REMOTE ACCESS WITHOUT PROTECTION IS A BREACH WAITING TO HAPPEN.

SSL VPN

Hussain

NETWORKING

SSL VPN

This document gives a clear understanding of SSL VPN before touching the lab. The first part explains SSL VPN from a real world perspective how it works, why companies use it, and what problems it solves. The second part breaks down the lab step by step, so the student knows exactly what they're configuring, why each step matters, and what outcomes to expect.

DISCLAIMER

This material is for educational and training purposes only.
It is not intended as a production configuration, security recommendation. All IP addresses, usernames, and passwords used in this document are for lab use only and must not be used in real networks.
Students are responsible for following their institution's policies, handling configurations responsibly, and applying security best practices when working on actual environments.

SSL VPN

Table of Contents

SSL VPN

Part 1: Explaining SSL VPN

Introduction

SSL VPN (Secure Sockets Layer Virtual Private Network) is a secure remote access technology that uses SSL/TLS, the same encryption used by HTTPS websites.

Instead of using IPsec or special VPN ports, SSL VPN works entirely over TCP port 443. This means:

- It works anywhere, even behind strict firewalls.

- It passes NAT easily.

- It behaves like normal web traffic.

- It is more user-friendly than IPsec.

SSL VPN creates an encrypted tunnel between the remote user and the company network so the user can work as if they are physically inside the building.

SSL VPN usage

Companies use SSL VPN because:

- Remote workers need secure access to internal systems.

- HTTPS traffic is rarely blocked.

- It supports laptops, phones, tablets.

- It is simpler to deploy than IPsec.

- It offers strong encryption.

- It allows full access to internal services.

SSL VPN

With SSL VPN, a remote user can:

- Access internal websites

- Reach file servers

- Use RDP or SSH

- Ping internal hosts

- Access databases

- Run internal applications

Types of SSL VPN

A) Clientless SSL VPN

No software needed.

User goes to:

https://public-ip

Logs in and gets a portal page.

Can access only web-based or limited internal resources.

B) Client-Based SSL VPN (AnyConnect, OpenVPN, etc.)

User installs a VPN application.

Creates a full encrypted tunnel.

User receives a virtual internal IP address.

User can access everything allowed by policy.

Client-based SSL VPN = full remote access

Clientless SSL VPN = limited access

SSL VPN

Advantages of SSL VPN

- Works behind NAT and firewalls.

- Uses standard HTTPS.

- No special configuration on the client side.

- Supports mobile devices easily.

- Easy to install and auto-update (AnyConnect).

- Good for large remote workforces.

- Strong encryption via TLS.

Security of SSL VPN

SSL VPN uses:

- TLS handshake

- Session keys

- Certificate-based trust

- Encrypted data packets

- Optional MFA or certificates

This encryption secures the connection between the device and the company network.

SSL VPN

Real-World Use Cases

- Corporate employees working from home
- IT administrators accessing internal servers remotely
- Contractors connecting to the network temporarily
- Access to internal applications without exposing them publicly

Part 2: Explanation Based on the lab

What You Are Building in This Lab

You will configure the Cisco ASA to act as a remote access SSL VPN server using AnyConnect.

This allows a remote PC to connect securely into the network using HTTPS and receive an internal IP address.

The VPN will allow:

- A remote host (PC-C) to access inside resources
- Full-tunnel connection (via AnyConnect client)
- Encrypted communication over the Internet

In this lab you will:

- Prepare routers and PCs in the topology
- Configure ASA interfaces (inside/outside/dmz)
- Enable ASDM access
- Use the AnyConnect VPN Wizard
- Upload AnyConnect package
- Create a VPN user
- Create a VPN address pool
- Configure DNS for VPN clients
- Exempt VPN traffic from NAT
- Connect from remote PC and test

Why Each Step Is Done

A) Configure ASA Interfaces

The ASA must know:

- Which interface is inside (LAN)
- Which is outside (Internet)
- Which is DMZ

This defines trust levels and where the VPN entry point is.

B) Enable ASDM

ASDM provides the GUI used to configure the SSL VPN parameters.

C) Start AnyConnect Wizard

This guides you through the full setup:

- Select SSL as the protocol
- Choose outside interface
- Upload AnyConnect client software
- Create VPN policies

D) Upload AnyConnect Client Image (.pkg)

Remote users need to download the VPN client.

The ASA must host this file so users can automatically download it when connecting via browser.

E) Create a VPN User

The remote user (REMOTE-USER) will authenticate using a username and password.

SSL VPN

F) Create VPN Address Pool

Example pool in lab:

192.168.1.100 – 192.168.1.125

This is the range of IPs assigned to VPN clients.

G) Configure DNS for VPN Clients

VPN users must resolve internal hostnames.

You assign DNS → 192.168.2.3 (DMZ server).

H) NAT Exemption

Without NAT exemption, the ASA would NAT VPN traffic and break connectivity.

NAT exemption ensures VPN traffic stays inside private addressing.

I) Connect from Remote PC

1. Visit https://209.165.200.226

2. Log in using REMOTE-USER

3. Download AnyConnect

4. Install it

5. Connect using AnyConnect

6. Verify assigned IP from VPN pool

7. Ping internal hosts to confirm full access