Fortigate 40F Firewall IPSec VPN Configuration

Andrew Pai

Period 5 Cybersecurity

Purpose:

The purpose of this lab was to have our group configure our Fortigate 40F firewall with an IPSec VPN. This will allow a PC within our firewall's network to remotely access another PC that's on a different firewall's network. This requires two different groups and firewalls for this lab as well as skills with the Fortigate GUI and RDP.

Background Information:

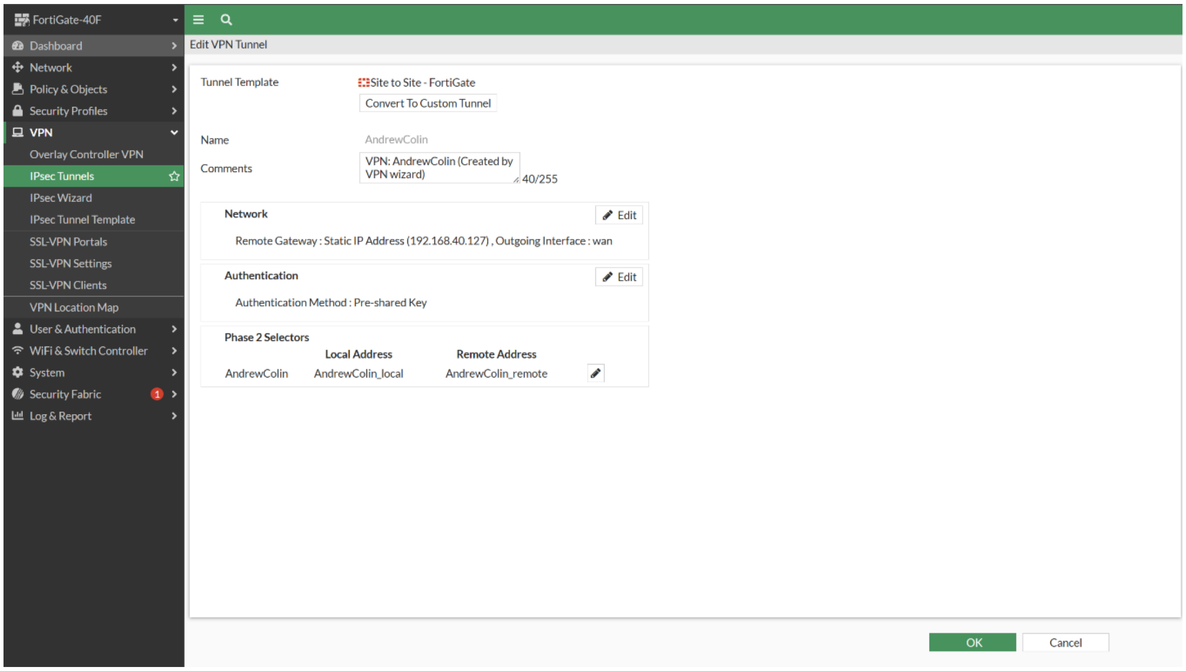
This lab focuses on implementing an IPSec VPN on our Fortigate 40F firewall. As has been covered in both our previous Global Protect VPN and our SSL VPN labs, VPNs stand for Virtual Private Networks. VPNs are used to remotely connect into a network from a device that isn't physically on that network. For companies and corporations this is a large help for people that want to work from home or are on a trip abroad. For the regular person, VPNs are useful to get past location restrictions on a certain site or to get past Internet censorship. VPNs are also just in general helpful to ensure that data is encrypted and secure compared to data that isn't transferred with a VPN.

The VPN that we'll be configuring on the Fortigate firewall in this lab uses the IPSec protocol, also known as Internet Protocol Security. IPSec is used for site to site VPNs, meaning that data goes from one firewall to another firewall, hence the need for two firewalls and groups in this lab. Compared to SSL VPNs, IPSec VPNs operate at the network layer whereas SSL VPNs operate at the transport layer. IPSec VPNs can work in either tunnel or transport mode, where tunnel mode is encryption of all data including packet headers, and tunnel is encryption of just the data payload. The main 2 protocols used by IPSec to authenticate its data is the Authentication Header and Encapsulating Security Protocols (AH and ESP). AH is used for authentication while ESP is used to encrypt data.

To connect to a PC on the other firewall, our group will be using Microsoft's Remote Desktop Protocol which is a Microsoft proprietary protocol meant for remote access. It uses a client-server architecture where the remote computer being accessed is the server and the user's device is the client. With a port of 3389, RDP essentially allows the user of a desktop to login and control the screen of another desktop while being able to access resources on a private network that it's not actually on.

