The Clavister

Quick VPN E Guide

A primer to understanding VPN, how to get the best security from it and what you need to know before you choose.

By Peter Nilsson
Published by Clavister
AB Sweden

Chapter 1: Introduction

In this guide our focus will be VPN (Virtual Private Network), introducing its value in security, its various forms and functions. We will mainly focus on IPsec and IPsec scenarios but we will also cover some scenarios involving L2TPv3 as well as troubleshooting VPNs using ping simulation in a longer book called VPN for cOS Core Cookbook.

If not yet familiar with Clavister, it is recommended that the first book “The Clavister cOS Core Cookbook” be read first in order to get a fundamental grasp of Clavister and some of our general principles.

Network diagram icons and screenshots

Throughout the book we will be using network schematics of various scenarios. The various icons used is shown and described in figure 1.0.1.

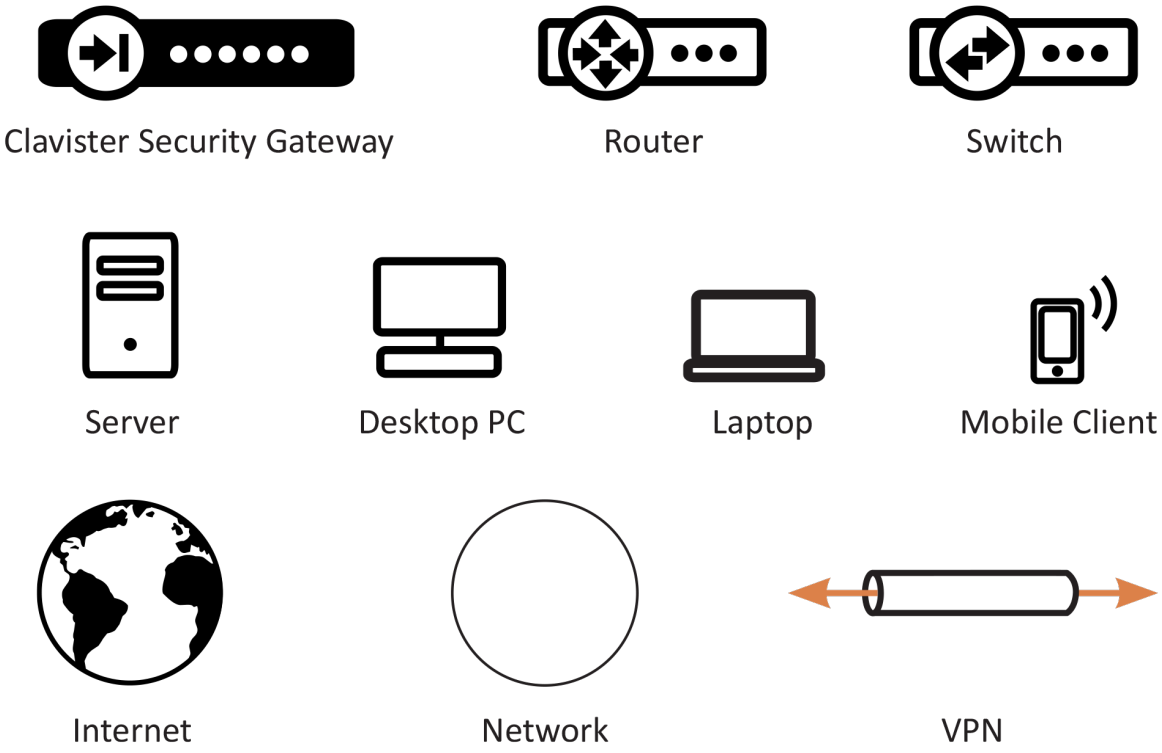

Figure 1.0.1 The various icons used throughout the book.

Screenshots

This book contains a large amount of screenshots primary taken from the Web User Interface (WebUI) of cOS Core. The screenshots are in most cases taken on a specific feature or function to highlight their use in the recipe context and may look different depending on what version of cOS Core that is used. Some pictures may be truncated slightly to make them fit better into the style and width of the book and also in an attempt to try limit the size of some screenshots to avoid them filling e.g. an entire page.

