



Fortinet Cybersecurity Academy: Configuring an SSL Remote Access VPN on a FortiGate 40-F Firewall

Colin J. Faletto, CCNA

Purpose

This lab is intended to show off the intricate VPN capabilities of the FortiGate-40F firewall by showing off an SSL VPN connection, which is a common type of connection used to provide secure outside access to an internal SOHO network. The lab employs the use of Microsoft's Remote Desktop Protocol (RDP) to show off a common use of an SSL VPN on a SOHO network.

Background

SOHO, short for Small Office/Home Office, is a network type commonly used by individuals or small businesses with less than 10 employees. This network type commonly uses smaller-scale routers, switches, and firewalls compared to their large enterprise counterparts. SOHO networks provide numerous advantages to teams of 1-10 people as they are easier to set up and are more affordable than full-size network equipment. SOHO networks often only have a single router, and may contain switches, wireless access points, and end devices such as computers and printers.

Fortinet is a cybersecurity company founded in 2000 in Sunnyvale, CA. They are known for their flagship product, the FortiGate firewall, as well as a wide variety of other networking and security devices, such as the FortiSwitch and the FortiAP, and services such as FortiSandbox, FortiAuthenticator, FortiVoice, and FortiDDoS. Fortigate is an S&P 500 component and is listed on the NASDAQ as \$FTNT.

The FortiGate 40-F is a firewall developed by Fortinet. It has capabilities expected of a modern firewall such as full routing capability, DHCP server capability, and support for a variety of filtering methods. The 40-F also supports running its own local RADIUS server with a feature called Local Auth (Authentication). The 40-F uses a fanless design, allowing it to operate silently. The 40-F has a small form factor at 1.5 x 8.5 x 6.3 inches, meaning it can easily fit into existing networking setups. By default, the 40-F gives out DHCP addresses in the 192.168.1.0/24 subnet to its clients (from .110-.210, specifically) and its GUI client can be accessed via HTTPS at 192.168.1.99.

Secure Socket Layer, or SSL, is a security protocol developed by Netscape Communications in 1994 that provides security to network connections. The protocol is now deprecated and replaced with Transport Layer Security, or TLS, a protocol developed by the Internet Engineering Task Force (IETF) in 1999. Both protocols are very similar and are often used interchangeably in the networking world. SSL/TLS's most common use case is for the HTTPS (Hypertext Transfer Protocol Secure) protocol, which provides security to HTTP connections over the Internet.

A virtual private network, or a VPN, is a method of creating a secure tunnel between networks. VPNs allow computers that are physically located offsite to be treated the same as computers physically inside of a network. There are two primary types of VPNs: remote access (RAVPN) and site-to-site, which create private tunnels for individual computers and entire networks respectively. In the business world, VPNs are often used to allow employees working from home to access company resources

located on internal servers. VPN services are commonly sold commercially, allowing consumers to connect to private network-sharing servers. These servers are often located in multiple countries or regions, enabling consumers to spoof their location and hide network traffic from their ISP.

Remote Desktop Protocol, or RDP, is a Microsoft-proprietary protocol that allows a user to remotely view and control a connected Windows PC. RDP employs a client/server model, with the client being included on all versions of Windows and the server being exclusive to the operating system's higher tiers. RDP uses port 3389 with both TCP and UDP. RDP was introduced during Microsoft's transition from MS-DOS to the NT kernel with Windows NT 4.0 Terminal Services Edition, and the server has been included on every version of Windows (other than Home) since XP.

FortiClient is a Fortinet Fabric Agent, which is a program that runs on an external host device and provides secure communication with the Fortinet Security Fabric. The full version of FortiClient provides a wide variety of security services, such as Zero Trust Network Access (ZTNA), content filtering, cloud-based application security, and telemetry information. FortiClient also offers a lighter VPN-only version for users that don't need advanced security services.

Lab Summary

In this lab, we created an SSL VPN connection to allow connections from the internet into computers on the internal network. The firewall assigns IP addresses from 192.168.2.1-192.168.2.254 to VPN clients internally and allows traffic from the VPN interface to reach both the LAN and WAN interfaces. We created a test VPN user to allow secure authentication into the network and used a remote desktop connection to a computer on the internal network to test the VPN connection.

