

SoftEther VPN Lab Activity

Virtual Private Networks Across the Internet

Renato Mignone

Student ID: s336973

MSc in Cybersecurity Engineering

Politecnico di Torino

June 12, 2025



License

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

You are free:

- **to Share:** to copy, distribute and transmit the work
- **to Remix:** to adapt the work

Under the following conditions:

- **Attribution:** you must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).
- **Noncommercial:** you may not use this work for commercial purposes.
- **Share Alike:** if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

More information on the Creative Commons website.

Acknowledgments

The author would like to thank Professor Daniele Bringhenti and the Politecnico di Torino for providing the foundational knowledge and laboratory environment that made this work possible.

Contents

1 Introduction

This laboratory activity focuses on the implementation and analysis of Virtual Private Networks (VPNs) using SoftEther VPN technology across an Internet infrastructure. VPNs are fundamental network security solutions that provide secure connectivity over shared, potentially untrusted networks by creating encrypted tunnels that preserve the confidentiality, integrity, and authenticity of data transmission.

The objective of this lab is to demonstrate how modern VPN technologies can establish secure communication channels between geographically distributed networks, simulating real-world scenarios where branch offices or remote users need secure access to corporate resources. Through practical implementation, we will explore two distinct VPN protocols: IPSec and TLS/SSL, analyzing their different approaches to achieving network security.

1.1 Laboratory Objectives

The primary goals of this laboratory activity include:

- **Understanding VPN Fundamentals:** Explore the theoretical foundations of Virtual Private Networks and their role in modern network security architectures.
- **SoftEther VPN Implementation:** Configure and deploy SoftEther VPN server to provide multi-protocol VPN services, as IPSec and TLS-based connections.
- **Network Topology Design:** Implement a realistic network topology using GNS3 that simulates Internet connectivity between two remote sites through an ISP infrastructure.
- **Protocol Comparison:** Analyze and compare different VPN protocols (IPSec vs. TLS) in terms of security properties, performance characteristics, and implementation complexity.
- **Traffic Analysis:** Perform detailed packet analysis using Wireshark to understand how different VPN protocols encapsulate and protect network traffic.
- **Security Assessment:** Evaluate the security features provided by each VPN implementation, including encryption, authentication, and integrity protection.

1.2 SoftEther VPN Overview

SoftEther VPN is a multi-protocol VPN software that supports various VPN protocols including IPSec, L2TP, OpenVPN (TLS/SSL), and proprietary protocols. Developed by the University of Tsukuba, it provides a unified platform for implementing different VPN technologies, making it an excellent choice for educational and research purposes.

The key advantages of SoftEther VPN include:

- Multi-protocol support enabling comparison of different VPN approaches
- Cross-platform compatibility (Windows, Linux, macOS)
- High performance with optimized networking code
- Comprehensive logging and monitoring capabilities
- Support for complex network topologies and routing scenarios

1.3 Laboratory Environment and Network Topology

This laboratory simulates a scenario where two geographically separated private networks need to establish secure communication across the Internet. The topology consists of:

- **Server Site:** A private network (10.0.1.0/24) hosting the SoftEther VPN server
- **Client Site:** A remote private network (10.0.2.0/24) with VPN client capabilities
- **Internet Infrastructure:** Simulated ISP network providing connectivity between sites
- **VPN Gateways:** Edge routers performing NAT and routing functions

The implementation demonstrates how VPN technology enables secure site-to-site connectivity, allowing hosts in different private networks to communicate as if they were on the same local network, while maintaining security properties across the untrusted Internet infrastructure.

1.4 System Requirements

To successfully complete this laboratory activity, the following system requirements must be met:

System Requirements

Operating System:

- Linux distribution (Ubuntu 20.04 LTS or newer recommended)
- Administrative (sudo) privileges required

Software Requirements:

- **GNS3:** Network simulation platform
- **Docker:** Container platform for VPN endpoints
- **Wireshark:** Network protocol analyzer

Hardware Requirements:

- Minimum 8GB RAM (16GB recommended for optimal performance)
- 20GB available disk space
- Network interface with Internet connectivity

Software Installation:

The required software can be installed on Ubuntu/Debian systems using the following commands:

```
# Update package repositories
sudo apt update
```

```
# Install GNS3 and dependencies
sudo apt install gns3-gui gns3-server

# Install Docker
sudo apt install docker.io

# Install network analysis tools
sudo apt install wireshark

# Add user to required groups
sudo usermod -aG docker $USER
sudo usermod -aG wireshark $USER
```

Note: After installation, a logout and login cycle may be required for group membership changes to take effect. The VPN client software (strongSwan for IPsec and OpenVPN for TLS) will be installed inside the Docker containers as part of the laboratory setup.

1.5 Laboratory Structure

This report is organized into the following sections:

1. **Theoretical Background:** Comprehensive overview of VPN technologies, SoftEther VPN architecture, and the security protocols involved.
2. **Network Topology:** Detailed description of the simulated network infrastructure and addressing scheme.
3. **Initial Configuration:** Step-by-step setup of the GNS3 environment, routers, and container infrastructure.
4. **SoftEther VPN Server:** Configuration and deployment of the VPN server with multi-protocol support.
5. **IPsec Configuration:** Implementation of IPsec-based VPN using strongSwan client.
6. **TLS Configuration:** Setup of TLS/SSL VPN using OpenVPN client.
7. **Verification and Analysis:** Testing procedures and traffic analysis for both VPN implementations.

