STUDY AND IMPLEMENTATION OF TLS/SSL VPN SOLUTION USING GNS3

Presented By
EL MOTAMID Houria

Professor
M. SADQI Yassine

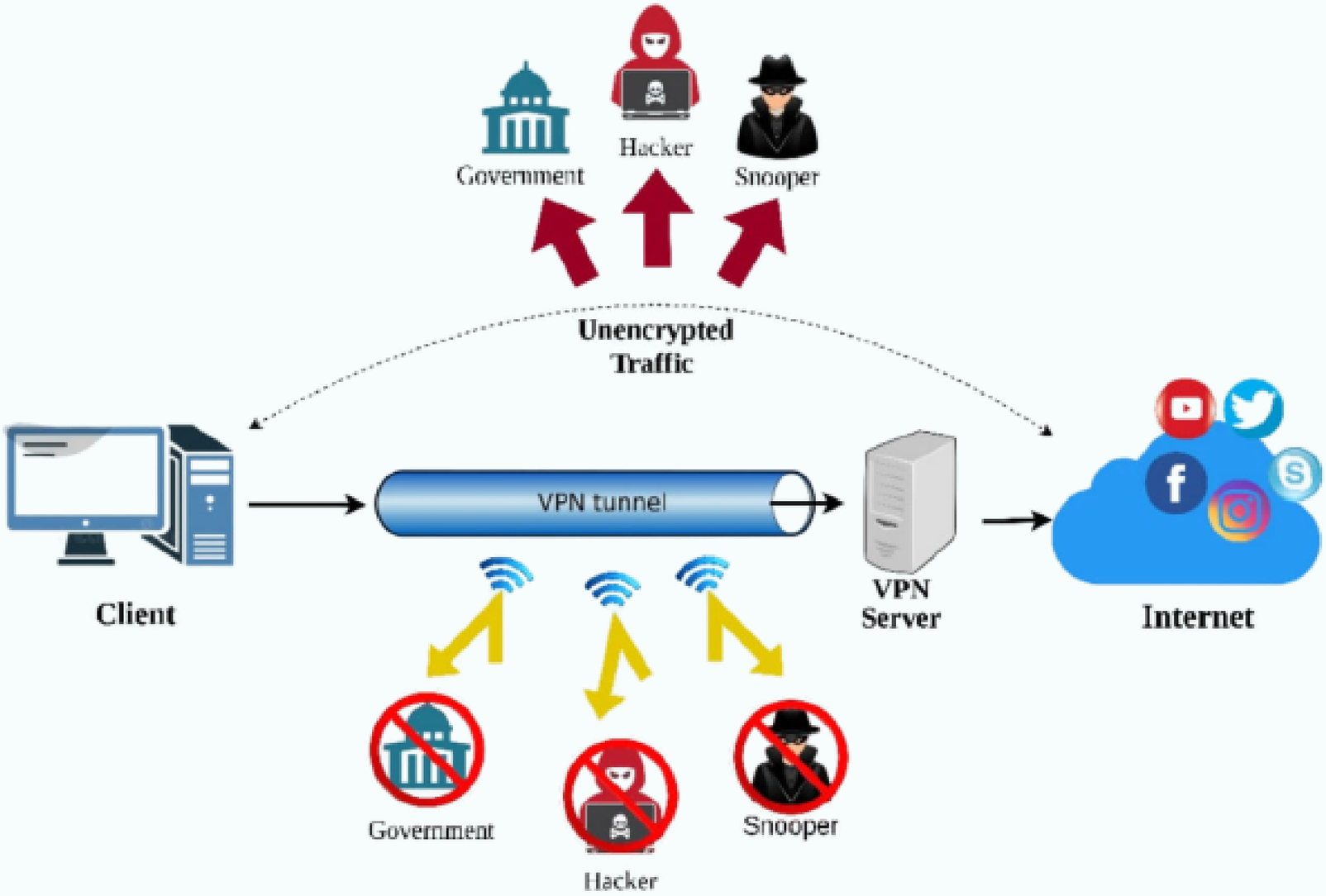
Contents

Introduction

The Internet has been the most incredible way of exchanging information, helping organizations manage activities.
As organizations grow, various techniques must be utilized to ensure secure network.
Virtual Private Networks (VPNs) play a vital role in developing business continuity plans of organizations securely through their tunneled network over the Internet.

