

ssl vpn

Depi final project



presented by

ABDELRAHAMAN SHERIF

21025744

**SSL VPN**

**SSL VPN (Secure Sockets Layer Virtual Private Network)** is a technology that allows secure remote access to a private network over the internet. Unlike traditional VPNs, SSL VPNs operate over standard web browsers, making them more accessible for users who may not want to install specific VPN client software. SSL VPNs use SSL/TLS protocols to encrypt the data transmitted between the client and the server, ensuring confidentiality and integrity.

**Objectives of the Lab**

In this lab, you will:

* Configure an SSL VPN on a FortiGate device.
* Set up user accounts and access policies.
* Test the SSL VPN connection from client machines.

**Components Used**

1. **FortiGate Device**: The firewall and VPN server (e.g., FortiGate 60F).
2. **Client Machines**: Devices running Windows, Linux, or macOS that will connect to the VPN.
3. **Internet Connection**: Required for remote access to the FortiGate device.

**Steps to Configure SSL VPN**

**1. Access FortiGate GUI**

* **Open a Web Browser**: Use a web browser like Chrome or Firefox.
* **Enter IP Address**: Type the IP address of the FortiGate device in the address bar (e.g., https://192.168.1.1).
* **Login**: Enter your admin credentials to access the FortiGate management interface.

**2. Configure SSL VPN Settings**

* **Navigate to VPN Settings**:
  + Go to **VPN > SSL-VPN Settings**.
* **Enable SSL VPN**:
  + Check the box to enable SSL VPN.
* **Listening Interface**:
  + Set the **Listen on Interface** to the WAN interface (the interface connected to the internet).
* **SSL VPN Port**:
  + The default port is 443. You can change this if needed, but 443 is standard for HTTPS traffic.
* **Authentication/Portal Mapping**:
  + Define how users will authenticate and what resources they will access. You can create different portals for different user groups.

**3. Create User Accounts**

* **User Definition**:
  + Navigate to **User & Device > User Definition**.
* **Create New User/Group**:
  + Click **Create New** to add individual users or user groups.
  + Fill in the necessary details, such as username, password, and authentication method (local, RADIUS, LDAP, etc.).

**4. Configure SSL VPN Portal**

* **Navigate to SSL VPN Portals**:
  + Go to **VPN > SSL-VPN Portals**.
* **Create New Portal**:
  + Click **Create New** to set up a new portal.
  + Configure the portal settings, including:
    - **Name**: Give the portal a name.
    - **Web Mode**: Specify the web resources users can access.
    - **Tunnel Mode**: If you want to provide full network access, enable tunnel mode.
* **Assign Access Permissions**:
  + Specify which user groups can access this portal.

**5. Configure Firewall Policies**

* **Policy & Objects**:
  + Navigate to **Policy & Objects > IPv4 Policy**.
* **Create New Policy**:
  + Click **Create New** to define a new policy.
* **Set Incoming/Outgoing Interfaces**:
  + Set the **Incoming Interface** to the SSL VPN interface and the **Outgoing Interface** to the internal network (e.g., LAN).
* **Define Source and Destination**:
  + Set the **Source** to the user group created for SSL VPN users.
  + Set the **Destination** to the internal resources (e.g., all or specific subnets).
* **Enable NAT**:
  + If users are accessing the internet through the VPN, enable NAT (Network Address Translation).

**6. Test the SSL VPN Connection**

* **Client Access**:
  + On a client machine, open a web browser and navigate to the SSL VPN URL (e.g., https://<FortiGate\_IP>).
* **Login**:
  + Enter the user credentials you created earlier.
* **Access Resources**:
  + After logging in, verify that you can access the internal resources defined in the portal settings.

**Testing and Monitoring**

* **Monitor Connections**:
  + Use the **Log & Report** section in the FortiGate GUI to monitor SSL VPN connections and user activity.
* **Troubleshooting**:
  + If users experience connectivity issues, check the following:
    - User credentials and authentication methods.
    - Firewall policy configurations.
    - SSL VPN settings and portal configurations.
    - Network connectivity to the FortiGate device.

**SSL VPN Lab Scenario**

**Scenario Overview**:  
You are a network administrator at a medium-sized company, "Tech Solutions," that has employees working remotely. To provide secure access to the company’s internal resources, you need to configure an SSL VPN on a FortiGate firewall.

**Lab Components**

1. **FortiGate Device**: FortiGate 60F (acting as the VPN server).
2. **Client Machines**:
   * One Windows 10 laptop (Remote Employee).
   * One macOS laptop (Remote Employee).
3. **Network Configuration**:
   * FortiGate WAN IP: 203.0.113.1
   * Internal Network: 192.168.1.0/24
   * VPN Subnet: 10.10.10.0/24 (for VPN clients)
4. **User Accounts**: Create two users:
   * User1: alice@techsolutions.com
   * User2: bob@techsolutions.com

**Step-by-Step Configuration**

**1. Access FortiGate GUI**

* **Open a Web Browser**: Use Chrome or Firefox.
* **Enter the IP Address**: Type https://203.0.113.1.
* **Login**: Enter admin credentials (default: admin/admin).

