



# Portfolio of labs in Cybersecurity

A collection of labs done within CISCO cybersecurity course using Palo Alto PA-220 and Fortigate-40F firewalls.

Jeffrey Yiu Cheung

## **Contents**

<b>Factory resetting a Palo Alto firewalls .....</b>	4
<b>Purpose .....</b>	5
<b>Background information.....</b>	5
<b>Lab summary.....</b>	5
<b>Problems .....</b>	8
<b>Conclusion .....</b>	8
<b>Setting a PA-220 as a SOHO router.....</b>	9
<b>Purpose .....</b>	10
<b>Background information.....</b>	10
<b>Lab summary.....</b>	10
<b>Problems .....</b>	22
<b>Conclusion .....</b>	23
<b>Setting up URL filter for K-12 students .....</b>	24
<b>Purpose .....</b>	25
<b>Background information.....</b>	25
<b>Lab summary.....</b>	26
<b>Problems .....</b>	29
<b>Conclusion .....</b>	29
<b>Setting up GlobalProtect VPN and Remote Desktop .....</b>	30
<b>Purpose .....</b>	31
<b>Background information.....</b>	31
<b>Lab summary.....</b>	32
<b>Problems .....</b>	55
<b>Conclusion .....</b>	56
<b>Setting a Fortinet Firewall as a SOHO router .....</b>	58
<b>Purpose .....</b>	59
<b>Background information.....</b>	59
<b>Lab summary.....</b>	60

<b>Problems</b> .....	70
<b>Conclusion</b> .....	70
<b>Setting up remote access with Fortigate-40F</b> .....	71
<b>Purpose</b> .....	72
<b>Background information</b> .....	72
<b>Lab summary</b> .....	73
<b>Problems</b> .....	87
<b>Conclusion</b> .....	87
<b>Setting up Site to Site VPN and Remote Access with Fortigate-40F</b> .....	88
<b>Purpose</b> .....	89
<b>Background information</b> .....	89
<b>Lab summary</b> .....	90
<b>Problems</b> .....	105
<b>Conclusion</b> .....	106



# Palo-Alto Pa-220

Factory resetting a Palo Alto firewalls



Palo Alto  
PA-220 Enterprise  
Hardware + Lizenz

Jeffrey Yiu Cheung

## **Purpose**

This lab helps us understand the steps necessary to perform a factory reset on a Palo Alto Pa-220 firewall.

## **Background information**

A factory reset is a function that erases and resets all configuration to original factory settings. When encountering a device that is already pre-configured, a factory reset allows us to still use a device that is already set with a password and start from a clean environment.

Palo Alto is a networking company that offers cybersecurity with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for 11<sup>th</sup> straight years. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day. ‘

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Palo Alto offers cybersecurity devices and programs like firewalls malware prevention programs.

The Palo Alto Pa-220 is a small firewall device designed to support small organizations and offices with many features that optimize networking and security. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior, and having many functions that blocks known threats. The raise in Cyber Attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

## **Lab summary**

Connect the console cable between the Palo Alto Pa-220 and the host computer to begin. To enter the “Maint” mode, we power cycled our device. After the reboot, this should be what it

looks like:

```
DRAM: 8 GiB
Clearing DRAM..... done
Octeon MMC/SD0: 0
Using default environment

MMC: Octeon MMC/SD0: 0, Octeon MMC/SD0: 0
Net: octeth0, octeth1, octeth2, octeth3, octeth4, octeth5, octeth6, octeth7,
octrgmii0 [PRIME]
Type the command 'usb start' to scan for USB storage devices.
```

```
Autoboot to default partition in 5 seconds.
Enter 'maint' to boot to maint partition.
```

Entry: maint

Booting to maint mode.

There is a short time frame when you have to type “maint” to get to the maintenance mode, where there is an option for factory reset.

This should be what it looks like after successfully entering maintenance mode:

```
Welcome to maintenance mode. For support please contact Palo Alto
Networks.
```

```
866-898-9087 or support@paloaltonetworks.com
```

```
< Continue
>
```

```
< Maintenance Entry Reason
< Get System Info >
< Factory Reset >
< Set FIPS-CC Mode >
< FSCK (Disk Check) >
< Log Files >
< Bootloader Recovery >
< Disk Image >
< Select Running Config >
< Content Rollback >
< Set IP Address >
< Diagnostics >
< Debug Reboot >
< Reboot >
```

Upon selecting Factory Reset, another menu comes up. Continue with the factory reset by selecting factory reset:

```
Using Image:
(X) panos-9.1.4
```

```
[ ] Scrub

If scrubbing, select scrub type:
(X) nnsa           ( ) dod
```

```
< Factory Reset
>
< Advanced >
```

After you continue to factory reset, it should show a progress bar. Now all we have to do is wait.



When it is done the option to reboot is available. After the reboot the device is clean and can be configured.

```
Factory Reset Status: Success

< Back
< Reboot
>
Bootstrapping [plugin ] into partition "panrepo"
```

## Problems

This lab was straightforward and did not have many issues, however, it did come at a risk of completely destroying the Palo Alto device, and one should always be careful when choosing options in the maintenance menu. Another problem was that this process is very time consuming, taking about 20 to 30 minutes to complete a reboot.

## Conclusion

This lab is straightforward but also necessary. The factory reset function will come up many times, besides cybersecurity. The steps to perform a factory reset on a Palo Alto Pa-22, you first reboot the firewall, enter maintenance mode, select factory reset twice, then wait. After the wait is over, reboot to find a clean device.



# Palo-Alto PA-220

Setting a PA-220 as a SOHO router



Palo Alto  
**PA-220 Enterprise**  
Hardware + Lizenz

## **Jeffrey Yiu Cheung**

### **Purpose**

This lab teaches a way to set up the Palo-Alto PA220 as a SOHO router for small offices and business.

### **Background information**

SOHO router, aka Small Office/Home Office router is designed to support small businesses or small offices, which is a perfect for the Palo Alto PA220 firewall's specifications. They are stronger than home routers, but weaker than enterprise routers. They are designed to have functions like firewall, VPN, security features tailored for needs of a small office, and great performance under load. They are usually the only point of entry and exit in a network, which makes features like security a necessity.

In the modern age, most modern offices are in large buildings requiring bigger networks, however, small office/home office routers can still benefit many, such as professions like lawyers, consultants, writers, IT workers, etc. Enterprise routers are designed to support bigger networks, redundancy, and scalability.

Palo Alto is a networking company that offers cybersecurity with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for the 11<sup>th</sup> straight year. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Palo Alto offers cybersecurity devices and programs like firewalls malware prevention programs.

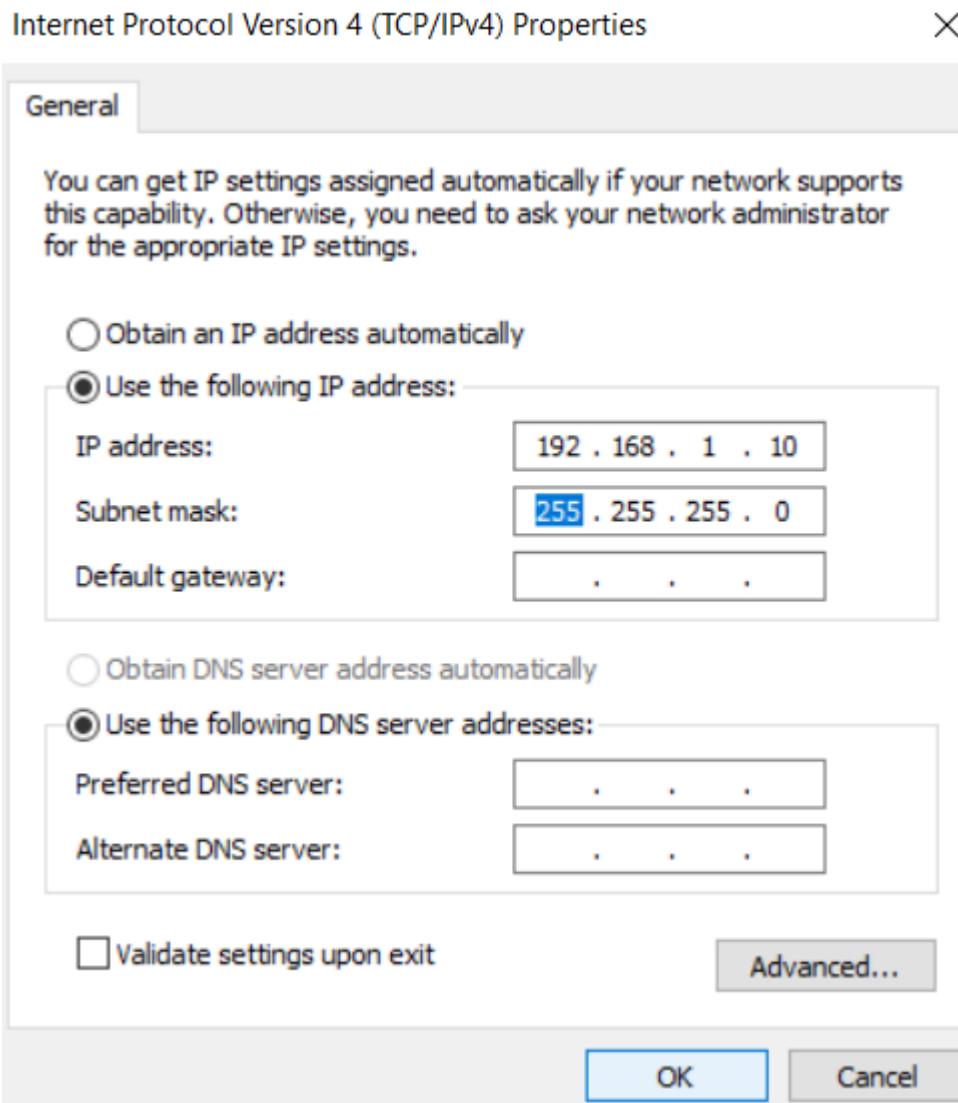
The Palo Alto Pa-220 is a small firewall device designed to support small organizations and offices with many features that optimize networking and security. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior and having many functions that blocks known threats. The raise in cyber-attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

### **Lab summary**

First, connect your computer to the management port of the Palo Alto 220.

Then, with a console connection and via Putty, commit the change of setting the IP address to 192.168.1.1 with a subnet mask of 255.255.255.0. and commit the change.

Then, configure a static address on your computer's Ethernet port, (e.g. 192.168.1.10) with the netmask 255.255.255.0 in control panel (a default gateway is not required).



Then, login via a web browser by typing <https://192.168.1.1> as URL, and log in with the username and password that you configured (e.g. username: admin, password: CiscoClass1)

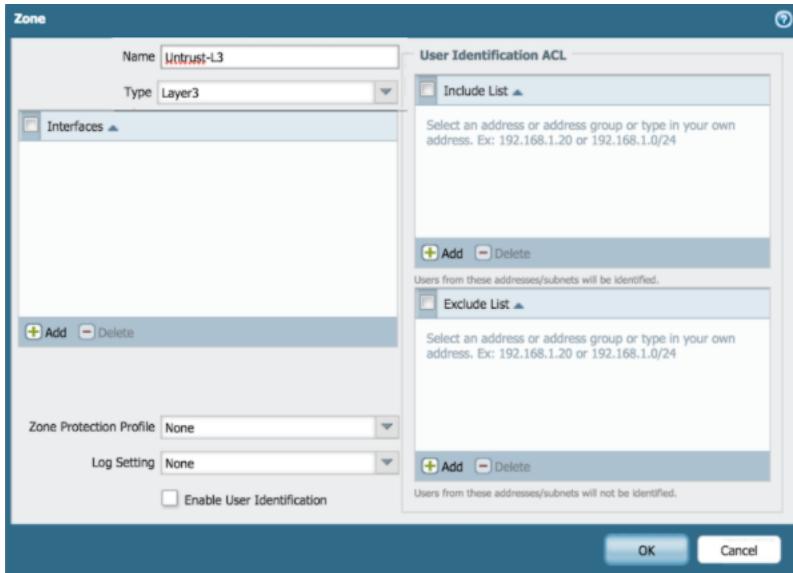


Next, create 3 security zones by navigating to Network to Zones, and click add.

A screenshot of the Palo Alto Networks Management Console. The URL in the address bar is https://192.168.1.1/#/network:vsys1:network/vlans. The navigation bar includes Dashboard, ACC, Monitor, Policies, Objects, Network (which is selected), and Device. On the left, a sidebar menu is open under the "Network" category, with "Zones" highlighted and circled in red. The main pane shows a table titled "VLAN Object" with one item listed: "Name: VLAN Interface: vlan". The bottom status bar shows the user is "admin" and last logged in at "09/23/2024 15:10:28".

Name	Interfaces	VLAN Interface
VLAN		vlan

The first zone with the name Untrust-L3, and the type as layer 3

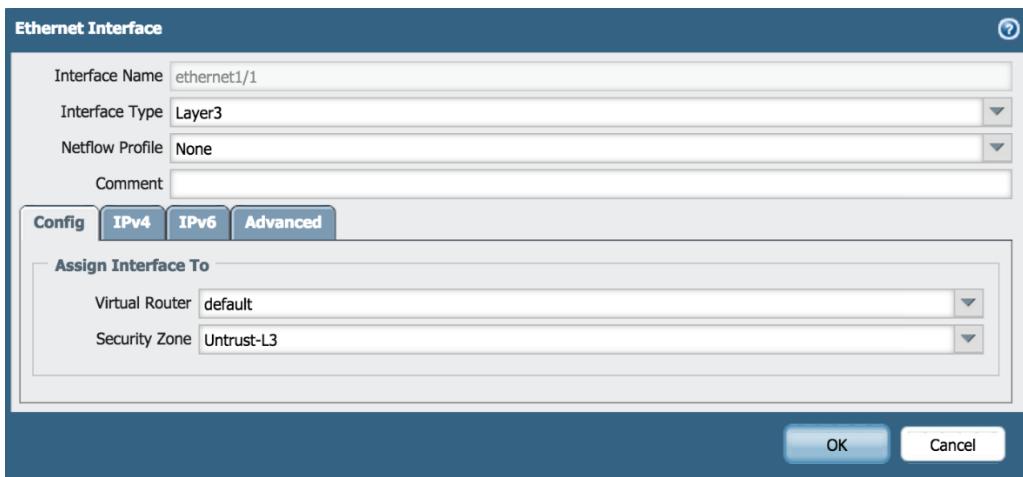


The second zone, with the name Trust-L3, and the type Layer3

The third zone, with the name Trust-L2, and the type Layer2

Next, configure the interfaces through Network then Interfaces tab.

Configure Ethernet1/1 Interface type to Layer3, set Virtual Router to default, and set the security zone to Untrust-L3. Under the IPv4 tab, set the type as DHCP client and tick on the options for Enable and Automatically creating default route.



**Ethernet Interface**

Interface Name	ethernet1/1
Interface Type	Layer3
Netflow Profile	None
Comment	
<input type="button" value="Config"/> <input type="button" value="IPv4"/> <input type="button" value="IPv6"/> <input type="button" value="Advanced"/>	
Type	<input type="radio"/> Static <input type="radio"/> PPPoE <input checked="" type="radio"/> DHCP Client
<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Automatically create default route pointing to default gateway provided by server	
Default Route Metric	[1 - 65535]
<a href="#">Show DHCP Client Runtime Info</a>	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

Next, go to Static routes under the default tab under Virtual Routers tab. Add a ipv4 static route pointing to the ISP's next hop.

**Virtual Router - default**

<input type="button" value="Router Settings"/> <input type="button" value="Static Routes"/> <input type="button" value="Redistribution Profile"/> <input type="button" value="RIP"/> <input type="button" value="OSPF"/> <input type="button" value="OSPFv3"/> <input type="button" value="BGP"/> <input type="button" value="Multicast"/>	<input type="button" value="IPv4"/> <input type="button" value="IPv6"/> <table border="1"> <thead> <tr> <th>Name</th> <th>Destination</th> <th>Interface</th> <th>Next Hop</th> <th>Admin Distance</th> <th>Metric</th> <th>Route Table</th> </tr> </thead> <tbody> <tr> <td>default route</td> <td>0.0.0.0/0</td> <td>ethernet1/1</td> <td>ip-address 192.168.4...</td> <td>default</td> <td>10</td> <td>unicast</td> </tr> </tbody> </table> <p> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Clone"/> </p>	Name	Destination	Interface	Next Hop	Admin Distance	Metric	Route Table	default route	0.0.0.0/0	ethernet1/1	ip-address 192.168.4...	default	10	unicast
Name	Destination	Interface	Next Hop	Admin Distance	Metric	Route Table									
default route	0.0.0.0/0	ethernet1/1	ip-address 192.168.4...	default	10	unicast									
<input type="button" value="OK"/> <input type="button" value="Cancel"/>															

Next, go to VLANs under the Network tab and add a Vlan Object, with the VLAN interface being vlan.

Next, go back to the Interfaces tab under Network, and edit ethernet1/2, and ethernet1/3.

They should all be in Layer2, assigned to VLAN Object, and the security zone Trust-L2.

Ethernet Interface

Interface Name	ethernet1/2
Comment	
Interface Type	Layer2
Netflow Profile	None

Config Advanced

Assign Interface To

VLAN	VLAN Object
Security Zone	Trust-L2

OK Cancel

Ethernet Interface

Interface Name	ethernet1/3
Comment	
Interface Type	Layer2
Netflow Profile	None

Config Advanced

Assign Interface To

VLAN	VLAN Object
Security Zone	Trust-L2

OK Cancel

Next, configure vlan under the VLAN interface under the Interfaces tab under Network to be assigned to VLAN Object, default Virtual Router, and the security zone Trust-L3. After that, add the IP address 192.168.1.254/24 under IPv4 tab.