Contents

What is a VPN


Government
Hacker
Snooper
Unencrypted
Traffic
VPN tunnel
Client
VPN
Server
Internet
Government
Hacker
Snooper

Types of VPN

Host-To-Host

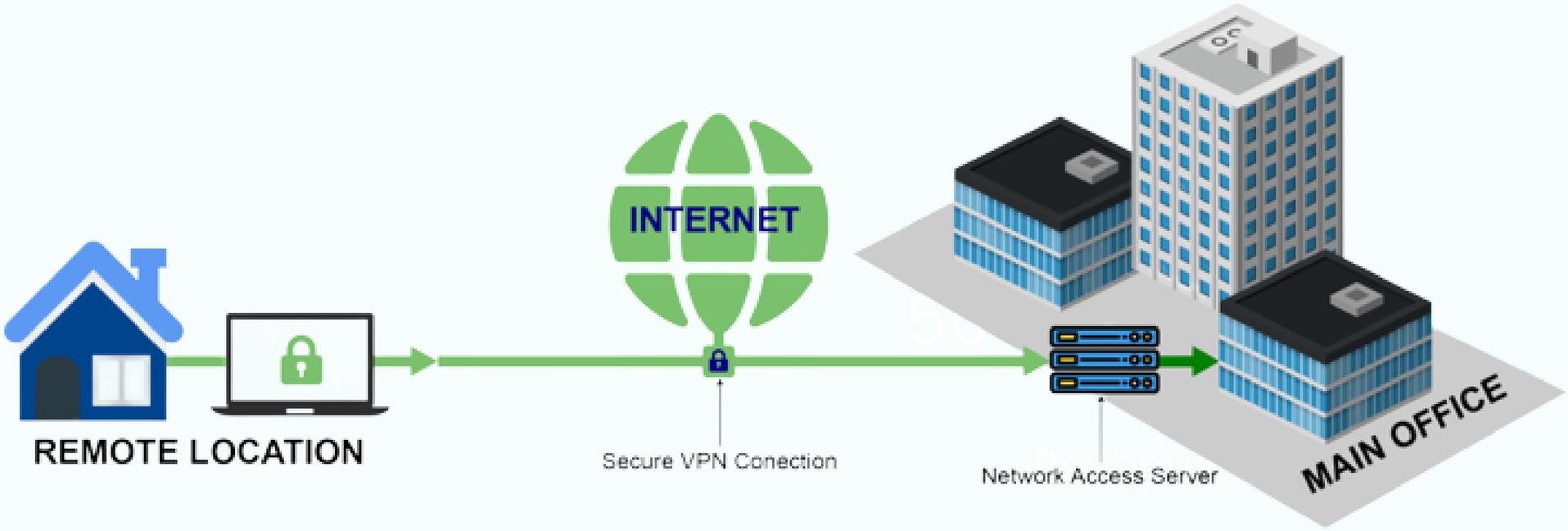
Host-to-Site

Site-to-Site

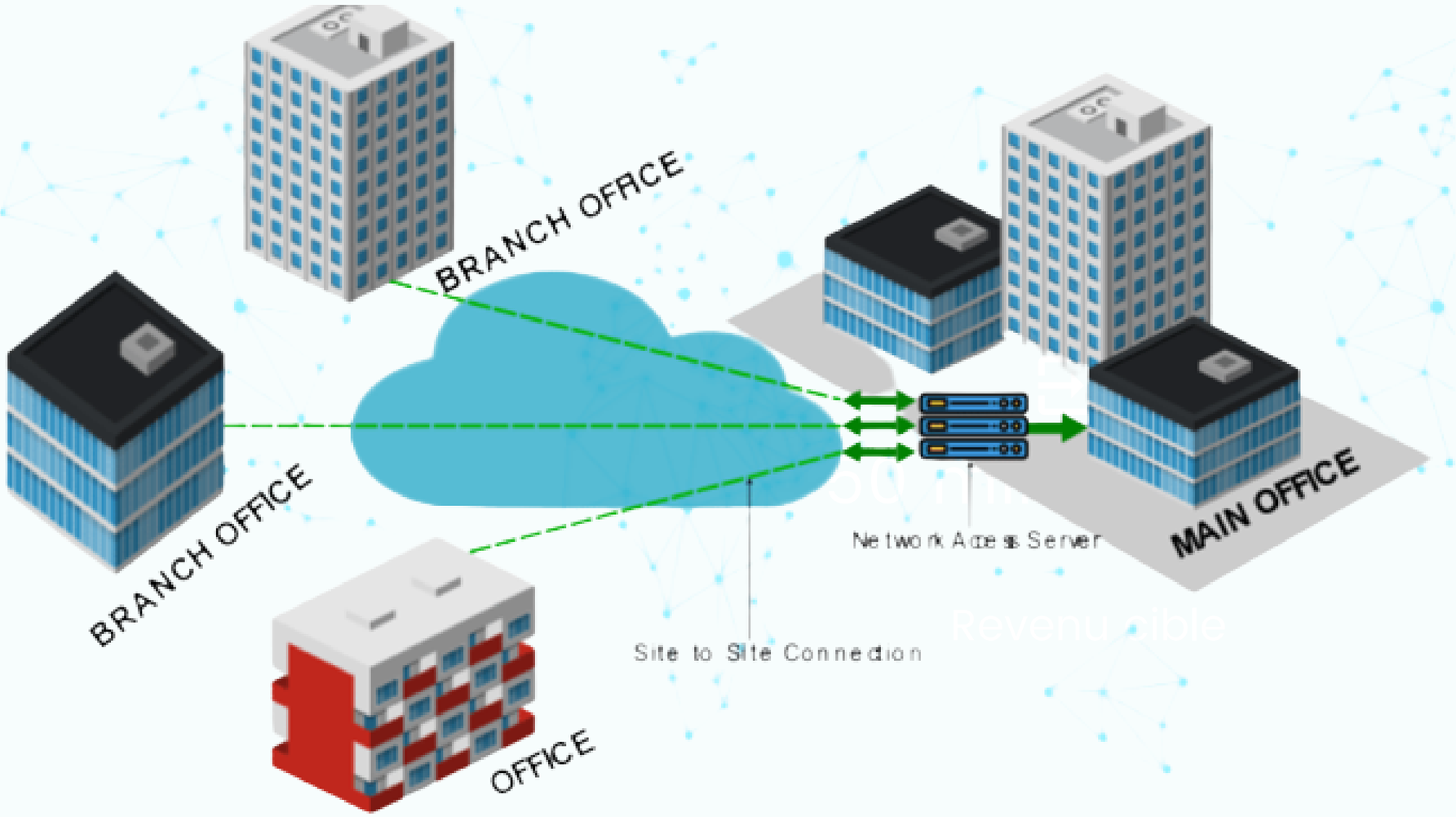
Host-to-Host


Encrypted tunnel
Internet or public infrastructure
Encrypted tunnel

Host-to-Site


INTERNET
REMOTE LOCATION
Secure VPN Conection
Network Access Server
MAIN OFFICE

Site-to-Site


BRANCH OFFICE
BRANCH OFFICE
OFFICE
Site to Site Connection
Network Access Server
MAIN OFFICE

Difference between the two types

Remote Access VPN	Site To Site VPN
A client software is used in the user's device	No client software is needed on the user's device
The user needs to initiate the VPN tunnel setup	The user doesn't need to initiate the VPN tunnel setup
The user's device communicates with the VPN gateway using VPN tunnel	The VPN gateway from one LAN communicates with the VPN gateway of the other LAN and creates secure VPN tunnel

