



Triển khai Windows Server Remote Access - VPN

- Nhóm 18 -

Môn học: Quản trị mạng và hệ thống

GVHD: Đỗ Hoàng Hiến

THÀNH VIÊN

- 21522067 - Lê Huy Hiệp
- 21522198 - Nguyễn Việt Khang
- 21522735 - Bùi Đức Anh Tú
- 21522701 - Hồ Minh Trí
- 21522800 - Nguyễn Long Vũ

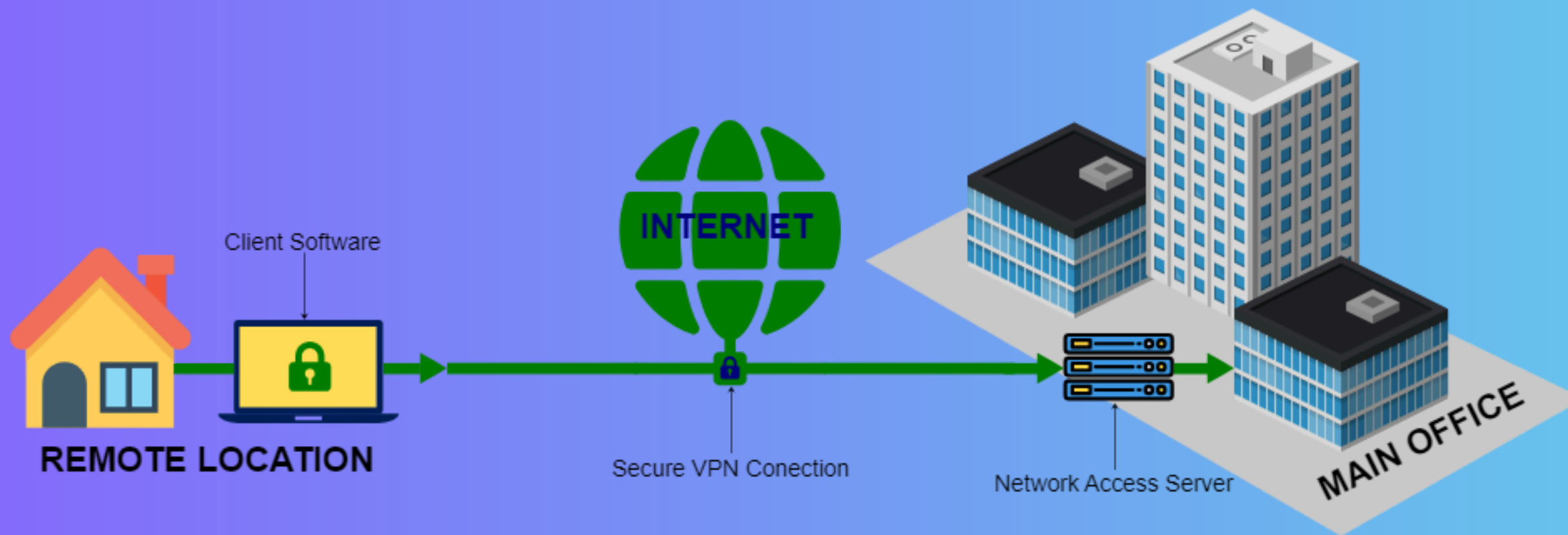


KHÃI NIỆM

VPN PROTOCOLS

Virtual Private Network - Mạng riêng ảo từ xa

Là một loại VPN cho phép người dùng kết nối an toàn và truy cập mạng nội bộ của công ty hoặc tổ chức từ xa. Khi kết nối, người dùng có thể truy cập vào các tài nguyên trên mạng như thể thiết bị của họ được kết nối trực tiếp tại văn phòng.



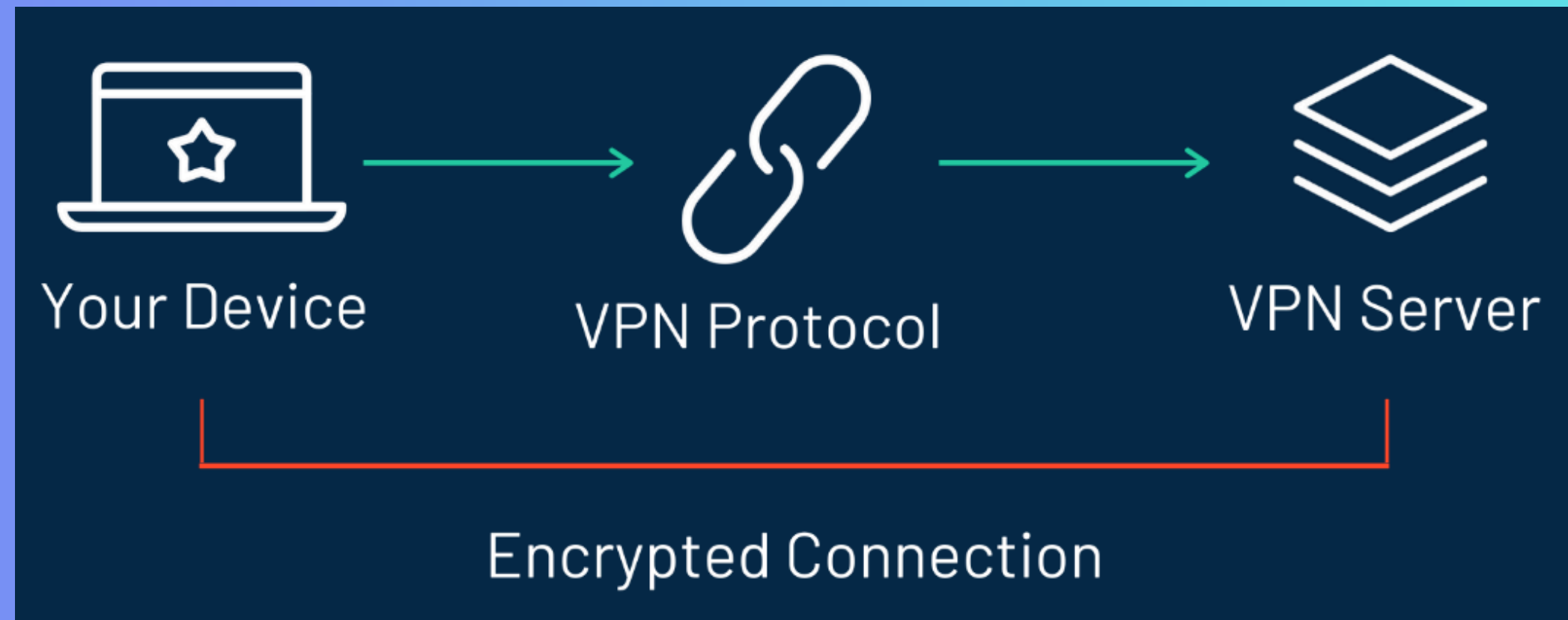
REMOTE ACCESS VPN

Virtual Private Network - Mạng riêng ảo từ xa

PPTP là giao thức VPN đầu tiên được phát triển bởi Microsoft, cho phép thiết lập kết nối riêng ảo dựa trên kết nối quay số. PPTP sử dụng chuẩn mã hóa 128-bit và xác thực MS-CHAP v2[1], nhưng có nhiều lỗ hổng bảo mật và dễ bị bẻ khóa bởi NSA[2]. PPTP nhanh và dễ cấu hình, nhưng không an toàn và không nên sử dụng

[1] MS-CHAP v2 là một giao thức xác thực dựa trên mật khẩu được sử dụng trong các giao thức VPN như PPTP và PEAP. MS-CHAP v2 cung cấp xác thực hai chiều giữa các đối tác bằng cách gửi thêm một thách thức và một phản hồi xác thực trong các gói tin trao đổi. MS-CHAP v2 sử dụng mã hóa DES để mã hóa băm mật khẩu NTLM và không truyền mật khẩu dưới dạng văn bản qua liên kết.