VLAN Interface

Interface Name:

Comment:

Netflow Profile:

**Config** **IPv4** **IPv6** **Advanced**

Assign Interface To:

VLAN:

Virtual Router:

Security Zone:

**OK** **Cancel**

VLAN Interface

Interface Name:

Netflow Profile:

Comment:

**Config** **IPv4** **IPv6** **Advanced**

Type:  Static  DHCP Client

<input type="checkbox"/> IP
<input checked="" type="checkbox"/> 192.168.1.254/24

**Add** **Delete** **Move Up** **Move Down**

**OK** **Cancel**

Next, under DHCP server in the DHCP tab under Network, add a DHCP server that is configured with the interface vlan, the inheritance source being ethernet1/1, and the ip pool subnet as 255.255.255.0. finally, set all the settings to inherited, except for DNS Suffix.

DHCP Server

Interface	vlan
Mode	enabled
<input checked="" type="radio"/> Lease <input type="radio"/> Options	
Inheritance Source	ethernet1/1
<a href="#">Check inheritance source status</a>	
Gateway	192.168.1.254
Subnet Mask	255.255.255.0
Primary DNS	inherited
Secondary DNS	inherited
Primary WINS	inherited
Secondary WINS	inherited
Primary NIS	inherited
Secondary NIS	inherited
Primary NTP	inherited
Secondary NTP	inherited
POP3 Server	inherited
SMTP Server	<b>inherited</b>
DNS Suffix	None

**Custom DHCP options**

Name	Code	Type	Value

Add
 Delete
 Move Up
 Move Down

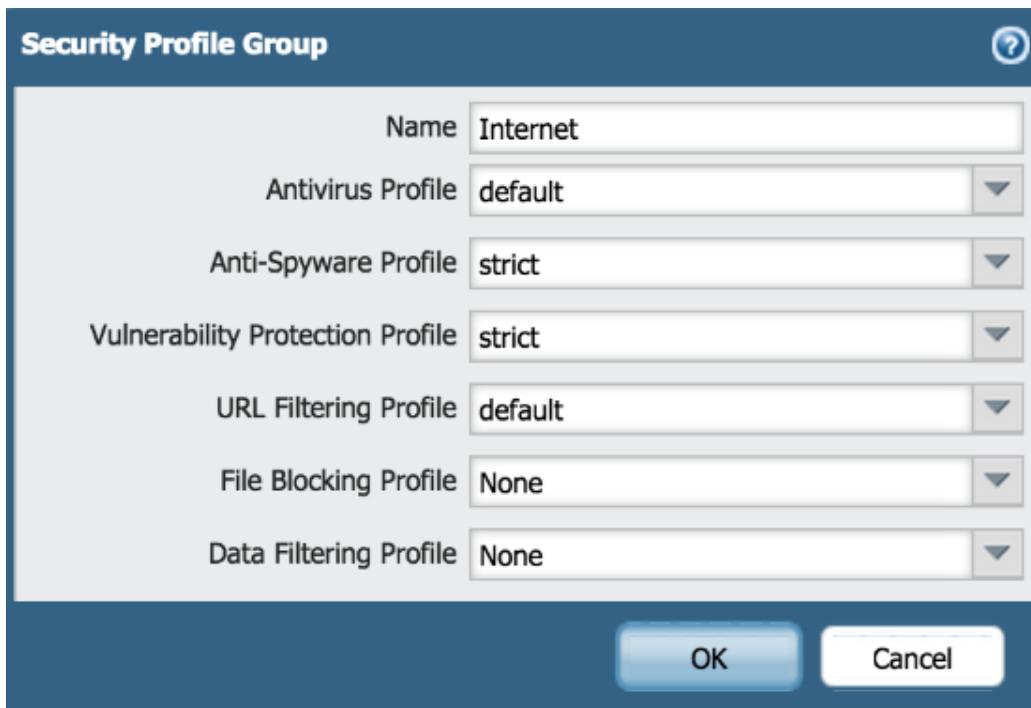
OK
Cancel

Next, add a Security Profile Group under Objects. Name it Internet, set the Antivirus Profile to default, set the Anti-Spyware Profile and Vulnerability Protection Profile to strict, URL filtering profile to default, and lastly, File Blocking Profile and Data Filtering Profile to none.

**Security Profile Group**

Name	Internet
Antivirus Profile	default
Anti-Spyware Profile	strict
Vulnerability Protection Profile	strict
URL Filtering Profile	default
File Blocking Profile	None
Data Filtering Profile	None

**OK**   **Cancel**

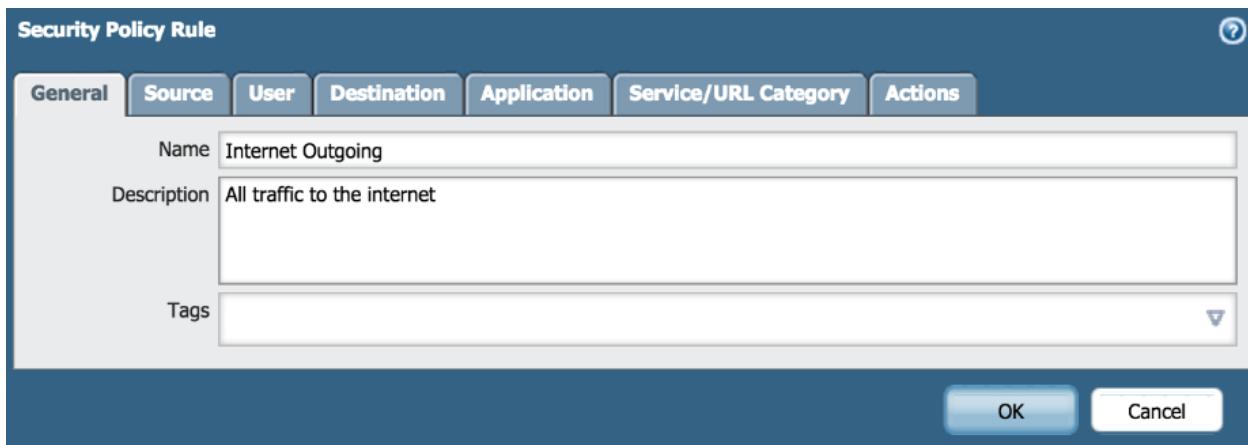


Next, configure the outbound internet security policy by adding a policy under the tab Policies in Security. In the general tab, enter a name and description (e.g. Internet Outgoing, All traffic to internet).

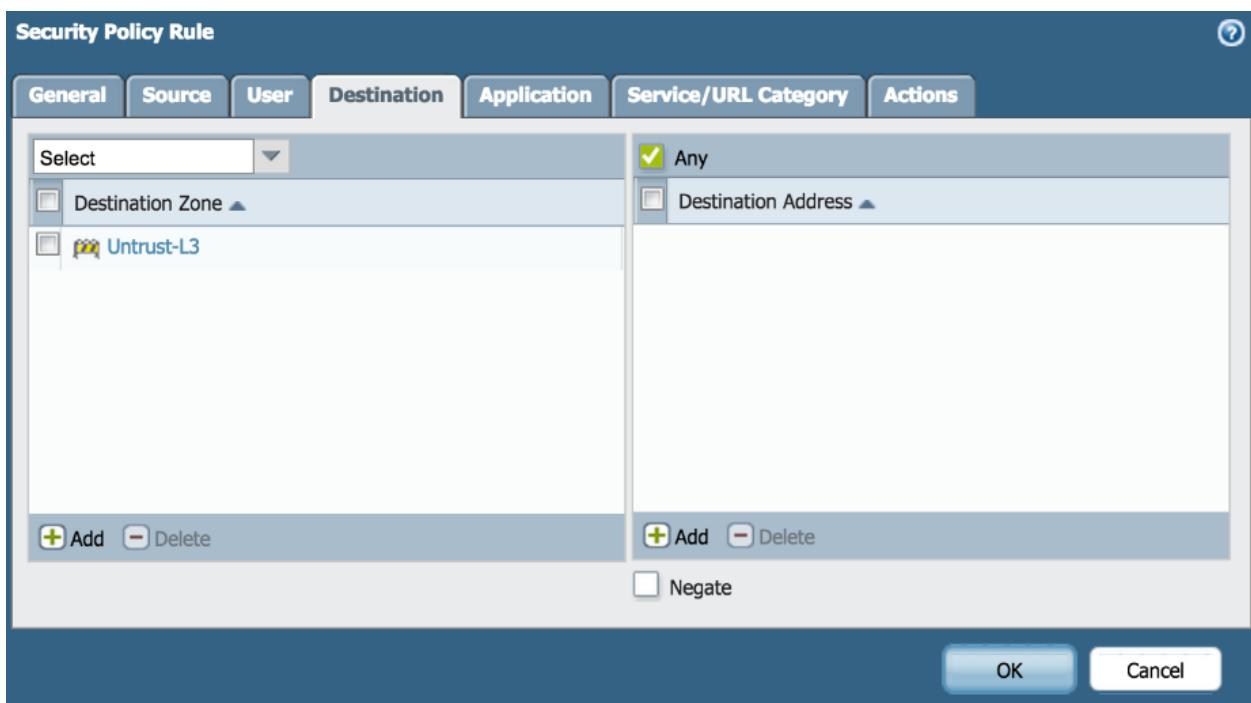
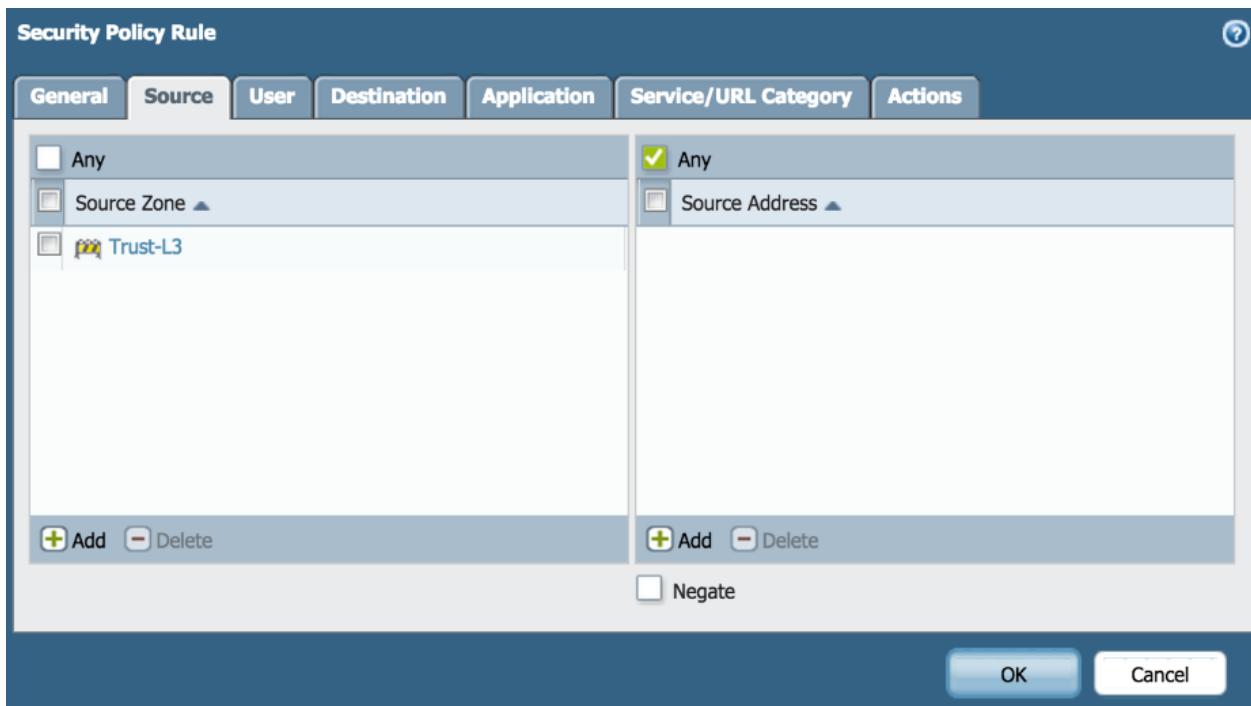
**Security Policy Rule**

General	Source	User	Destination	Application	Service/URL Category	Actions
Name	Internet Outgoing					
Description	All traffic to the internet					
Tags						

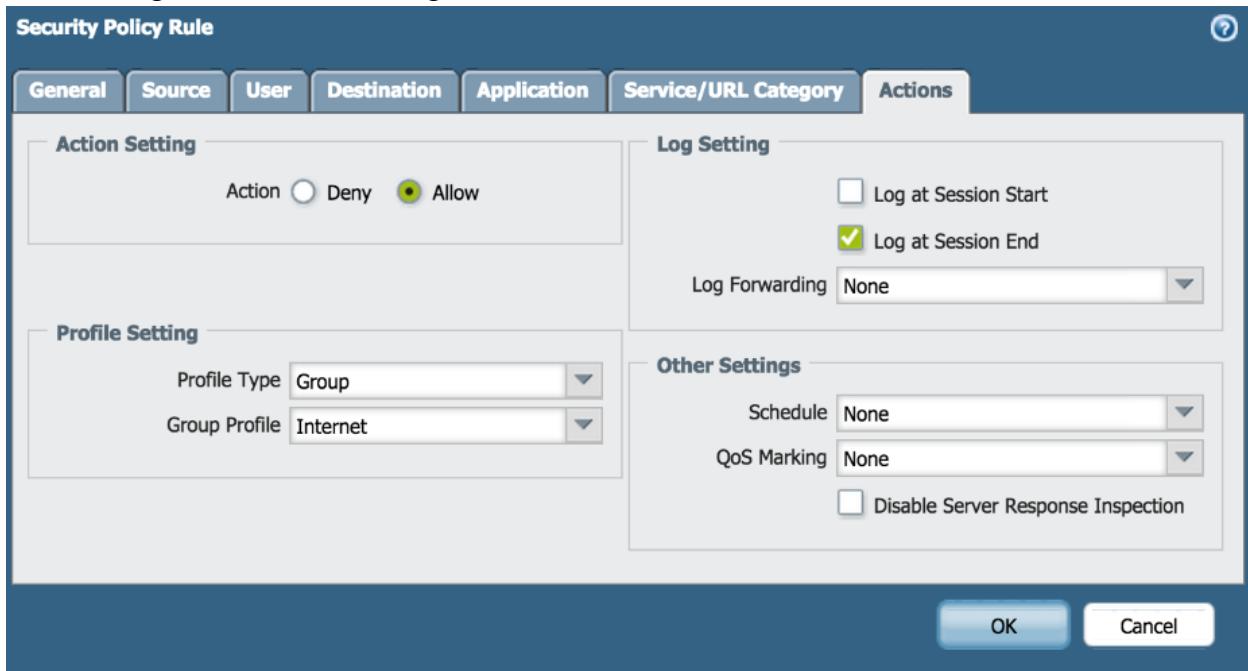
**OK**   **Cancel**



Next, in the Source and Destination tab, Add Source zone and Destination Zone.



Next, configure the Profile setting in Actions tab.



Next, configure outbound NAT policy under Policies in Security. Add a name (e.g. Internet Outgoing), and specify and Source, Destination zones, and Destination Interface.

**NAT Policy Rule**

**General Original Packet Translated Packet**

Name	Internet Outgoing
Description	
Tags	
NAT Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> NAT64

**OK Cancel**

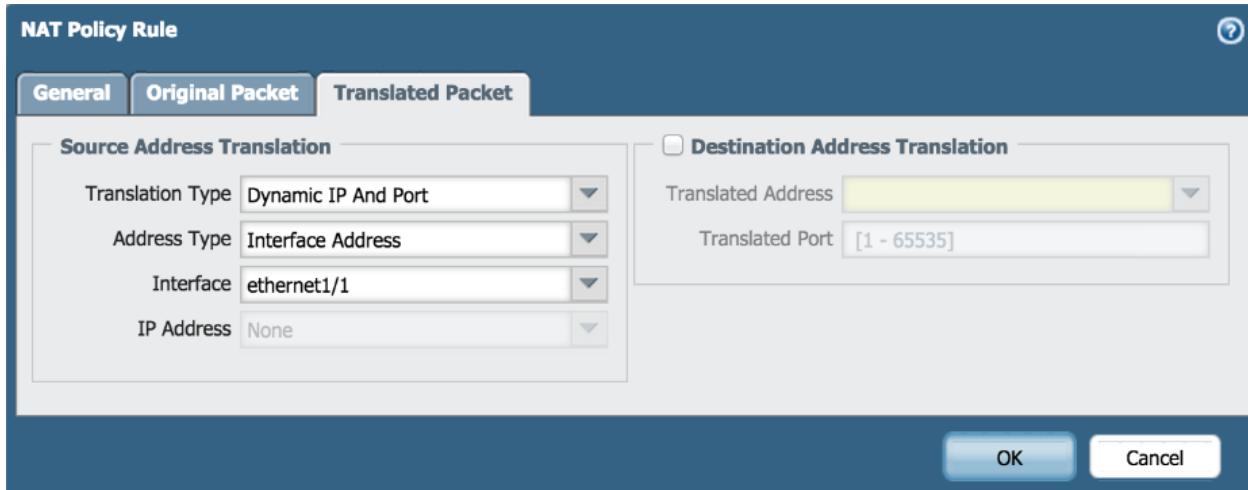
**NAT Policy Rule**

**General Original Packet Translated Packet**

Any	Destination Zone	Any	Any
Source Zone ▲	Untrust-L3	Source Address ▲	Destination Address ▲
Trust-L3			
Destination Interface			
ethernet1/1			
Service			
any			
<b>Add Delete</b>		<b>Add Delete</b>	

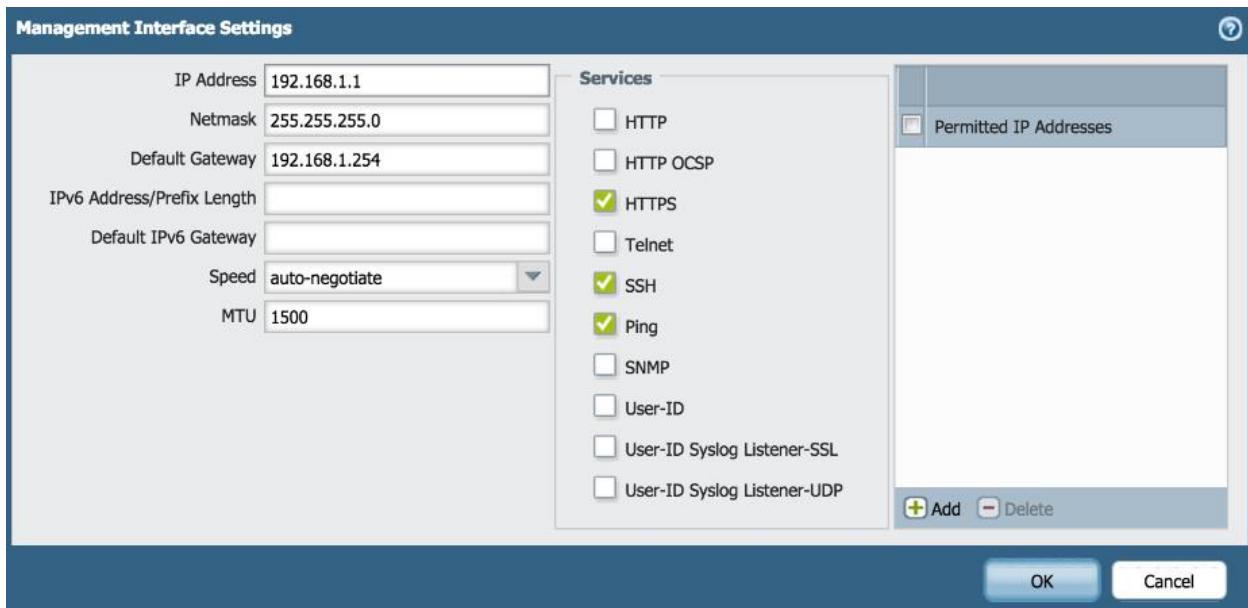
**OK Cancel**

Next, in the Translated Packet part, set translation type to Dynamic IP and Port, Address type to Interface Address, Interface to ethernet1/1.



