PONTIFICAL CATHOLIC UNIVERSITY OF RIO GRANDE DO SUL
POSTGRADUATE PROGRAM IN COMPUTER SCIENCE

Virtual Private Networks
Theory and Practice using Core Emulator

Student: Telcio Cardoso - telcio.cardoso@edu.pucrs.br
Advisor: Tiago Ferreto - tiago.ferreto@pucrs.br

Agenda

1. Context
2. Pros & Cons
3. Core emulator
4. OpenVPN Protocol
5. Example 1 - Privacy
6. Example 2 - Network Traffic
7. Q&A

Context

History

- In 1996, a Microsoft employee(most sources say Gurdeep Singh-Pall) started developing the Peer to Peer Tunneling Protocol (PPTP). In 1999, the specification was officially published.
- Make communication and file-sharing between different offices possible, and to allow employees to access important files remotely without there being any risk of unauthorized users stealing sensitive data.
- Over the years, different types of VPN have emerged. Business VPNs, and personal VPNs, with different protocols (L2TP/IPsec, OpenVPN, PPTP, SSTP).

Context

What is a Virtual Private Network(VPN)

- Programming to create a safe encrypted connection over a less secure network, such as WAN.
- Uses tunneling protocols to encrypt data at the sending and decrypt it at the receiving.
- Virtual: it runs over a physical and existing network, therefore, is Virtual.
- Private: the data shared between the devices is encrypted and private.
- Network: A VPN is a network. It allows the transmission of information between peers, over long distances.

Context

Tunneling Protocols

- IP in IP (Protocol 4): IP in IPv4/IPv6
- SIT/IPv6 (Protocol 41): IPv6 in IPv4/IPv6
- GRE (Protocol 47): Generic Routing Encapsulation
- OpenVPN (UDP port 1194): Openvpn
- SSTP (TCP port 443): Secure Socket Tunneling Protocol
- IPSEC (Protocol 50 and 51): Internet Protocol Security
- L2TP (Protocol 115): Layer 2 Tunneling Protocol
- VXLAN (UDP port 4789): Virtual Extensible Local Area Network.

Context

Security

- Encryption is the process of encoding data so only an individual with the right decoder can understand such data.
- Common encryption methods are symmetric-key encryption and public-key encryption or asymmetric-key encryption.
- Digital Certificates used for public-keys reliance.

Context

Architectures

- Site-to-Site: connects two networks from different locations. No VPN clients are required.
- Remote Access: remote VPN client connects to a VPN server.
- Mobile: VPN servers use logical IP addresses providing seamlessy services to the mobile users.

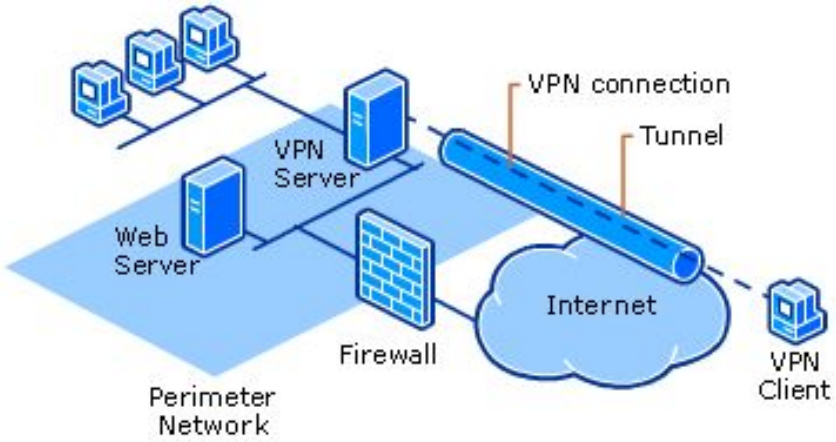
Context

OpenVPN Protocol

- Open-source Protocol, released in 2001
- Uses SSL/TLS for key exchange to create secure point-to-point or site-to-site connections
- Runs over TCP or UDP protocols
- Web traffic indistinguishable from the traffic using standard HTTPS over SSL
- Use of up to 256 bit encryption
- Support for dynamic IP addresses and DHCP
- No support for IPSec, L2TP and PPTP

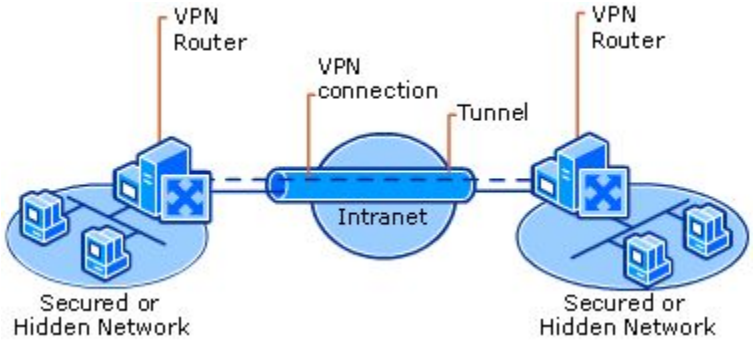
Context

VPN Remote Client/Server Architecture



Context

VPN Site-to-Site Architecture



Pros & Cons

Pros

- Security enhanced
- Privacy
- Bypass Geo-Restrictions on Websites and Content
- Anonymous Downloads
- File sharing between remote clients

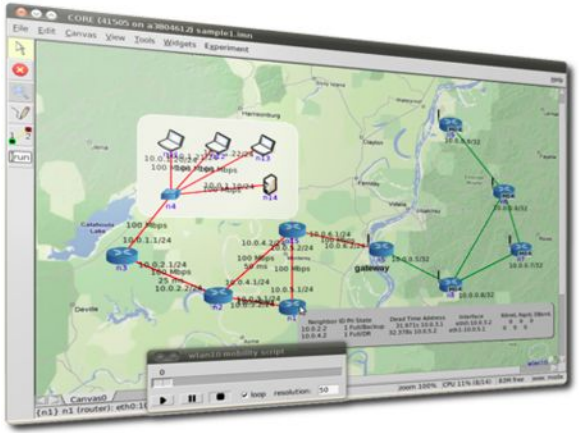
Cons

- Slower internet connection
- Increased network complexity
- Security issues

Core Emulator

Introduction

The Common Open Research Emulator (CORE) is a tool for building virtual networks. As an emulator, CORE builds a representation of a real computer network that runs in real time, as opposed to simulation, where abstract models are used: https://www.nrl.navy.mil/itd/ncs/products/core



Example

Example 1 - Privacy

DEMO

Example

Example 2 - Network Traffic

DEMO

Q&A