Lab Commands

From the dashboard, open the command-line interface.



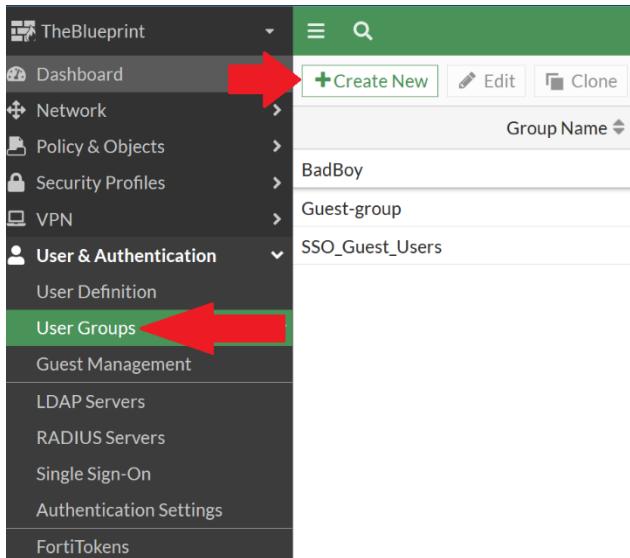
Type the following commands:

```
config system settings  
    set gui-sslvpn enable  
end
```

Reload the page.



Go to User & Authentication > User Groups and click Create New.



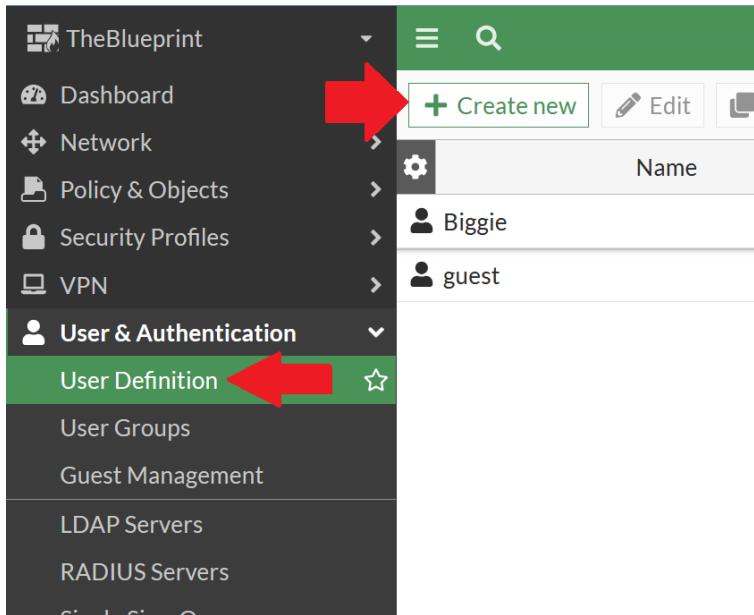
Name the group and set the type to Firewall.

This is a screenshot of a 'Create New User Group' dialog box. It has three fields: 'Name' (containing 'VPN Group'), 'Type' (set to 'Firewall', which is highlighted with a red arrow), and 'Members' (empty). The 'Type' field has a dropdown menu showing 'Fortinet Single Sign-On (FSSO)', 'RADIUS Single Sign-On (RSSO)', and 'Guest'.

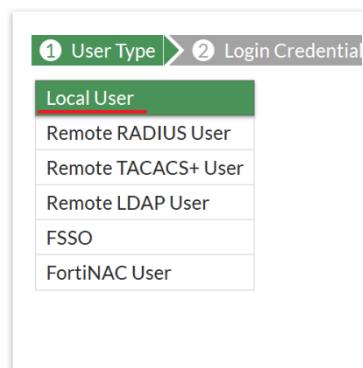
Click OK.



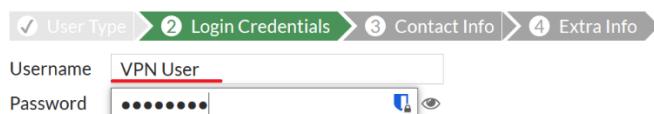
Go to User & Authentication > User Definition and click Create New.