Click OK once the confirming the configuration.

Next, hop over to the Management tab under Setup under Device. Configure the management interface settings to have a IP address of 192.168.1.1, netmask of 255.255.255.0, and a default gateway of 192.168.1.254.



Finally, finalize by Committing the changes. Check for internet.

## Problems

First, the firewall takes a bit to boot up (about 10 to 15 minutes) before things can be configured. On top of that, the setup within the Palo Alto GUI is complex, and is would be hard to do without a guide. Though navigating through the Palo Alto may be challenging, help can usually be found in the Palo Alto forums or other Palo Alto communities. On another note, I suggest checking for updates in the GUI, it may be easier to navigate and load.

## **Conclusion**

In an increasingly digital age, the Palo Alto firewall is an exceptional device that can be set up for SOHO purposes. It provides a balances performance and security and has specifications perfect for being a Small Office/Home Office router.



# Palo-Alto PA-220

Setting up URL filter for K-12 students



Palo Alto  
PA-220 Enterprise  
Hardware + Lizenz

Jeffrey Yiu Cheung

## **Purpose**

This lab introduces a way to filter out inappropriate or unnecessary websites to students k-12's learning.

## **Background information**

Palo Alto is a networking company that offers cybersecurity innovations to help with organizations with products like firewalls and cloud-based applications. It was founded in 2005 and has been the leader in cybersecurity research around the globe for the 11<sup>th</sup> straight year. With cybersecurity threats constantly emerging and improving, the need for cybersecurity is growing by day.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these learning disruptions or cybersecurity threats, Palo Alto PA-220 offers URL filtering for its customers.

The Palo Alto PA220 firewall is a firewall designed to support small and medium-sized organizations and can be an excellent option for a small, medium-sized school. It is able to mitigate many threats by having the ability to identify unknown malware and automatically generate protection upon analyzing the behavior and having many functions that blocks known threats. The raise in cyber-attacks have become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions. However, if the school has high bandwidth usage, or many instances of video streaming/online activity, then it is not recommended.

URL filtering is a cybersecurity tool that prevents users from accessing sites that the admin has blocked. We can use the URL filters to filter out cybersecurity threats or learning disruptions to maximize cyber safety and focus during class.

The Palo Alto PA-220 firewall uses the Palo Alto database to categorize websites into categories like Government, Games, Artificial Intelligences, Adult, Nudity. This technique is called Category-based filtering.

Palo Alto can also detect malicious websites with grayware, malware, phishing attacks, etc. This is a technique called Reputation-Based Filtering. Their cloud-database constantly gets updates about malicious activity and flags them as dangerous to block malicious activities.

While URL filtering is helpful tool which can improve productivity, control over content, and reducing inappropriate activity, URL filters might also categorize legitimate websites as inappropriate and blocked. There are also techniques which can bypass filters to be wary of.

## Lab summary

First, under Objects tab, in security profiles, there should be a subtab named URL Filtering. Add a new one, and name it (e.g. School URL). Then within the categories, select the ones you would like to block or override. If you would like to completely block a site (no access from students and no access from admins), you would select block for site access and user credential submission.

The screenshot shows the FortiGate configuration interface. On the left, the navigation tree includes Service Groups, Tags, Devices, GlobalProtect (with HIP Objects and HIP Profiles), External Dynamic Lists, Custom Objects (Data Patterns, Spyware, Vulnerability, URL Category), Security Profiles (Antivirus, Anti-Spyware, Vulnerability Protection, URL Filtering), and various other modules like Log Forwarding, Authentication, Decryption, and SD-WAN Link Management. The URL Filtering node is highlighted with a red circle. Below the tree, there's an 'Add' button circled in red. The main panel displays the 'URL Filtering Profile' configuration for 'School URL'. It has fields for Name ('School URL') and Description. Below these are tabs for Categories, URL Filtering Settings, User Credential Detection, HTTP Header Insertion, and Inline ML. The Categories tab shows a list of pre-defined URL categories: abortion, abused-drugs, adult, alcohol-and-tobacco, artificial-intelligence, and auctions. The 'abused-drugs' category is selected, and its row in the table is circled in red. The table columns are CATEGORY, SITE ACCESS, and USER CREDENTIAL SUBMISSION. The 'abused-drugs' row shows SITE ACCESS as 'block' and USER CREDENTIAL SUBMISSION as 'block'. Other rows show 'allow' for both columns. At the bottom of the table, there's a note: "\* indicates a custom URL category, + indicates external dynamic list". There are 'OK' and 'Cancel' buttons at the bottom right.

If you want to allow admin override, you change site access to override and user credential submission. To allow, both should be set to allow. We blocked abused-drugs, alcohol and tobacco, auctions, cryptocurrency, nudity, phishing, and weapons. We allowed admin override in categories in games and shopping. We allowed everything else.

NAME	LOCATION	SITE ACCESS	USER CREDENTIAL SUBMISSION	HTTP HEADER INSERTION	INLINE ML
default	Predefined	Allow Categories (60) Alert Categories (6) Continue Categories (0) Block Categories (12) Override Categories (0)	Allow Categories (76) Alert Categories (0) Continue Categories (0) Block Categories (0)		Allow Categories (0) Alert Categories (1) Block Categories (1)
School URL		Allow Categories (64) Alert Categories (0) Continue Categories (0) Block Categories (8) Override Categories (6)	Allow Categories (69) Alert Categories (0) Continue Categories (1) Block Categories (8)		Allow Categories (2) Alert Categories (0) Block Categories (0)

It should look like this after it is finished.

Next, after finishing site access, navigate to the security policy for outbound internet (e.g. Internet Outgoing). You have to attach the URL filter you just created into the internet policy, in the actions tab of the policy.

PA-220 DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Security Policy

NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION
Internet Outgoing	none	universal	Trust-L3	any	any	any	Untrust-L3	any	any	any	application-all	Allow
Intrazone-default	none	intrazone	any	any	any	any	[inzone]	any	any	any	any	Allow
Interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Policy Optimizer

Object : Addresses + Add Delete Clone Override Revert Enable Disable Move PDF/CSV Highlight Unused Rules View Rulebase as Groups Reset Rule Hit Counter Group Test Policy Match

Security Policy Rule

General | Source | Destination | Application | Service/URL Category Actions Usage

Action Setting

Action: Allow  Send ICMP Unreachable

Profile Setting

Profile Type: Profiles  
Antivirus: default  
Vulnerability Protection: None  
Anti-Spyware: default  
URL Filtering: School URL (circled in red)  
File Blocking: None  
Data Filtering: None  
WildFire Analysis: None

Log Setting

Log at Session Start  Log at Session End

Log Forwarding: None

Other Settings

Schedule: None  
QoS Marking: None  Disable Server Response Inspection

OK Cancel

After this process, the websites you blocked should not be accessible.

Finally, we need to set an admin password allowing admin override. Navigate to Setup under the Device tab. In Content-ID, there should be a section named URL Admin Override. This is where we create the password for Admin Override.

The screenshot shows the PA-220 device setup interface. The left sidebar has sections like Management, Operations, Services, Interfaces, Telemetry, Content-ID (which is selected), WildFire, Session, and DLP. Under Content-ID, there's a 'URL Admin Override' section. A table lists 'LOCATION' (PA-220), 'SSL/TLS SERVICE PROFILE' (None), and 'MODE' (transparent). To the right are several configuration panels: 'Content-ID Settings' (with checkboxes for various forwarding and inspection options), 'Realtime Signature Lookup' (with a DNS signature timeout of 100ms), 'X-Forwarded-For Headers' (disabled), and 'Content-ID Features' (Manage Data Protection and Container Pages).

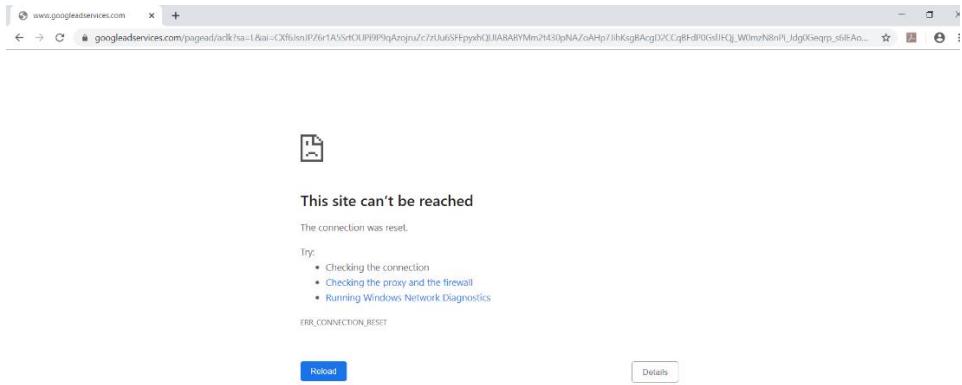
## URL Admin Override

?

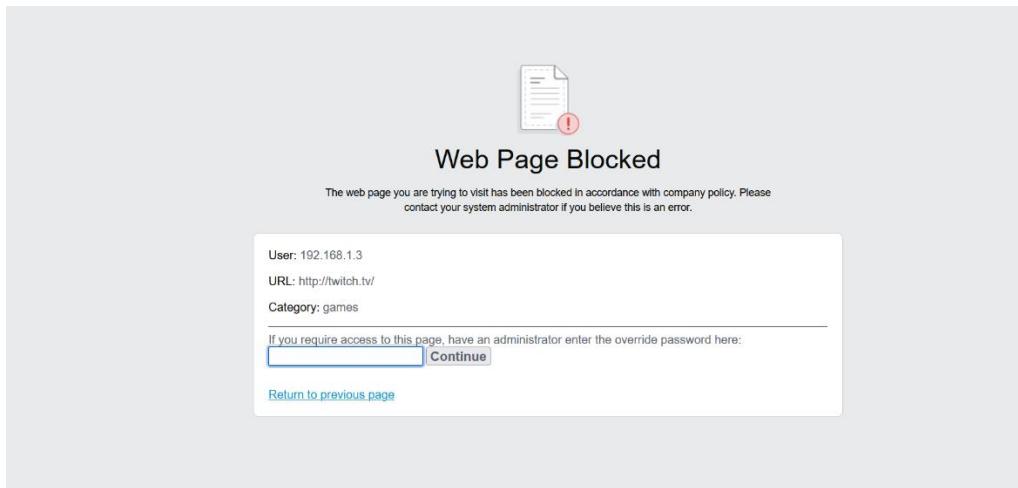
Password	<input type="password" value="*****"/>
Confirm Password	<input type="password" value="*****"/>
SSL/TLS Service Profile	<input type="button" value="None"/>
Mode	<input checked="" type="radio"/> Transparent <input type="radio"/> Redirect

**OK** **Cancel**

This is what it should look like when the site is blocked:



This is what it should look like when the site can be overridden:



## Problems

This lab was straightforward, however time-consuming. For every change and every confirmation, we had to commit, which takes about 5-10 minutes. On top of this, we are on an older version, a newer option may be more optimized. Also, it was hard to deduce how Palo Alto categorizes its websites, so the site <https://urlfiltering.paloaltonetworks.com/> can help a lot.

## Conclusion

In conclusion, in a increasingly digital age, more malicious activities are online and it is important to block dangerous sites (not only sites that may steal sensitive information, but also inappropriate sites), especially for children in a k-12 environment. URL filtering is a great tool that can block those sites.



# Palo-Alto PA-220

Setting up GlobalProtect VPN and Remote Desktop



Palo Alto  
PA-220 Enterprise  
Hardware + Lizenz

Jeffrey Yiu Cheung

## **Purpose**

The purpose of this lab is to set up a GlobalProtect VPN on a PA-220 Firewall to enable secure connection with remote networks. This lab also demonstrates how to use Remote Desktop Connection to utilize a computer on a different network.

## **Background information**

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Palo Alto Networks designed and offered GlobalProtect VPN to its customers.

GlobalProtect VPN is a feature on the PA-220 firewall which allows secure remote connections to the internal network. It creates a tunnel between the user and the destined network and encrypts the data with IPsec or SSL/TLS which passes through. Users can thus use this ability to safely access their internal network while away from home/company. GlobalProtect VPN is a service designed by the Palo Alto Networks to work seamlessly with the PA-220 firewall. Although it is reliable and secure, it can impact the performance of the network due to taking more bandwidth. GlobalProtect also requires a lot of complex setups to get up and running.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

IPsec, an encryption protocol used by GlobalProtect, is a combination of other security protocols to create a protocol that ensures security, integrity, and authentication. It uses protocols like Authentication Header and Encapsulation Security Payload. IPsec follows AES (Advanced Encryption Standard), a highly secure and efficient encrypting algorithm. Although IPsec is secure, it is resource intensive and may drop performance.

Palo Alto Networks is a cybersecurity company headquartered in Santa Clara, California. Palo Alto Networks offers cybersecurity products and innovations like firewalls and cloud-based applications. It was founded in 2005 and has been awarded as the leader in cybersecurity research around the globe for the 11<sup>th</sup> straight year.

The Palo Alto PA-220 firewall is a firewall designed to support small and medium-sized organizations and can be an excellent option for a small office. It offers features such as URL filtering, GlobalProtect VPN, WildFire (cloud-based threat analysis service), DNS security... etc. Due to cyber-attacks having become more common and sophisticated, it is important to have protection against these threats. The Palo Alto device has a throughput of up to 500 Mbps, requires 50-60Hz voltage, and is about 3 pounds of weight. It can support up to 64,000 firewall sessions.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

## Lab summary

First, we need to generate 3 certificates to match the picture below.

The screenshot shows the PA-220 device interface with the 'DEVICE' tab selected. In the left sidebar, under 'Certificate Management', the 'Certificates' option is highlighted. The main pane displays a table titled 'Device Certificates' with the subtitle 'Default Trusted Certificate Authorities'. The table has columns: NAME, SUBJECT, ISSUER, CA, KEY, EXPIRES, STATUS, ALGORITHM, and USAGE. There are three entries:

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
RootCert	CN = RootCert	CN = RootCert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 20 20:03:47 2025 G...	valid	RSA	
IntermediateCert	CN = IntermediateCert	CN = RootCert	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Dec 20 20:04:13 2025 G...	valid	RSA	
ServerCert	CN = gp.portal-gw01.local	CN = IntermediateCert	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 6 20:09:58 2026 GMT	valid	RSA	
ServerCert	CN = 192.168.40.13	CN = IntermediateCert	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Jan 6 20:32:08 2026 GMT	valid	RSA	

A red box highlights the first two rows (RootCert and IntermediateCert).

For the first certificate, we need to generate a root certificate. It is under Device > Certificate Management > Certificates > generate. Use the any name for Certificate name and Common Name (except for an IP or FQDN) and check on Certificate Authority.

## Generate Certificate



Certificate Type  Local  SCEP

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By  ▼

Certificate Authority

Block Private Key Export

OCSP Responder  ▼

**^ Cryptographic Settings**

Algorithm	RSA
Number of Bits	2048
Digest	sha256
Expiration (days)	365

**Certificate Attributes**

<input type="checkbox"/>	TYPE	VALUE

+ Add - Delete

Generate

Cancel

For the second certificate, generate a similar certificate, but signed by the first certificate.

## Generate Certificate

Certificate Type  Local  SCEP [?](#)

Certificate Name

Common Name

IP or FQDN to appear on the certificate

Signed By  [▼](#)

Certificate Authority

Block Private Key Export

OCSP Responder [▼](#)

[^ Cryptographic Settings](#)

Algorithm	RSA
Number of Bits	2048
Digest	sha256
Expiration (days)	365

[^ Certificate Attributes](#)

<input type="checkbox"/>	TYPE	VALUE

[+ Add](#) [- Delete](#)

[Generate](#) [Cancel](#)

For the third certificate, pick any name you want for the certificate name, but assign the IP of the DNS server address. You can check via Interfaces in the Network tab. It should not be checked as Certificate Authority and should be signed by the second certificate. It should also have an attribute, which is just the DNS server address again.