Lab Summary:

To start configuring your IPSec VPN, navigate to the Fortigate's "IPSec Wizard" section under the VPN section of the left taskbar. Create a new Custom IPSec Tunnel with a proper name, the IP address of your other firewall, and the networks of both firewalls.



Edit VPN Tunnel

Tunnel Template: Site to Site - FortiGate

Convert To Custom Tunnel

Name: AndrewColin

Comments: VPN: AndrewColin (Created by VPN wizard) 40/255

Network

Remote Gateway : Static IP Address (192.168.40.127) , Outgoing Interface : wan

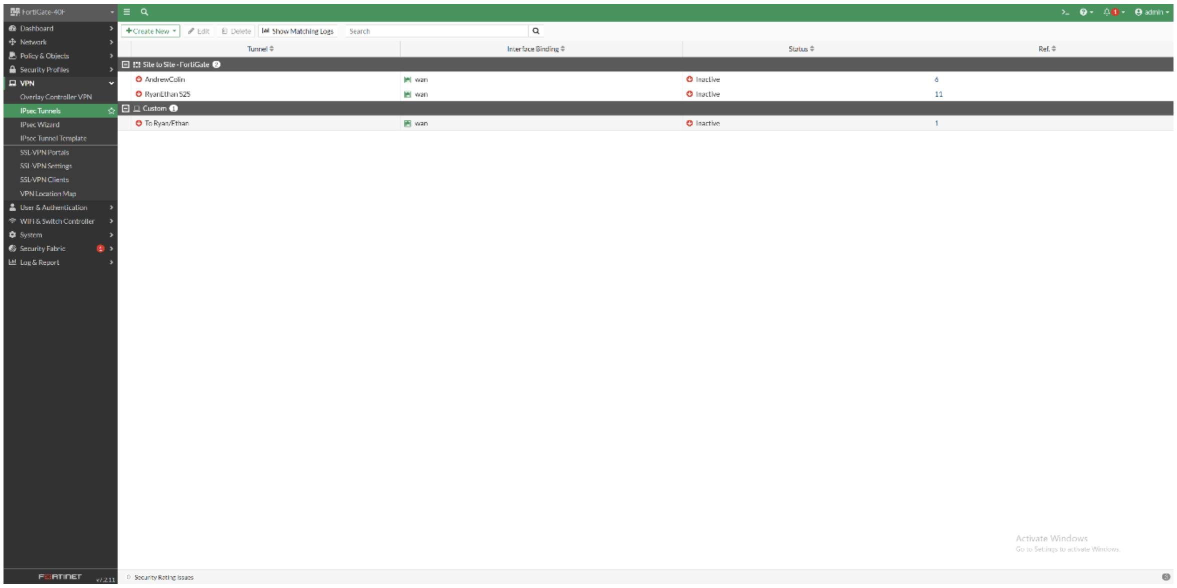
Authentication

Authentication Method : Pre-shared Key

Phase 2 Selectors

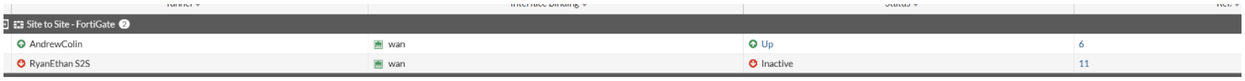
	Local Address	Remote Address
AndrewColin	AndrewColin_local	AndrewColin_remote

Now in IPSec Tunnels, your tunnel should show up with the proper name as "Inactive."