[2] NSA là viết tắt của National Security Agency, cơ quan an ninh quốc gia của Hoa Kỳ. NSA có nhiệm vụ thu thập và phân tích các tín hiệu truyền thông nước ngoài, đồng thời bảo vệ các kênh truyền thông của chính phủ Hoa Kỳ

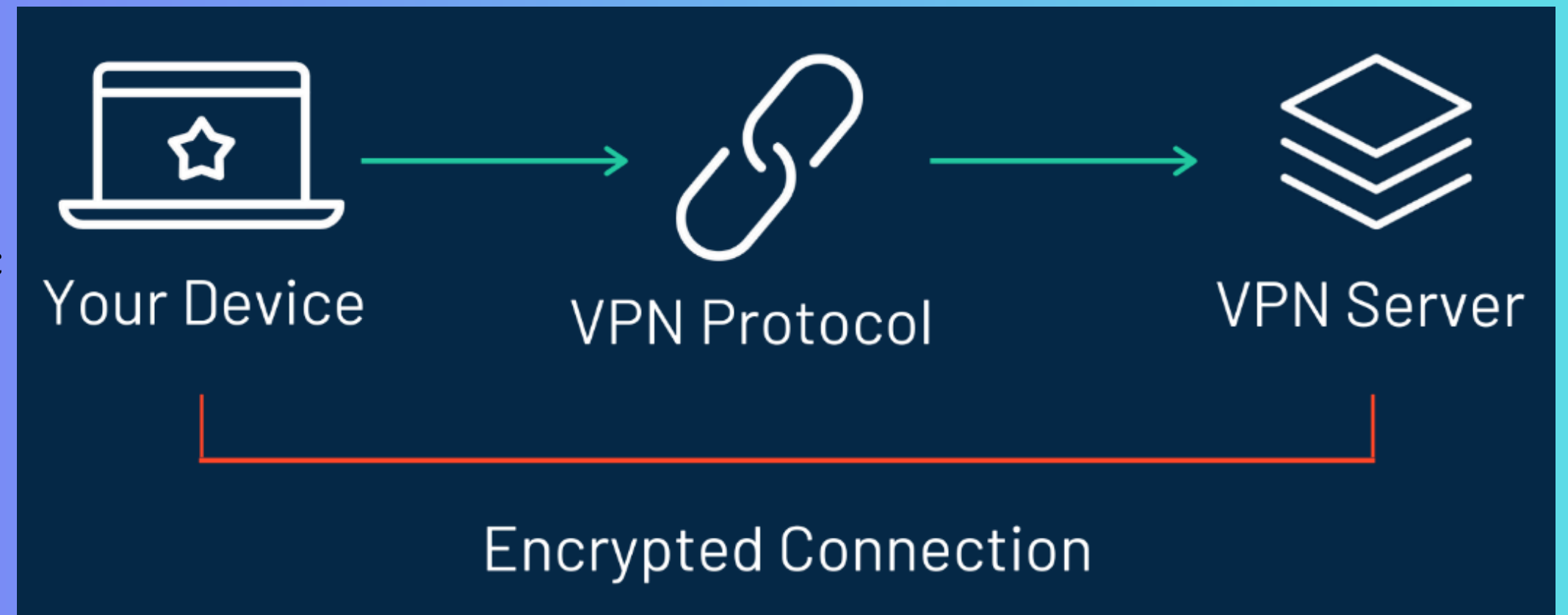


REMOTE ACCESS VPN

Virtual Private Network - Mạng riêng ảo từ xa

L2TP là giao thức VPN mở rộng từ PPTP, không mã hóa dữ liệu mà phải kết hợp với IPsec[1] để bảo mật. L2TP sử dụng cổng UDP 500, nên có thể bị chặn bởi tường lửa NAT. L2TP có bảo mật cao hơn PPTP, nhưng cũng có thể bị NSA can thiệp. L2TP có sẵn trên nhiều nền tảng và là lựa chọn thay thế khi không thể sử dụng OpenVPN

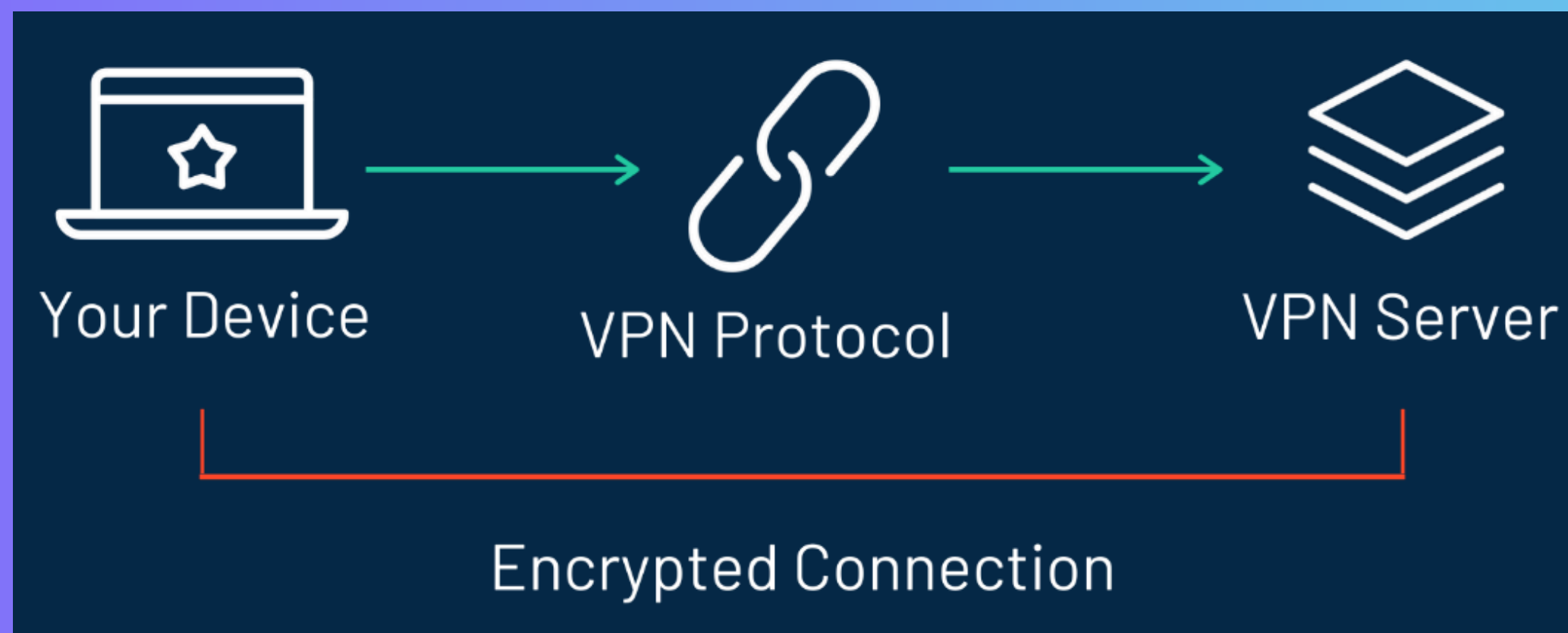
[1] IPsec (Internet Protocol Security) là một bộ giao thức bảo mật mạng IP, cung cấp xác thực, tính toàn vẹn và tính bảo mật cho dữ liệu truyền qua mạng Internet. IPsec sử dụng các giao thức như ESP, AH và IKE để mã hóa, xác thực và trao đổi khóa cho các kết nối bảo mật giữa hai điểm cuối.