**Generate Certificate**

Certificate Type  Local  SCEP

Certificate Name

Common Name   

IP or FQDN to appear on the certificate

Signed By

Certificate Authority

Block Private Key Export

OCSP Responder

**Cryptographic Settings**

Algorithm

Number of Bits

Digest

Expiration (days)

**Certificate Attributes**

TYPE	VALUE
<input checked="" type="checkbox"/>	IP = "IP Address" from Subject Alternative Name (SAN) field 192.168.40.13

+ Add - Delete

**Dynamic IP Interface Status**

Interface ethernet1/1  
State Bound  
Remaining Lease Time 6 days 20:41:22

IP Address **192.168.40.13**  

Gateway **192.168.40.1**

Primary DNS 9.9.9.9  
Secondary DNS 1.1.1.1  
Primary WINS 0.0.0.0  
Secondary WINS 0.0.0.0  
Primary NIS 0.0.0.0  
Secondary NIS 0.0.0.0  
POP3 Server 0.0.0.0  
SMTP Server 0.0.0.0  
DNS Suffix

Renew Release Close

Next, make an SSL/TLS certificate profile. In Device > Certificate Management > SSL/TLS Service Profile > create. Link the third certificate you made (in my case it is ServerCert).

The screenshot shows the PA-220 device configuration interface. The left sidebar contains various management and security profiles. The main area displays the 'SSL/TLS Service Profile' configuration dialog. The profile is named 'SSL-TLS-Server' and is associated with a certificate named 'ServerCert'. The 'Protocol Settings' section specifies a minimum version of 'TLSv1.0' and a maximum version of 'Max'. The dialog has 'OK' and 'Cancel' buttons.

Next, head to Network > Interfaces > Tunnel and create a new tunnel.

The screenshot shows the PA-220 device configuration interface. The left sidebar lists network-related profiles like GlobalProtect, QoS, and LLDP. The main area shows the 'Tunnel' tab selected under 'Interfaces'. A new tunnel interface is being created, with the interface name set to 'tunnel'. The 'Config' tab is active, showing options for assigning the interface to a 'Virtual Router' (set to 'default') and a 'Security Zone' (set to 'VPN'). The 'Assign Interface To' section includes dropdown menus for 'Virtual Router' and 'Security Zone'. The bottom navigation bar features a red circle around the '+ Add' button, which is used to create new interfaces.

Afterwards, make a new security zone in Network>Zones and attach the newly made tunnel to it.

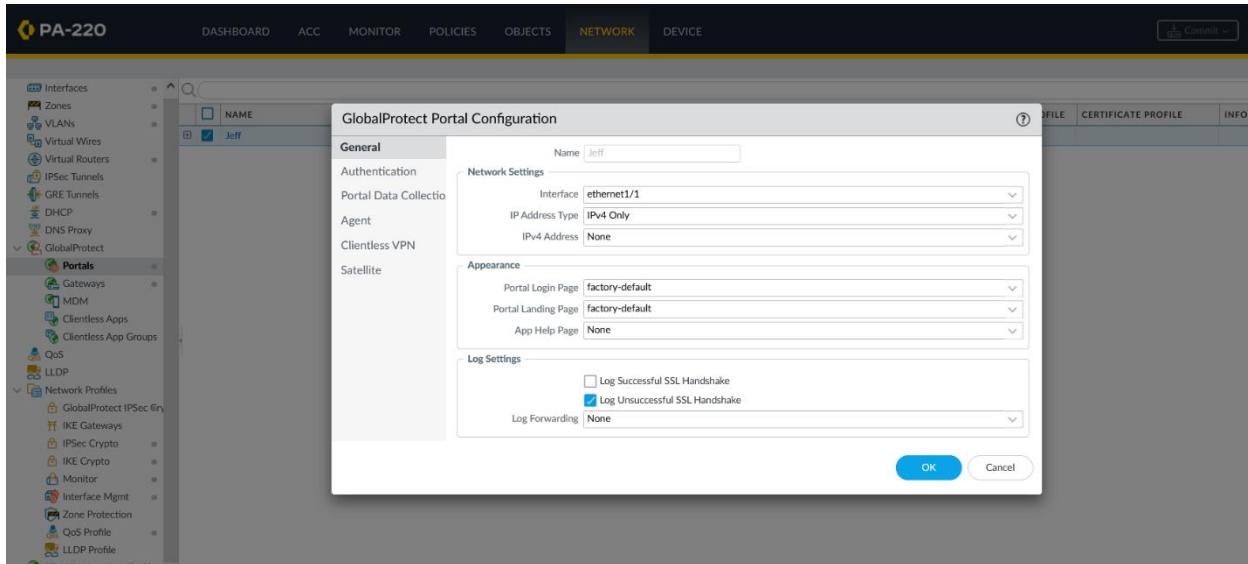
The screenshot shows the PA-220 interface under the 'NETWORK' tab. On the left, the navigation menu includes 'Interfaces', 'Zones' (selected), 'VLANs', 'Virtual Wires', 'Virtual Routers', 'IPSec Tunnels', 'GRE Tunnels', 'DHCP', 'DNS Proxy', 'GlobalProtect' (expanded), 'Portals', 'Gateways', 'MDM', 'Clientless Apps', 'Clientless App Groups', 'QoS', 'LLDP', and 'Network Profiles' (expanded). In the main pane, a 'Zone' dialog is open for 'VPN'. The 'NAME' field contains 'VPN' and is circled in red. The 'INTERFACES' dropdown is set to 'Layer3' and shows 'tunnel.10' selected. The 'User Identification ACL' section has 'Enable User Identification' checked and an 'INCLUDE LIST' section. The 'Zone Protection' section shows 'Zone Protection Profile' set to 'None'.

Next, go to Policies>Security Policies and make a couple of security policy that would allow the traffic. One for zone VPN to Trust-L3 and one from Trust-L3 to VPN is necessary.

NAME	TAGS	TYPE	Source				Destination				APPLICATION	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1 untrust_vpn	none	universal	[Untrust-L3]	any	any	any	[VPN]	any	any	any	application...	Allow	
2 trust	none	universal	[VPN]	any	any	any	[Trust-L3]	any	any	any	any	Allow	
3 vpn-untrust	none	universal	[VPN]	any	any	any	[Untrust-L3]	any	any	any	any	Allow	
4 Internet Outgoing	none	universal	[Trust-L3]	any	any	any	[Untrust-L3]	any	any	any	application...	Allow	
5 VPN2	none	universal	[Trust-L3]	any	any	any	[VPN]	any	any	any	application...	Allow	
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow	
7 interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny	

The screenshot shows the PA-220 interface under the 'POLICIES' tab. On the left, the navigation menu includes 'Security' (selected), 'NAT', 'QoS', 'Policy Based Forwarding', 'Decryption', 'Tunnel Inspection', 'Application Override', 'Authentication', 'DoS Protection', and 'SD-WAN'. In the main pane, a table lists security policies. Several policies are highlighted with red circles: row 1 (untrust\_vpn), row 2 (trust), row 3 (vpn-untrust), row 5 (VPN2), and row 7 (interzone-default).

Next, go to Network>GlobalProtect>Portals, and add a new portal configuration.



In authentication, attach the SSL/TLS server profile you made earlier and add a authentication profile which allows all.

	NAME	OS	AUTHENTIC... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTI... MESSAGE	ALLOW AUTHENTI... WITH USER CREDENTI... OR CLIENT CERTIFICA...
<input type="checkbox"/>	gp	Any	Jeffrey	<input type="checkbox"/>	Username	Password	Enter login credentials	No

## Client Authentication



Name

OS

Authentication Profile

Automatically retrieve passcode from SoftToken application

### GlobalProtect App Login Screen

Username Label

Password Label

Authentication Message

Authentication message can be up to 256 characters.

Allow Authentication with User Credentials OR Client Certificate

To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.

OK

Cancel

Next, under Agent, add a config, and also add the first and second certificate (Root Cert and Intermediate Cert in my example) in the trusted CA.

GlobalProtect Portal Configuration

General  
Authentication  
Portal Data Collection  
**Agent**  
Clientless VPN  
Satellite

**Agent**

CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
<input checked="" type="checkbox"/> Jeffportal	any	any	Extn_GW01	

**Install Certificates**

**Agent User Override Key:**

**Confirm Agent User Override Key:**

**Install in Local Root Certificate Store:**

TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE
<input type="checkbox"/> RootCert	<input checked="" type="checkbox"/>
<input type="checkbox"/> IntermediateCert	<input checked="" type="checkbox"/>

**Add** **Delete**

**OK** **Cancel**

Name it whatever you'd like, set the Certificate to encrypt/decrypt as the first certificate (Root Cert in my case)

Configs

**Authentication** | Config Selection Criteria | Internal | External | App | HIP Data Collection

Name:

Client Certificate:

The selected client certificate including its private key will be installed on client machines.

Save User Credentials:

**Authentication Override**

Generate cookie for authentication override  
 Accept cookie for authentication override

Cookie Lifetime:

Certificate to Encrypt/Decrypt Cookie:

**Components that Require Dynamic Passwords (Two-Factor Authentication)**

Portal       External gateways-manual only  
 Internal gateways-all       External gateways-auto discovery

Select the options that will use dynamic passwords like one-time password (OTP) to authenticate users as opposed to using saved credentials. As a result, the user will always be prompted to enter new credentials for each selected option.

**OK** **Cancel**

Next, in the External tab, add a gateway with the IP of the DNS server (the same as the Server Certificate's CN)

Configs

External

Cutoff Time (sec) 5

**External Gateways**

NAME	ADDRESS	PRIORITY RULE	MANUAL
Extn_GW01	192.168.40.13	US (Highest)	<input type="checkbox"/>

**THIRD PARTY VPN**

**App**

OK Cancel

In the App tab, make sure that you've got this setting.

PA-220

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Configurations

App Configurations

Connect Method	User-logon (Always On)
GlobalProtect App Config Refresh Interval (hours)	24 (1 - 168)
Allow user to disconnect GlobalProtect App (Always-on mode)	Allow
Display the following reasons to disconnect GlobalProtect (Always-on mode)	
Allow User to Uninstall GlobalProtect App (Windows Only)	Allow
Allow User to Upgrade GlobalProtect App	Allow with Prompt
Allow user to Sign Out from GlobalProtect App	Yes
Allow user to extend GlobalProtect License	No

Welcome Page None

Disconnect GlobalProtect App (Always-on mode)

Passcode

Confirm Passcode

Max Times User Can Disconnect

Disconnect Timeout (min)

Uninstall GlobalProtect App

Uninstall Password

Confirm Uninstall Password

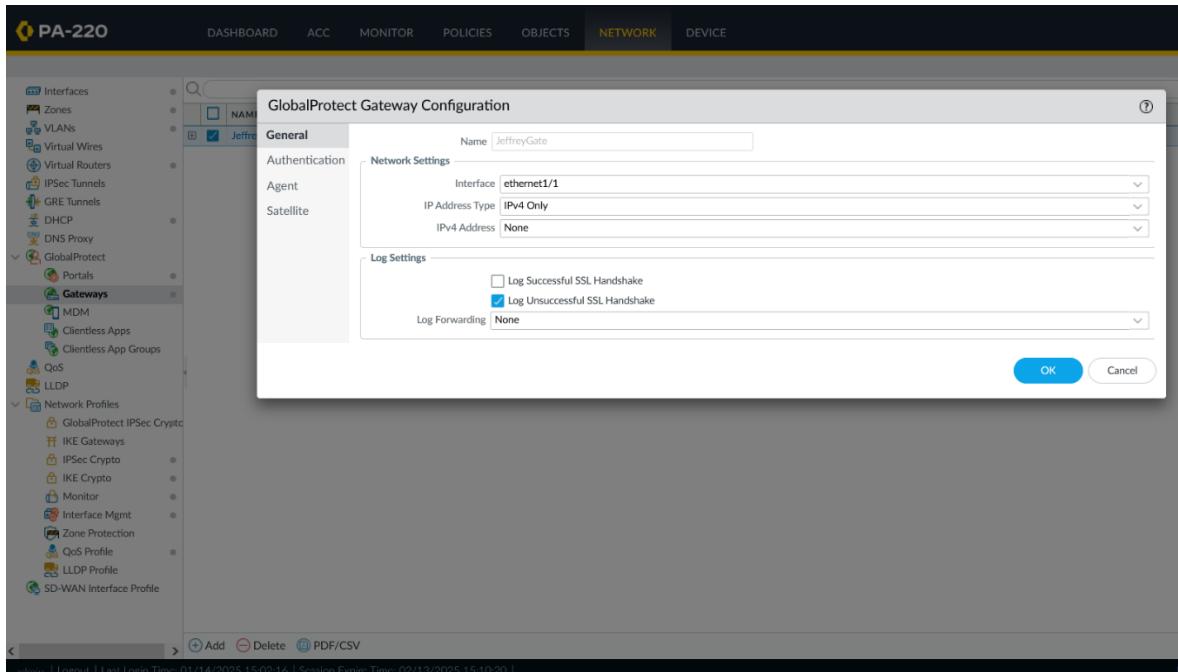
Mobile Security Manager Settings

Mobile Security Manager

Enrollment Port 443

OK Cancel

Next, go GlobalProtect>Gateway, and add a configuration.



Next, under Authentication, attach the SSL/TLS profile you've made, and also add a Client Authentication profile.

	NAME	OS	AUTHENTICATION PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTICATI... MESSAGE	ALLOW AUTHENTICATI... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
<input checked="" type="checkbox"/>	test	Any	Jeffrey	<input type="checkbox"/>	Username	Password	Enter login credentials	Yes

The Client Authentication should look like this.

**Client Authentication**

Name	<input type="text" value="test"/>
OS	<input type="text" value="Any"/>
Authentication Profile	<input type="text" value="Jeffrey"/>
<input type="checkbox"/> Automatically retrieve passcode from SoftToken application	
<b>GlobalProtect App Login Screen</b>	
Username Label	<input type="text" value="Username"/>
Password Label	<input type="text" value="Password"/>
Authentication Message	<input type="text" value="Enter login credentials"/>
Authentication message can be up to 256 characters.	
Allow Authentication with User Credentials OR Client Certificate	<input type="text" value="Yes (User Credentials OR Client Certificate Required)"/>
To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.	
<b>OK</b> <b>Cancel</b>	

Next, in the Agent tab, put the tunnel you've made as the Tunnel Interface.

**GlobalProtect Gateway Configuration**

General	<b>Tunnel Settings</b>	Client Settings	Client IP Pool	Network Services	Connection Settings	Video Traffic	HIP Notification												
Authentication																			
<b>Agent</b>																			
Satellite																			
<table border="1"> <tr> <td><input checked="" type="checkbox"/> Tunnel Mode</td> <td>Tunnel Interface <input type="text" value="tunnel.10"/></td> </tr> <tr> <td>Max User</td> <td><input type="text" value="1 - 250"/></td> </tr> <tr> <td><input checked="" type="checkbox"/> Enable IPSec</td> <td>GlobalProtect IPSec Crypto <input type="text" value="default"/></td> </tr> <tr> <td><input type="checkbox"/> Enable X-Auth Support</td> <td>Group Name <input type="text"/></td> </tr> <tr> <td>Group Password <input type="text"/></td> <td>Confirm Group Password <input type="text"/></td> </tr> <tr> <td colspan="2"><input checked="" type="checkbox"/> Skip Auth on IKE Rekey</td> </tr> </table>								<input checked="" type="checkbox"/> Tunnel Mode	Tunnel Interface <input type="text" value="tunnel.10"/>	Max User	<input type="text" value="1 - 250"/>	<input checked="" type="checkbox"/> Enable IPSec	GlobalProtect IPSec Crypto <input type="text" value="default"/>	<input type="checkbox"/> Enable X-Auth Support	Group Name <input type="text"/>	Group Password <input type="text"/>	Confirm Group Password <input type="text"/>	<input checked="" type="checkbox"/> Skip Auth on IKE Rekey	
<input checked="" type="checkbox"/> Tunnel Mode	Tunnel Interface <input type="text" value="tunnel.10"/>																		
Max User	<input type="text" value="1 - 250"/>																		
<input checked="" type="checkbox"/> Enable IPSec	GlobalProtect IPSec Crypto <input type="text" value="default"/>																		
<input type="checkbox"/> Enable X-Auth Support	Group Name <input type="text"/>																		
Group Password <input type="text"/>	Confirm Group Password <input type="text"/>																		
<input checked="" type="checkbox"/> Skip Auth on IKE Rekey																			
<b>OK</b> <b>Cancel</b>																			

Next, in Client settings, add a configuration.

GlobalProtect Gateway Configuration

Client Settings

	CONFIGS	USERS	OS	REGION	IP ADDRESS	IP POOL	INCLUDE ACCESS ROUTE
<input type="checkbox"/>	JeffTunnel	any	any			192.168.2.2-192.168.2.254	192.168.1.0/24

(+) Add Delete Clone ↑ Move Up ↓ Move Down

OK Cancel

In Config Selection Criteria, the source user and OS should be checked to any.