Components to establish VPN

Authentication

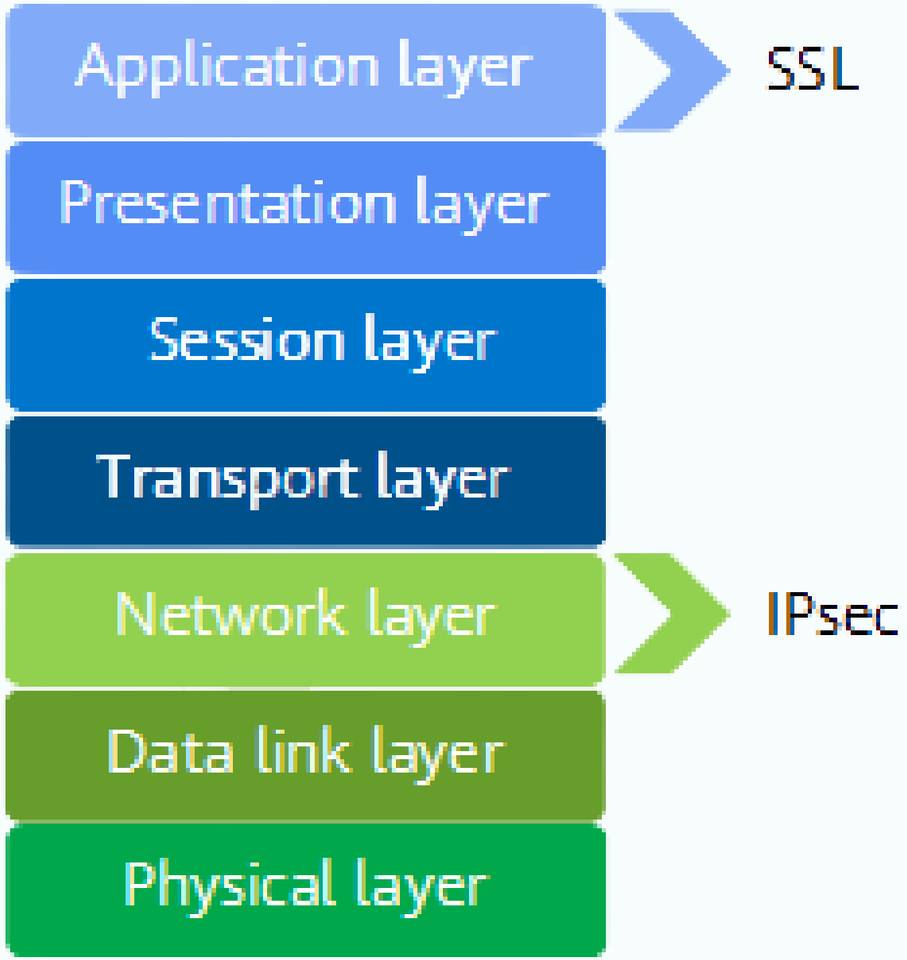
Encryption

Tunneling

VPN tunneling protocols

PPTP	It uses the TCP port 1723 for communication which uses the Generic Routing Encapsulation (GRE) protocol to encapsulate PPP packets. These packets are encrypted with MPPE.
L2TP	It is an extension of the PPP protocol that merges the best features of two other tunneling protocols PPTP (Point-to-Point Tunneling Protocol) and L2F (Layer 2 Forwarding Protocol)
IpSec	It sits at layer 3 of the stack and protects IP packets exchanged between remote networks or hosts and an IPsec gateway located at the edge of an organization's private network.
SSL/TLS	It create a vpn connection where the web browser acts as the client and the user access is restricted to specific applications instead of entire network