REMOTE ACCESS VPN

Virtual Private Network - Mạng riêng ảo từ xa

IKEv2 là giao thức VPN được phát triển bởi Cisco và Microsoft, nổi bật với khả năng kết nối nhanh và ổn định, đặc biệt khi chuyển đổi mạng hoặc khôi phục kết nối sau khi mất internet. IKEv2 sử dụng các thuật toán mã hóa và mã hóa mạnh mẽ như AES, ChaCha20 hoặc Camellia. IKEv2 được hỗ trợ trên một số nền tảng (như iOS, Windows và Blackberry), nhưng không phải trên tất cả (như Android), đòi hỏi phải có ứng dụng bên thứ ba



A decorative graphic consisting of a large blue circle in the center. Two orange lines, one above and one below the circle, extend horizontally from the left and right edges of the frame. Each line has a small orange circle at its end. The lines are slightly offset from the top and bottom edges of the frame.

ƯU ĐIỂM



Ưu điểm

1. Bảo mật dữ liệu

2. Bảo vệ khỏi xâm nhập và tấn công mạng

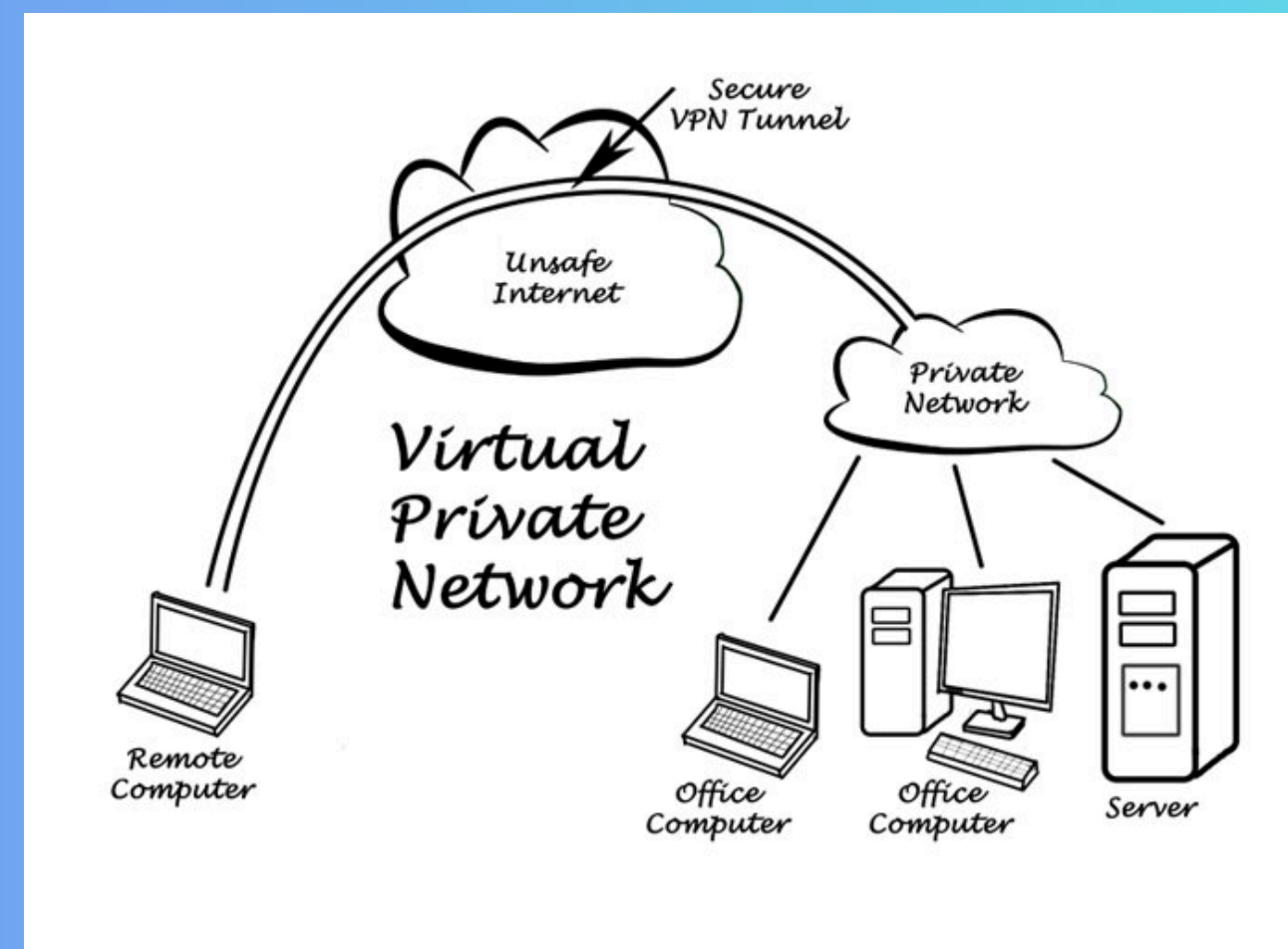
3. Khả năng di động và tăng hiệu suất làm việc.


4. Tiết kiệm chi phí

NGUYÊN LÝ HOẠT ĐỘNG

Nguyên lý hoạt động

- Người dùng sử dụng một phần mềm VPN Client để tạo một kết nối ảo đến VPN Server trên Windows Server.
- VPN Server xác thực người dùng và cấp cho họ một địa chỉ IP thuộc mạng nội bộ.
- VPN Client và VPN Server sử dụng các giao thức đóng gói và mã hóa để truyền dữ liệu qua Internet một cách bảo mật.
- Người dùng có thể truy cập các tài nguyên trên mạng nội bộ như máy tính, máy in, máy chủ, v.v. như thể họ đang ở trong mạng đó.