Configs

Config Selection Criteria

<input type="checkbox"/> any	<input checked="" type="checkbox"/> Any
<input type="checkbox"/> SOURCE USER	<input type="checkbox"/> OS

(+) Add (-) Delete

Source Address

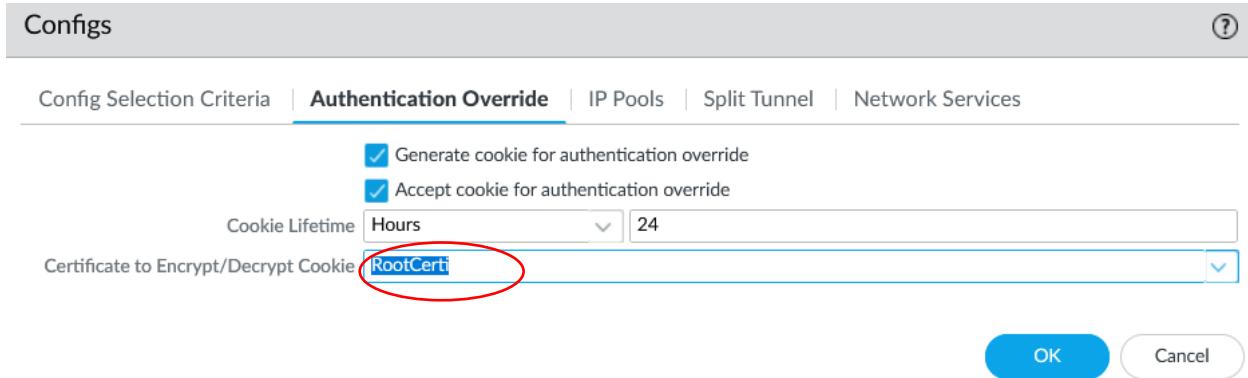
<input type="checkbox"/> REGION	<input type="checkbox"/> IP ADDRESS
---------------------------------	-------------------------------------

(+) Add (-) Delete

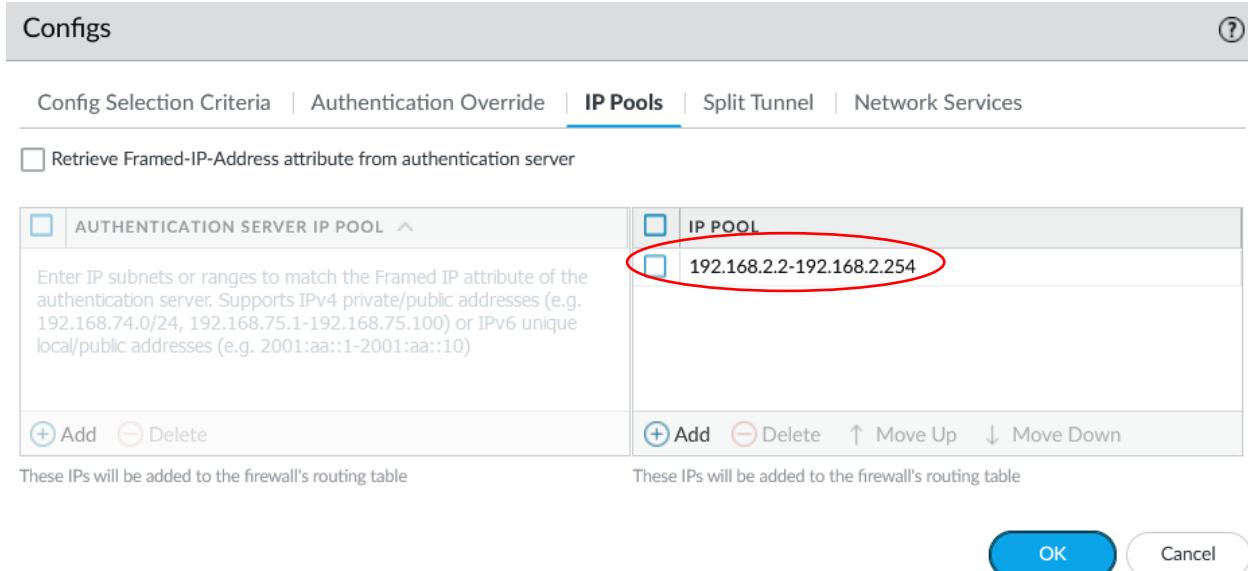
The configuration must match User and OS and either Region or IP Address if specified.

OK Cancel

In Authentication Override, the certificate to encrypt/decrypt should be set to your first Certificate (RootCert in my case).



Next, in IP Pools, add an IP pool. Any network except for the one in use by the firewall should suffice.



In Split Tunnel, specify your internal network so that the tunnel will only reach it. (Ex. 192.168.x.0/24).

## Configs



Config Selection Criteria | Authentication Override | IP Pools | **Split Tunnel** | Network Services

**Access Route** | Domain and Application

No direct access to local network

No direct access to local network is applicable to Windows, Mac and Linux only

<input type="checkbox"/> INCLUDE ^	<input type="checkbox"/> EXCLUDE ^
<input checked="" type="checkbox"/> 192.168.1.0/24	Enter subnets that clients should exclude (e.g. 172.16.1.0/24)
<a href="#">+ Add</a> <a href="#">Delete</a>	<a href="#">+ Add</a> <a href="#">Delete</a>

These routes will be added to the client's routing table. More-specific routes take precedence over less-specific routes.

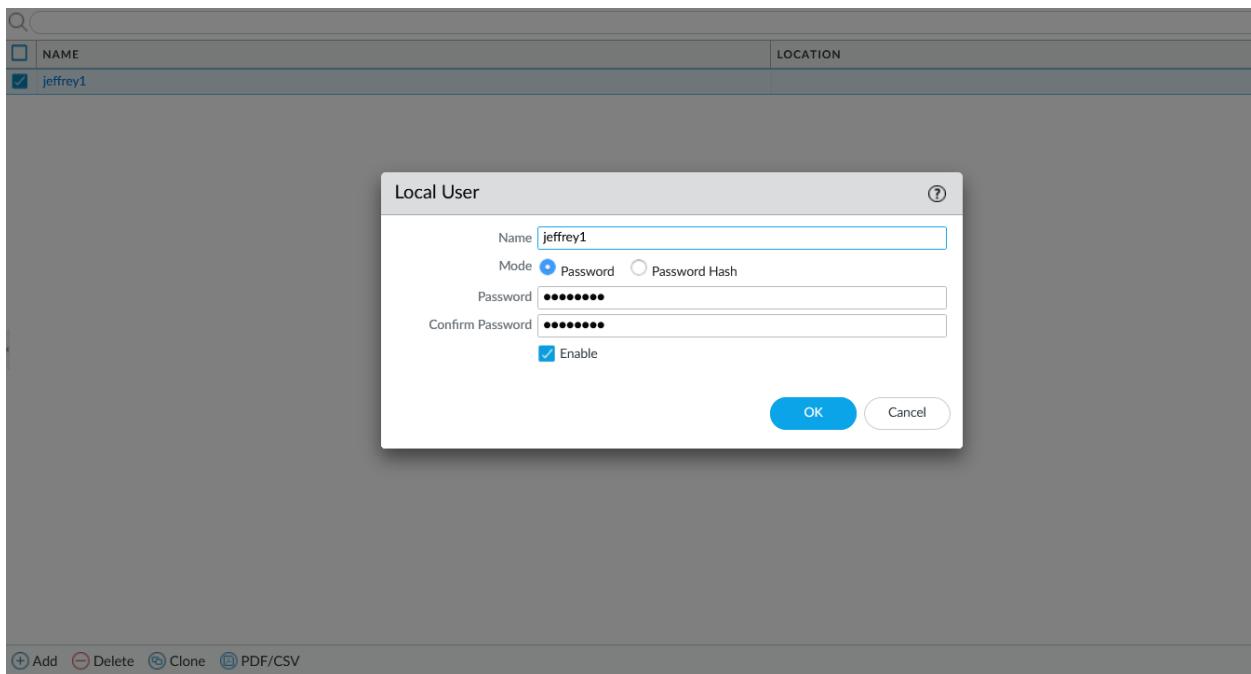
OK

Cancel

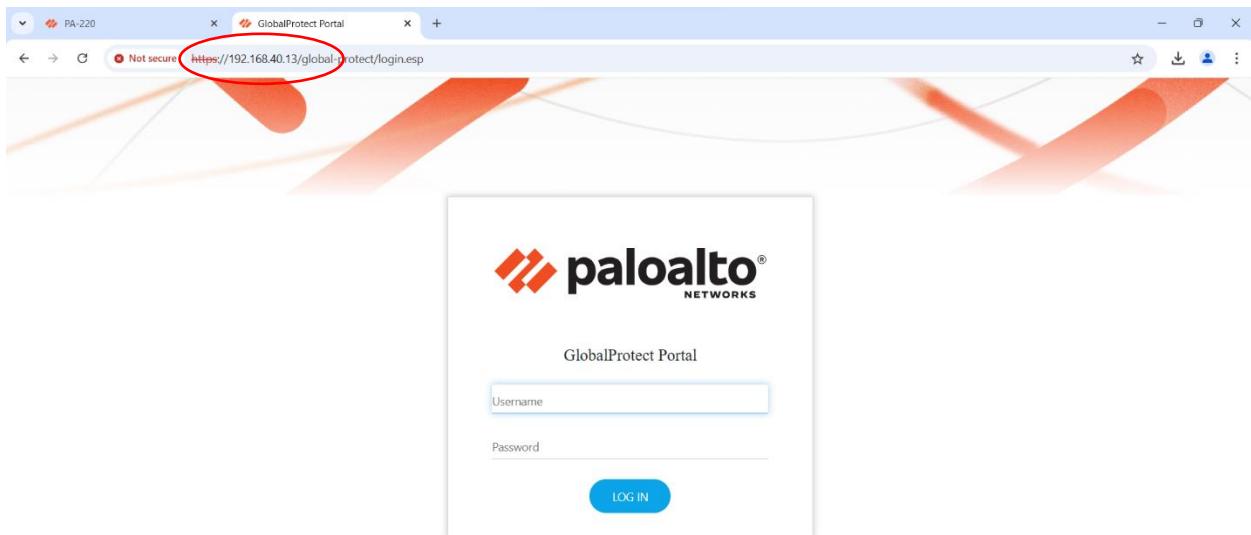
Next, create a local user in Device>Local User Database>Users and give it a password.

The screenshot shows the GlobalProtect Device interface with the following details:

- Left Sidebar:** Contains sections like Response Pages, Log Settings, Server Profiles (with sub-options like SNMP Trap, Syslog, Email, HTTP, Netflow, RADIUS, SCP, TACACS+, LDAP, Kerberos, SAML Identity Provider, Multi Factor Authentication), Local User Database (with sub-options like Users, Groups, Scheduled Log Export, Software, GlobalProtect Client, Dynamic Updates, Plugins, Licenses, Support, Master Key and Diagnostics), and Policy Recommendation (with sub-options like IoT, SaaS).
- Central Area:** A table titled "NAME" with one entry: "jeffrey1". There is also a "LOCATION" column, but no entries are visible.
- Bottom Navigation:** Buttons for "+ Add" and "- Delete" are located at the bottom left. At the bottom right, there are buttons for "OK" and "Cancel".



Finally, test if the Global Protect Portal works by visiting the IP of the DNS server. (192.168.40.13 in my case). If it works, login with the user you just created and download GlobalProtect. It should look like this.



A screenshot of a web browser window. The address bar shows a 'Not secure' warning and the URL <https://192.168.40.13/global-protect/getsoftwarepage.esp?user=...>. The page itself features a red and orange abstract background. At the top center is the **paloalto** logo with 'NETWORKS' underneath. Below the logo, the text 'GlobalProtect Portal' is centered. Underneath this, there are links for downloading GlobalProtect agents for different operating systems: 'Download Windows 32 bit GlobalProtect agent', 'Download Windows 64 bit GlobalProtect agent', and 'Download Mac 32/64 bit GlobalProtect agent'. Below these links is explanatory text: 'Windows 32 bit OS needs to download and install Windows 32 bit GlobalProtect agent.', 'Windows 64 bit OS needs to download and install Windows 64 bit GlobalProtect agent.', and 'Mac OS needs to download and install Mac 32/64 bit GlobalProtect agent.'

Once it's downloaded, VPN into the internal network using the DHCP address.



## Disconnected

Enter the portal address to connect  
and secure access to your applications  
and the internet.

Portal

192.168.40.13

Connect



GlobalProtect



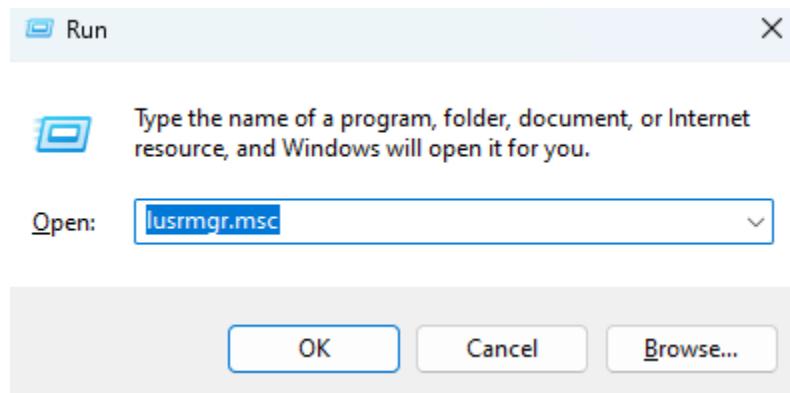
## Connected

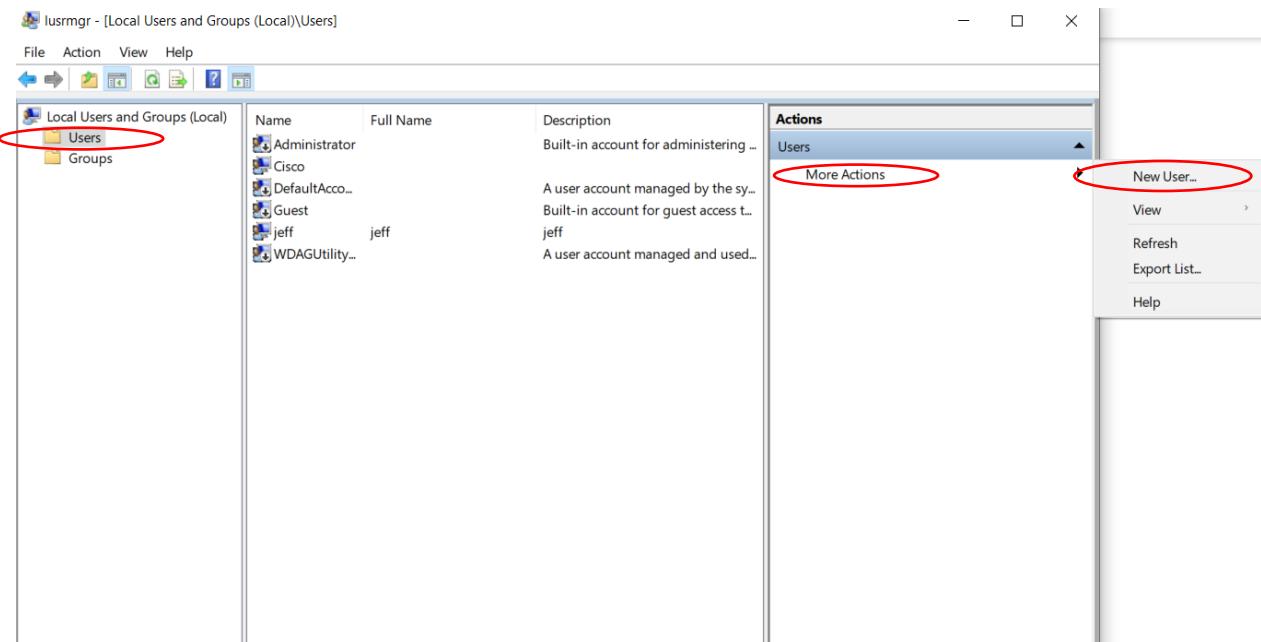
Extn\_GW01

Best Available Gateway

Now, in the device in the internal network, you have to create a user or give an existing user permission to access Remote Desktop.

First, open Run (windows + r on windows, command + space on mac), and type in lusrmgr.msc. This should pop up.





Next, add a user, give it a username and password. You can check off requiring changing password next logon (optional).

New User

User name:

Full name:

Description:

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

---

**Help**      **Create**      **Close**

It should look like this.