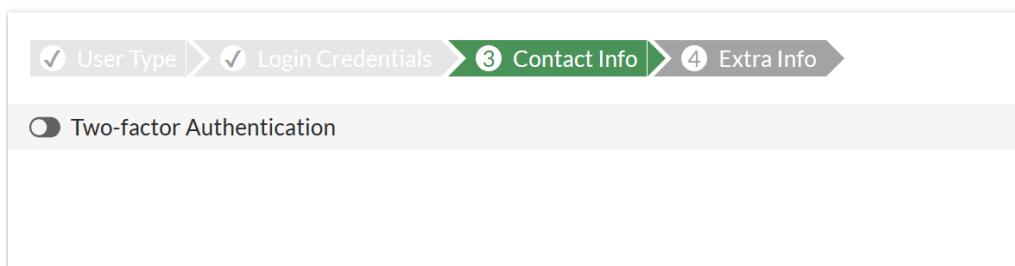
Select Local User and click Next.



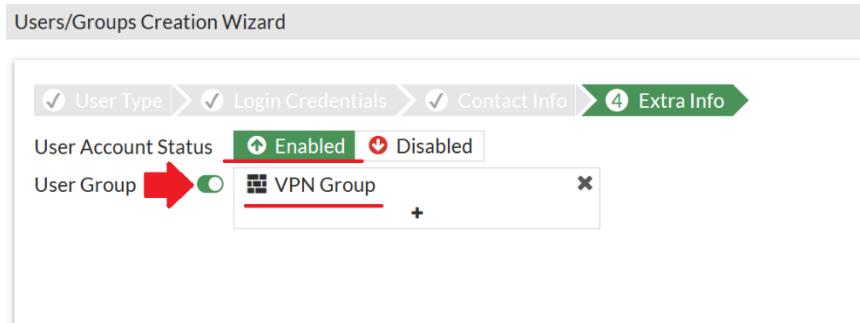
Enter an appropriate username and password for your VPN user, then click Next.



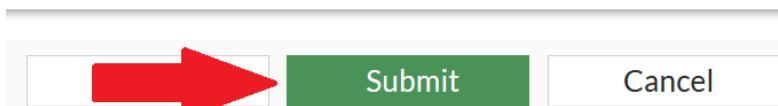
Turn on two-factor authentication if desired and click Next.



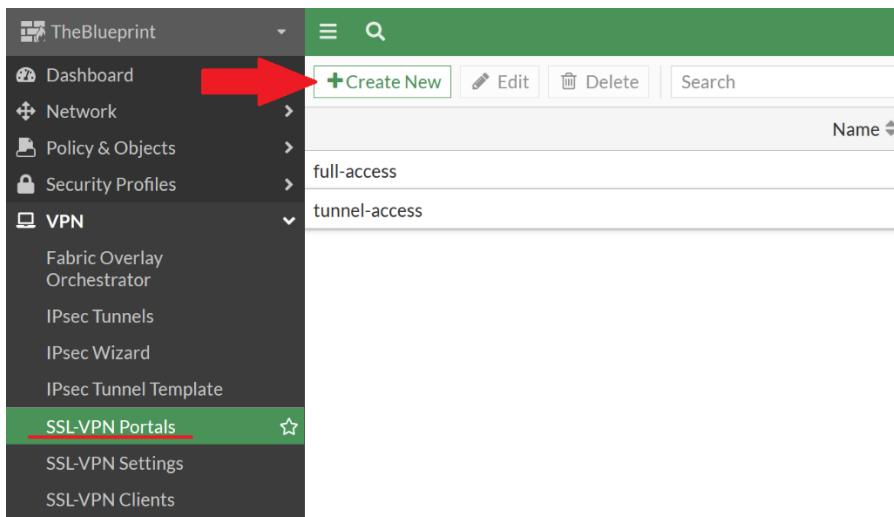
Ensure the account is enabled, enable the user group, and select the group you created earlier.



Click Submit.



Go to VPN > SSL-VPN Portals and click Create New.