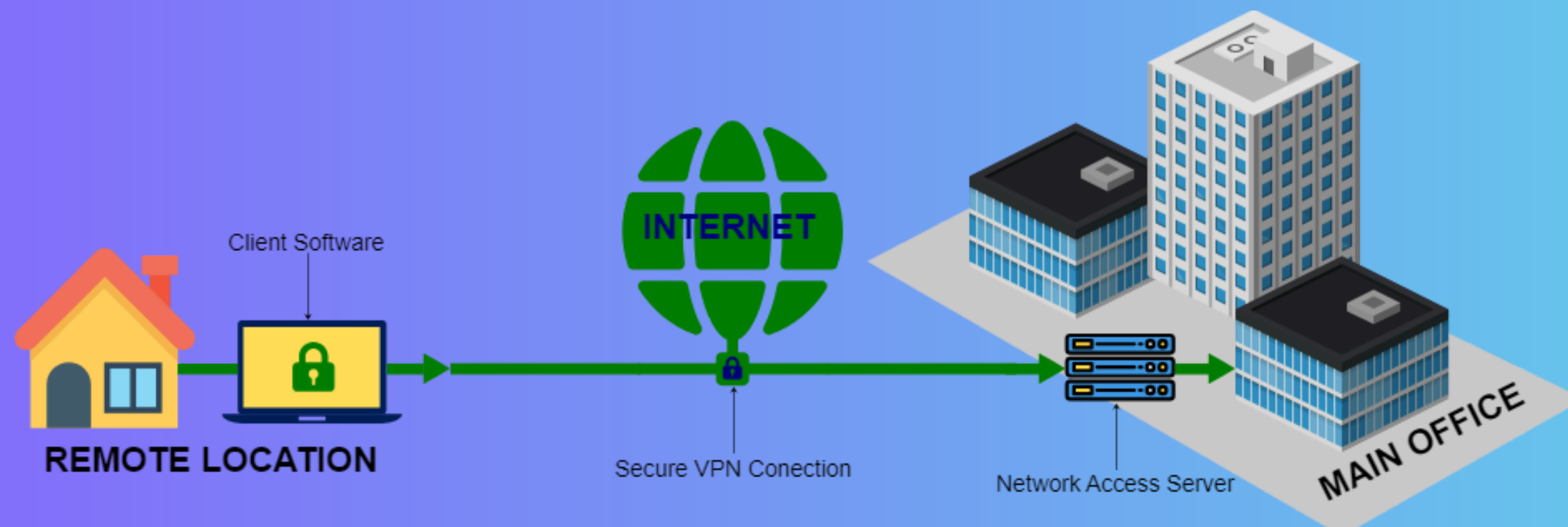


MÔ HÌNH NGŨ CẢNH

Ngữ cảnh

Bạn là một nhân viên làm việc từ chi nhánh của một công ty quốc tế tại Việt Nam. Công ty đã thiết lập một hệ thống VPN để đảm bảo an toàn và bảo mật thông tin quan trọng. Khi bạn cần truy cập dữ liệu từ máy chủ ở trụ sở chính của công ty ở Mỹ, VPN giúp bạn kết nối an toàn và riêng tư.

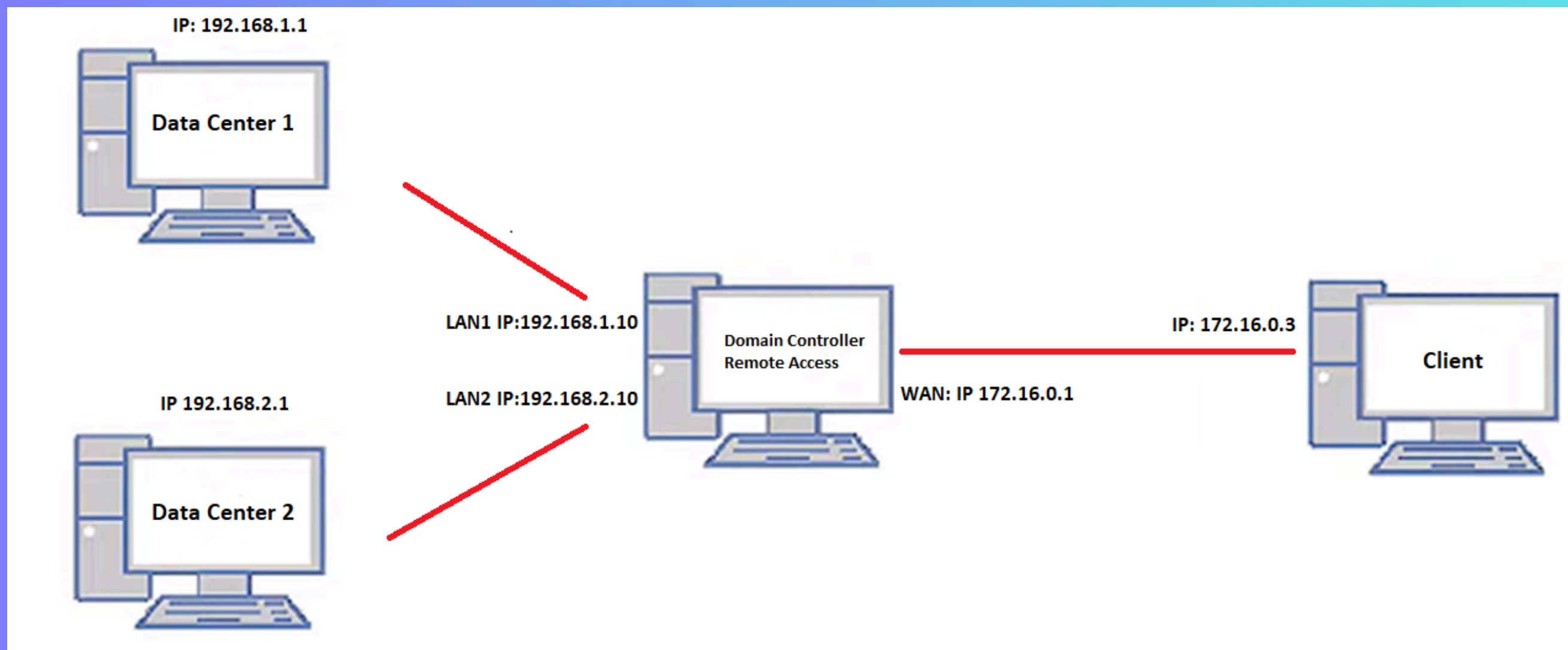
Bằng cách sử dụng VPN, bạn thiết lập một kết nối an toàn và được mã hóa giữa máy tính của bạn tại Việt Nam và máy chủ ở Mỹ. Điều này đảm bảo rằng thông tin của bạn được bảo vệ khỏi các mối đe dọa an ninh mạng. Khi bạn đã kết nối thành công qua VPN, bạn có khả năng truy cập vào tài liệu và tài nguyên trên máy chủ ở Mỹ một cách an toàn. Dựa trên VPN, bạn có thể hoàn thành công việc của mình mà không cần lo lắng về việc thông tin nhạy cảm bị rò rỉ.