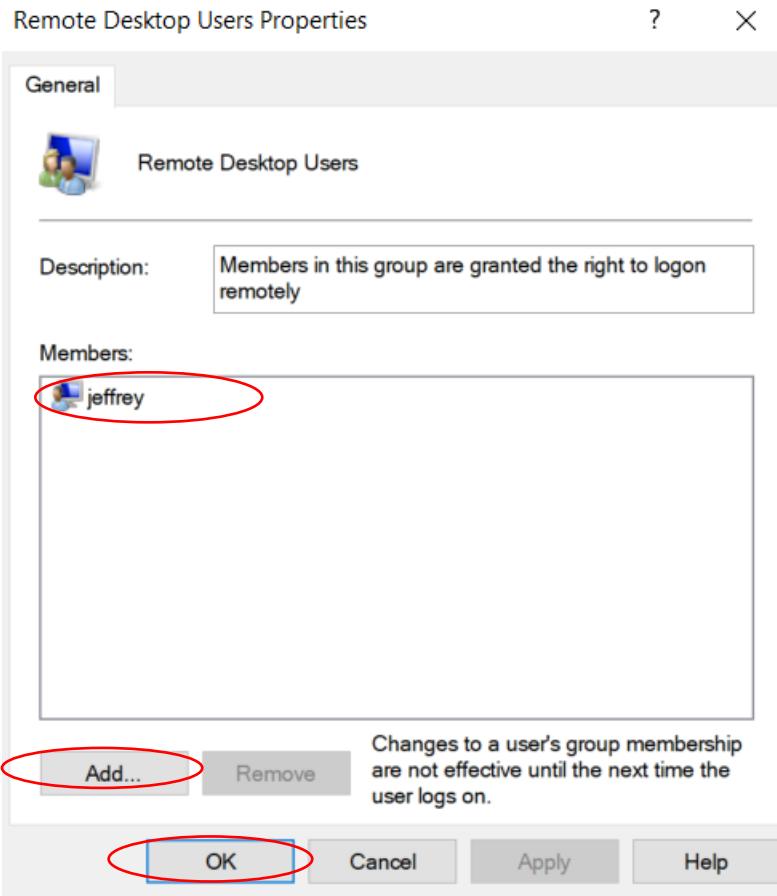
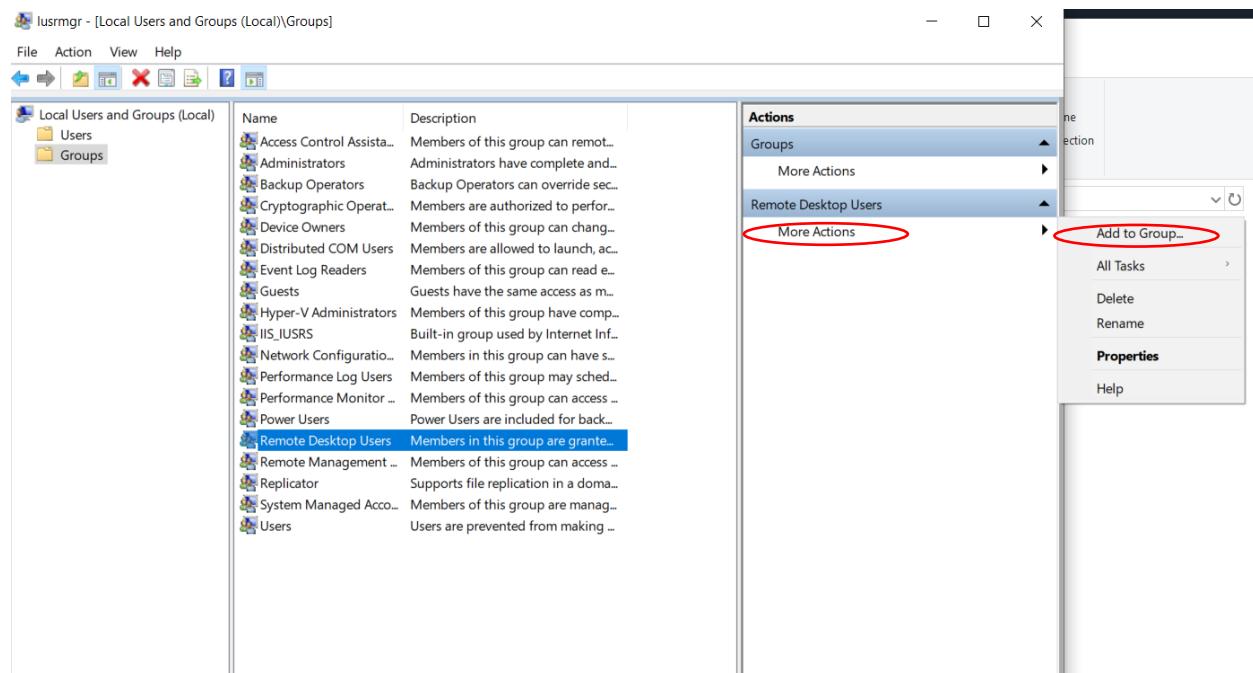
Name	Full Name	Description
Administrator		Built-in account for administering ...
Cisco		
DefaultAcco...		A user account managed by the sy...
Guest		Built-in account for guest access t...
jeff	jeff	jeff
WDAGUtility...		A user account managed and used...

Next, go to groups. There should be a group named Remote Desktop Users.

The screenshot shows the Windows Local Users and Groups snap-in. The left pane displays a tree view with 'Local Users and Groups (Local)' expanded, showing 'Users' and 'Groups'. The 'Groups' node is highlighted with a red circle. The right pane lists a group named 'Remote Desktop Users' with its description 'Members in this group are granted ...' also circled in red. The 'Actions' pane on the right is collapsed.

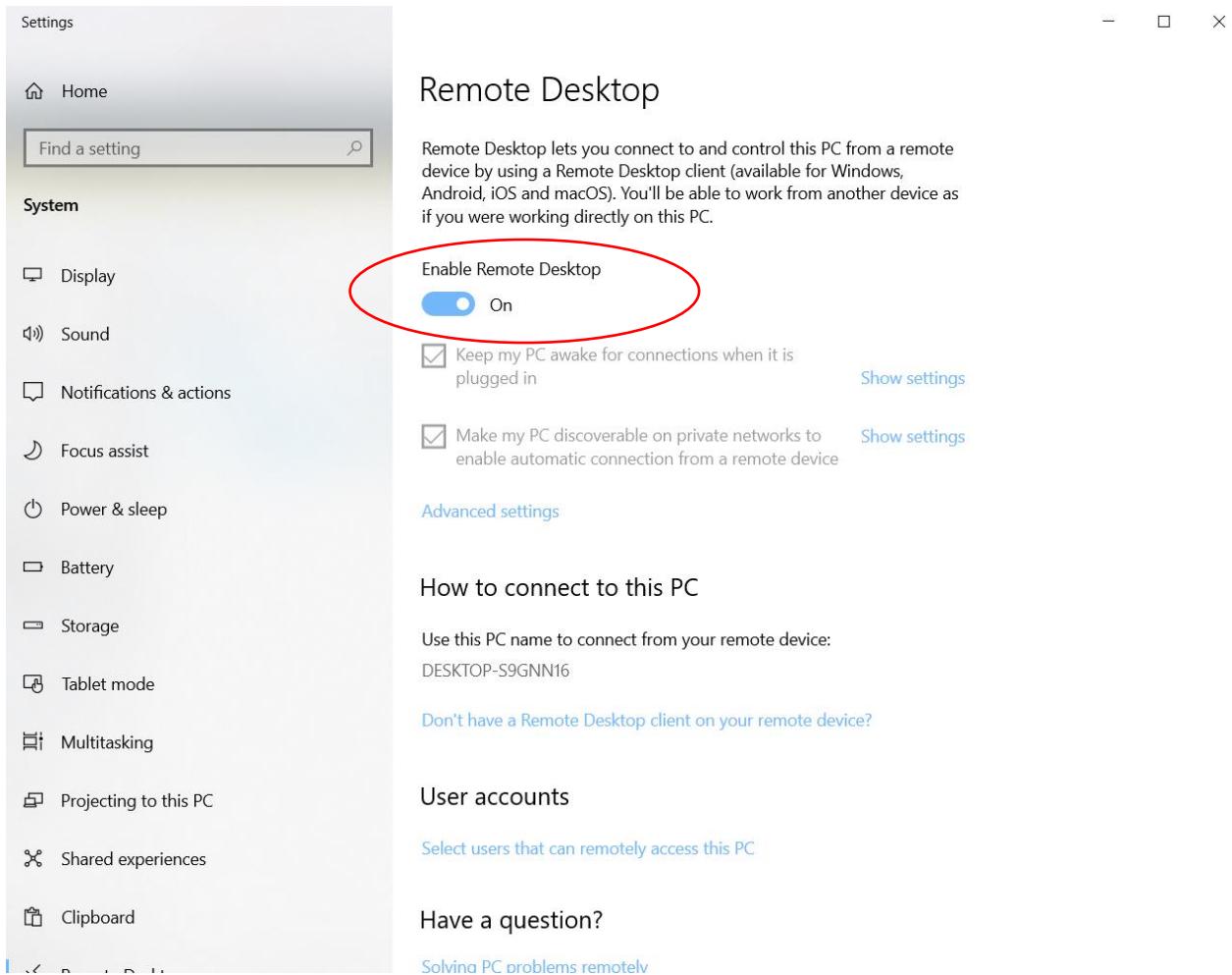
Name	Description
Access Control Assista...	Members of this group can remot...
Administrators	Administrators have complete and...
Backup Operators	Backup Operators can override sec...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, ac...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have comp...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sched...
Performance Monitor ...	Members of this group can access ...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are granted ...
Remote Management ...	Members of this group can access ...
Replicator	Supports file replication in a doma...
System Managed Acco...	Members of this group are manag...
Users	Users are prevented from making ...

Next, add the user you've made, or an existing user, into the group to give them permission.



If you have reset password on next logon enabled, you have to reset the password before you can use the user.

Next, enable Remote Desktop in settings.

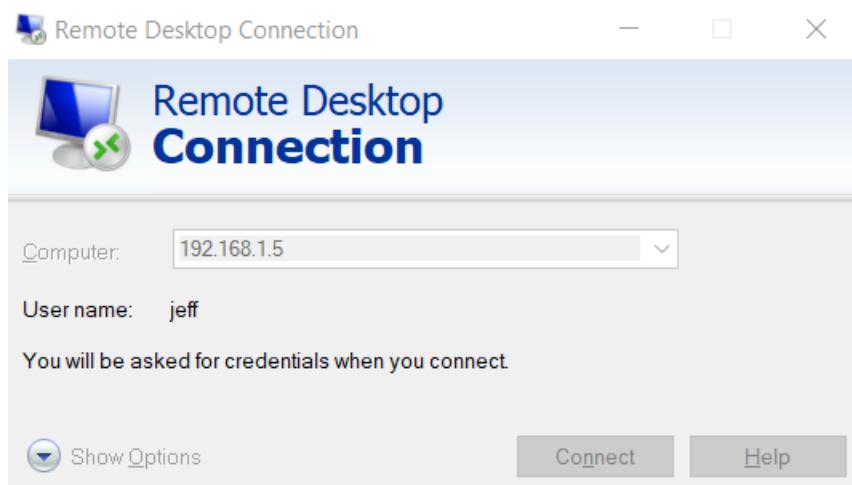


Next, you can use Command Prompt to check the PC's IP address.

