SecurePlusVPN

Even Safer VPN

SecurePlusVPN

Introduction

- In today's world, working from home is becoming trendy, and with the increase in work outside the office, the security and efficiency of network connections become crucial.
- Wireguard represents the most modern and, so far, the safest VPN technology we have chosen for our project.
- For the technology and hardware for our VPN application, we opted for Linux and Mikrotik.
- Our client-side application is multi-platform (Windows, Linux, macOS).

SecurePlusVPN

WireGuard

- It is a modern VPN protocol: WireGuard is a new, high-performance VPN protocol that focuses on simplicity and speed.
- Minimalist Design: Designed to be easily implementable, it has a much smaller codebase than most traditional VPN protocols.
- State-of-the-Art Encryption: Utilizes the latest encryption techniques, including Curve25519 for key exchange, ChaCha20 for encryption, Poly1305 for message authentication, and BLAKE2s for hashing.
- Fast and Reliable Connections: WireGuard's design ensures high performance and quick response, making VPN connections more stable and faster.
- Easy Configuration and Management: Offers a simple and intuitive interface for configuration, making setup and management easier.
- Enhanced Security and Privacy: Its minimalist approach and strong encryption provide an increased level of security and privacy compared to traditional VPN protocols.

SecurePlusVPN

Mikrotik

- RouterOS: At the heart of MikroTik products lies RouterOS, a robust and flexible Linux-based operating system that provides extensive networking management capabilities, including routing, switching, security, and wireless features.
- Customizability and Flexibility: Thanks to RouterOS, users can finely configure their devices, which includes advanced routing, firewall, VPN, wireless settings, and many more options.
- Scalability: MikroTik solutions can be easily scaled, allowing users to expand their networks as needed without the need to radically change the existing infrastructure.
- Community and Support: There is a strong community.

SecurePlusVPN

Linux

- Open-Source: Linux is an open-source operating system, meaning its source code is freely available for the public to view, allowing users to study, change, and distribute the software according to their needs.
- Variety of Distributions: There are many Linux distributions (distros) such as Ubuntu, Fedora, Debian, and CentOS, each with its own set of software and package management, tailored to different user needs.
- Security and Stability: Linux is known for its high level of security and stability, making it a popular choice for servers, embedded systems, and enterprise environments.
- Flexibility and Customizability: Users can customize Linux to their needs, from graphical user interfaces to the types of installed applications, making the system ideal for a wide range of uses.
- Community Support: Linux has a vast and active community of users and developers who provide support, advice, and continuously work on improvements and updates.
- Wide Usage: Linux is used in a range of devices from personal computers, servers, mobile devices (Android is based on Linux), to supercomputers, and embedded systems in consumer electronics.

SecurePlusVPN

MFA Security

- 2FA is a security process where users provide two distinct authentication factors to confirm their identity (e.g., SMS OTP, TOTP, U2F, Fingerprint, Push-Based, etc.).
- It includes verifying whether the hardware matches the assigned VPN and whether the login attempt is made by a human rather than a machine.
- There are opportunities for machine learning, thereby deepening security.
- We are open to adding more options.

SecurePlusVPN

Push route Wireguard !!!

- WireGuard is a point-to-point technology.
- We only set allowed subnets into the tunnel.

Our solution addresses this through dynamics (which you set in the address list in MikroTik).

- Push route in the context of VPN means that the VPN server automatically sends routing information for network traffic to clients upon connection. This allows clients to know which network paths to use for accessing certain network resources through the VPN, simplifying client configuration since they don't have to manually set up routes to access network resources.
- Push DNS means that the VPN server provides DNS servers (DNS server addresses) to clients upon their connection. This ensures that all DNS queries from clients are routed through the VPN, enhancing privacy and security by preventing DNS query leaks outside the encrypted VPN tunnel. Thus, push DNS ensures that all client DNS queries are resolved using a specific, often more secure or private DNS server.

SecurePlusVPN

What SecurePlusVPN does and is capable of

- SecurePlusVPN provides security layers on top of VPN communication, such as Multi-Factor Authentication (MFA).
- It allows for the pushing of routes and connects to Active Directory (AD).
- It offers remote assistance akin to TeamViewer, includes monitoring capabilities, etc.
- The solution is modular.