Mô hình

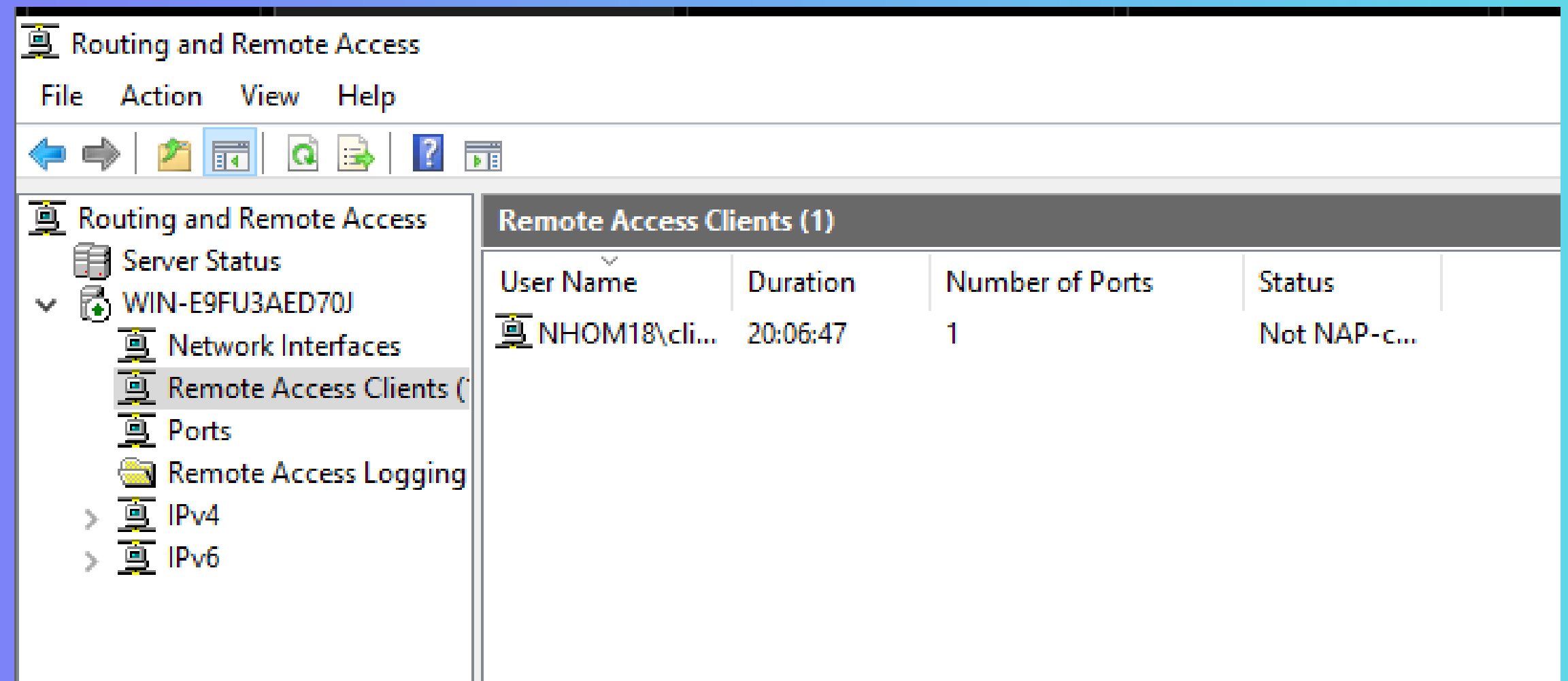
- 1 máy Domain Controller có cài đặt Remote Access quản lý tài nguyên cũng như cho phép client kết nối VPN
- 2 máy lưu dữ liệu sẽ join vào domain để dễ dàng quản lý

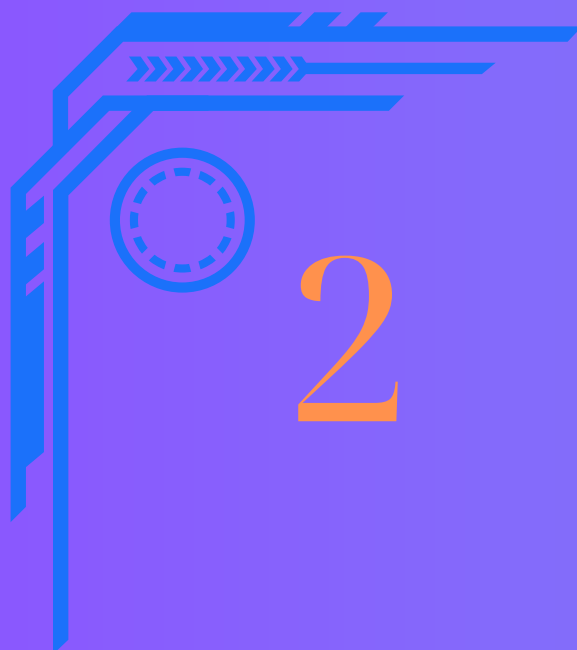


CÁCH CÀI ĐẶT

1

Tiến hành cài đặt dịch vụ Remote Access trên Domain Controller để cung cấp dịch vụ VPN








Tất cả các máy lưu trữ dữ liệu sẽ join vào domain để chia sẻ dữ liệu cũng như quản lý phân quyền các thư mục cho từng đối tượng

PROPERTIES For Datacenter1	
Computer name	Datacenter1
Domain	nhom18.local
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.1.1