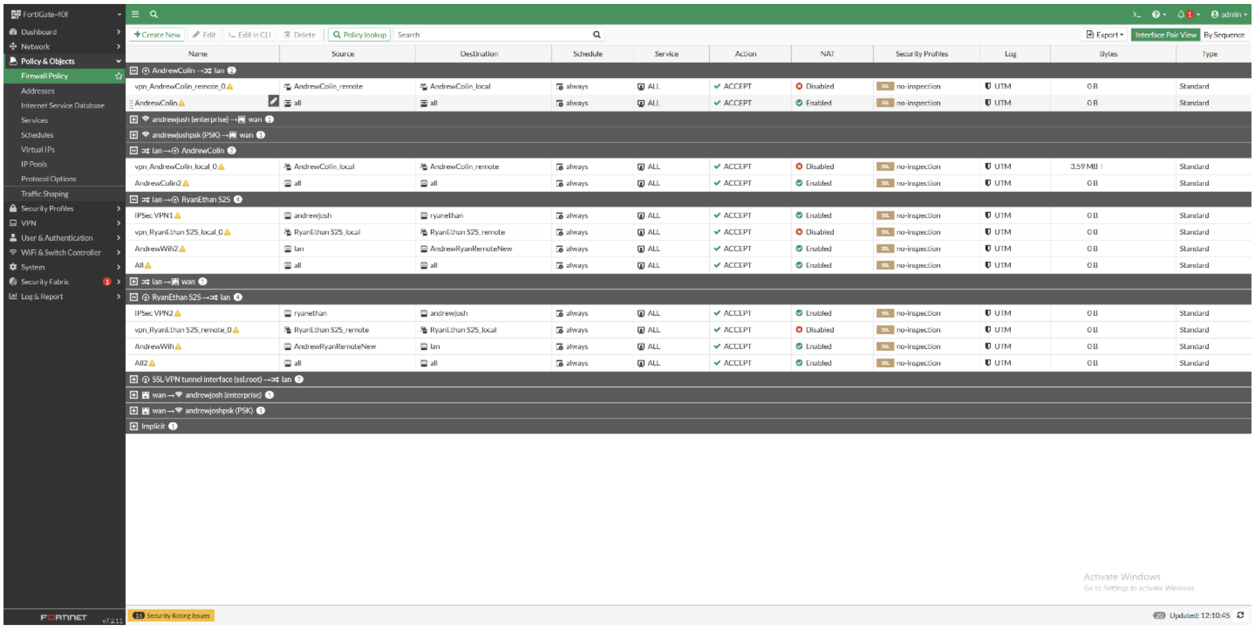
Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 2			
AndrewColin	wan	Inactive	6
RyanEthan S25	wan	Inactive	11
Custom 1			
To Ryan/Ethan	wan	Inactive	1

Configure a similar VPN tunnel on your opposite firewall but with reversed destination and source networks, as well as a different remote IP. Once both tunnels are done, click on one of the tunnels and select the “bring up” option. This will cause your tunnel to come up and be active.



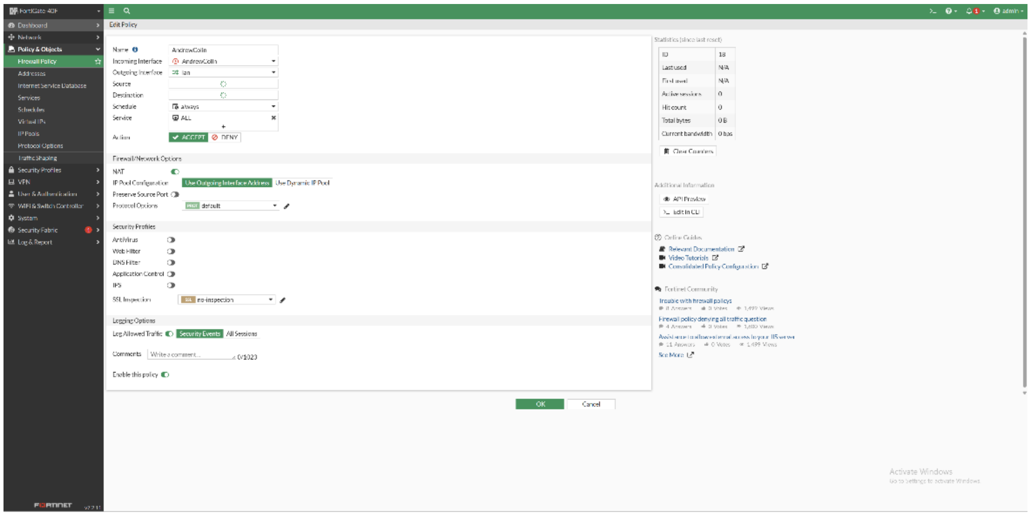
Tunnel	Interface Binding	Status	Ref.
Site to Site - FortiGate 2			
AndrewColin	wan	Up	6
RyanEthan S2S	wan	Inactive	11

Navigate to the Firewall Policy section under “Policy and Objects” on the left taskbar.



Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
AndrewColin → lan 2										
vpn_AndrewColin_remote_0	AndrewColin_remote	AndrewColin_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B	Standard
AndrewColin	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
andrewjosh (enterprise) → wan 1										
andrewjoshpsk (PSK) → wan 1										
lan → AndrewColin 2										
vpn_AndrewColin_local_0	AndrewColin_local	AndrewColin_remote	always	ALL	ACCEPT	Disabled	no-inspection	UTM	3.59 MB	Standard
AndrewColin2	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
lan → RyanEthan S2S 4										
IPSec VPN1	andrewjosh	ryanethan	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
vpn_RyanEthan S2S_local_0	RyanEthan S2S_local	RyanEthan S2S_remote	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B	Standard
AndrewWifi2	lan	AndrewRyanRemoteNew	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
All	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
lan → wan 1										
RyanEthan S2S → lan 4										
IPSec VPN2	ryanethan	andrewjosh	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
vpn_RyanEthan S2S_remote_0	RyanEthan S2S_remote	RyanEthan S2S_local	always	ALL	ACCEPT	Disabled	no-inspection	UTM	0 B	Standard
AndrewWifi	AndrewRyanRemoteNew	lan	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
All2	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B	Standard
SSL-VPN tunnel interface (ssl.root) → lan 2										
wan → andrewjosh (enterprise) 1										
wan → andrewjoshpsk (PSK) 1										
Implicit 1										

Create a new policy with the VPN Tunnel as the incoming interface, LAN as your outgoing interface, and add in the proper user groups that you want to be able to use the VPN for.



Edit Policy

Name: AndrewColin
Incoming Interface: AndrewColin
Outgoing Interface: lan
Source:
Destination:
Schedule: always
Service: ALL
Action: [✓ ACCEPT] DENY

Firewall/Network Options
NAT: ●
IP Pool Configuration: [✓ Use Outgoing Interface Address] Use Dynamic IP Pool
Preserve Source Port: ○
Protocol Options: PROT default

Security Profiles
AntiVirus: ○
Web Filter: ○
DNS Filter: ○
Application Control: ○
IPS: ○
SSL Inspection: SSL no-inspection

Logging Options
Log Allowed Traffic: ● [✓ Security Events] All Sessions

Comments: Write a comment... 0/1023

Enable this policy: ●

Statistics (since last reset)

ID	18
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

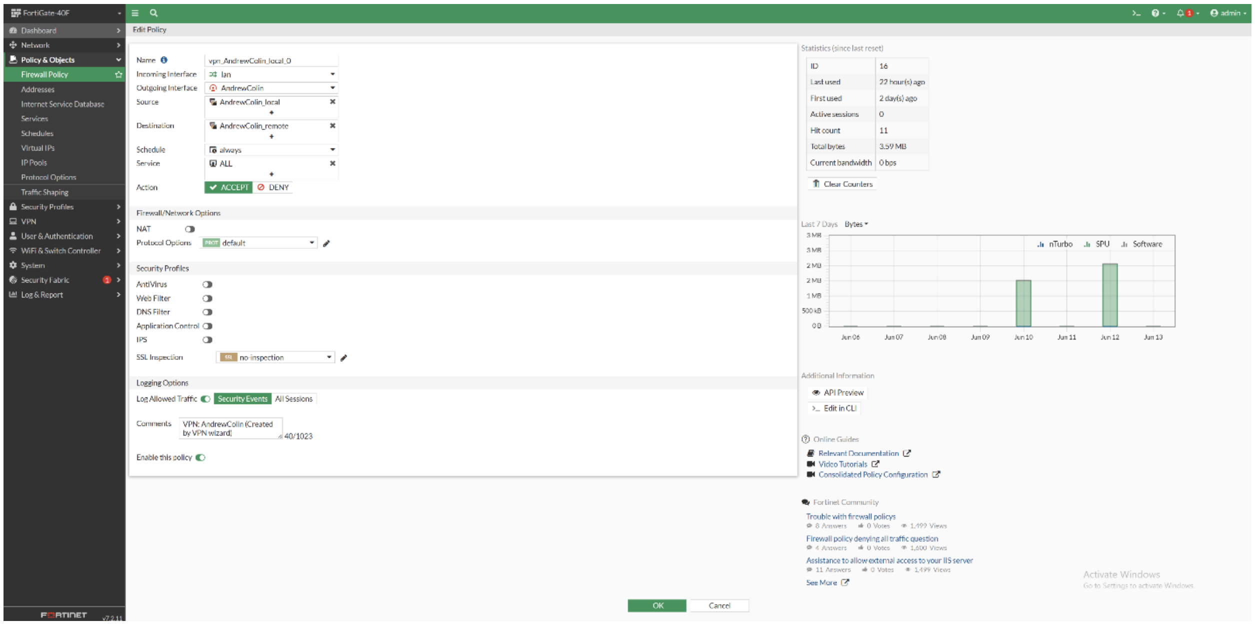
Additional Information

Online Guides
- Relevant Documentation
- Video Tutorials
- Consolidated Policy Configuration