Name the VPN portal, turn on tunnel mode, and disable split tunneling.



Click on Source IP Pools and click Create.

New SSL-VPN Portal

Name: chad-full-tunnel-portal

Limit Users to One SSL-VPN Connection at a Time:

Tunnel Mode: Tunnel Mode

Split tunneling:

- Disabled: All client traffic will be directed over the SSL-VPN tunnel.
- Enabled Based on Policy Destination: Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.
- Enabled for Trusted Destinations: Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

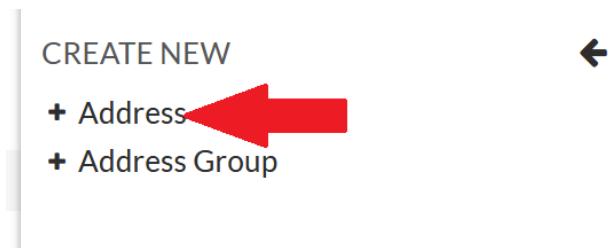
Source IP Pools: + This field is required.

Select Entries

+ Create

- ADDRESS (6)
 - 2-PAC address
 - BIG address
 - Chad_range
 - Ian
 - SSLVPN_TUNNEL_ADDR1
 - VPN Subnet
- ADDRESS GROUP (1)

Click Address.



Name the range, set the type to IP range, and configure an appropriate range of IP addresses for VPN clients.

New Address

Name: Chad Range

Color:

Interface: any

Type: IP Range

IP Range: 192.168.2.2-192.168.2.254

Comments: Write a comment... 0/255

Ensure the range you created is selected, turn on FortiClient Download, then click OK.

New SSL-VPN Portal

Name

Limit Users to One SSL-VPN Connection at a Time

Tunnel Mode

Split tunneling **Disabled**
All client traffic will be directed over the SSL-VPN tunnel.

Enabled Based on Policy Destination
Only client traffic in which the destination matches the destination of the configured firewall policies will be directed over the SSL-VPN tunnel.

Enabled for Trusted Destinations
Only client traffic which does not match explicitly trusted destinations will be directed over the SSL-VPN tunnel.

Source IP Pools

Tunnel Mode Client Options

Allow client to save password

Allow client to connect automatically

Allow client to keep connections alive

DNS Split Tunneling

Host Check

Restrict to Specific OS Versions

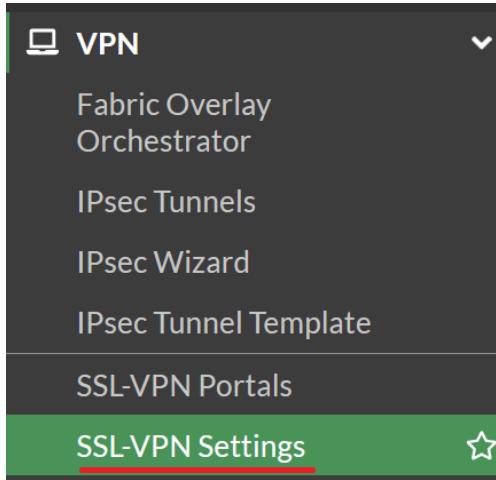
FortiClient Download

Download Method Direct SSL-VPN Proxy

Customize Download Location



Go to VPN > SSL-VPN Settings.



Under server certificate, click create.

Server Certificate

Redirect HTTP to SSL-VPN

Restrict Access

Negate Source

A screenshot of the FortiGate configuration interface. On the left, there are several configuration options with checkboxes: 'Server Certificate' (unchecked), 'Redirect HTTP to SSL-VPN' (checked), 'Restrict Access' (checked), and 'Negate Source' (checked). To the right is a search bar with the placeholder 'Search' and a red arrow pointing to a 'Create' button. Below the search bar is a list of certificates: 'Fortinet_Factory' and 'Fortinet_Factory_Backup'. A vertical scroll bar is visible on the right side of the list.

Click Generate Certificate.

Generate New Certificate

FortiGate can generate a certificate using our self-signed CA: [Fortinet_CA_SSL](#).
Using a server certificate from a trusted CA is strongly recommended.