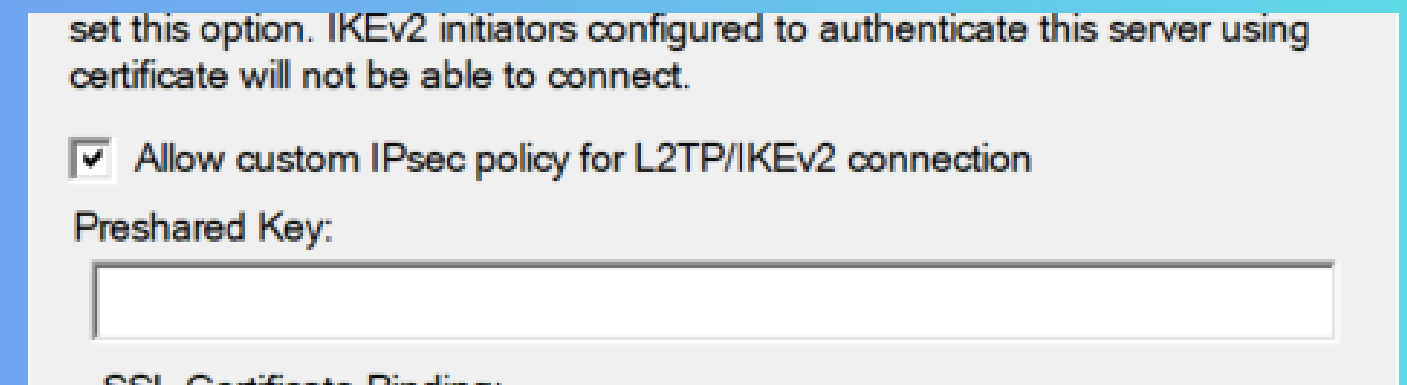
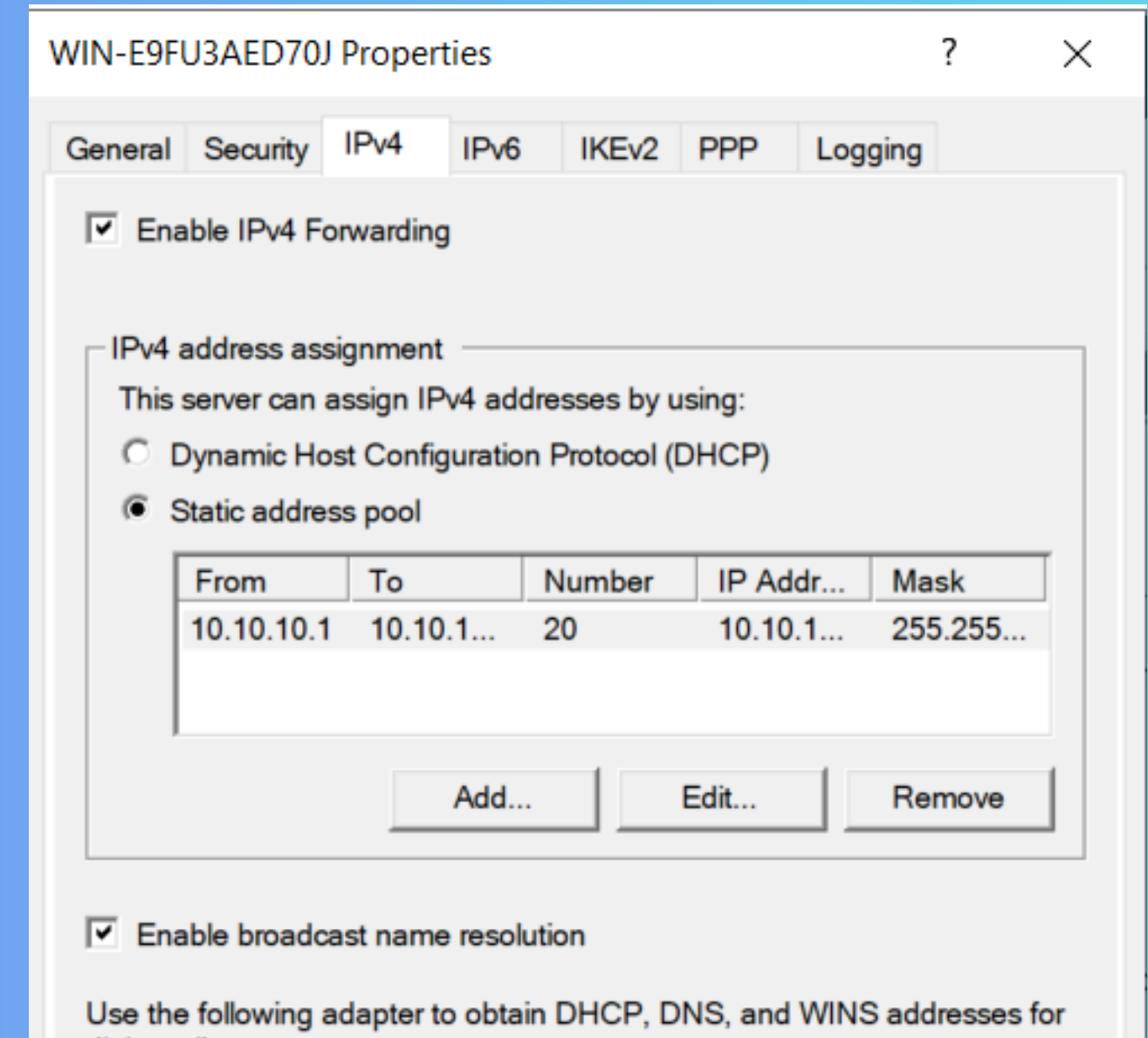
PROPERTIES For Datacenter2	
Computer name	Datacenter2
Domain	nhom18.local
Windows Defender Firewall	Domain: Off
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet0	192.168.2.1

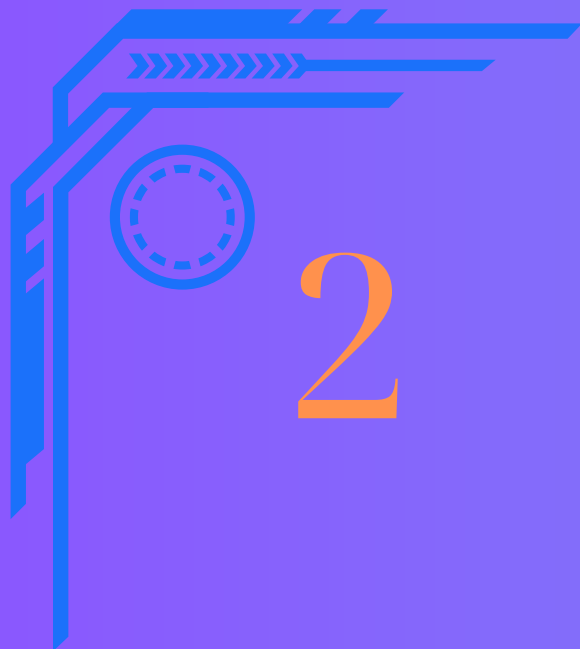
Name	Permission Level
 Administrator	Read/Write ▼
 Administrators	Owner
 NHOM18\client	Read/Write ▼