The book is based on the graphical style and feature set of cOS Core version 11.20.

1.1. An introduction to VPN – What is it?

The Internet is increasingly used as a means to connect computers since it offers efficient and inexpensive communication. The requirement therefore exists for data to traverse the Internet to its intended recipient without another party being able to read or alter the integrity of the message.

It is equally important that the recipient can verify that no one is falsifying data, in other words, pretending to be someone else. Virtual Private Networks (VPNs) meet this need, providing a highly cost effective means of establishing secure links between two co-operating computers so that data can be exchanged in a secure manner. VPN allows the setting up of a tunnel between two devices known as tunnel endpoints as shown in figure 1.1.1.

Figure 1.1.1 Connecting two devices together from different parts of the globe. Both sides have their own endpoint

All data flowing through a tunnel between the two endpoints is secured using encryption.

Encryption of VPN

Encryption of VPN traffic is done using the science of cryptography. Cryptography is an umbrella Expression, which covers 3 techniques and benefits:

1. **Confidentiality**

   No one but the intended recipients is able to receive and understand the communication. Confidentiality is accomplished by encryption.

2. **Authentication and Integrity**

   Proof for the recipient that the communication was actually sent by the expected sender, and that the data has not been modified in transit. This is accomplished by authentication, and is often implemented through the use of cryptographic keyed hashing.

3. **Non-repudiation**

   Proof that the sender actually sent the data; the sender cannot later deny having sent it. Non-repudiation is usually a side-effect of authentication.

VPNs are normally only concerned with confidentiality and authentication. Non-repudiation is normally not handled at the network level but rather is usually done at a higher, transaction level.

1.2. Planning VPN

An attacker, targeting a VPN connection, will typically not attempt to crack the VPN encryption since this requires enormous effort. They will, instead, see VPN traffic as an indication that there is something worth targeting at the other end of the connection. Typically, mobile clients and branch offices are far more attractive targets than the main corporate network. Once an attacker gains access inside mobile clients or branch offices, getting to the corporate network then becomes easier. In designing a VPN there are many issues that need to be addressed which aren't always obvious. These include:

- Protecting mobile and home computers.
- Restricting access through the VPN to needed services only, since mobile computers are vulnerable.
- Creating DMZs for services that need to be shared with other companies through VPNs.
- Adapting VPN access policies for different groups of users.
- Creating key distribution policies.

Endpoint Security

A common misconception is that VPN-connections are equivalent to the internal network from a security standpoint and that they can be connected directly to it with no further precautions. It is important to remember that although the VPN-connection itself may be secure, the total level of security is only as high as the security of the tunnel endpoints.

It is becoming increasingly common for users on the move to connect directly to their company's network via VPN from their laptops or tablets. However, the client equipment itself is often not protected. In other words, an intruder can gain access to the protected network through an unprotected laptop and already-opened VPN connections.

Placement in a DMZ

A VPN connection should never be regarded as an integral part of a protected network. The VPN gateway should instead be located in a special DMZ or outside a gateway dedicated to this task. By doing this, the administrator can restrict which services can be accessed via the VPN and ensure that these services are well protected against intruders.

In cases where the router, firewall or gateway features an integrated VPN feature, it is usually possible to dictate the types of communication permitted and cOS Core has this feature.

Key Distribution

Key distribution schemes are best planned in advance. An example of a key distribution would be the Pre-shared key or Certificates needed for an IPsec tunnel.

Issues that need to be addressed include:

- How will keys be distributed? Email is not a good solution. Phone conversations might be secure enough.
- How many different keys should be used? One key per user? One per group of users? One per LAN-to-LAN connection? One key for all users and one key for all LAN-to-LAN connections? It is probably better using more keys than are necessary today, since it will be easier to adjust access per user (group) in the future.

