

Virtual Private Networks

CISC 3325 — CUNY Brooklyn College

Lecture Notes



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks

2

In this chapter, we will:

1. Define what Virtual Private Networks are.
2. List the advantages of using a VPN.
3. Discuss Virtual Private Network types.
4. Provide several examples where VPNs are useful.



Virtual Private Networks

3

A **Virtual Private Network**, or **VPN**, is a private network that creates a tunnel between two devices/networks, and data is transmitted securely through this tunnel but on a public shared network.

A VPN is a private network, but uses the public network (Internet) to connect to remote sites. VPN creates a 'virtual' tunnel connection routed through the Internet from the company's or user's trusted network to the remote server, office, or a mobile work force. With VPN, you can send data via the public network which **emulates** (= electronically simulates) a private link between the two parties or two networks.

A secure VPN encrypts data before passing it through the tunnel to ensure privacy. Data integrity and authenticity are also maintained before the creation of the tunnel. Thus, VPN protects data with privacy, integrity, and authenticity. With VPN, you can provide many services such as the Internet, e-mail, applications, and database services to users in remote locations with secured communication.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks

4

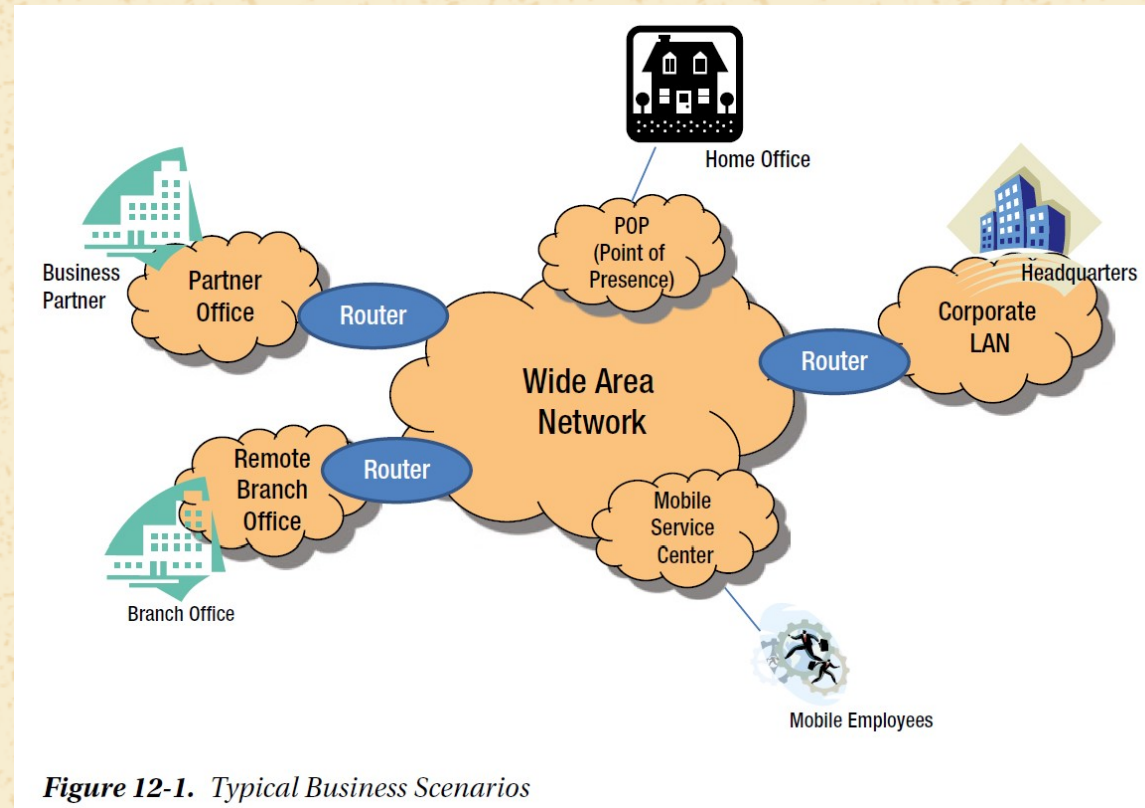


Figure 12-1. *Typical Business Scenarios*

"Figure 12-1: Typical Business Scenarios" (page 245), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks

5

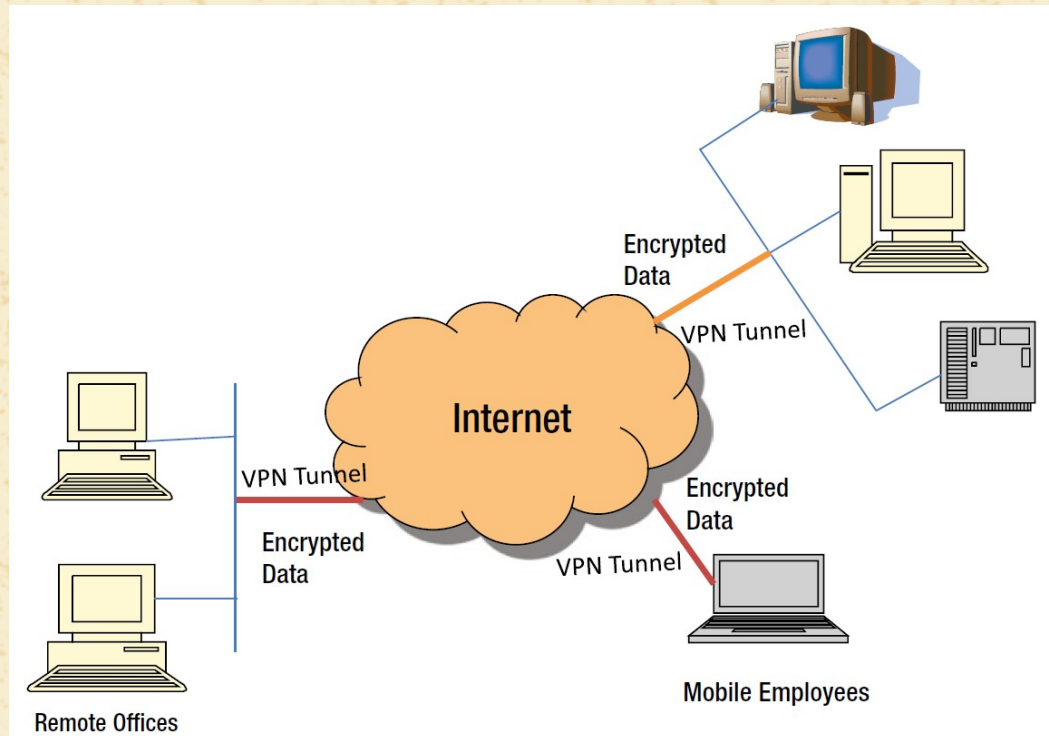


Figure 12-2. *Virtual Private Network scenario*

"Figure 12-2: Virtual Private Network scenario" (page 246), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Advantages

6

A Virtual Private Network (VPN) allows two computers to communicate securely over the public network such as the Internet. Advantages of using VPN include:

- Cost savings: A VPN is an inexpensive alternative to using a private, physical network and infrastructure, allowing the full advantage of cost savings of the Internet and providing a superior level of security.
- Smooth and Seamless Integration: There is no need to change your network architecture or any network software component to use a VPN.
- Secure Remote Access: VPN technology allows the same connectivity whether it is network to network, host to host, client to server, dial-up connections, or home office or mobile users.
- Extranet Connections: A VPN creates a secured connection between two business partners/companies, allowing even proprietary information to be shared without the risk of it being exposed to the world.
- Low Maintenance: VPN eliminates much of the day-to-day maintenance such as cryptographic key management.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Advantages

7

Any questions?



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

8

VPN can be categorized as one of the following 2 types:

1. Remote Access (Host-to-Site) VPN: Remote Access (Host-to-Site) VPN is a connection between a user and the LAN inside a company where the user is an employee who needs to connect to the corporate network from outside the company.

This type of connection is used mainly by telecommuting or sales force employees who want to connect to the corporate LAN from remote locations.

It provides a secure, encrypted communication between two parties that are connected via the Internet.

Another variation of Remote Access connection includes Host-to-Host VPN, in which two host devices are connected through a VPN tunnel and transfer data with each other (but don't access any other resources on the network.)