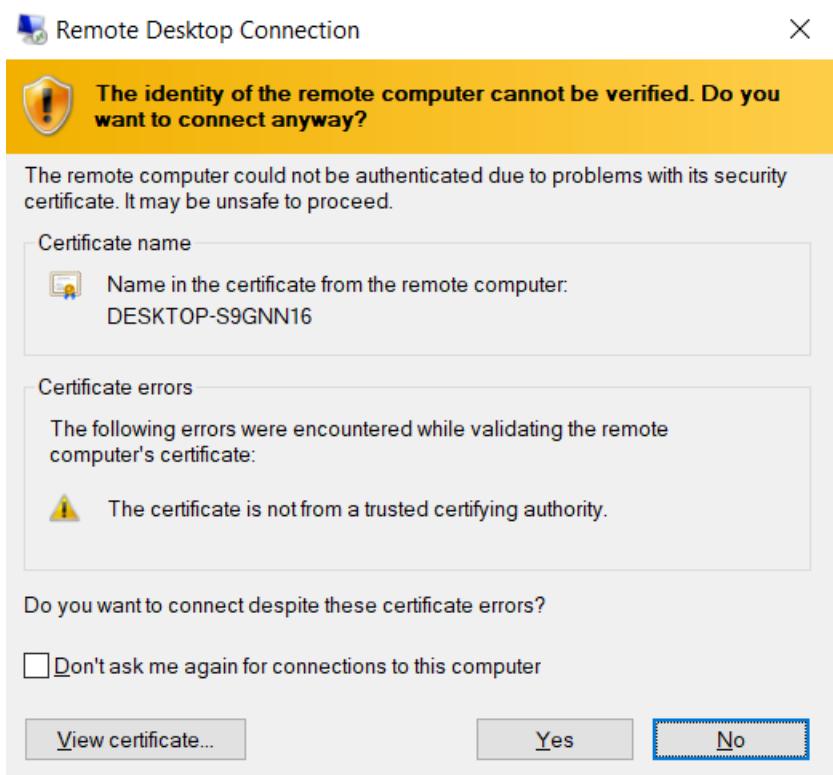
```
Ethernet adapter Ethernet:
```

```
Connection-specific DNS Suffix . . . . .
Description . . . . . : Intel(R) Ethernet Connection (3) I218-LM
Physical Address. . . . . : 54-EE-75-75-94-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, January 6, 2025 3:06:37 PM
Lease Expires . . . . . : Tuesday, January 7, 2025 3:06:36 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 206892661
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
DNS Servers . . . . . : 9.9.9.9
                                         1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

If you've VPN'd into the network, just open up Remote Desktop Connection and connect with the IP of the PC you just found.



If it is successful, you should be prompted with this.



Just click yes, and then it is all set.

## Problems

One of the first problems we encountered was unable to reach the portal despite having the configurations right. One possible issue is that common browsers detect dangerous sites, and the IP of the DNS server gets flagged if you don't use secure hypertext transfer protocol (https). The commit time of the firewall is also time consuming, taking almost 10 minutes every time. When I was debugging, it took a long time to find the bug due to having to commit every time to see the results. If GlobalProtect VPN has trouble recognizing your certificates, there are many details that may contribute to this issue. First, for settings that asks for authentication with user

credentials and/or client certificate, select YES.

Client Authentication

Name	test
OS	Any
Authentication Profile	Jeffrey
<input type="checkbox"/> Automatically retrieve passcode from SoftToken application	
<b>GlobalProtect App Login Screen</b>	
Username Label	Username
Password Label	Password
Authentication Message	Enter login credentials  <small>Authentication message can be up to 256 characters.</small>
Allow Authentication with User Credentials OR Client Certificate	
<b>Yes (User Credentials OR Client Certificate Required)</b> <small>To enforce client certificate authentication, you must also select the certificate profile in the Client Authentication configuration.</small>	
<b>OK</b> <b>Cancel</b>	

Next, it could be some details in the Portal configuration. In the App tab, there are some important details that may turn into an issue. However, it may be hard to tell because all the greyed out.

PA-220

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Commit ▾

Item ▾ X

Configs

Authentications | Config Selection Criteria | Internal | External | **App** | HIP Data Collection

App Configurations

Connect Method	User login (Always-On)
GlobalProtect App Config Refresh	24 [1 - 168]
Allow user to disconnect GlobalProtect App (Always-on mode)	Allow
Display the following reasons to disconnect GlobalProtect (Always-on mode)	
Allow User to Uninstall GlobalProtect App (Windows Only)	Allow
Allow User to Upgrade GlobalProtect App	Allow with Prompt
Allow user to Sign Out from GlobalProtect App	Yes
Allow user to extend GlobalProtect Home Session	No

Welcome Page: None

Disconnect GlobalProtect App (Always-on mode)

Passcode:

Confirm Passcode:

Max Times User Can Disconnect: 0

Disconnect Timeout (min): 0

Uninstall GlobalProtect App

Uninstall Password:

Confirm Uninstall Password:

Mobile Security Manager Settings

Mobile Security Manager:

Enrollment Port: 443

OK Cancel

## Conclusion

In conclusion, GlobalProtect VPN is a powerful tool that can mitigate threats and allow private and secure remote access to users. GlobalProtect VPN uses advanced protocols like IPsec and

AES encrypting algorithms to ensure data is encrypted securely and reliably. It also allows users to remote desktop and bypass physical and geographical limitations. GlobalProtect VPN can benefit a wide range of users, from individual use to corporate organizations.



# FortiGate FortiGate-40F

Setting a Fortinet Firewall as a SOHO router



Jeffrey Yiu Cheung

## Purpose

This lab showcases how to factory reset a FG-40F and how to set up a SOHO router on the Fortinet firewall with an access point.

## Background information

SOHO router, AKA Small Office/Home Office router configurations are designed to support small businesses and small offices, which is a good fit for the Fortinet FG40F firewall's specifications. They are designed with functions that maximize security, and performance for small offices. The Fortinet FG40F has a user-friendly GUI (Graphic User Interface).

In the modern age, most offices are in large buildings and uses enterprise routers, however, SOHO routers can still benefit many occupations, such as lawyers, authors, researchers, consultants, accountants, etc.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. it is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There are useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

A factory reset is a function that erases and resets all configuration to original factory settings. When encountering a device that is already pre-configured, a factory reset allows us to still use a device that is already set with a password and start from a clean environment.

An Access Point (AP) is a device that allows wireless connectivity to users. It is often used to extend WiFi.

WiFi, AKA Wide Fidelity, is a wireless technology that uses radio waves to wirelessly provide internet access. It connects a local area, and is designed for SOHO uses. It provides flexibility as it is wireless and is less equipment oriented as traditional wired connections. However, WiFi can be easily overwhelmed with high traffic, many devices, environment variables...etc, potentially leading to slower speeds.

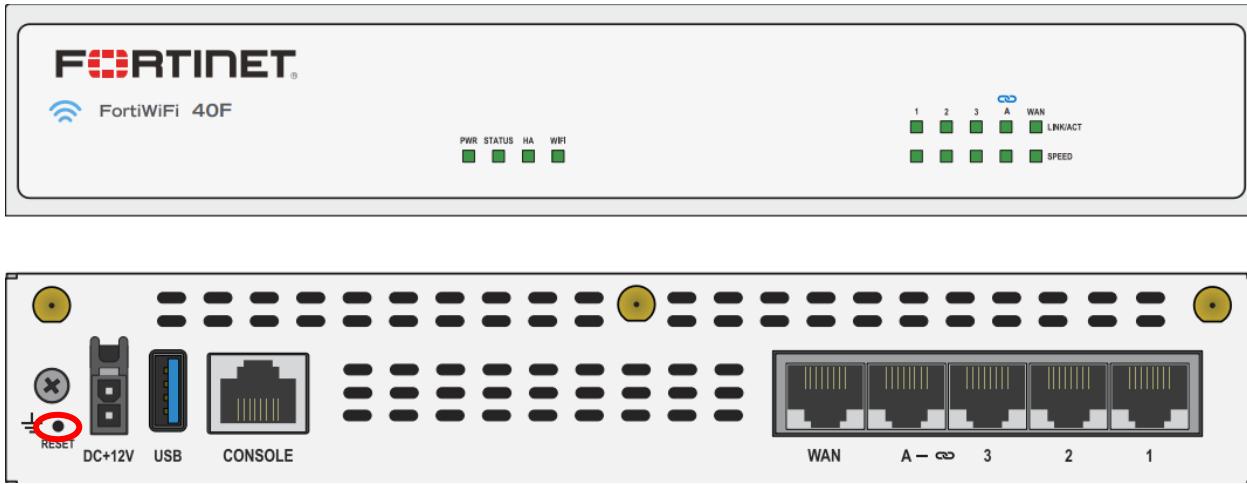
DHCP (Dynamic Host Configuration) is a network protocol that automatically assigns IP addresses to users. Without it, admins would have to manually administer IPs to users for them to connect to the internet, taking more time, effort, and money.

GUI or Graphics Users Interface, is a really good aspect of the Fortinet Firewalls. Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade from other firewalls. GUI is

an underrated and important aspect of firewalls in my opinion. It can have a big impact on efficiency, reduced errors, and improved user experiences.

## Lab summary

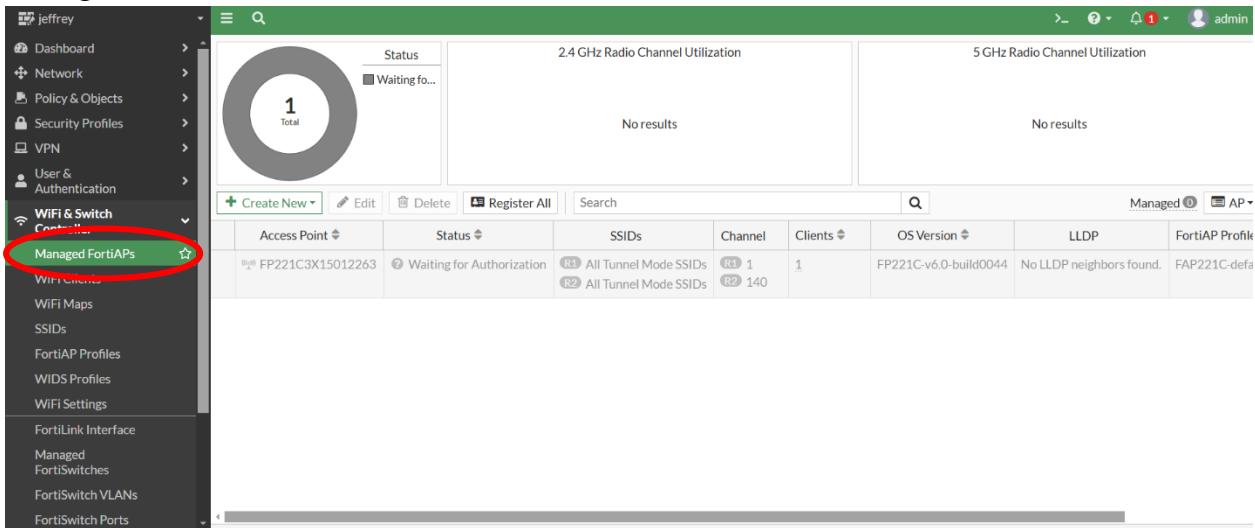
First, to start with a clean configuration, you may want to factory reset first.



To factory reset, you need to power cycle the device first, then press and hold the factory reset button (you're going to need a pin) until the lights on the switch start flashing. Then wait for the reboot.

Once with a new config, you can start configuring SOHO on the firewall.

First, when you plug the access point in, the AP will be offline at first. You have to authorize it in Manage FortiAPs.



Access Point	Status	SSIDs	Channel	Clients	OS Version	LLDP	FortiAP Profile
FP221C3X15012263	Waiting for Authorization	All Tunnel Mode SSIDs All Tunnel Mode SSIDs	R1 1 R2 140	1	FP221C-v6.0-build0044	No LLDP neighbors found.	FAP221C-defa

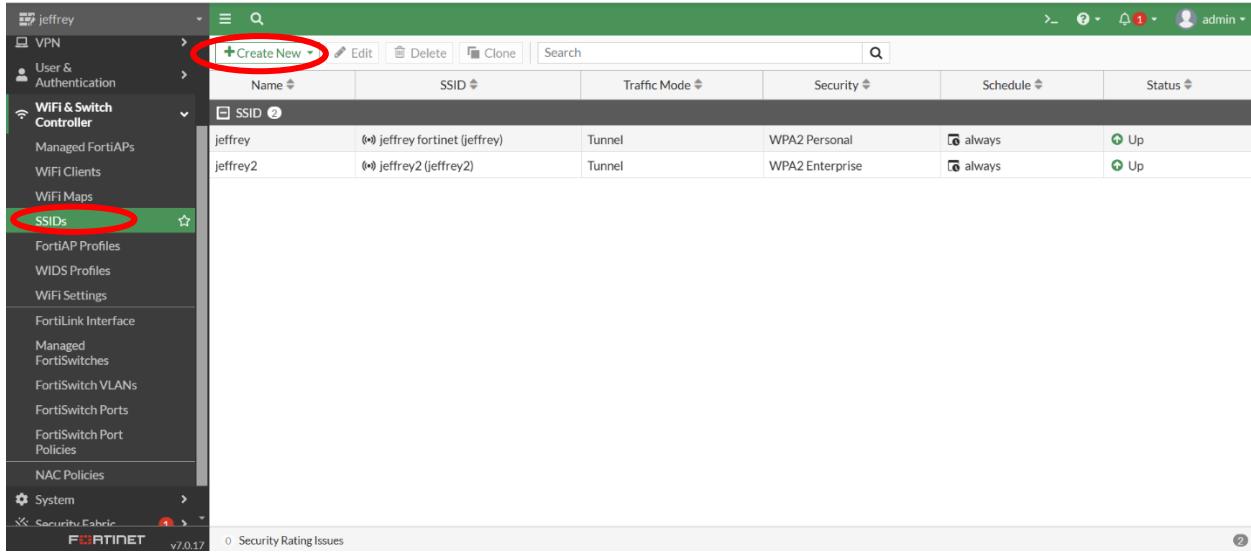
The screenshot shows the FortiManager interface under the 'WIFI & Switch Controller' section. In the left sidebar, 'Managed FortiAPs' is selected. The main area displays a table of APs, with one entry for 'FP221C3X15012263' highlighted. A context menu is open over this entry, with the 'Authorize' option circled in red.

This screenshot shows the 'Edit Managed AP' dialog for the same AP. The 'State' section shows 'Authorized' with a green checkmark, which is circled in red. Other settings like 'Wireless Settings' and 'Override Radio 1' are also visible.

Once authorized, it should turn on. Wait for the lights to flash, and once stable, it will be functional. The interface should look like this after.

The screenshot shows the FortiManager interface again, but now the AP is listed as 'Online' (green status). The radio utilization charts have changed: the 2.4 GHz chart is yellow ('Fair') and the 5 GHz chart is green ('Good'). The table at the bottom reflects these changes, showing 'R1 1' and 'R2 149' clients connected.

Next, in SSIDs, create 2 new SSIDs, one of them should be for enterprise while the other is personal.



The screenshot shows the FortiManager web interface. The left sidebar is titled 'jeffrey' and contains several sections: VPN, User & Authentication, WiFi & Switch Controller, Managed FortiAPs, WiFi Clients, WiFi Maps, and SSIDs. The 'SSIDs' option is highlighted with a green circle. The main content area is titled 'SSID ②' and lists two entries:

Name	SSID	Traffic Mode	Security	Schedule	Status
jeffrey	(*) jeffrey fortinet (jeffrey)	Tunnel	WPA2 Personal	always	Up
jeffrey2	(*) jeffrey2 (jeffrey2)	Tunnel	WPA2 Enterprise	always	Up

In NAME, name it whatever you'd like (it is not what shows up as the WiFi name), and create the desired ranges in netmask (should have enough space for another network due to making another WiFi).

Edit Interface

Name	<input type="text" value="jeffrey2 (jeffrey2)"/>		
Alias	<input type="text"/>		
Type	<input type="radio"/> WiFi SSID		
Traffic mode	<input type="radio"/> <input checked="" type="radio"/> Tunnel		
Address			
IP/Netmask	<input type="text" value="192.168.2.33/255.255.255.240"/>		
Create address object matching subnet	<input checked="" type="checkbox"/>		
Name	<input type="text" value="jeffrey2 address"/>		
Destination	<input type="text" value="192.168.2.33/255.255.255.240"/>		
Secondary IP address	<input type="checkbox"/>		
Administrative Access			
IPv4	<input type="checkbox"/> HTTPS <input type="checkbox"/> FMG-Access <input type="checkbox"/> FTM <input type="checkbox"/> Speed Test	<input type="checkbox"/> HTTP <small>i</small> <input type="checkbox"/> SSH <input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> PING <input type="checkbox"/> SNMP <input type="checkbox"/> Security Fabric <small>i</small> Connection <small>i</small>

The SSID is what the WiFi will actually show up as, and the toggle for broadcast SSID will determine if it shows up by itself or having to search for it. The security mode is what makes it WPAPersonal or WPAEnterprise. The difference is that WPAEnterprise requires a made username and password so that only authorized people are allowed on the network (it requires a username and password on top of the passphrase). The passphrase is the password for the WiFi.

WiFi Settings

SSID **jeffrey fortinet**

Client limit

Broadcast SSID

Beacon advertising  Name  Model  Serial number

Security Mode Settings

Security mode **WPA2 Personal**

Pre-shared Key

Mode  Single  Multiple

Passphrase **••••••••**

Client MAC Address Filtering

RADIUS server

This screenshot shows the WiFi Settings configuration page. The SSID is set to 'jeffrey fortinet'. The security mode is set to 'WPA2 Personal'. The passphrase is '••••••••'. Other options like Client limit, Broadcast SSID, Beacon advertising, and RADIUS server are also visible.

For Enterprise networks, there will be an option for authentication. Select Local and use the default User Group, if there is none, add one with the plus symbol.

WiFi Settings

SSID **jeffrey2**

Client limit

Broadcast SSID

Beacon advertising  Name  Model  Serial number

Security Mode Settings

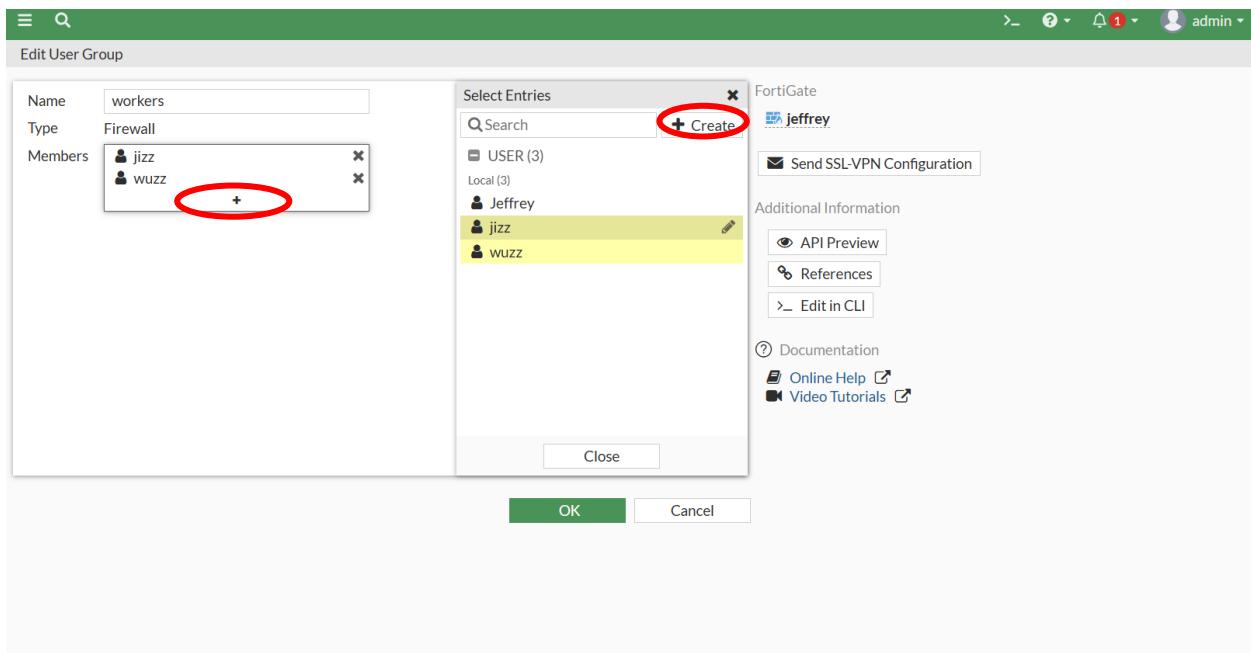
Security mode **WPA2 Enterprise**

Authentication **Local** RADIUS Server

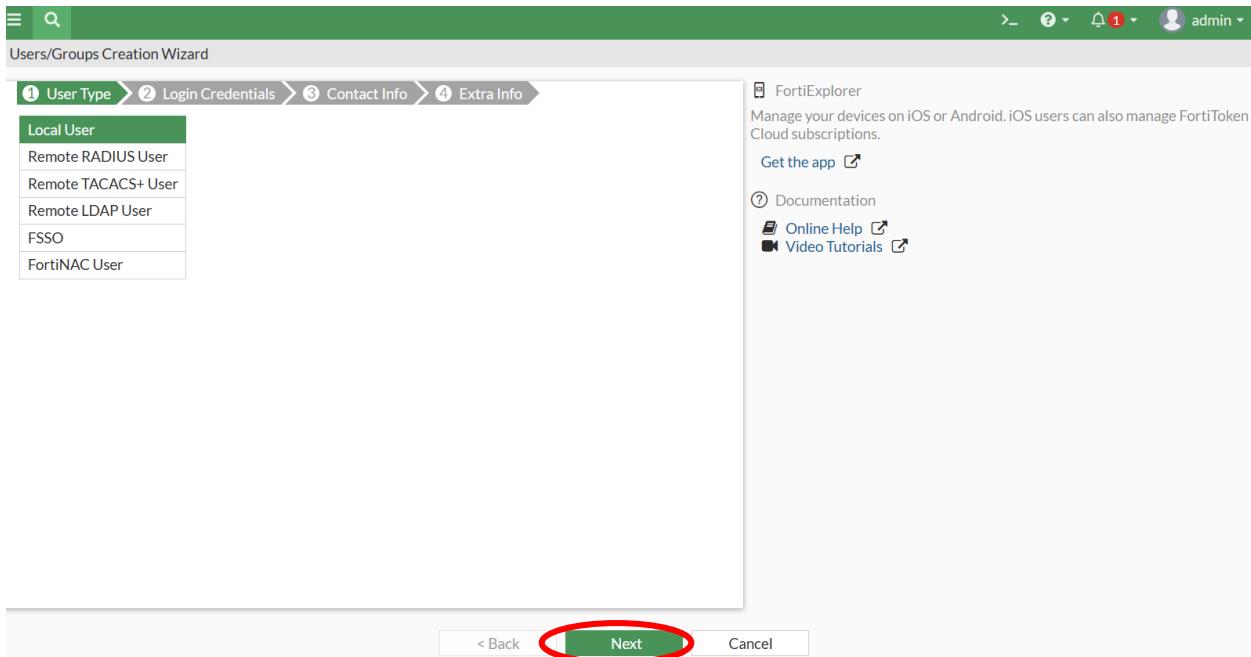
**workers**

This screenshot shows the WiFi Settings configuration page for an enterprise network. The SSID is 'jeffrey2'. The security mode is 'WPA2 Enterprise'. The authentication method is 'Local', and there is a user group named 'workers' listed. Other options like Client limit, Broadcast SSID, Beacon advertising, and RADIUS server are also visible.

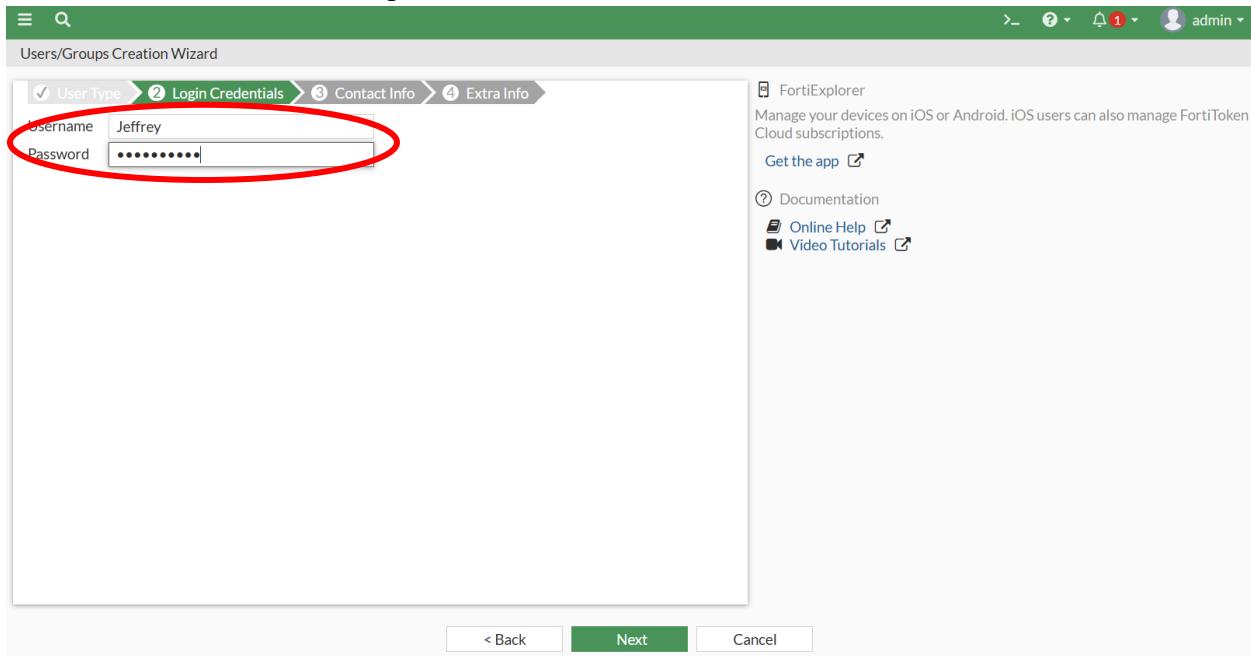
After creating the group, name it and add members to the group.



In the wizard, select local user and click next.

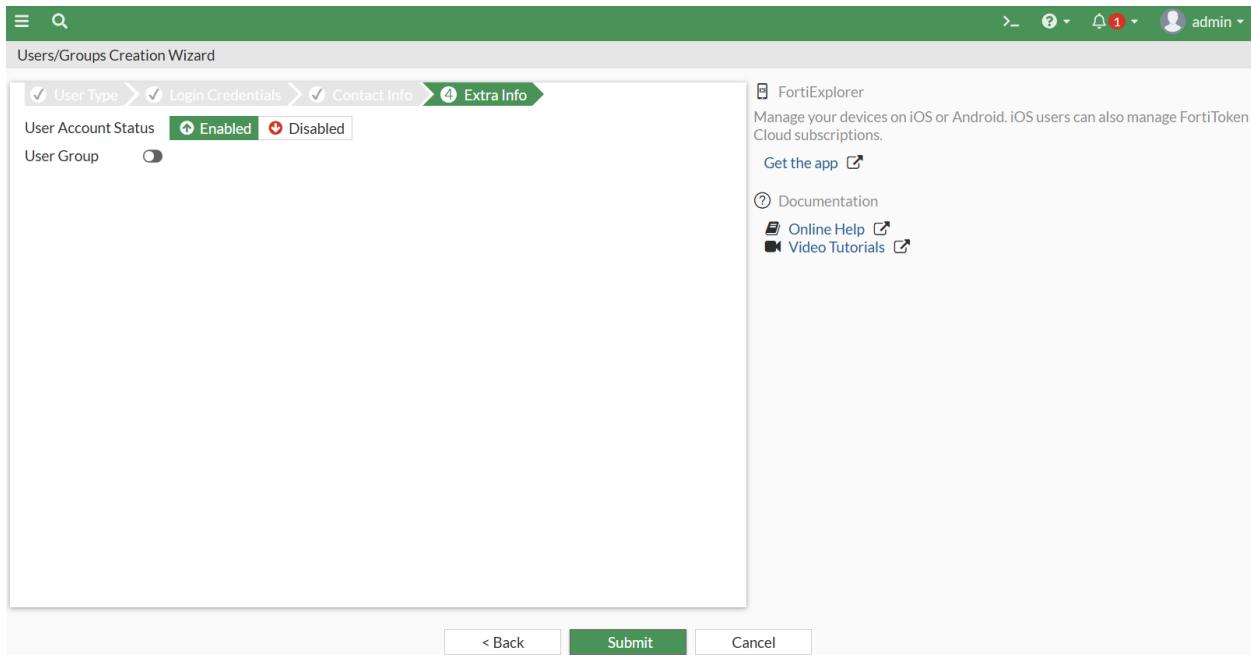


Next, choose a username and password for the user.



The screenshot shows the 'Users/Groups Creation Wizard' interface. The current step is '2 Login Credentials'. The 'Username' field is populated with 'Jeffrey' and the 'Password' field contains a redacted password. A red oval highlights both the 'Username' and 'Password' fields. At the bottom, there are '< Back', 'Next', and 'Cancel' buttons.