VPN tunneling protocols and OSI

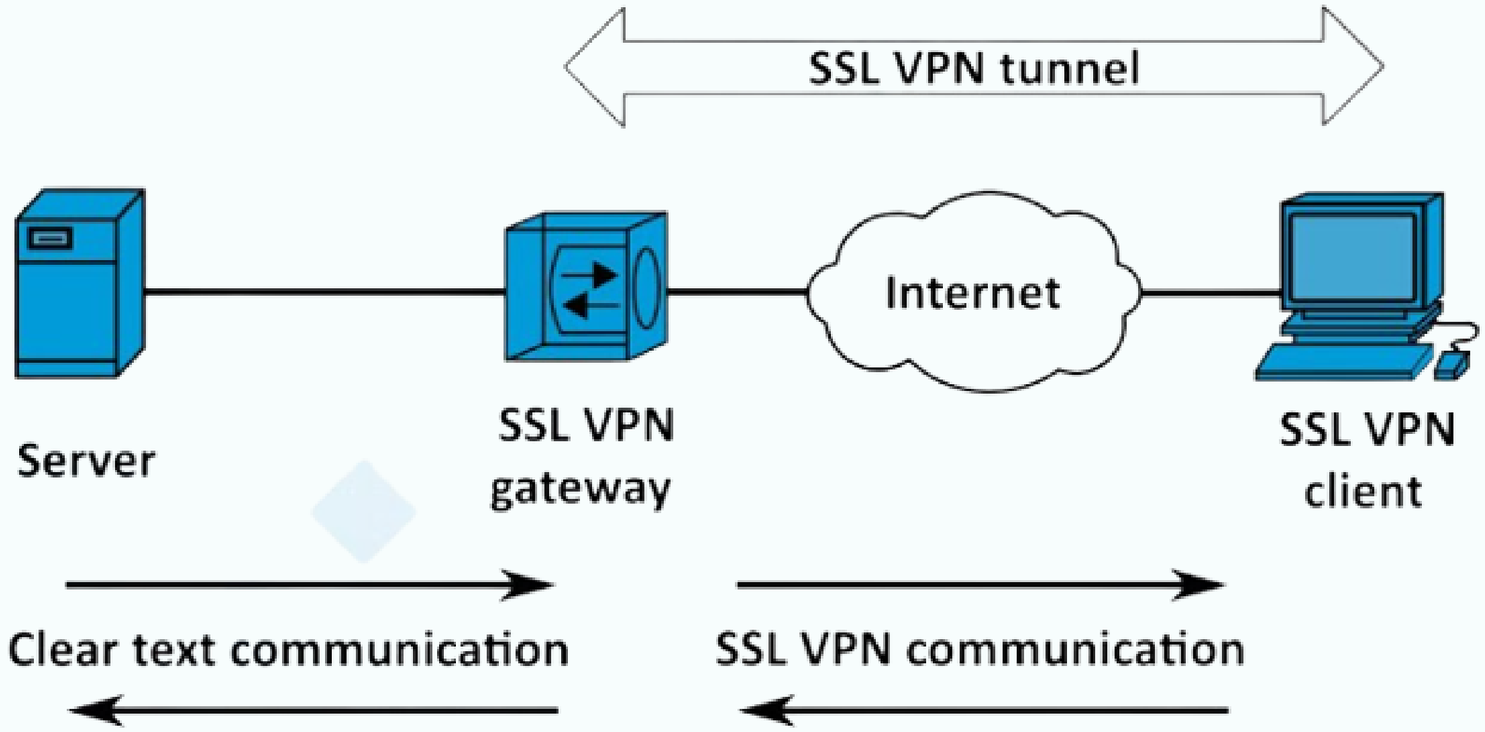


Contents

SSL/TSL VPN

An SSL VPN (Secure Sockets Layer virtual private network) is a form of VPN that can be used with a standard Web browser. In contrast to the traditional Internet Protocol Security (IPsec) VPN, an SSL VPN does not require the installation of specialized client software on the end user's computer

How SSL/TSL VPN works



SSL/TSL VPN types

SSL portal VPN

- It allows a user to use a single standard SSL connection to a Web site to securely access multiple network services.
- The site accessed is typically called a portal because it has a single page that leads to many other resources.

SSL tunnel VPN

- allows a user to use a typical Web browser to securely access multiple network services through a tunnel that is running under SSL.
- It requires that the Web browser be able to handle specific types of active content (e.g., Java, JavaScript, Flash, or ActiveX) and that the user be able to run them.

The advantages of using SSL VPN

THE SECURITY OF SSL VPN

THE FLEXIBILITY OF SSL VPN

THE COST REDUCTION OF SSL VPN

SSL VPN Features

Manageability	Such as status reporting, logging, and auditing
Availability	High availability is a failover feature to ensure availability during device interruptions.
Scalability	It is often integrated with high availability by balancing the VPN load amongst multiple SSL VPN devices.
Customization	Customized portals are often necessary to support PDAs and smart phones over the SSL VPN