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

9

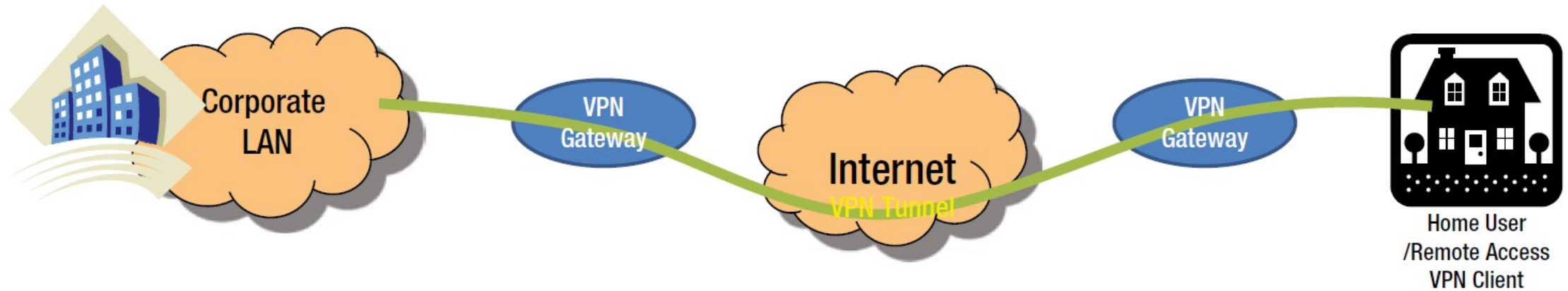


Figure 12-3. *Remote Access VPN*

"Figure 12-3: Remote Access VPN" (page 248), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

10

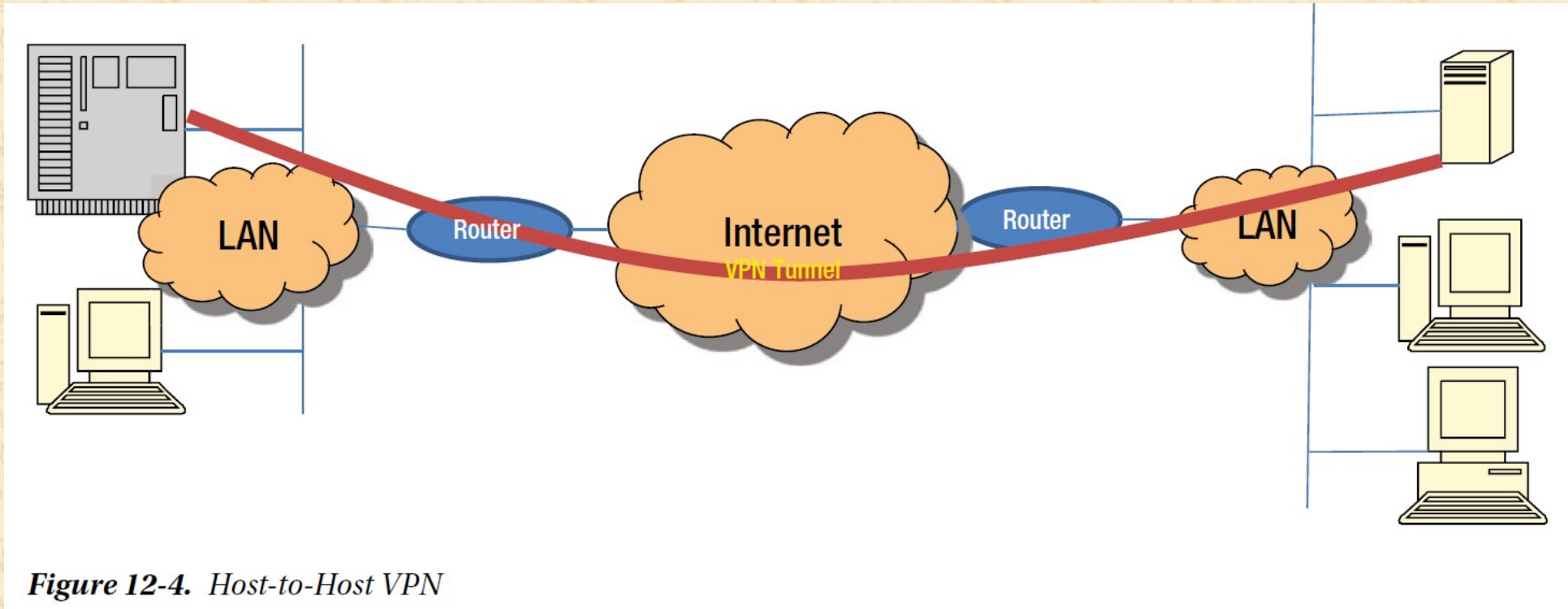


Figure 12-4. *Host-to-Host VPN*

"Figure 12-4: Host-to-Host VPN" (page 248), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

11

2. Site-to-Site (Intranet and Extranet) VPN: Site-to-site VPN connects one network to another network over the Internet, such as connecting a remote branch office to the corporate headquarters LAN. In this setup, the tunnel is created between two VPN gateways.

The VPN gateway is responsible for authentication of the user/network, encryption, and integrity of data.

The VPN tunnel is created between two sites allowing the company's network and resources available to the remote location. This solution is ideal for small offices located in remote parts of the world.