SecurePlusVPN

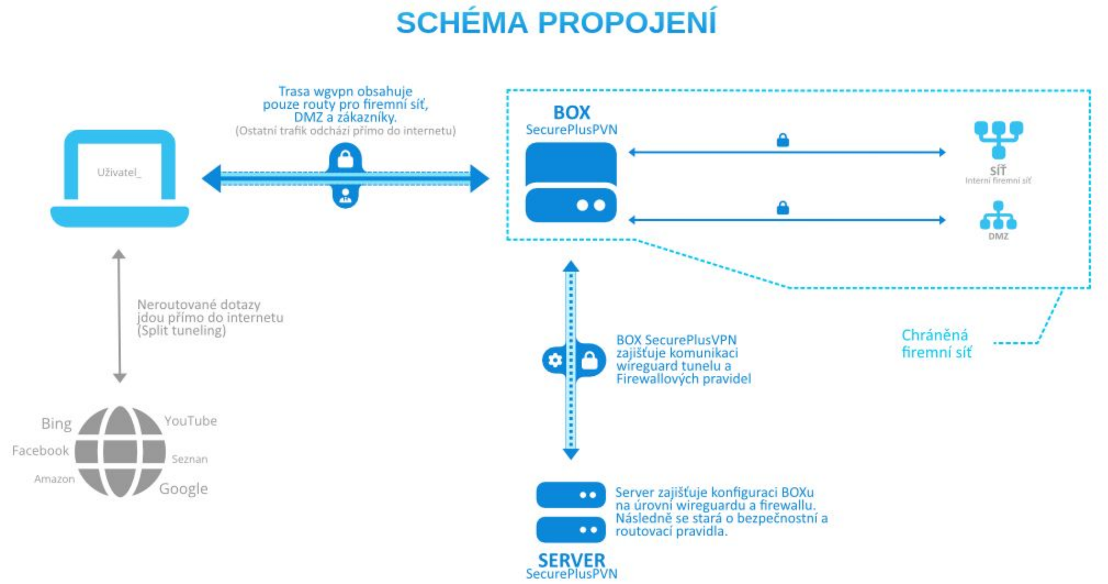


SCHÉMA PROPOJENÍ

Trasa wgvpn obsahuje pouze routy pro firemní síť, DMZ a zákazníky.
(Ostatní trafik odchází přímo do internetu)

Neroutované dotazy jdou přímo do internetu (Split tuneling)

BOX SecurePlusVPN zajišťuje komunikaci wireguard tunelu a Firewallových pravidel

Server zajišťuje konfiguraci BOXu na úrovni wireguardu a firewallu. Následně se stará o bezpečnostní a routovací pravidla.