Fortinet Community
- Trouble with firewall policys — 8 Answers, 0 Votes, 1,492 Views
- Firewall policy denying all traffic question — 4 Answers, 0 Votes, 1,600 Views
- Assistance to allow external access to your IIS server — 11 Answers, 0 Votes, 1,499 Views

See More

Create another similar firewall policy, but the interfaces are reversed and the destination / source networks are reversed.



Edit Policy

Name	vpn_AndrewColin_local_0
Incoming Interface	lan
Outgoing Interface	AndrewColin
Source	AndrewColin_local
Destination	AndrewColin_remote
Schedule	always
Service	ALL
Action	✓ ACCEPT ⊘ DENY

Firewall/Network Options

NAT ○
Protocol Options: PROT default

Security Profiles

AntiVirus ○
Web Filter ○
DNS Filter ○
Application Control ○
IPS ○
SSL Inspection: SSL no-inspection

Logging Options

Log Allowed Traffic ● Security Events | All Sessions

Comments: VPN: AndrewColin (Created by VPN wizard) 40/1023

Enable this policy ●

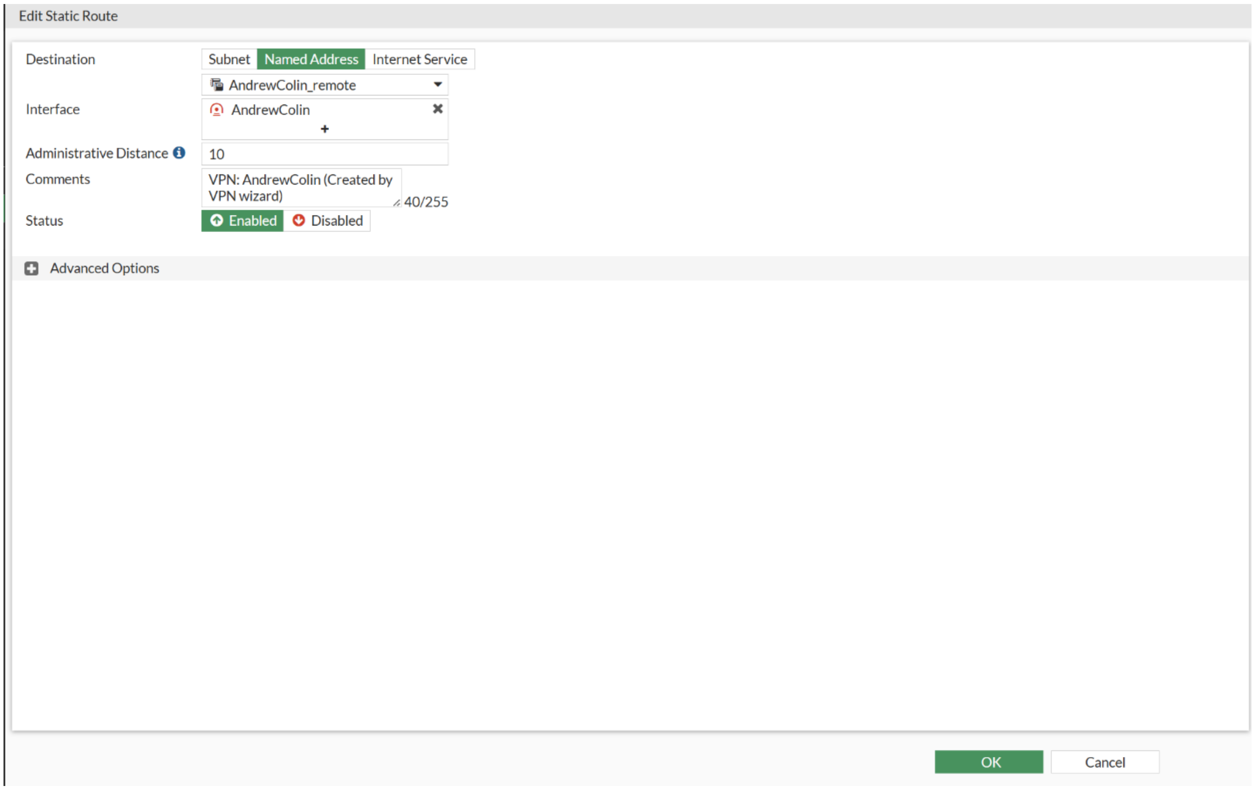
Statistics (since last reset)