Each section includes practical implementation steps, configuration examples, and analysis of the results, providing a comprehensive understanding of VPN technologies and their real-world applications in network security.

2 Theoretical Background

This section provides the theoretical foundation necessary to understand the Virtual Private Network technologies implemented in this laboratory. We examine the fundamental concepts of VPNs, the specific architecture of SoftEther VPN, and the security protocols that enable secure communication across untrusted networks.

2.1 Virtual Private Networks (VPNs)

Virtual Private Networks are network security solutions that provide connectivity over shared infrastructure while maintaining properties typically associated with private networks. VPNs create secure communication channels over potentially untrusted networks by implementing various security mechanisms at different layers of the network stack.

Core VPN Properties:

A VPN must provide several essential properties to ensure secure communication:

- **Data Confidentiality:** Encryption algorithms protect data content from unauthorized access during transmission across public networks.
- **Data Integrity:** Cryptographic hash functions and message authentication codes ensure that data has not been modified in transit.
- **Authentication:** Both peer authentication (verifying the identity of communicating endpoints) and data origin authentication are essential for secure VPN operation.
- **Access Control:** VPNs implement policies that determine which traffic is permitted and how it should be processed.
- **Anti-Replay Protection:** Sequence numbers and timestamps prevent malicious replay of previously captured packets.

VPN Classification:

VPNs can be classified based on their implementation approach and the network layers where security is enforced:

- **Network Layer VPNs:** Operate at the IP layer (L3), such as IPSec-based ones
- **Transport Layer VPNs:** Implement security at L4, including TLS/SSL VPNs
- **Application Layer VPNs:** Provide security services at the application level

2.2 SoftEther VPN Architecture

SoftEther VPN represents a unique approach to VPN implementation by providing a unified platform that supports multiple VPN protocols simultaneously. This multi-protocol capability enables direct comparison and evaluation of different VPN technologies within a single deployment.

Multi-Protocol Support:

SoftEther VPN's architecture is designed around the concept of *protocol abstraction*, where different VPN protocols are implemented as modules within a common framework:

- **IPSec Support:** Native implementation of both AH (Authentication Header) and ESP (Encapsulating Security Payload) protocols in tunnel mode
- **SSL/TLS Support:** Built-in TLS server compatible with OpenVPN clients and other SSL VPN solutions
- **L2TP Support:** Layer 2 Tunneling Protocol implementation for broader client compatibility
- **SSTP Support:** Secure Socket Tunneling Protocol for environments with restrictive firewalls

Virtual Hub Architecture:

The core of SoftEther VPN is the Virtual Hub concept, which acts as a virtual Ethernet switch that can:

- Aggregate multiple VPN sessions from different protocols
- Implement advanced routing and bridging capabilities
- Provide centralized policy enforcement and logging
- Support complex network topologies including site-to-site and remote access scenarios

SecureNAT Functionality:

SoftEther VPN includes an integrated NAT (Network Address Translation) and DHCP server functionality called SecureNAT, which simplifies VPN client configuration by:

- Automatically assigning IP addresses to VPN clients
- Providing DNS resolution services
- Enabling Internet access for VPN clients through NAT
- Supporting both IPv4 and IPv6 addressing schemes

2.3 IPSec Protocol Suite

Internet Protocol Security (**IPSec**) is a framework providing security at the IP layer by adding headers to IP packets. It can operate in transport mode (protecting payload only) or tunnel mode (encapsulating the entire packet), the latter being common for VPN gateways.

One key component is the **Encapsulating Security Payload (ESP)**, which provides confidentiality through encryption and may also include integrity and authentication. ESP protects the payload while leaving the outer header for routing. **Security Associations (SAs)** are agreements between peers that specify parameters such as cryptographic algorithms, keys, and endpoints; each SA is identified by a Security Parameter Index (SPI). Automated management of these SAs is typically handled by Internet Key Exchange protocols: **IKEv1** (with main and aggressive modes) and **IKEv2** (which improves performance and security). In this project, IPSec (via ESP, SA, and IKE) is used to establish secure tunnels at the network layer for scenarios requiring kernel-level packet protection.

2.4 TLS/SSL for VPN Implementation

Transport Layer Security (TLS) provides session-layer security by performing a handshake to negotiate cipher suites, authenticate the server (and optionally the client), exchange keys—often providing perfect forward secrecy—and then protecting application data in a record layer. TLS-based VPNs (such as **OpenVPN**) encapsulate arbitrary IP traffic within a TLS channel, leveraging TLS’s widespread support and flexible cipher negotiation. This approach places security processing in user space, which can be easier to deploy and customize, though with some performance trade-offs compared to kernel-based solutions.

2.5 Client-Side VPN Technologies

StrongSwan (IPSec):

strongSwan is an open-source IPSec implementation used in this project to establish and manage IPSec tunnels. It supports IKEv1 and IKEv2, a range of cryptographic algorithms, and features like NAT traversal and Dead Peer Detection. Configuration is driven by simple files (e.g., `ipsec.conf` and `ipsec.secrets`), and it integrates with the Linux kernel’s IPSec stack. In our setup, strongSwan handles automated key exchanges and maintains SAs for secure network-layer tunnels.