- Should the keys be changed? If they are changed, how often? In cases where keys are shared by multiple users, consider using overlapping schemes, so that the old keys work for a short period of time when new keys have been issued.
- What happens when an employee in possession of a key leaves the company? If several users are using the same key, it should be changed.
- In cases where the key is not directly programmed into a network unit, such as a VPN gateway, how should the key be stored? On an USB stick? As a pass phrase to memorize? On a smart card? If it is a physical token, how should it be handled?

This means that it is very important to make sure that no unauthorized access can be made to a Laptop, for example, that has the required encryption keys or Certificates installed.

Good Anti-Virus software and strong passwords to access the laptop in question, are pretty much a requirement in such scenarios.

An example how a third party could gain access to a secure server is shown in figure 1.2.1.

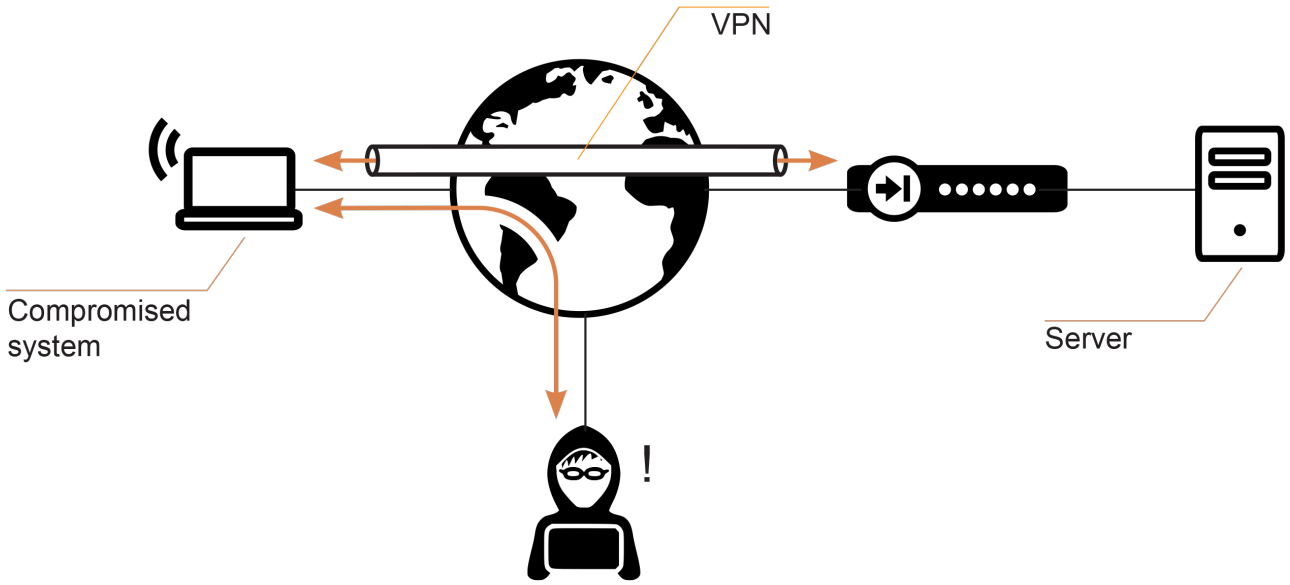

Figure 1.2.1 Very important to secure the system that establishes a VPN tunnel

If we take the scenario in figure 1.2.1 as an example we have a situation where we have an encrypted VPN connection between .e.g. a user's home PC and a Firewall located in the company the user works. The user uses the VPN tunnel in order to perform work from home.

The user has setup all the necessary VPN keys and encryption algorithms but if the home users PC get infected by a Trojan, an external third party could gain access to the company server by using the VPN tunnel already configured and established by the home user.

We will go through some of the common VPN tunnel scenarios as well as describe the various principles and how VPN works and how to apply it in various situations. But no matter how strong encryption and secure the VPN tunnel is, there may still be weak points in the network if a home users PC is lacking e.g. anti-virus software.

Want to read the full cOS Core VPN cookbook? Download it here