Two networks are connected as if they are one. Any device on one network can communicate with the device on the other network securely as if the other device is part of the same network.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

12

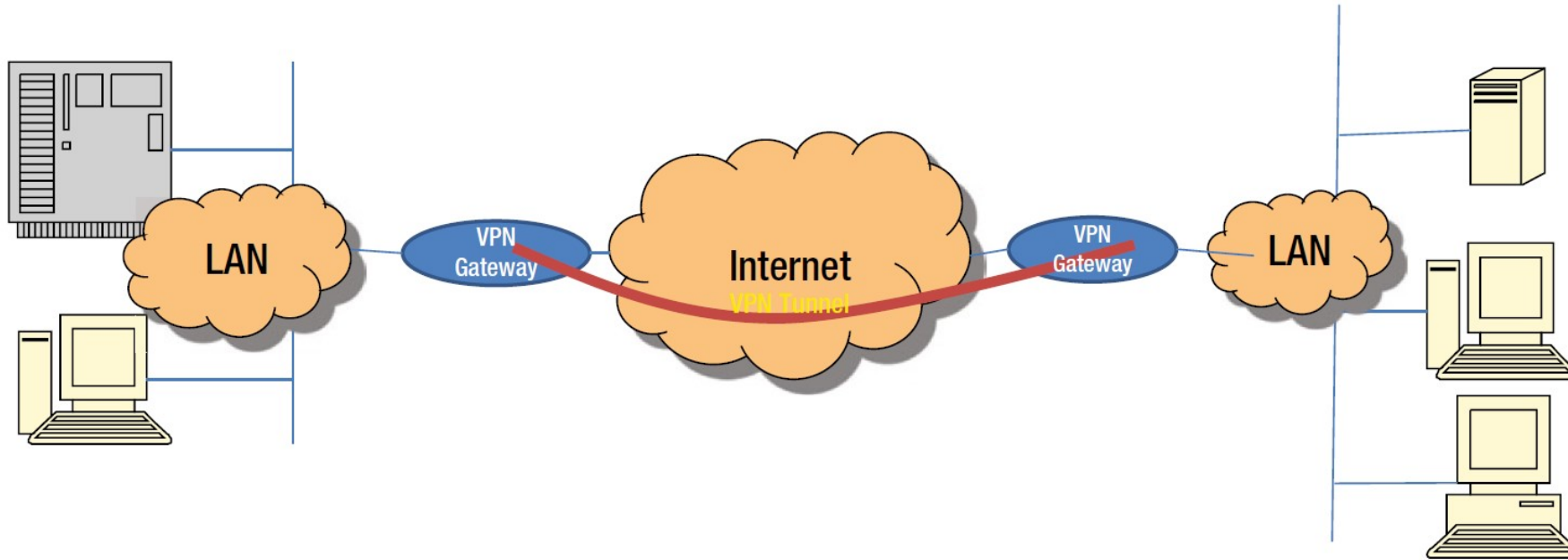


Figure 12-5. Site-to-site VPN

"Figure 12-5: Site-to-site VPN" (page 249), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Types

13

Any questions?



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPNs & Firewalls

14

Recall that a firewall is used to control the access into the network so that it can stop the spread of 'fire' in the surrounding area.

A VPN, on the other hand, provides the secured channel between the two parties who are exchanging information. A combination of VPN and Firewall would ensure only authorized applications and users are accessing the information.

A VPN Firewall ensures that malicious intentions are impeded and only authentic traffic enters into the VPN.

VPN and firewall can be deployed separately. Normally VPN is deployed after the firewall. First check of entry is firewall.

Some of the VPN gateway vendors are now providing firewall functions also. This has an added advantage of using a single device to configure both as VPN gateway and firewall.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPNs & Firewalls