OpenVPN Client (TLS):

OpenVPN is the TLS-based client solution in this project. It uses OpenSSL for cryptography, handles both UDP and TCP transports, and can operate in tun (Layer 3) or tap (Layer 2) mode. Certificate-based authentication via an X.509 PKI ensures that only authorized endpoints connect. OpenVPN’s user-space implementation allows flexible scripting hooks and logging, making it suitable for custom remote-access scenarios in the laboratory.

2.6 Comparative Analysis Framework

Understanding the theoretical differences between IPSec and TLS implementations lays the groundwork for practical comparison:

- **Architecture Differences:** IPSec is implemented at the network layer (often in kernel space), whereas TLS-based VPNs run in user space at the session layer.
- **Performance Considerations:** IPSec generally has lower overhead due to kernel integration; TLS-based VPNs offer more flexibility but may incur extra processing in user space.
- **Deployment Complexity:** IPSec setups can be more complex but follow well-established standards, while TLS-based VPNs like OpenVPN often allow simpler initial configuration and greater customization.

This theoretical foundation establishes the necessary knowledge base for understanding the practical implementation and comparison of SoftEther VPN’s multi-protocol capabilities in the subsequent sections of this laboratory activity.

3 Network Topology and Architecture

This section presents the network topology designed for the SoftEther VPN laboratory activity. The implementation simulates a realistic scenario where two geographically separated private networks communicate securely across the Internet through VPN tunnels.

3.1 Topology Overview

The laboratory network topology consists of five main components that work together to create a realistic Internet-based VPN scenario:

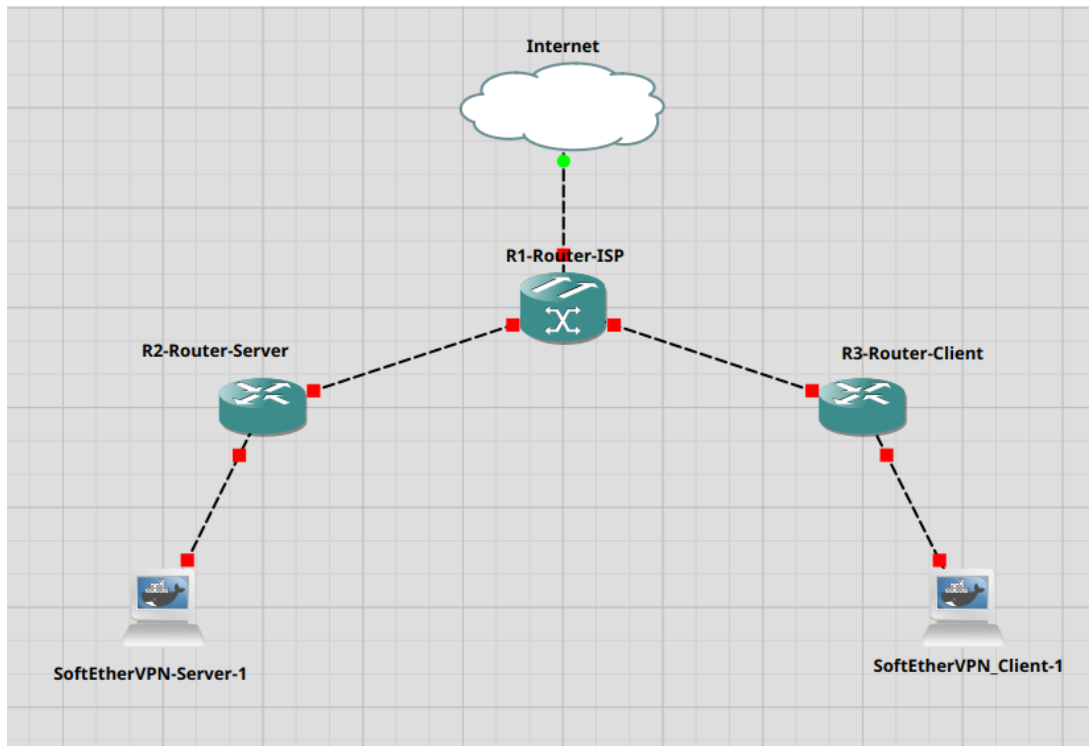


Figure 1: GNS3 Network Topology - VPN Across the Internet

The network architecture follows an end-to-end VPN design where:

- **Server Site:** Contains the SoftEther VPN server hosted within a private network
- **Client Site:** Represents a remote branch office requiring VPN connectivity
- **Internet Infrastructure:** Simulated ISP network providing public connectivity
- **Edge Routers:** Perform NAT and routing functions, providing Internet connectivity for the private networks
- **VPN Endpoints:** Docker containers hosting the actual VPN software (server and client)

This topology effectively demonstrates how end-to-end VPN technology enables secure communication between hosts in different private networks across untrusted public infrastructure, representing common real-world deployment scenarios where VPN software runs directly on the endpoints rather than on gateway devices.

3.2 IP Addressing Scheme

The network addressing scheme uses a combination of private and public IP addresses to simulate realistic Internet connectivity. The addressing follows RFC standards for private addressing (RFC 1918) and uses documentation addresses (RFC 5737) for public IP simulation.