[Generate Certificate](#)

Name the certificate accordingly and click Create.

The screenshot shows the 'Generate New Certificate' dialog. It includes fields for 'Certificate authority' (set to 'Fortinet_CA_SSL'), 'Certificate name' (containing 'FORTINET-SSL-CERT'), 'Common name' (containing '192.168.40.57'), and 'Subject alternative name' (empty). A note below the common name field states: 'The common name should match the FQDN or IP of the primary SSL-VPN interface.' At the bottom, there is a 'Create' button and a 'Back' button. A large red arrow points to the 'Create' button.

Ensure the VPN is listening on the WAN interface on port 10443 using the certificate you created. Turn on Redirect HTTP to SSL-VPN and turn off Idle Logout.

Connection Settings ⓘ

Listen on Interface(s)	wan	x
Listen on Port	10443	▼
Server Certificate	FORTINET-SSL-CERT	▼
Redirect HTTP to SSL-VPN	On	
Restrict Access	Allow access from any host	Limit access to specific hosts
Negate Source	Off	
Idle Logout	On	
Require Client Certificate	Off	

Tunnel Mode Client Settings ⓘ

Under Authentication/Portal Mapping, click on All Other Users/Groups.

Authentication/Portal Mapping ⓘ

The legacy SSL-VPN web mode feature is
will not be accessible in portals.

+ Create New Edit Delete

Users/Groups

All Other Users/Groups

Set the portal to tunnel-access.

Edit Default Authentication/Portal Mapping

Users/Groups All Other Users/Groups

Portal tunnel-access ▼

Click Create New.

The legacy SSL-VPN web mode feature is no longer supported. This feature will not be accessible in portals.

+ Create New

Delete

Users/Groups

All Other Users/Groups

Set the group to the VPN group you created and set the portal to the tunnel you created.

New Authentication/Portal Mapping

Users/Groups: VPN Group

Portal: chad-full-tunnel-portal

Click Apply.

Apply

Go to Policy & Objects > Firewall Policy.

Policy & Objects

Firewall Policy

Click Create New.

+ Create new

Give the policy an appropriate name, set the incoming interface to the SSL-VPN tunnel interface, the outgoing interface to LAN, the source address to all, the source user

group to the VPN group, the destination to all, the schedule to always, the service to all, and the action to accept.

Create New Policy

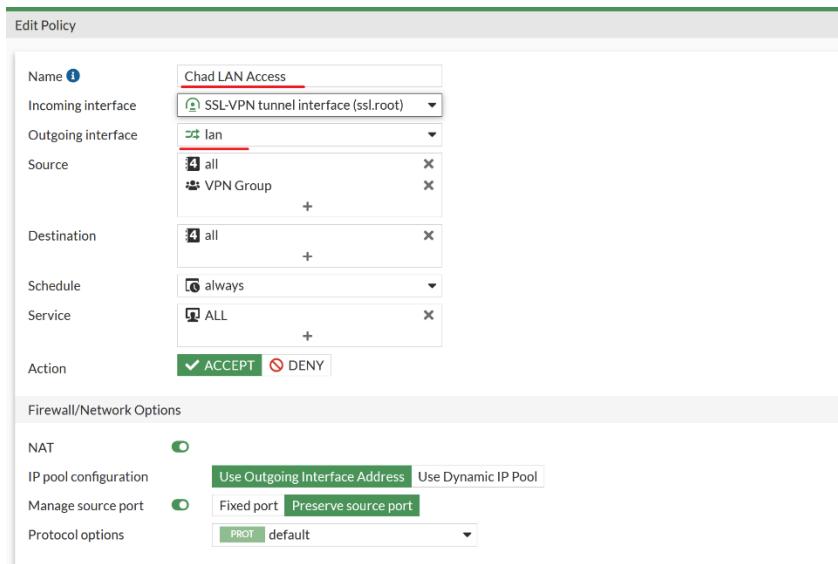
Name	chad-access
Incoming interface	SSL-VPN tunnel interface (ssl.root)
Outgoing interface	wan
Source	{4} all VPN Group
Destination	{4} all
Schedule	always
Service	ALL
Action	<input checked="" type="button"/> ACCEPT <input type="button"/> DENY

(Note: for the source, you will have to select options from two different columns using the dropdown at the top. Select all from the Address column and VPN Group from the User column.)