2

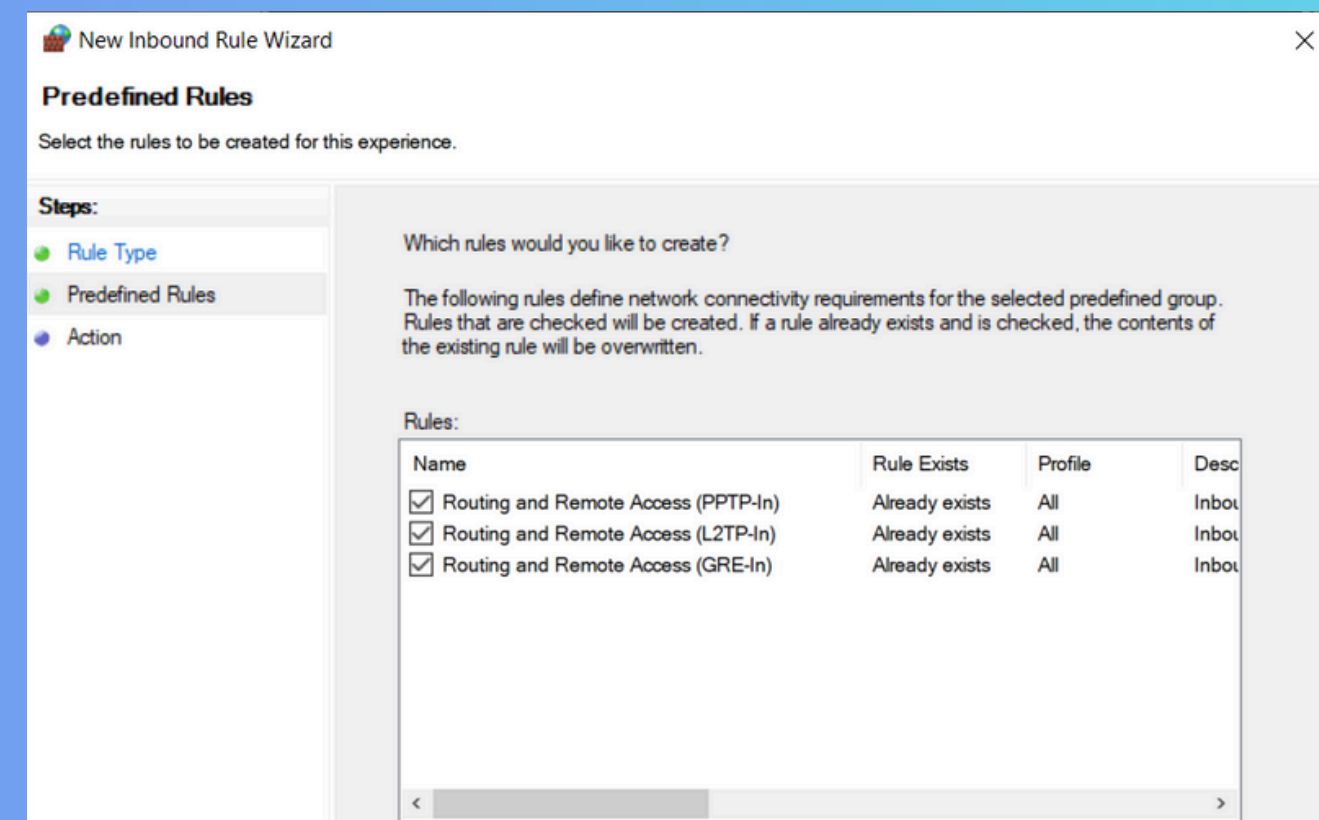
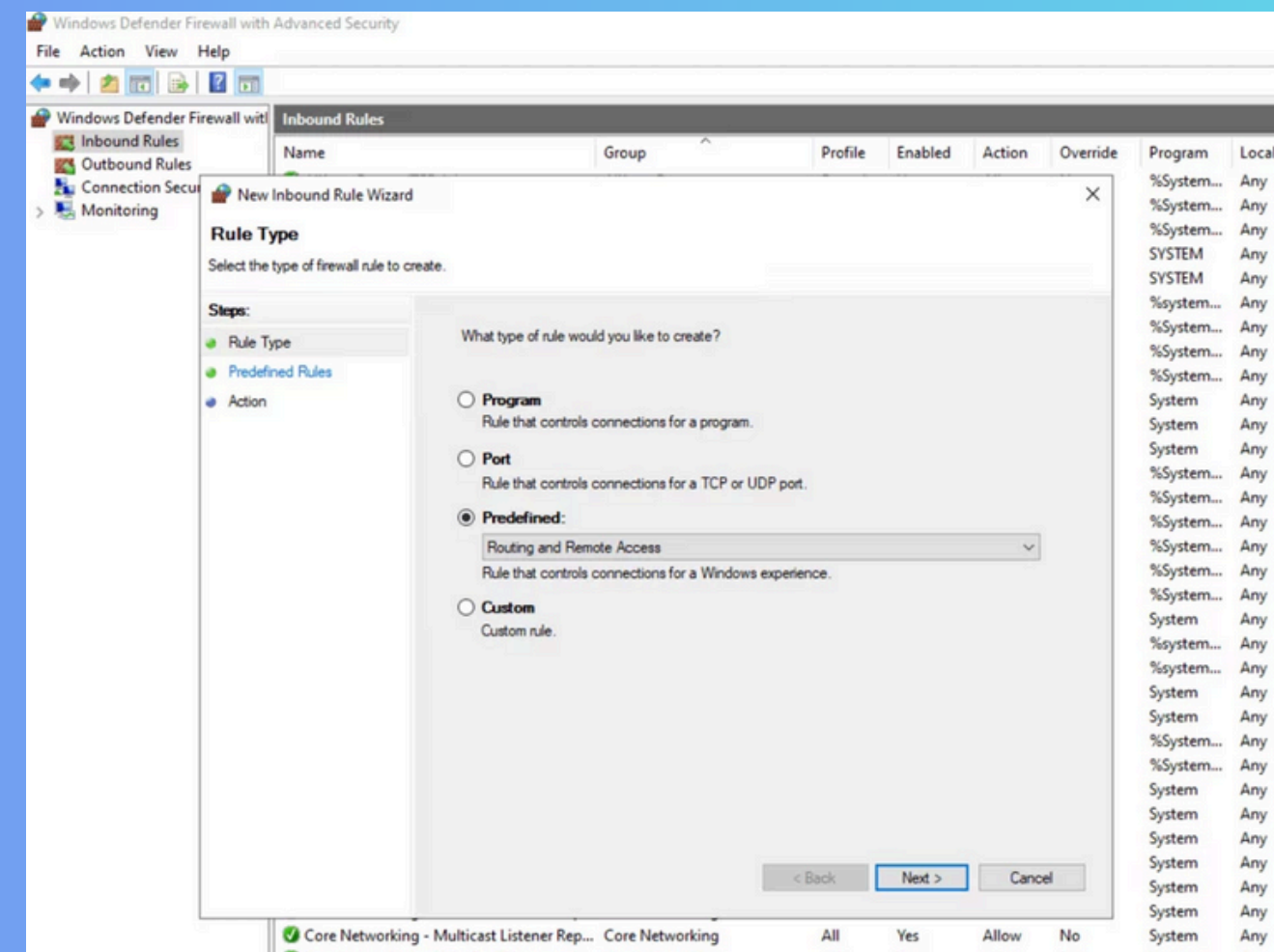
Chúng ta có thể cũng cấp 1 địa chỉ VPN cho user kết nối tới VPN cũng như quản lý được số lượng người có thể kết nối tới VPN

Để an toàn thì chúng ta có thể thêm key để thêm 1 lớp mã hoá cho VPN





Thêm các quy tắc tường lửa để
cho phép máy client có thể kết
nối VPN



3

Ở phía client
chúng ta sẽ nhập
ip mạng Wan của
server cũng như
tài khoản mật
khẩu đã được cấp
bởi server để kết
nối tới VPN đó

Edit VPN connection

These changes will take effect the next time you connect.