Table 1: Network Interface Configuration

| Device | Interface | IP Address | Description |
|------------------------|-----------------|-------------------|-----------------------|
| Router 2 (Server-side) | LAN (Fa0/0) | 10.0.1.1/24 | Private Network 1 |
| | WAN (Fa0/1) | 203.0.113.1/24 | Public IP (RFC 5737) |
| ISP Router | Interface Fa0/0 | 203.0.113.254/24 | Connected to Router 2 |
| | Interface Fa0/1 | 198.51.100.254/24 | Connected to Router 3 |
| | Interface Fa1/0 | DHCP Assigned | Internet Cloud |
| Router 3 (Client-side) | WAN (Fa0/1) | 198.51.100.1/24 | Public IP (RFC 5737) |
| | LAN (Fa0/0) | 10.0.2.1/24 | Private Network 2 |
| SoftEther Server | eth0 | 10.0.1.2/24 | VPN Server Host |
| VPN Client | eth0 | 10.0.2.2/24 | VPN Client Host |

Network Segments:

- **Server Network (10.0.1.0/24):** Private subnet hosting the SoftEther VPN server
- **Client Network (10.0.2.0/24):** Remote private subnet with VPN client
- **ISP Segment 1 (203.0.113.0/24):** Public network between ISP and server-side
- **ISP Segment 2 (198.51.100.0/24):** Public network between ISP and client-side
- **VPN Tunnel Networks:** Virtual addressing for VPN connectivity (assigned dynamically)

3.3 Device Roles and Functions

Each component in the network topology serves a specific purpose in demonstrating VPN functionality:

3.3.1 ISP Router (R1-Router-ISP)

The ISP router simulates Internet Service Provider infrastructure and provides:

- **Internet Connectivity:** DHCP-assigned public IP address with MAC address spoofing for network access.
- **Inter-Site Routing:** Routes traffic between the two remote sites through simulated Internet infrastructure
- **NAT Traversal Support:** Enables VPN protocols to function through Network Address Translation
- **Public IP Assignment:** Provides public addressing for both edge routers

The ISP router configuration includes static routes for both private networks and implements a default route to the Internet cloud.

3.3.2 Server-Side Router (R2-Router-Server)

This edge router connects the server's private network to the Internet and implements:

- **Network Address Translation:** Port Address Translation management
- **VPN Port Forwarding:** Static NAT rules to forward VPN traffic to the server:
 - Port 500/UDP: ISAKMP forwarded to SoftEther server
 - Port 4500/UDP: NAT-T forwarded to SoftEther server
 - Port 443/TCP: HTTPS/TLS forwarded to SoftEther server
- **Default Gateway:** Routing for the server's private network
- **Transparent Routing:** Routes VPN traffic between Internet and private network without VPN processing

3.3.3 Client-Side Router (R3-Router-Client)

The client-side edge router provides similar functionality for the remote site:

- **PAT Configuration:** Network address translation for client network connectivity
- **Default Routing:** Internet access for the client private network
- **Transparent VPN Support:** Allows VPN client software to establish connections through NAT without router-based VPN processing

3.3.4 SoftEther VPN Server Container

The server container runs the SoftEther VPN software with the following configuration:

- **Container Image:** siomiz/softethervpn:latest
- **Multi-Protocol Support:** Simultaneous IPsec and TLS/SSL VPN services
- **Virtual Hub:** DEFAULT hub for client connections
- **User Management:** Configured with test user accounts for VPN authentication
- **Certificate Management:** Self-signed certificates for TLS-based connections

3.3.5 VPN Client Container

The client container simulates a remote user or branch office with:

- **Container Image:** ubuntu:latest
- **IPsec Client:** StrongSwan software for IPsec connectivity
- **TLS Client:** OpenVPN client for SSL/TLS VPN connections

3.4 Network Communication Flow

The network design enables several communication scenarios:

1. **Direct Internet Communication:** Both sites can access Internet resources through their respective ISP connections
2. **End-to-End VPN Tunnel Establishment:** The VPN client container initiates direct VPN connections to the SoftEther server container using either:
 - IPsec protocol (strongSwan client to SoftEther server)
 - TLS/SSL protocol (OpenVPN client to SoftEther server)
3. **Encrypted Inter-Site Communication:** Once VPN tunnels are established, the client can communicate securely with resources in the server's network
4. **NAT Traversal:** VPN protocols handle NAT traversal automatically, allowing encrypted tunnels to pass through the edge routers

3.5 Security Considerations

The network topology incorporates several security features:

- **Private Addressing:** Internal networks use RFC 1918 private addresses, preventing direct Internet access
- **NAT Protection:** Edge routers provide implicit firewall protection through NAT
- **VPN Encryption:** All inter-site communication is protected by VPN encryption
- **Authentication:** VPN connections require user credentials and/or certificates
- **Protocol Separation:** Different VPN protocols operate on distinct ports for protocol isolation

This topology provides a foundation for comparing different VPN implementations while maintaining realistic network security practices and demonstrating practical deployment scenarios.

4 Initial Network Configuration

This section details the step-by-step process of setting up the laboratory environment, including GNS3 configuration, router setup, and Docker container deployment. The configuration establishes the basic network infrastructure that will support the VPN implementations.

4.1 GNS3 Environment Setup

The laboratory utilizes GNS3 (Graphical Network Simulator-3) to create a realistic network topology. GNS3 provides the platform for simulating Cisco routers, Docker containers, and network connectivity required for the VPN demonstration.