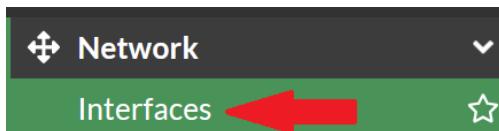
Select Entries

Address	all
User	VPN Group
Internet Service	ne.com
Selected	2
Recently Used	5
gmail.com	
wildcard.google.com	
wildcard.dropbox.com	
* {4} all	
{4} FIREWALL_AUTH_PORTAL_ADDRESS	

Create another firewall policy that's identical except for the outgoing interface being the LAN interface.



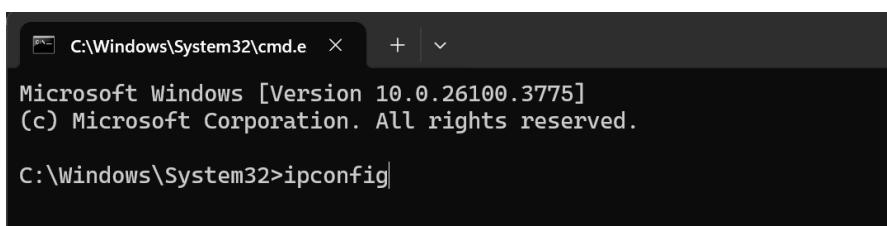
Go to Network > Interfaces.



Note down the IP address of the WAN interface. You will need this later.



On your inside PC, open command prompt and run the command ipconfig.



Note down the IP address; you will need this later.

```
Command Prompt

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 192.168.1.111
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.1.99

Ethernet adapter Ethernet 5:
  Connection-specific DNS Suffix . :
  IPv4 Address . . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 1:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 10:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Wi-Fi:
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :
```

On your outside PC, download the FortiClient VPN-only client from <https://www.fortinet.com/support/product-downloads>.

You may have to enter some personal information to download the client. Click Download Now to download.

FortiClient VPN-only

Please complete the form below to download and get additional information on FortiClient

Jeffrey	Mason
Newport Cisco	jeffrey@cisco.nation
United States	<input type="button" value="▼"/>

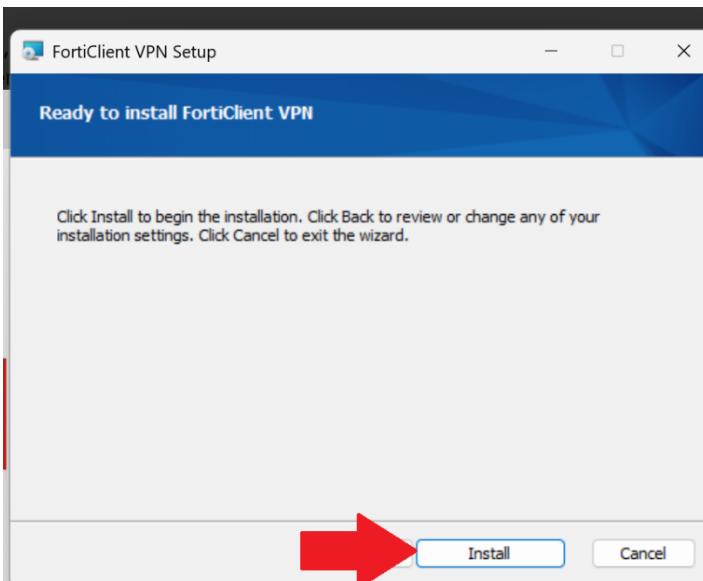
Click the downloaded .exe file.