ID	16
Last used	22 hour(s) ago
First used	2 day(s) ago
Active sessions	0
Hit count	11
Total bytes	3.59 MB
Current bandwidth	0 bps

Clear Counters

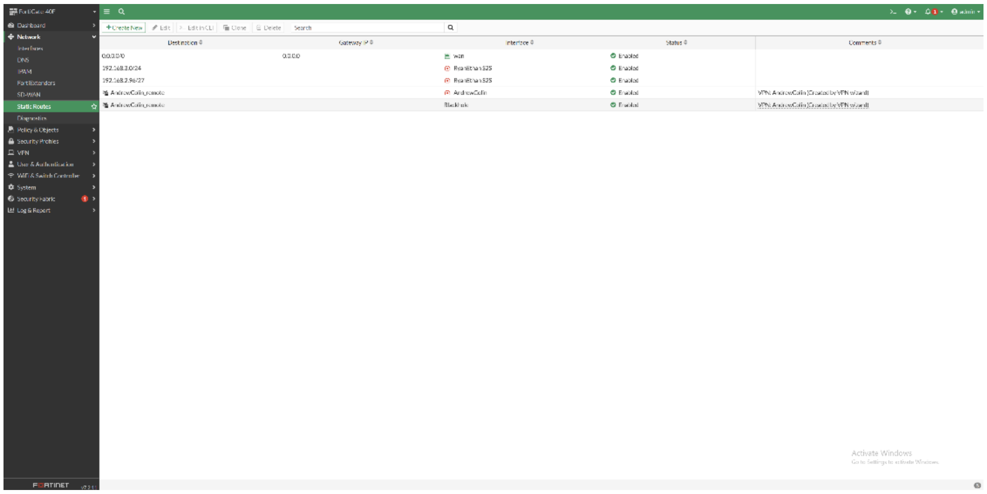
Last 7 Days Bytes

Navigate to Static Routes under the Network section on the left taskbar. Add in a static route that points any traffic going to your other firewall's network towards the VPN tunnel you configured.



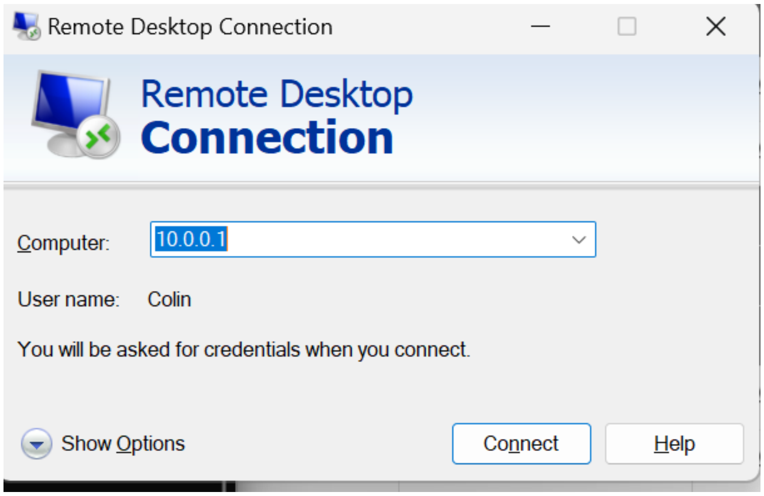
Edit Static Route

Destination	Subnet | Named Address | Internet Service AndrewColin_remote
Interface	AndrewColin
Administrative Distance	10
Comments	VPN: AndrewColin (Created by VPN wizard) 40/255
Status	Enabled | Disabled



Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	0.0.0.0	wan	Enabled	
192.168.3.0/24		RyanEthan525	Enabled	
192.168.2.96/27		RyanEthan525	Enabled	
AndrewColin_remote		AndrewColin	Enabled	VPN: AndrewColin (Created by VPN wizard)
AndrewColin_remote		Blackhole	Enabled	VPN: AndrewColin (Created by VPN wizard)

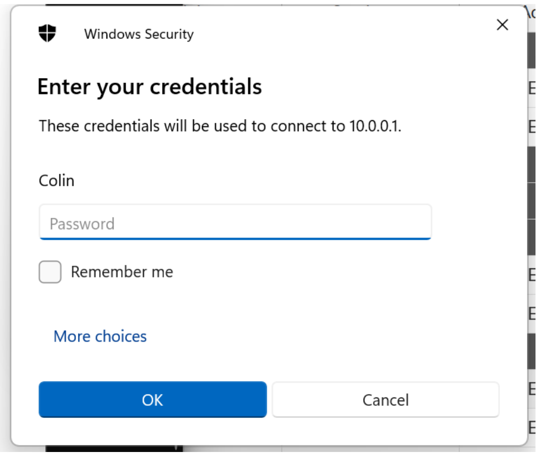
Exit out of the firewall’s GUI and open RDP on your device. Type in the IP address of the computer you’re trying to access on the other firewall’s network and enter user credentials.