**2. Configure SSL VPN Settings**

* **Navigate to VPN Settings**:
  + Go to **VPN > SSL-VPN Settings**.
* **Enable SSL VPN**:
  + Check the box to enable SSL VPN.
* **Listening Interface**:
  + Set **Listen on Interface** to the WAN interface (e.g., wan1).
* **SSL VPN Port**:
  + Keep the default port as 443.
* **Authentication/Portal Mapping**:
  + Set up a mapping for user authentication. You can create a default portal or specific portals for different user groups.

**3. Create User Accounts**

* **User Definition**:
  + Navigate to **User & Device > User Definition**.
* **Create New Users**:
  + Click **Create New** for User1:
    - Username: alice
    - Password: Password123
    - Email: alice@techsolutions.com
  + Click **Create New** for User2:
    - Username: bob
    - Password: Password123
    - Email: bob@techsolutions.com

**4. Configure SSL VPN Portal**

* **Navigate to SSL VPN Portals**:
  + Go to **VPN > SSL-VPN Portals**.
* **Create a New Portal**:
  + Click **Create New**:
    - Name: Employee\_Portal
    - Web Mode: Enable access to web applications.
    - Tunnel Mode: Enable to allow full network access.
    - Set the **IP Range** to 10.10.10.0/24.

**5. Configure Firewall Policies**

* **Policy & Objects**:
  + Navigate to **Policy & Objects > IPv4 Policy**.
* **Create a New Policy**:
  + Click **Create New**:
    - **Incoming Interface**: Select ssl.root (the SSL VPN interface).
    - **Outgoing Interface**: Select internal.
    - **Source**: Set to all or specify the VPN subnet 10.10.10.0/24.
    - **Destination**: Set to all or specify the internal resources.
    - **Action**: Accept.
    - Enable NAT if users need to access the internet through the VPN.

**6. Testing the SSL VPN Connection**

* **Client Access**:
  + On the Windows laptop, open a web browser.
  + Navigate to https://203.0.113.1.
* **Login**:
  + Enter the credentials for User1 (alice@techsolutions.com and Password123).
* **Access Resources**:
  + After logging in, verify access to internal resources, such as shared folders or internal web applications.

**7. Validate the Connection**

* **Check IP Address**:
  + Once connected, open a command prompt and type ipconfig (Windows) or ifconfig (macOS) to check the assigned IP address.
  + You should see an IP address from the VPN subnet (e.g., 10.10.10.x).
* **Ping Internal Resources**:
  + Ping an internal server (e.g., 192.168.1.10) to ensure connectivity.
* **Log Monitoring**:
  + Go to **Log & Report > Event Log > VPN Events** on the Fort

**Log Monitoring Results for SSL VPN Configuration**

After configuring the SSL VPN on the FortiGate device and successfully connecting with the remote client, you will want to monitor the logs to verify that everything is functioning correctly. Below is a simulated result of the log monitoring for the SSL VPN connections.

**1. Accessing the Logs**

* **Navigate to Logs**:
  + In the FortiGate GUI, go to **Log & Report**.
  + Click on **Event Log** and then select **VPN Events**.

**2. Log Entries**

Here’s an example of what the log entries might look like after a successful connection and activities performed by the users:

| Date/Time | User | Action | Source IP | Destination IP | Status | |---------------------|--------------------|--------------|------------------|------------------|-------------| | 2023-10-01 09:15:23 | alice@techsolutions.com | Login | 203.0.113.10 | 203.0.113.1 | Successful | | 2023-10-01 09:15:25 | alice@techsolutions.com | Assigned IP | 203.0.113.10 | 10.10.10.2 | Successful | | 2023-10-01 09:15:30 | alice@techsolutions.com | Resource Access | 10.10.10.2 | 192.168.1.10 | Successful | | 2023-10-01 09:16:00 | bob@techsolutions.com | Login | 203.0.113.11 | 203.0.113.1 | Successful | | 2023-10-01 09:16:05 | bob@techsolutions.com | Assigned IP | 203.0.113.11 | 10.10.10.3 | Successful | | 2023-10-01 09:16:15 | bob@techsolutions.com | Resource Access | 10.10.10.3 | 192.168.1.20 | Successful | | 2023-10-01 09:20:45 | alice@techsolutions.com | Logout | 10.10.10.2 | 203.0.113.1 | Successful | | 2023-10-01 09:21:00 | bob@techsolutions.com | Logout | 10.10.10.3 | 203.0.113.1 | Successful |

**Explanation of Log Entries**

* **Date/Time**: The timestamp when the event occurred.
* \*\*User \*\*: The username of the person who performed the action.
* **Action**: The type of action performed (e.g., Login, Assigned IP, Resource Access, Logout).
* **Source IP**: The public IP address of the client machine that initiated the connection.
* **Destination IP**: The IP address of the FortiGate device or the internal resource accessed.
* **Status**: Indicates whether the action was successful or failed.

**Analysis of Log Monitoring Results**

1. **Successful Logins**:
   * Both users, Alice and Bob, successfully logged into the SSL VPN. This is indicated by the "Login" actions showing a status of "Successful".
2. **IP Assignment**:
   * After logging in, each user was assigned an IP address from the VPN subnet (10.10.10.x), confirming that the VPN configuration is correctly assigning IPs to connected clients.
3. **Resource Access**:
   * Both users accessed internal resources (e.g., 192.168.1.10 and 192.168.1.20). The logs show successful access attempts, indicating that the firewall policies are correctly allowing traffic from the VPN subnet to the internal network.
4. **Logouts**:
   * The logs also show that both users logged out successfully, which is important for security and resource management.