15

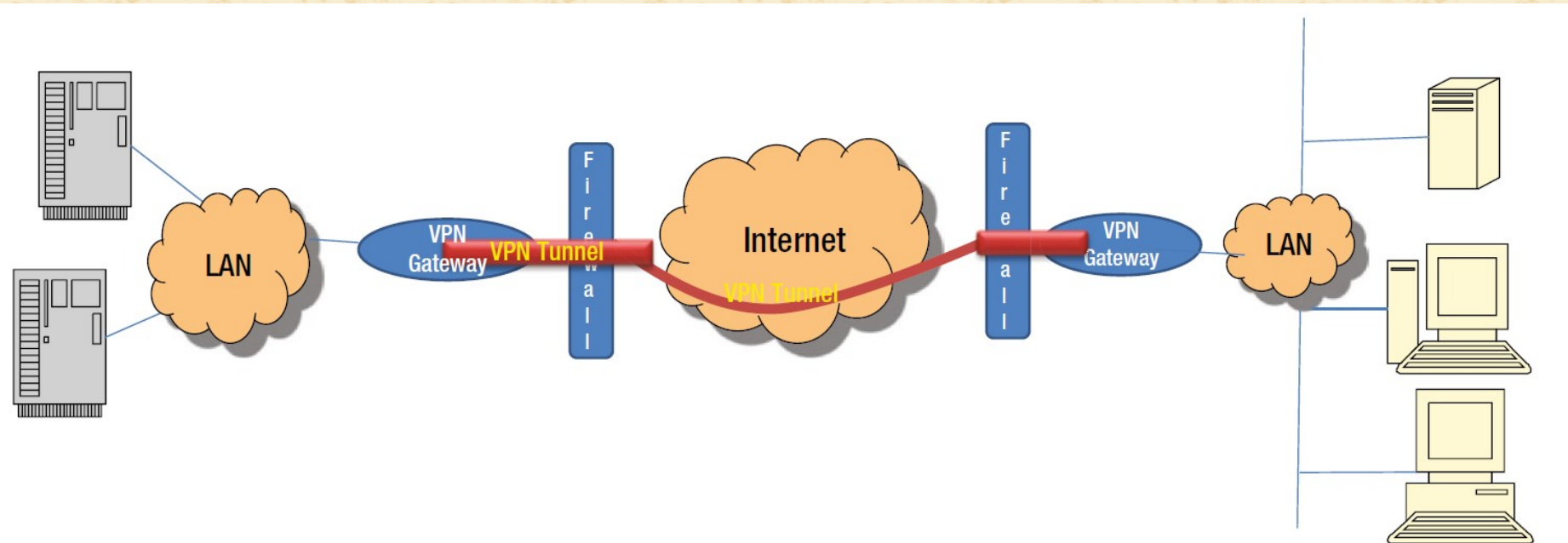


Figure 12-6. *VPN and Firewall Deployment*

"Figure 12-6: VPN and Firewall Deployment" (page 250), Nayak, U., & Rao, U. H. (2014). *The InfoSec handbook: An introduction to information security* (1st ed.). APRESS.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPN: Uses

16

Besides the VPN Advantages that we already listed on [slide 6](#), following are 8 common reasons to use a VPN:

1. **Enhanced Privacy:** A VPN encrypts your internet traffic, making it difficult for third parties like hackers, ISPs, or advertisers to monitor your activities. This ensures your online activities remain confidential, especially when using public Wi-Fi networks.
2. **Secure Data Transmission:** VPNs use encryption protocols to secure the data you send and receive, protecting sensitive information like passwords, financial data, or personal details. This is particularly useful for remote work or online banking.
3. **Access to Geo-Restricted Content:** By masking your IP address and rerouting your connection through servers in different locations, a VPN allows you to access region-specific content, such as streaming services, websites, or apps not available in your region.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPN: Uses

17

4. **Bypassing Censorship:** VPNs can circumvent government or network restrictions on certain websites or services by routing traffic through servers in unrestricted regions. This supports freedom of access, especially in regions with strict internet regulations.
5. **Anonymity:** A VPN hides your real IP address, making it difficult for websites or entities to track your identity or location. This helps avoid targeted advertising, identity theft, or unwanted surveillance.
6. **Improved Security for Remote Work:** VPNs establish secure connections for employees accessing corporate networks remotely. This ensures safe communication of proprietary information and protects against data breaches.
7. **Protection on Public Wi-Fi:** Public Wi-Fi networks are often insecure, making them a hotspot for hackers. VPNs encrypt your connection even on these networks, shielding your device from threats when using Wi-Fi in cafes, airports, or hotels.
8. **Prevent Bandwidth Throttling:** ISPs sometimes reduce your connection speed based on your online activities. A VPN hides these activities, preventing throttling and maintaining consistent connection speeds for tasks like streaming or gaming.



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPNs

18

An excellent video showing what VPNs are used for and how they work:



<https://www.youtube.com/watch?v=R-JUOpCgTZc>



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

VPNs

19

Any questions?



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).

Virtual Private Networks: Sources

Rao, Umesh Hodeghatta, and Umesha Nayak. "Chapter 12: Virtual Private Networks." *The InfoSec handbook: An introduction to information security*. Springer Nature, 2014, pp. 245-262. URL: <https://link.springer.com/content/pdf/10.1007/978-1-4302-6383-8.pdf#chapter+12:+virtual+private+networks>



These notes by [Miriam Briskman](#) are licensed under [CC BY-NC 4.0](#) and based on [sources](#).