4.1.1 Device Import and Template Creation

Cisco Router Template:

The topology requires Cisco 7200 routers running IOS version 124-24.T5. This specific IOS image is chosen because it represents a freely available alternative to modern commercial Cisco IOS versions. While newer platforms like IOSv (IOS Virtual) offer enhanced features and performance, they require valid Cisco licensing agreements which can be costly for educational purposes. The 124-24.T5 image, although older and not widely deployed in current production environments, provides all the fundamental routing and NAT capabilities required for this laboratory exercise.

To import the router template:

1. Open GNS3 and click the router icon in the left panel
2. Select "New Template" at the bottom
3. Choose "Install an appliance from the GNS3 server"
4. Filter by "CISCO" and locate "Cisco 7200"
5. Install the template and select version "124-24.T5"
6. Import the router image file to complete the setup

Docker Container Setup:

Two Docker containers are required for the VPN endpoints:

- **Server Container Image:** siomiz/softethervpn:latest
- **Client Container Image:** ubuntu:latest

To add containers to the GNS3 project:

1. Navigate to Edit → Preferences in GNS3
2. Select "Docker containers" from the left panel
3. Click "New" to add a container

4. Enter the image name (e.g., `siomiz/softethervpn:latest`)
5. Configure the container name and complete the setup
6. Repeat for the Ubuntu client container

You will now see the containers in the left panel of GNS3, ready to be dragged into the workspace.

4.2 Router Configuration

The network topology requires three routers with specific configurations to simulate realistic Internet connectivity and routing behavior.

4.2.1 ISP Router (R1-Router-ISP)

The ISP router provides Internet connectivity and inter-site routing. The configuration includes interface setup, MAC address spoofing for DHCP, and routing table entries.

```
enable
configure terminal

# Configure interface to Router 2 (Server-side)
interface FastEthernet0/0
  ip address 203.0.113.254 255.255.255.0
  no shutdown
exit

# Configure interface to Router 3 (Client-side)
interface FastEthernet0/1
  ip address 198.51.100.254 255.255.255.0
  no shutdown
exit

# Configure Internet interface with DHCP and MAC spoofing
interface FastEthernet1/0
  mac-address xxxx.xxxx.xxxx # Replace with host machine MAC
  ip address dhcp
  no shutdown
exit

# Configure static routes for private networks
ip route 198.51.100.0 255.255.255.0 FastEthernet0/1
ip route 203.0.113.0 255.255.255.0 FastEthernet0/0

# Configure default route to Internet
ip route 0.0.0.0 0.0.0.0 FastEthernet1/0

end
write memory
```

Important Note - MAC Address Spoofing:

The MAC address spoofing is necessary because the Politecnico di Torino WiFi network's DHCP server implements MAC address filtering for security purposes. Without using the host machine's MAC address, the DHCP server will not assign a valid IP address to the router interface, preventing Internet connectivity for the simulated network.

To obtain your host machine's MAC address:

```
# Display all network interfaces and their MAC addresses
ip a

# Look for the active network interface (usually wlan0 for WiFi
# or eth0 for Ethernet)
# The MAC address appears after "link/ether"
# Example output:
# 2: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq
#   state UP group default qlen 1000
#       link/ether 1c:ce:51:3f:98:20 brd ff:ff:ff:ff:ff:ff
```

Copy the MAC address from your active network interface and convert it to Cisco format by adding dots every four characters:

- **Linux format:** 1c:ce:51:3f:98:20
- **Cisco format:** 1cce.513f.9820

Replace xxxx.xxxx.xxxx in the configuration with your converted MAC address.

4.2.2 Server-Side Router (R2-Router-Server)

This router connects the server's private network to the Internet and implements NAT with port forwarding for VPN services.

```
enable
configure terminal

# Configure LAN interface (connected to server)
interface FastEthernet0/0
 ip address 10.0.1.1 255.255.255.0
 ip nat inside
 no shutdown
exit

# Configure WAN interface (connected to ISP)
interface FastEthernet0/1
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 no shutdown
exit

# Configure static NAT for VPN services
ip nat inside source static udp 10.0.1.2 500 203.0.113.1 500
ip nat inside source static udp 10.0.1.2 4500 203.0.113.1 4500
ip nat inside source static tcp 10.0.1.2 443 203.0.113.1 443
```



```
# Configure PAT for general Internet access
access-list 1 permit 10.0.1.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet0/1 overload

# Configure default route
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1

end
write memory
```

Port Forwarding Explanation:

- **Port 500/UDP:** ISAKMP (Internet Security Association and Key Management Protocol)
- **Port 4500/UDP:** NAT-T (NAT Traversal for IPsec)
- **Port 443/TCP:** HTTPS/TLS for SSL VPN connectivity

4.2.3 Client-Side Router (R3-Router-Client)

The client-side router provides NAT and routing for the client's private network.

```
enable
configure terminal

# Configure LAN interface (connected to client)
interface FastEthernet0/0
  ip address 10.0.2.1 255.255.255.0
  ip nat inside
  no shutdown
exit

# Configure WAN interface (connected to ISP)
interface FastEthernet0/1
  ip address 198.51.100.1 255.255.255.0
  ip nat outside
  no shutdown
exit

# Configure default route
ip route 0.0.0.0 0.0.0.0 FastEthernet0/1

# Configure PAT for Internet access
access-list 1 permit 10.0.2.0 0.0.0.255
ip nat inside source list 1 interface FastEthernet0/1 overload

end
write memory
```

4.3 Container Configuration

The Docker containers require specific configuration for persistent storage and network setup.