Connection name

Server name or address

VPN type

Point to Point Tunneling Protocol (PPTP) ▾

Type of sign-in info

User name and password ▾

User name (optional)

Password (optional)

☒ Remember my sign-in info

Save Cancel

3

Khi truy cập được vào VPN thì sẽ lấy được các tài liệu mà user đăng nhập được cho phép

```
C:\Users\Númmm>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

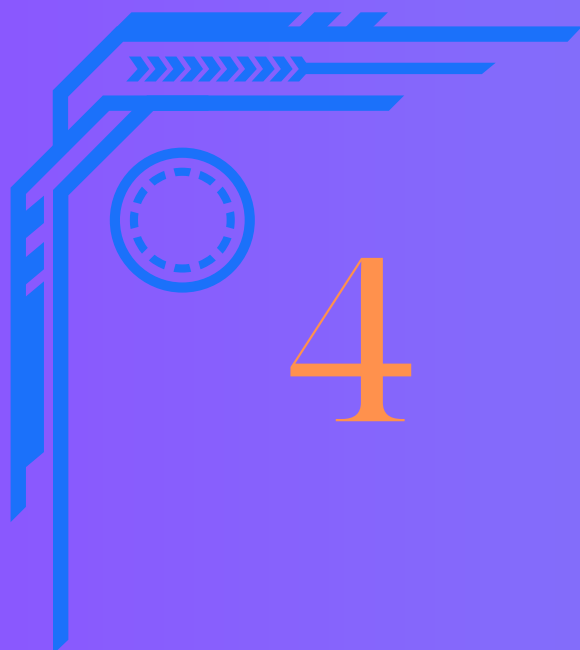
    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::95df:f757:cc6d:9b31%13
    IPv4 Address. . . . . : 172.16.0.3
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : 

PPP adapter VPN1:

    Connection-specific DNS Suffix  . : 
    IPv4 Address. . . . . : 10.10.10.9
    Subnet Mask . . . . . : 255.255.255.255
    Default Gateway . . . . . : 0.0.0.0

C:\Users\Númmm>
```

Home Share view				
Network > 192.168.2.1 > qtm >				
Name		Date modified	Type	Size
NT132.011.ANTT.Nhom18		12/3/2023 12:38 PM	File folder	
Merry Chrissasss		12/3/2023 12:38 PM	Text Document	0 KB



Server sẽ giám sát,
quản lý các client
đã kết nối, ghi nhật
ký hoạt động của
các client

Remote Access Management Console

Configuration
VPN
Web Application Proxy

Dashboard

Operations Status

Remote Client Status

Reporting

WIN-E9FU3AED70J

Remote Access Clients Status

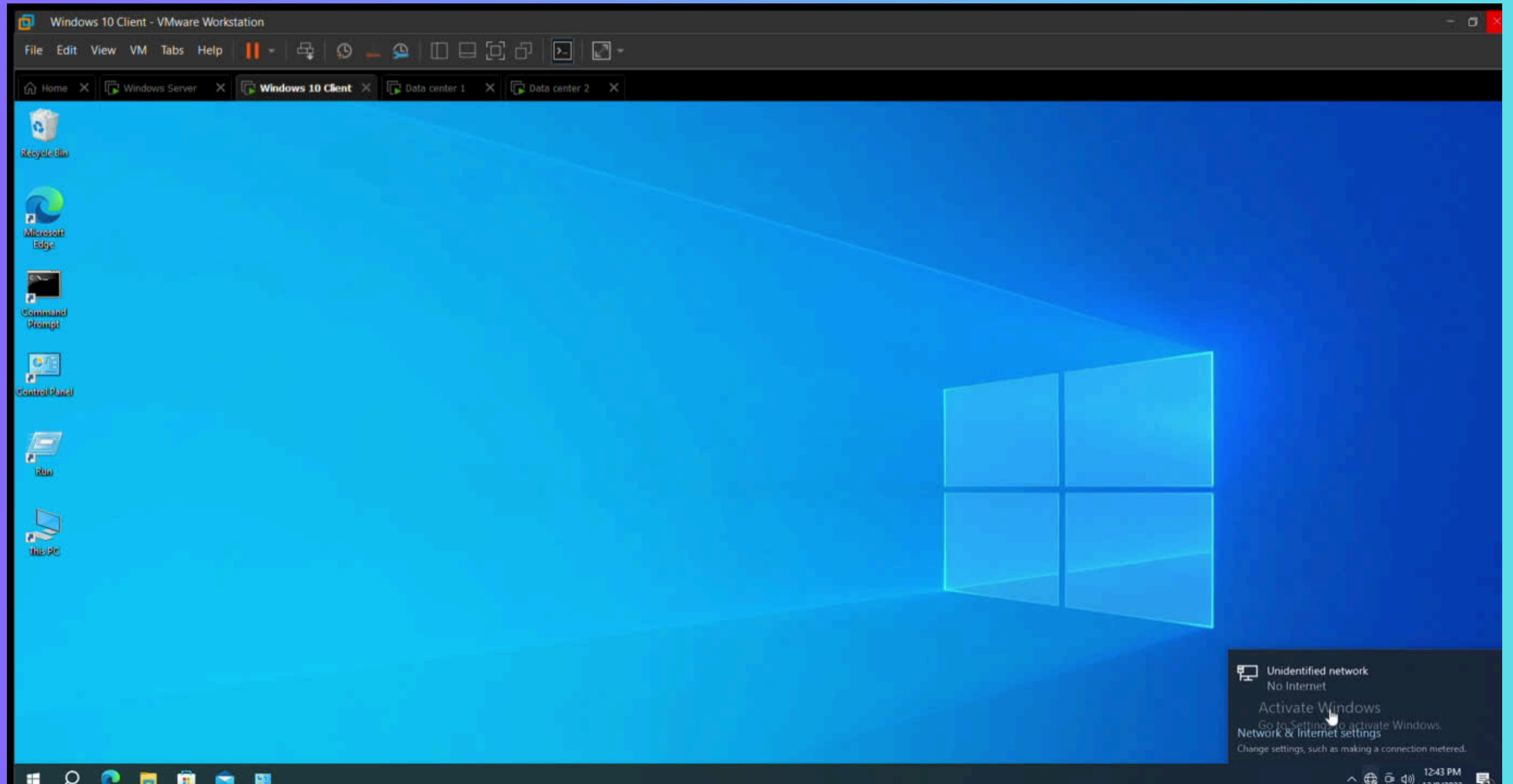
Connected Clients

Search Search

User Name	Host Name	ISP Address	Protocol/Tunnel	Duration
NHOM18\client	-	172.16.0.3	Pptp	20:19:45

4

Video demo



KẾT LUẬN ĐỀ XUẤT



Kết luận

- VPN đóng vai trò quan trọng trong việc bảo mật thông tin, ngăn chặn xâm nhập và tấn công mạng khi truy cập từ xa, đồng thời cải thiện hiệu suất làm việc.
- Việc cài đặt và quản lý VPN trên máy chủ Domain Controller đơn giản và tiện lợi. Chúng em tin rằng VPN sẽ tiếp tục phát triển và được áp dụng rộng rãi trong tương lai để đáp ứng nhu cầu bảo mật thông tin và truy cập an toàn.



Đề xuất trong tương lai

- Tối ưu hóa hiệu suất: Tiếp tục nghiên cứu và áp dụng các phương pháp để tăng cường hiệu suất của VPN trên Windows Server 2019, đảm bảo tốc độ truyền dữ liệu và giảm độ trễ trong quá trình kết nối VPN.
- Tăng cường bảo mật: Tiếp tục nghiên cứu và áp dụng các công nghệ bảo mật mới nhất để đảm bảo tính an toàn và bảo mật của kết nối VPN trên Windows Server 2019
- Mở rộng tính năng: Nghiên cứu và triển khai các tính năng mới như VPN điện toán đám mây (cloud VPN), VPN cho thiết bị di động và ứng dụng VPN trong các môi trường IoT (Internet of Things)
- Quản lý và giám sát: Phát triển các công cụ quản lý và giám sát VPN để dễ dàng quản lý và theo dõi hoạt động của hệ thống VPN trên Windows Server 2019.



**Thanks for
watching!**