Computer: 10.0.0.1

User name: Colin

You will be asked for credentials when you connect.



Enter your credentials

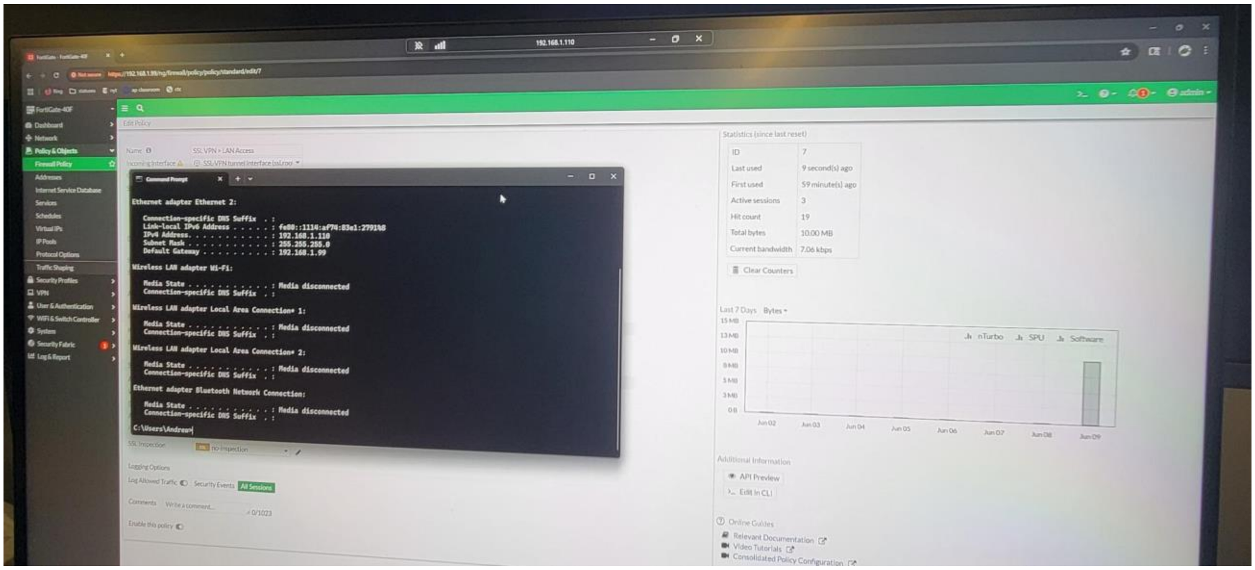
These credentials will be used to connect to 10.0.0.1.

Colin

Password

□ Remember me

Once you enter your credentials, you should be able to access the other computer through RDP.



https://192.168.1.99/ng/firewall/policy/policy/standard/edit/7

Edit Policy

Name: SSL VPN > LAN Access

Incoming Interface: SSL-VPN tunnel interface (ssl.root)

```
Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1114:af74:83e1:2791%8
   IPv4 Address. . . . . . . . . . . : 192.168.1.110
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.99

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Andrew>
```

SSL Inspection: no-inspection

Logging Options

Log Allowed Traffic: Security Events | All Sessions

Comments: Write a comment... 0/1023

Enable this policy

Statistics (since last reset)

ID	7
Last used	9 second(s) ago
First used	59 minute(s) ago
Active sessions	3
Hit count	19
Total bytes	10.00 MB
Current bandwidth	7.06 kbps

Problems:

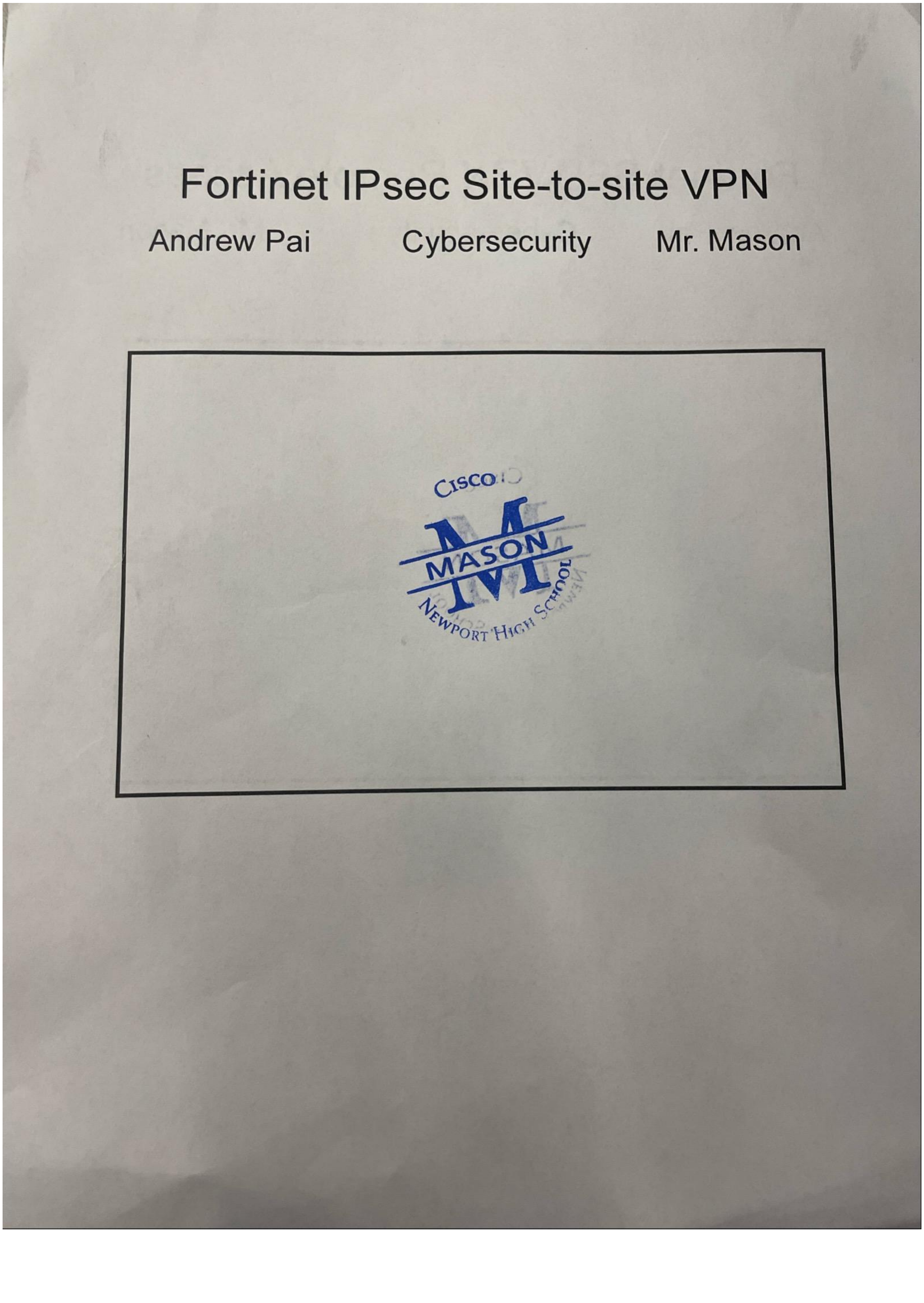
One of the problems that our group had was that our VPN wasn't working with Ryan and Ethan's group's firewall. Despite being able to ping each other's firewalls, our PCs couldn't ping each other even if we allowed all traffic through. This meant that the VPN couldn't work. To solve this, I set up site to site with Colin's firewall instead.

We also had the same problem as last lab where we forgot to DHCP our PC and had a static IP, meaning no default gateway. We caught it much earlier on this time around though, leading to us simply setting our PC's IP to be from a DHCP server and working.

Conclusion:

In conclusion, this lab has familiarized our group with creating and setting up an IPSec VPN. We gained skills relating to how to set up firewall policies on the Fortigate, how to create IPSec VPN Tunnels on the Fortigate using the VPN Wizard, how to set up static routes, and how to successfully use RDP for site to site VPNs.

Lab Signoff:



Fortinet IPsec Site-to-site VPN

Andrew Pai Cybersecurity Mr. Mason

CISCO

M

MASON

NEWPORT HIGH SCHOOL