4.3.1 Server Container Setup

The SoftEther VPN server container needs persistent directories for configuration files:

1. Open the server container configuration in GNS3
2. Navigate to Advanced Settings
3. Add the following additional directories:
 - /server
 - /usr/vpnserver

These directories will be created in the GNS3 project folder, allowing persistent storage of configuration files between container restarts.

Server Network Configuration:

Configure the server container's network interface:

```
# Configure IP address and default route
ip addr add 10.0.1.2/24 dev eth0
ip route add default via 10.0.1.1

# Verify network configuration
ip addr show
ip route show

# Test connectivity to gateway
ping 10.0.1.1
```

4.3.2 Client Container Setup

The client container requires similar configuration for persistent storage:

1. Open the client container configuration in GNS3
2. Navigate to Advanced Settings
3. Add the additional directory: /client

Client Network Configuration:

Configure the client container's network interface and install required VPN software:

```
# Configure network interface
ip addr add 10.0.2.2/24 dev eth0
ip route add default via 10.0.2.1

# Update package repositories
apt update
```

```
# Install strongSwan for IPSec VPN
apt install strongswan -y

# Install OpenVPN for TLS VPN
apt install openvpn -y

# Copy configuration files from persistent storage
cp /client/ipsec.conf /etc/
cp /client/ipsec.secrets /etc/

# Verify network configuration
ip addr show
ip route show

# Test connectivity to gateway
ping 10.0.2.1
```

4.4 Basic Connectivity Testing

Before proceeding with VPN configuration, verify that the basic network infrastructure is functioning correctly.

4.4.1 Inter-Router Connectivity

Test connectivity between routers to ensure proper routing:

```
# From ISP Router - test connectivity to edge routers
ping 203.0.113.1      # Should reach Server-side router
ping 198.51.100.1     # Should reach Client-side router

# From Server-side Router - test connectivity to ISP
ping 203.0.113.254    # Should reach ISP router

# From Client-side Router - test connectivity to ISP
ping 198.51.100.254   # Should reach ISP router
```

4.4.2 End-to-End Connectivity

Test connectivity between the container endpoints:

```
# From Server Container - test connectivity to public IPs
ping 198.51.100.1     # Should reach Client-side router public IP

# From Client Container - test connectivity to public IPs
ping 203.0.113.1      # Should reach Server-side router public IP
```

4.4.3 Service Verification

Verify that the SoftEther VPN server is running and listening on required ports:

```
# Check if SoftEther VPN server is listening
ss -tuln | grep -E '(443|500|4500)'

# Expected output should show:
# tcp LISTEN 0.0.0.0:443
# udp LISTEN 0.0.0.0:500
# udp LISTEN 0.0.0.0:4500
```

4.5 Network Infrastructure Validation

At this point, the basic network infrastructure should be operational with:

- Three routers configured with appropriate IP addressing and routing
- NAT services functioning on edge routers
- Docker containers with network connectivity
- SoftEther VPN server operational and accessible
- Basic inter-site connectivity through the simulated Internet

This foundation enables the implementation of VPN services detailed in the subsequent sections. Any connectivity issues at this stage should be resolved before proceeding with VPN configuration, as they will prevent proper VPN tunnel establishment.

The next section will detail the configuration of the SoftEther VPN server to provide multi-protocol VPN services for both IPSec and TLS-based connections.

5 SoftEther VPN Server Configuration

This section details the configuration and deployment of the SoftEther VPN server within the Docker container environment. The server provides multi-protocol VPN services, supporting both IPSec and TLS/SSL connections simultaneously through a unified management interface.

5.1 Server Installation and Initialization

The SoftEther VPN server runs within a Docker container using the pre-built image `siomiz/softethervpn:latest`. This containerized approach provides several advantages including isolation, portability, and simplified deployment.

5.1.1 Container Deployment

The server container has been configured in GNS3 with persistent storage directories as detailed in Section 4. When the container starts, the SoftEther VPN service initializes automatically with the following characteristics:

- **Automatic Service Start:** The VPN server daemon starts automatically when the container boots, thanks to the persistent storage configuration that we will see later, the server will start already with the proper configuration.
- **Multi-Protocol Listeners:** Simultaneous support for IPSec, SSL/TLS
- **Default Configuration:** Initial setup with basic security settings and a default virtual hub
- **Network Integration:** Automatic integration with the container's network interface (eth0)

5.1.2 Service Verification

To verify the SoftEther VPN server is running correctly, execute the following commands within the server container:

```
# Check if SoftEther VPN server process is running
ps aux | grep vpnserver

# Verify VPN server is listening on required ports
ss -tuln | grep -E '(443|500|4500|992|5555)'

# Expected output should show listeners on:
# tcp LISTEN 0.0.0.0:443    (HTTPS/SSL VPN)
# udp LISTEN 0.0.0.0:500    (ISAKMP/IKE)
# udp LISTEN 0.0.0.0:4500   (NAT-T)
# tcp LISTEN 0.0.0.0:992    (Alternative SSL port)
# tcp LISTEN 0.0.0.0:5555   (Management/API)
```

5.2 Configuration File Analysis

The SoftEther VPN server configuration is managed through the `vpn_server.config` file, which contains comprehensive settings for all VPN protocols, virtual hubs, user management, and security policies.