SecurePlusVPN

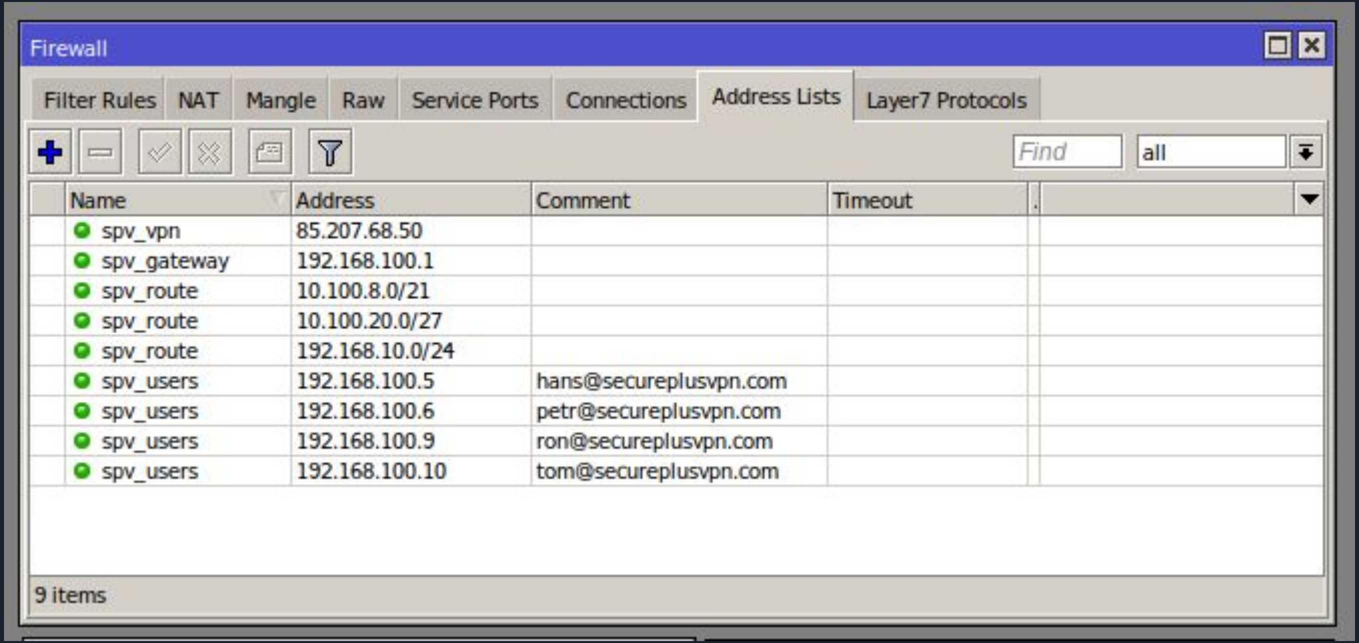
Basic MikroTik extension, minimum version 7, for use with the SecurePlusVPN client.

In MikroTik, the following must be set up for proper functionality:

- DNS resolver
- NTP server
- SMTP for sending configuration emails
- IP address list with the correct parameters
    - spv_vpn: The public IP address of the VPN server
    - spv_gateway: The IP address of the VPN gateway (the mask for the VPN is /24)
    - spv_route: IP addresses and ranges that we want to push to the client
    - spv_users: The IP address (/32) of the user and in the comment mention their email

After registering for SecurePlusVPN via email, you will receive a basic configuration file for connecting to the cloud platform that provides the MikroTik extension.