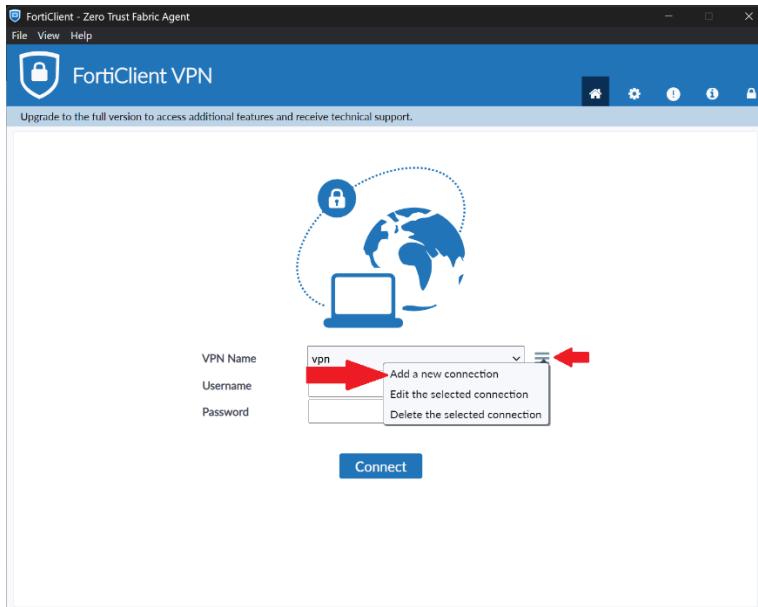
Read and accept the license agreement, then click Next.



Click Install.



Open the FortiClient window and click on the hamburger menu. Click Add a new connection.



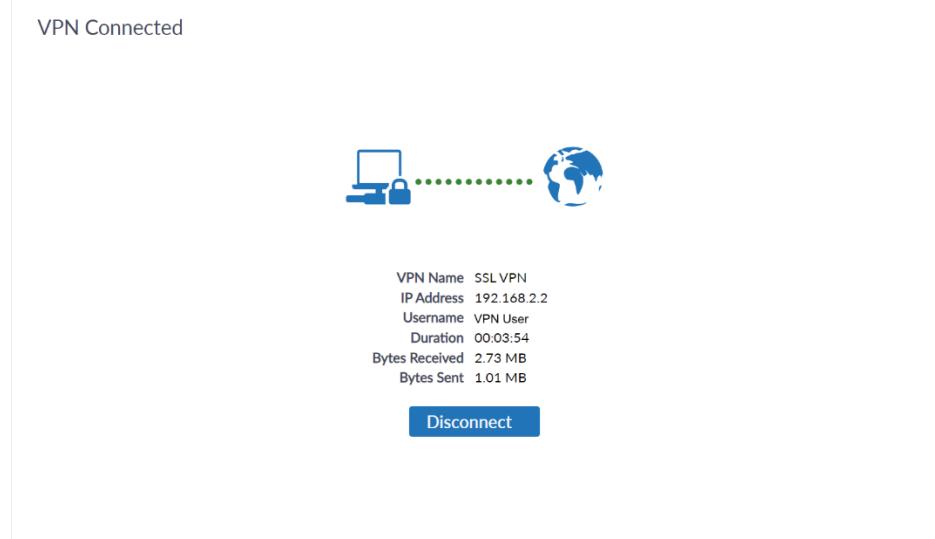
Set the VPN type to SSL-VPN. Configure an appropriate connection name and description. Configure the remote gateway as the IP address of the firewall's WAN interface that you found earlier. Ensure that the port is set to 10443 as configured earlier. Turn on Save Login and set the username to VPN User. Click Save.

A screenshot of the "New VPN Connection" dialog box. The tab "SSL-VPN" is selected. The "Connection Name" field contains "SSL VPN". The "Description" field contains "SSL". The "Remote Gateway" field contains "192.168.40.57". The "Customize port" checkbox is checked, and the port number "10443" is entered in the adjacent field. Under "Single Sign On Settings", the "Save login" radio button is selected. The "Username" field contains "VPN User". The "Client Certificate" dropdown is set to "None". At the bottom are "Cancel" and "Save" buttons, with "Save" highlighted by a red arrow.