5.2.1 Core Server Settings

The server configuration includes several critical components:

```
# Core server configuration parameters
declare ServerConfiguration
{
    bool AcceptOnlyTls false           # Accept non-TLS
    connections
    string CipherName DHE-RSA-AES256-SHA # Default cipher
    suite
    bool DisableIPsecAggressiveMode false # Allow IPsec
    aggressive mode
    bool DisableNatTraversal false      # Enable NAT
    traversal
    bool DisableOpenVPNServer false     # Enable OpenVPN
    compatibility
    bool DisableSSTPServer false        # Enable SSTP
    protocol
    uint MaxConnectionsPerIP 256        # Connection limit
    per IP
    bool SaveDebugLog true              # Enable debug
    logging
}
```

Key Configuration Parameters:

- **Multi-Protocol Support:** All major VPN protocols are enabled by default
- **NAT Traversal:** Essential for clients behind NAT devices
- **Security Settings:** Strong cipher suites with DHE for perfect forward secrecy
- **Connection Limits:** Reasonable limits to prevent resource exhaustion
- **Logging:** Comprehensive logging for troubleshooting and analysis

5.2.2 Protocol Listener Configuration

The server configures multiple listeners for different VPN protocols:

```
declare ListenerList
{
    declare Listener0 # HTTPS/SSL VPN
    {
        bool Enabled true
        uint Port 443
    }
}
```

```

declare Listener1  # ISAKMP/IKE
{
    bool Enabled true
    uint Port 500
}
declare Listener2  # Alternative SSL
{
    bool Enabled true
    uint Port 992
}
declare Listener3  # NAT-T
{
    bool Enabled true
    uint Port 4500
}
declare Listener4  # Management/API
{
    bool Enabled true
    uint Port 5555
}
}

```

5.3 Virtual Hub and User Management

SoftEther VPN organizes connections through Virtual Hubs, which act as virtual Ethernet switches. The default configuration includes a single hub named "DEFAULT" with basic user authentication.

5.3.1 Default Virtual Hub Configuration

The DEFAULT hub provides the following services:

- **User Authentication:** Password-based authentication for VPN clients
- **SecureNAT:** Integrated DHCP and NAT services for client IP assignment
- **Access Control:** Configurable policies for traffic filtering and routing
- **Logging:** Comprehensive logging of user sessions and traffic

5.3.2 User Account Management

The server includes a test user account for VPN authentication:

```

declare UserList
{
    declare user1
    {
        byte AuthPassword ObNWU1DckHLOXg4HuyRAMKiIANY=      #
            Password: "ciao"
        uint AuthType 1                                       #
            Password authentication
    }
}

```

```
    string Note $                                # No
        additional notes
    string RealName $                             # No
        real name specified
}
}
```

User Authentication Details:

- **Username:** user1
- **Password:** ciao (hashed in configuration)
- **Authentication Method:** Password-based (Type 1)
- **Access Level:** Standard user privileges

5.4 IPsec Protocol Configuration

The SoftEther VPN server includes native IPsec support, allowing standard IPsec clients to connect without additional software.

5.4.1 IPsec Settings

```
declare IPsec
{
    bool EtherIP_IPsec true                # Enable EtherIP
        over IPsec
    string IPsec_Secret ciao              # Pre-shared key
        for IPsec
    string L2TP_DefaultHub DEFAULT        # Default hub for
        L2TP connections
    bool L2TP_IPsec false                 # Disable L2TP/
        IPsec (using native IPsec)
    bool L2TP_Raw false                   # Disable raw L2TP
}
```

IPsec Configuration Details:

- **EtherIP Support:** Enables Ethernet-over-IP tunneling for layer-2 VPN functionality
- **Pre-Shared Key:** "ciao" - used for IPsec authentication (matches client configuration)
- **Default Hub:** All IPsec connections are directed to the DEFAULT virtual hub
- **Protocol Mode:** Native IPsec implementation rather than L2TP/IPsec combination

5.5 SSL/TLS Protocol Configuration

The server provides SSL/TLS VPN services compatible with OpenVPN clients and other SSL VPN solutions.

5.5.1 TLS Settings and Certificates

The server uses self-signed certificates for TLS connections:

```
# TLS configuration parameters
string OpenVPNDefaultClientOption dev-type$20tun,link-mtu$201500,
    tun-mtu$201500,cipher$20AES-128-CBC,auth$20SHA1,keysize$20128,
    key-method$202,tls-client
string OpenVPN_UdpPortList 1194
bool DisableOpenVPNServer false
```

SSL/TLS Features:

- **OpenVPN Compatibility:** Full compatibility with standard OpenVPN clients
- **Cipher Support:** AES-128-CBC encryption with SHA1 authentication
- **TUN Interface:** Layer-3 tunneling for IP packet forwarding
- **UDP Transport:** Default UDP transport on port 1194 (configurable)
- **Certificate-Based Authentication:** X.509 certificate validation for enhanced security

5.6 SecureNAT Configuration

SecureNAT provides integrated DHCP and NAT services for VPN clients, simplifying client configuration and enabling Internet access.