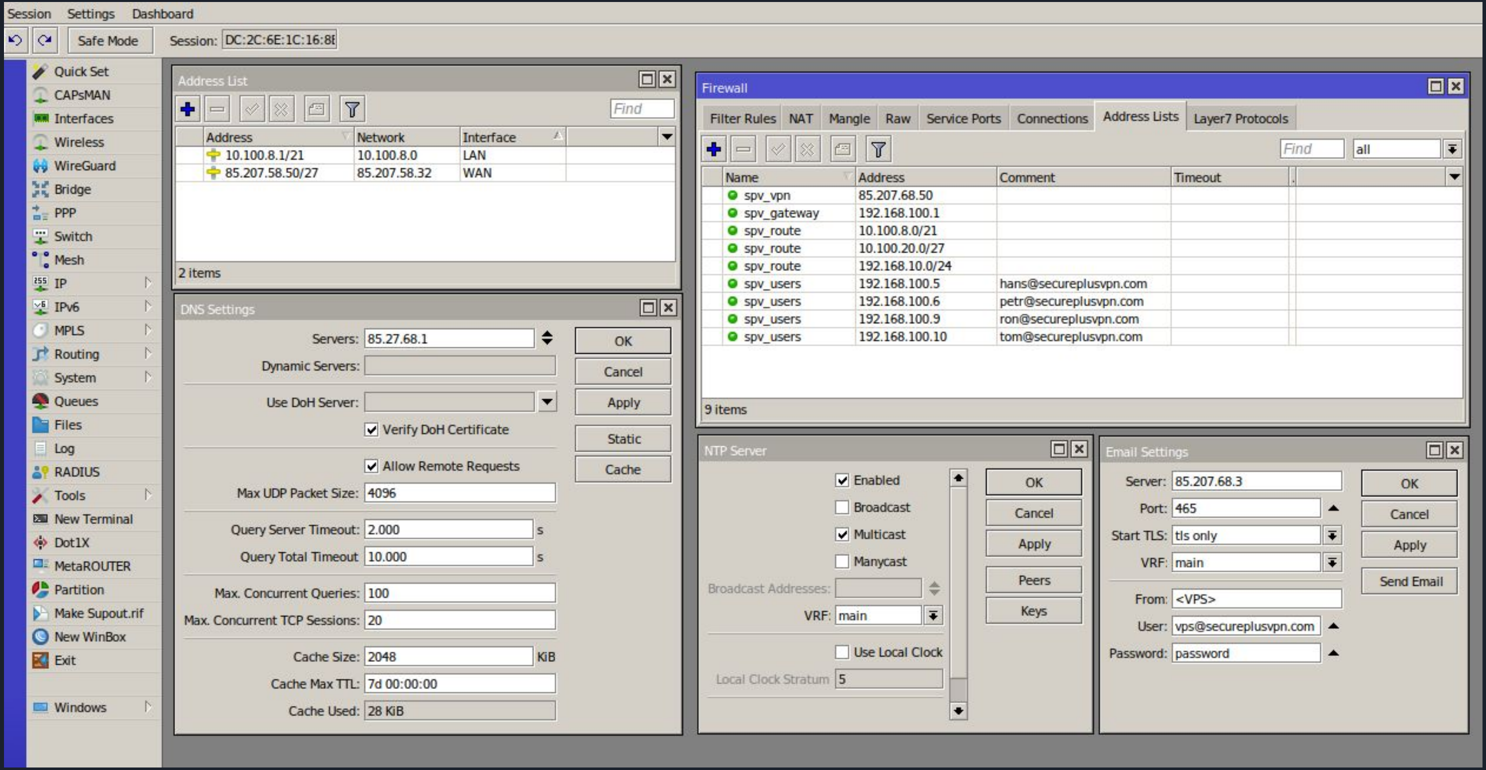
SecurePlusVPN



Name	Address	Comment	Timeout
● spv_vpn	85.207.68.50		
● spv_gateway	192.168.100.1		
● spv_route	10.100.8.0/21		
● spv_route	10.100.20.0/27		
● spv_route	192.168.10.0/24		
● spv_users	192.168.100.5	hans@secureplusvpn.com	
● spv_users	192.168.100.6	petr@secureplusvpn.com	
● spv_users	192.168.100.9	ron@secureplusvpn.com	
● spv_users	192.168.100.10	tom@secureplusvpn.com	

9 items

SecurePlusVPN



Session: DC:2C:6E:1C:16:8E

Address List

Address	Network	Interface
10.100.8.1/21	10.100.8.0	LAN
85.207.58.50/27	85.207.58.32	WAN

2 items

Firewall

Name	Address	Comment	Timeout
spv_vpn	85.207.68.50		
spv_gateway	192.168.100.1		
spv_route	10.100.8.0/21		
spv_route	10.100.20.0/27		
spv_route	192.168.10.0/24		
spv_users	192.168.100.5	hans@secureplusvpn.com	
spv_users	192.168.100.6	petr@secureplusvpn.com	
spv_users	192.168.100.9	ron@secureplusvpn.com	
spv_users	192.168.100.10	tom@secureplusvpn.com	

9 items

DNS Settings

Servers: 85.27.68.1

Dynamic Servers:

Use DoH Server:

☑ Verify DoH Certificate

☑ Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout 10.000 s

Max. Concurrent Queries: 100

Max. Concurrent TCP Sessions: 20

Cache Size: 2048 KiB

Cache Max TTL: 7d 00:00:00

Cache Used: 28 KiB

NTP Server

☑ Enabled

☐ Broadcast

☑ Multicast

☐ Manycast

Broadcast Addresses:

VRF: main

☐ Use Local Clock

Local Clock Stratum 5

Email Settings

Server: 85.207.68.3

Port: 465

Start TLS: tls only

VRF: main

From: <VPS>

User: vps@secureplusvpn.com

Password: password

SecurePlusVPN

Thank you for your attention!

info@secureplusvpn.com