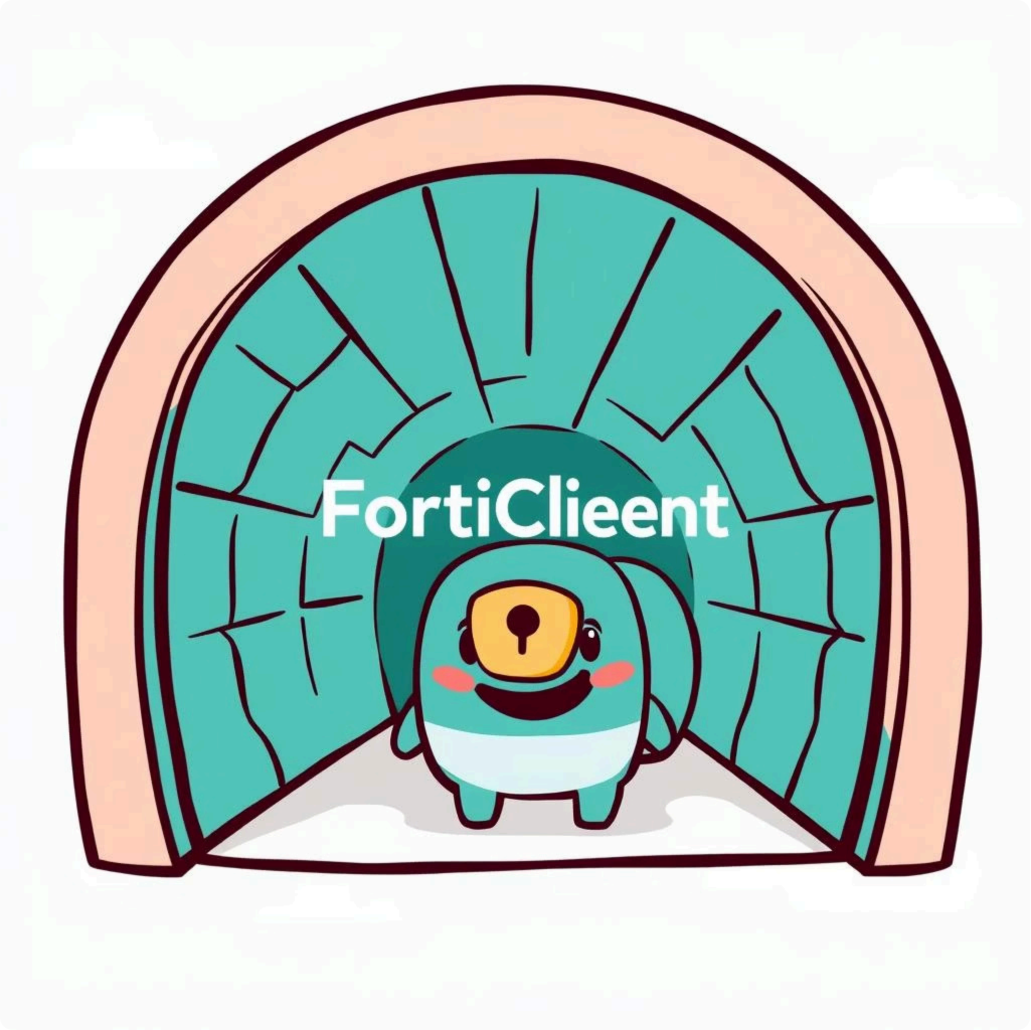
Designed to operate effectively and securely even over untrusted public networks, making it ideal for diverse work environments.

# Types of SSL VPN with FortiGate

## Portal Mode (Clientless / Web Mode)

- Access is entirely browser-based, requiring no software installation on the user's device.
- Provides granular access to specific applications such as RDP, SSH, SMB, and HTTP/HTTPS services.
- Ideal for users needing quick, on-demand access to a limited set of internal resources.

## Tunnel Mode



- Requires the installation of FortiClient software on the endpoint device.
- Establishes a full network-layer tunnel, granting comprehensive access to the corporate network.
- Utilizes a virtual adapter on the client device to route all network traffic through the secure VPN tunnel.

# How FortiGate SSL VPN Works

## User Connects

User initiates connection to the FortiGate SSL VPN portal via a web browser or FortiClient.

## Authentication

User provides credentials, which FortiGate verifies against internal or external authentication servers.

## Secure Session

An SSL/TLS encrypted session is established, protecting all subsequent communication.

## Resource Access

Authenticated users are granted secure, encrypted access to authorized internal network resources.

# Benefits of FortiGate SSL VPN

## User-Friendly Accessibility

Browser-based access ensures ease of use for all users, minimizing training and support needs.

## Robust Security

Provides strong SSL/TLS encryption for all data in transit, safeguarding sensitive information from interception.

## Device Agnostic

Compatible with a wide range of devices including laptops, smartphones, and tablets, supporting a flexible workforce.

## Empowers Remote Work

An ideal solution for remote employees, enabling them to access corporate resources securely from anywhere, anytime.

رواد مصر الرقمية

# SD-WAN

Ahmed Mohamed Mostafa

# SD-WAN Overview

- SD-WAN (Software-Defined Wide Area Network) is a technology that improves WAN performance and reliability by using software-based path selection.
- It dynamically selects the best WAN link based on availability and performance.
- Provides more flexibility, better failover, and cost-effective connectivity compared to traditional WAN.

# Why SD-WAN Was Used in Our Project?

- To ensure continuous connectivity between **HQ and Branch** even if one WAN link fails.

- To simulate real enterprise environments where redundancy is required.

- To maintain the stability of the **IPsec Site-to-Site VPN tunnel**.

- To create a realistic WAN failover scenario using GNS3.

# SD-WAN Topology in Our Project

**HQ FortiGate:**

- **WAN1 (port2) → Connected to R3 (Primary path)**
- **WAN2 (port4) → Connected to R4 (Backup path)**

**Branch FortiGate:**

- **Connected to HQ through routed WAN and IPsec VPN**

**Goal:**

- **Automatically switch between WAN1 and WAN2 if the primary link becomes unavailable.**

# Failover Testing

Testing Procedure:

- Simulated WAN1 failure by shutting down R3 on GNS3.

- Observed routing table on FortiGate → default route changed to WAN2 (port4).

- Verified continuous HQ ↔ Branch communication through the IPsec tunnel.

- Restored R3 → Firewall automatically returned to WAN1.

# Result & Benefits

**SD-WAN Simulation Successfully Implemented:**

- **Achieved automatic WAN failover.**

- **Ensured stable IPsec VPN connectivity between HQ and Branch.**

- **Demonstrated real-world redundancy behavior using simple static SD-WAN.**

- **Enhanced the network reliability and resilience of the project.**