5.6.1 Virtual DHCP Server

```
declare VirtualDhcpServer
{
    string DhcpDnsServerAddress 192.168.30.1          # DNS server
        for clients
    string DhcpDnsServerAddress2 0.0.0.0              # Secondary
        DNS (disabled)
    bool DhcpEnabled true                             # Enable DHCP
        service
    uint DhcpExpireTimeSpan 7200                       # 2-hour lease
        time
    string DhcpGatewayAddress 192.168.30.1            # Default
        gateway
    string DhcpLeaseIPStart 192.168.30.10             # DHCP pool
        start
    string DhcpLeaseIPEnd 192.168.30.200              # DHCP pool
        end
    string DhcpSubnetMask 255.255.255.0               # Subnet mask
}
```

5.6.2 Virtual Router and NAT

```
declare VirtualRouter
{
    bool NatEnabled true           # Enable NAT
        functionality
    uint NatMtu 1500               # MTU for NAT
        interface
    uint NatTcpTimeout 3600        # TCP
        connection timeout (1 hour)
    uint NatUdpTimeout 1800       # UDP
        connection timeout (30 minutes)
}
```

SecureNAT Benefits:

- **Automatic IP Assignment:** Clients receive IP addresses from 192.168.30.10-200 range
- **DNS Services:** Integrated DNS resolution for VPN clients
- **Internet Access:** NAT functionality enables clients to access external resources
- **Simplified Configuration:** Clients require minimal manual network configuration

5.7 Security and Certificate Management

The SoftEther VPN server implements several security mechanisms to protect VPN communications and server integrity.

5.7.1 Server Certificates

The server uses self-signed X.509 certificates for TLS operations:

- **Certificate Subject:** da3af5075c51 (unique identifier)
- **Key Length:** 2048-bit RSA
- **Validity Period:** Long-term validity for laboratory use
- **Usage:** Server authentication for TLS/SSL connections

5.7.2 Security Policies

The server implements several security policies:

```
# Security-related settings
bool DisableDosProction false      # Enable DoS
    protection
bool DisableSessionReconnect false # Allow session
    reconnection
uint MaxConcurrentDnsClientThreads 512 # DNS thread
    limit
```

```
uint MaxUnestablishedConnections 1000          # Connection
    limit
bool NoSendSignature false                     # Send server
    signature
```

Security Features:

- **DoS Protection:** Built-in protection against denial-of-service attacks
- **Connection Limits:** Prevents resource exhaustion through connection limiting
- **Session Management:** Secure session handling with reconnection support
- **Authentication:** Multiple authentication methods including certificates and passwords

5.8 Operational Verification

After configuration, verify the server is operating correctly and ready to accept VPN connections.

5.8.1 Service Status Check

```
# Verify all VPN protocols are listening
netstat -tuln | grep -E '(443|500|4500|992|5555)'

# Check server logs for any errors
tail -f /usr/vpnserver/server_log/vpn_*

# Test connectivity from client network
# From client container:
ping 203.0.113.1      # Should reach server's public IP
telnet 203.0.113.1 443 # Should connect to HTTPS port
```

5.8.2 Configuration Validation

Ensure the server configuration supports both IPsec and SSL/TLS protocols:

- **IPsec Listeners:** Ports 500 (ISAKMP) and 4500 (NAT-T) are active
- **SSL/TLS Listeners:** Ports 443 and 992 are accepting connections
- **User Authentication:** Test user "user1" is configured and accessible
- **Virtual Hub:** DEFAULT hub is operational with SecureNAT enabled
- **NAT Forwarding:** Router forwarding rules are directing traffic correctly

The SoftEther VPN server is now configured and ready to accept connections from both IPsec and SSL/TLS VPN clients. The next sections will detail the configuration of these client types and demonstrate secure tunnel establishment across the simulated Internet infrastructure.

6 IPsec VPN Configuration

6.1 strongSwan Client Setup

[PLACEHOLDER: strongSwan installation and basic configuration]

6.2 IPsec Configuration Files

6.2.1 ipsec.conf Analysis

[PLACEHOLDER: Detailed explanation of ipsec.conf parameters]

6.2.2 ipsec.secrets Configuration

[PLACEHOLDER: Pre-shared key configuration]

6.3 Connection Establishment

[PLACEHOLDER: IPsec tunnel establishment process]

6.4 Traffic Analysis

[PLACEHOLDER: Packet capture and analysis of IPsec traffic]

7 TLS/SSL VPN Configuration

7.1 OpenVPN Client Setup

[PLACEHOLDER: OpenVPN installation and configuration]

7.2 Certificate and Credential Management

[PLACEHOLDER: Client certificates and authentication]

7.3 OpenVPN Configuration Analysis

[PLACEHOLDER: Detailed explanation of .ovpn file parameters]

7.4 TLS Handshake and Connection

[PLACEHOLDER: TLS connection establishment process]

7.5 Encrypted Traffic Analysis

[PLACEHOLDER: Analysis of TLS-encrypted VPN traffic]

8 Verification and Traffic Analysis

8.1 Connectivity Testing

[PLACEHOLDER: Ping tests and connectivity verification]

8.2 Packet Capture and Analysis

8.2.1 IPSec Traffic Analysis

[PLACEHOLDER: Wireshark captures of IPSec traffic]

8.2.2 TLS Traffic Analysis

[PLACEHOLDER: Wireshark captures of TLS/OpenVPN traffic]

8.3 Header Structure Analysis

[PLACEHOLDER: Detailed analysis of packet headers and encapsulation]

8.4 Security Feature Verification

[PLACEHOLDER: Verification of encryption, authentication, and integrity]

9 Conclusion

[PLACEHOLDER: Conclusion content will be added here]