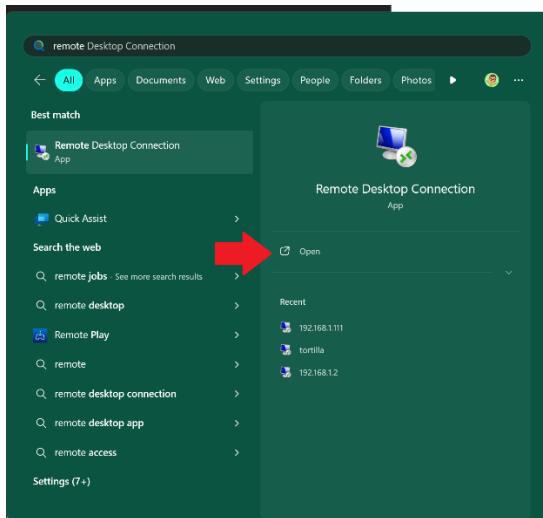
Select your VPN profile, type in the VPN User's username and password, and click connect.



If the VPN connects successfully, you should see a screen like this:



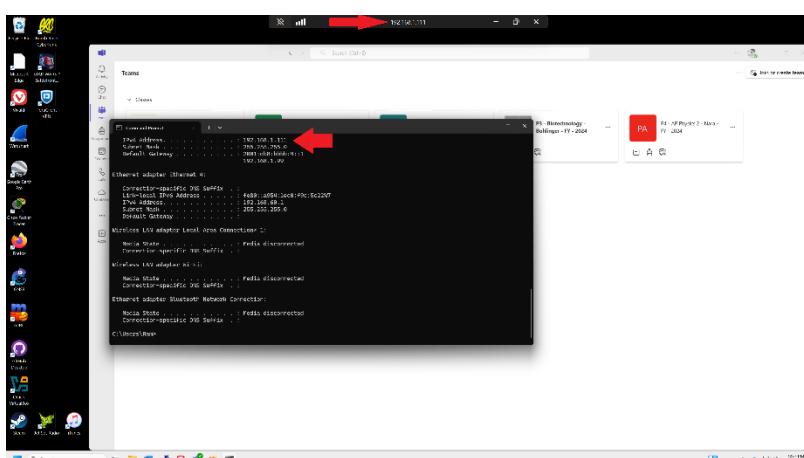
To test if the connection works, open the Remote Desktop Connection app.



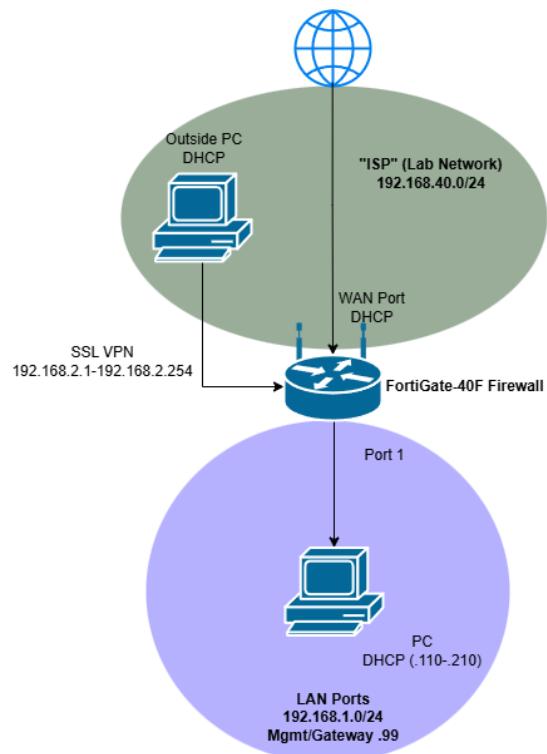
Enter the IP address of the inside computer and click Connect.



Here's a screenshot of the remote desktop connection from the outside PC to the inside PC, with the IP address of the inside PC visible:



Network Diagram (IPv4)



Problems

We originally tried to complete this lab with an IPSec VPN. For some reason, the IPSec VPN refused to work for anyone in our lab, so we decided to complete the lab with an SSL VPN instead.

Conclusion

To wrap up, while it's bizarre that this lab didn't work with IPSec, I was still very impressed with the ease of use that the Fortinet interface provides for setting up an SSL VPN. I am fully confident that I could set up this VPN configuration outside of a lab environment, especially with the refreshing change of pace from other firewall configuration interfaces.