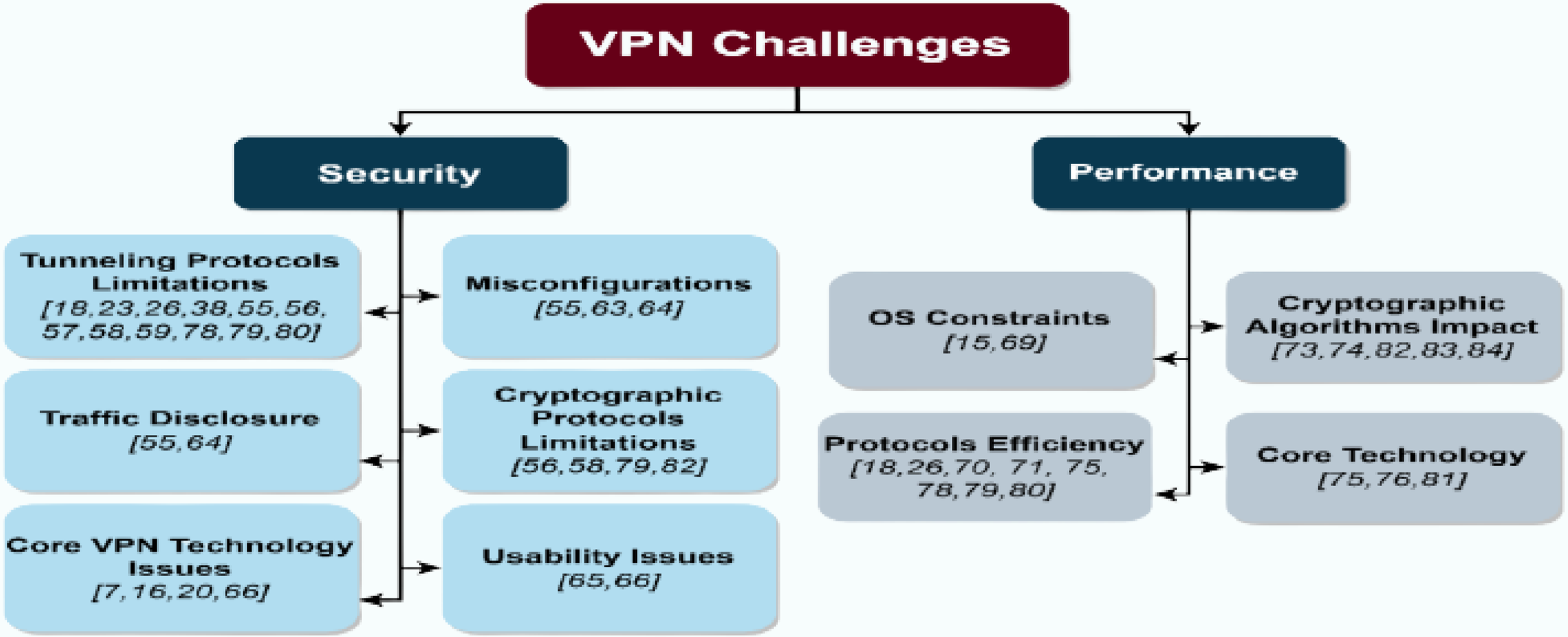
SSL VPN security services

Authentication	This feature includes the ability to support strong authentication.
Encryption and integrity protection	Both are inherent in SSL.
Access control	Access control permits or restricts access to applications at a granular level,
Endpoint security controls	It validates the security compliance of the client system that is attempting to use the SSL VPN.
Intrusion prevention	IIt involves inspecting the data after it has been decrypted in the SSL VPN for potential attacks.

Implementation

Conclusion

SSL VPNs offer versatility and ease of use because they use the SSL protocol, which is included with all standard Web browsers, so the client usually does not require configuration by the user.


VPN Challenges
Security
Performance
Tunneling Protocols Limitations
[18,23,26,38,55,56, 57,58,59,78,79,80]
Misconfigurations
[55,63,64]
Traffic Disclosure
[55,64]
Cryptographic Protocols Limitations
[56,58,79,82]
Core VPN Technology Issues
[7,16,20,66]
Usability Issues
[65,66]
OS Constraints
[15,69]
Cryptographic Algorithms Impact
[73,74,82,83,84]
Protocols Efficiency
[18,26,70, 71, 75, 78,79,80]
Core Technology
[75,76,81]

Ressources

You can find here some ressources that i used to build this presentation

1. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=890029

2. https://doi.org/10.1016/S1353-4858(09)70112-6

3. https://doi.org/10.1016/S1361-3723(05)70254-2

4. https://csrc.nist.gov/publications/detail/sp/800-113/final

5. 10.1109/ICSESS.2011.5982375

6.https://www.researchgate.net/publication/270271647_A_Review_on_IPsec_and_SSL_VPN

Thank You