Contact information is optional, and finally, enable the user.



The screenshot shows the 'Users/Groups Creation Wizard' interface. The current step is '4 Extra Info'. The 'User Account Status' is set to 'Enabled' (green button), while 'Disabled' is shown in red. Below it, there is a 'User Group' section with a radio button. At the bottom, there are '< Back', 'Submit', and 'Cancel' buttons.

You can also edit the users and groups in its own tab.

Groups			
Group Name	Group Type	Members	Ref.
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)		1
workers	Firewall	wuzz	1

Users					
Name	Type	Two-factor Authentication	Groups	Status	Ref.
jizz	LOCAL	✗		Enabled	0
wuzz	LOCAL	✗	workers	Enabled	1

After creating the users, toggle on DHCP Server, and it will automatically assign IPs to those on your network. it should automatically fill the address range.

**DHCP Server**

DHCP status	<input checked="" type="button"/> Enabled <input type="button"/> Disabled
Address range	192.168.2.2-192.168.2.254  <input type="button"/>
Netmask	255.255.255.0
Default gateway	<input checked="" type="button"/> Same as Interface IP <input type="button"/> Specify
DNS server	<input checked="" type="button"/> Same as System DNS <input type="button"/> Same as Interface IP <input type="button"/> Specify
Lease time <small>i</small>	<input type="text"/> 604800 second(s)
<input type="button"/> Advanced	

---

**Network**

Device detection i

DHCP Server

DHCP status	<span>Enabled</span>	<span>Disabled</span>
Address range	192.168.2.34-192.168.2.46	
	<span>+</span>	
Netmask	255.255.255.240	
Default gateway	<span>Same as Interface IP</span>	<span>Specify</span>
DNS server	<span>Same as System DNS</span>	<span>Same as Interface IP</span>
Lease time	<span>i</span>	<span>604800 second(s)</span>

+ Advanced

## Network

Device detection  

After finishing the WiFi SSID, move on to firewall policies. You need to make multiple policies, from your SSIDs to your WAN, and from your WAN to your SSIDs.

**Edit Policy**

Name	fortinet to wan
Incoming Interface	jeffrey fortinet (jeffrey)
Outgoing Interface	wan
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY
Inspection Mode	Flow-based
Firewall / Network Options	
NAT	<input checked="" type="radio"/>
IP Pool Configuration	<input checked="" type="radio"/> Use Outgoing Interface Address <input type="radio"/> Use Dynamic IP Pool
Preserve Source Port	<input type="radio"/>
Protocol Options	PROT default

**OK**   **Cancel**

**Edit Interface**

Name	jeffrey fortinet (jeffrey)		
Alias			
Type	WiFi SSID		
Traffic mode	<input checked="" type="radio"/> Tunnel		
Address			
IP/Netmask	192.168.2.2/255.255.255.224		
Create address object matching subnet	<input checked="" type="radio"/>		
Name	jeffrey address		
Destination	192.168.2.2/255.255.255.224		
Secondary IP address	<input type="radio"/>		
Administrative Access			
IPv4	<input type="checkbox"/> HTTPS <input type="checkbox"/> FMG-Access <input type="checkbox"/> FTM <input type="checkbox"/> Speed Test	<input type="checkbox"/> HTTP <small>i</small> <input type="checkbox"/> SSH <input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> PING <input type="checkbox"/> SNMP <input type="checkbox"/> Security Fabric Connection <small>i</small>

FortiGate  
jeffrey

Status Up

MAC address 00:ff:3c:4d:bb:59

Additional Information

API Preview  
 References  
 Edit in CLI

() SSID

Guides

FortiAP-S and FortiAP-U Bridge Mode Security Profiles i

Documentation

Online Help i  
 Video Tutorials i

## **Problems**

One problem we encountered when doing this lab was our switch did not support the AP. Thankfully, we had another PoE switch and it worked. Another thing is, the AP may not be compatible with some Fortinet versions, like some of the new versions.

## **Conclusion**

In conclusion, Fortinet firewall is a great firewall that comes with many options, easy to understand GUI, is small and compact, and would be a perfect fit for those working in SOHO settings.



# FortiGate FortiGate-40F

**Setting up remote access with Fortigate-40F**



**Jeffrey Yiu Cheung**

## **Purpose**

The purpose of this lab is to demonstrate a way to set-up remote access/desktop for users with FortiGate-40F and FortiClient.

## **Background information**

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Fortinet designed and offers its own VPN to its customers.

Remote Access technology enables users to connect to a computer, network, or system regardless of geographical barriers. This technology can enable the ease of accessing files, managing systems, and running applications. While not all businesses may benefit from this, this technology is a staple to telecommuters (those who work from home), business travels, or those needing to work offsite due to distance or other barriers. While this technology is convenient, it requires a lot of security to maintain.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. It is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

GUI or Graphics Users Interface, is a really nice aspect of the Fortinet Firewalls. Compared to other firewalls like for example the Palo Alto firewalls' GUI, Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade. GUI is an underrated and important aspect of firewalls and their configurability. It can have a big impact on efficiency, reduced errors, and improved user experiences.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

SSL, or Secure Sockets Layer, is a protocol that encrypts data through the application layer. Compared to IPsec, or internet protocol security, it is easier to set up, and completes the same goal if users use web-based applications. However, unlike IPsec, it does not provide end-to-end

encryption for all network traffic and is less broad. While SSL VPN is good for this demonstration, one should consider IPsec to be the better option.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

FortiClient is a software designed by Fortinet to ensure secure remote access, ease of access, end-point connection and protection. It also allows secure remote connections to the internal network. It creates a tunnel between the user and the destined network and encrypts the data with SSL/TLS which passes through.

## Lab summary

First, configure the SSL-VPN settings in the VPN tab, enable it and set it to listen on your WAN interface. Then, since the default port is 443 (HTTPS) and may interfere with some configuration, you can change the port, in my example I chose port 4433.

You can also make a Server Certificate for more safety, but in my case, I just use the default Fortinet certificate.

The screenshot shows the FortiManager interface with the 'SSL-VPN Settings' tab selected. In the main pane, the 'Connection Settings' section is configured with 'Enable SSL-VPN' checked and 'Listen on Interface(s)' set to 'wan'. A red circle highlights these settings. Below them, 'Listen on Port' is set to '4433'. A yellow warning box notes that 'Web mode access will be listening at https://192.168.40.169:4433'. The right sidebar contains various setup guides and troubleshooting links.

Afterwards, everything should be default in Tunnel Mode Client Settings. In Authentication/Portal Mapping, you can give different users different types of access. Tunnel-access gives access to secure an encrypted tunnel between a device and a remote network. Web-access gives access via a web-portal. Full-access gives full access to users, like using files, websites...

The screenshot shows two configuration sections. The top section is 'Tunnel Mode Client Settings' with tabs for 'Address Range' (selected), 'Automatically assign addresses' (highlighted in green), and 'Specify custom IP ranges'. A note below says 'Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210'. The bottom section is 'Authentication/Portal Mapping' with tabs for 'DNS Server' (selected) and 'Specify'. Under 'Specify', there is a checkbox for 'Specify WINS Servers' which is checked. The main table lists users and their access types:

Users/Groups	Portal
guest	tunnel-access
jeffrey	
guest	web-access
jeffrey	
guest	full-access
jeffrey	
All Other Users/Groups	jeffreySSL

A red circle highlights the 'Create New' button in the top bar of the mapping table.

You can configure the types of access or edit existing portals in SSL-VPN Portals. I have created one such and named it jeffreySSL. You can also configure users and their groups.

The screenshot shows the Fortinet FortiGate management interface. On the left, a navigation sidebar lists various settings like Dashboard, Network, Policy & Objects, VPN, and SSL-VPN Portals. Under SSL-VPN Portals, 'SSL-VPN Settings' is selected. In the main content area, there's a table titled 'SSL-VPN Portals' with columns for Name, Tunnel Mode, and Web Mode. The table lists four entries: full-access (Enabled), jeffreySSL (Enabled), tunnel-access (Enabled), and web-access (Disabled). At the top of this table, there's a search bar and a '+Create New' button, which is circled in red.

Next, create the Firewall policies so the different interfaces can communicate with each other.

For the first one, create a firewall policy from LAN to the SSL-VPN tunnel interface, and one from SSL-VPN to LAN.

This screenshot shows the 'Edit Policy' dialog for a new firewall rule. The left sidebar has 'Policy & Objects' selected, with 'Firewall Policy' highlighted by a red circle. The main dialog shows a rule named 'jeffrey\_SSL\_TO'. The 'Incoming Interface' is set to 'lan' (circled in red) and the 'Outgoing Interface' is set to 'SSL-VPN tunnel interface (sslvpn)'. The 'Source' and 'Destination' fields are both set to 'all'. The 'Schedule' is 'always' and the 'Service' is 'ALL'. The 'Action' is set to 'ACCEPT'. Below the dialog, there's a 'Statistics (since last reset)' section with details like ID, Last used, First used, Active sessions, Hit count, Total bytes, and Current bandwidth. To the right, there's a chart titled 'Last 7 Days' showing Bytes over time, with categories for inTurbo, SPU, and Software. At the bottom of the dialog are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Edit Policy' dialog box. The 'Name' field is set to 'jeff\_SSL'. The 'Incoming Interface' dropdown is circled in red and shows 'SSL-VPN tunnel interface (ssl.root)'. The 'Outgoing Interface' dropdown shows 'lan'. Other settings include 'Source' and 'Destination' both set to 'any', 'Schedule' set to 'always', 'Service' set to 'ALL', and 'Action' set to 'ACCEPT'. The 'Inspection Mode' is 'Flow-based'. On the right, there's a 'Statistics (since last reset)' section and a 'Last 7 Days Bytes' chart.

You'd also need firewall policies from LAN to WAN and WAN to LAN if you don't have them already.

The screenshot shows the 'Edit Policy' dialog box. The 'Name' field is set to 'lan'. The 'Incoming Interface' dropdown is circled in red and shows 'lan'. The 'Outgoing Interface' dropdown shows 'wan'. Other settings include 'Source' and 'Destination' both set to 'any', 'Schedule' set to 'always', 'Service' set to 'ALL', and 'Action' set to 'ACCEPT'. The 'Inspection Mode' is 'Flow-based'. On the right, there's a 'Statistics (since last reset)' section and a 'Last 7 Days Bytes' chart.

**Edit Policy**

**Name:** jeffrey3

**Incoming Interface:** wan

**Outgoing Interface:** lan (highlighted by a red circle)

**Source:** all

**Destination:** all

**Schedule:** always

**Service:** ALL

**Action:** ✓ ACCEPT   ✘ DENY

**Inspection Mode:** Flow-based   Proxy-based

**Firewall / Network Options:**

- NAT
- IP Pool Configuration: Use Outgoing Interface Address   Use Dynamic IP Pool
- Preserve Source Port
- Protocol Options: PRO default

**Security Profiles:**

**Statistics (since last reset):**

ID	9
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B
Current bandwidth	0 bps

**Additional Information:**

- API Preview
- Edit in CLI
- Documentation
- Online Help
- Video Tutorials
- Consolidated Policy Configuration

Afterwards, you should be set to use the Fortinet Firewall via SSL-VPN. Download FortiClient from Fortinet's website. Select remote access.

**File View Help**

**FortiClient - Zero Trust Fabric Agent**

**FortiClient - Disconnected**  
Zero Trust Fabric Agent

**Register with Zero Trust Fabric**  
Enter Server address or Invitation code:

Server address or Invitation code  Connect

**ZERO TRUST TELEMETRY**

**REMOTE ACCESS**

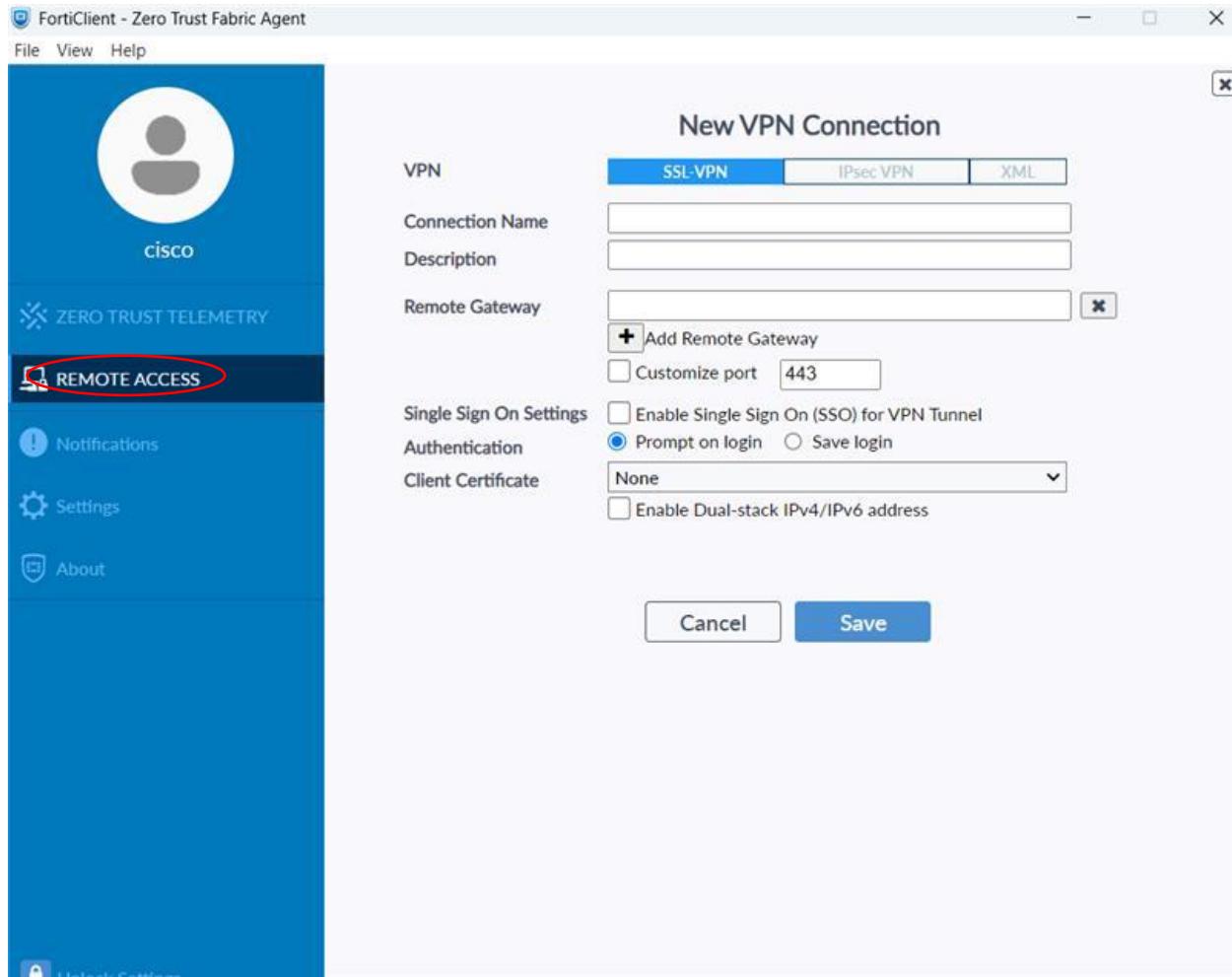
**Notifications**

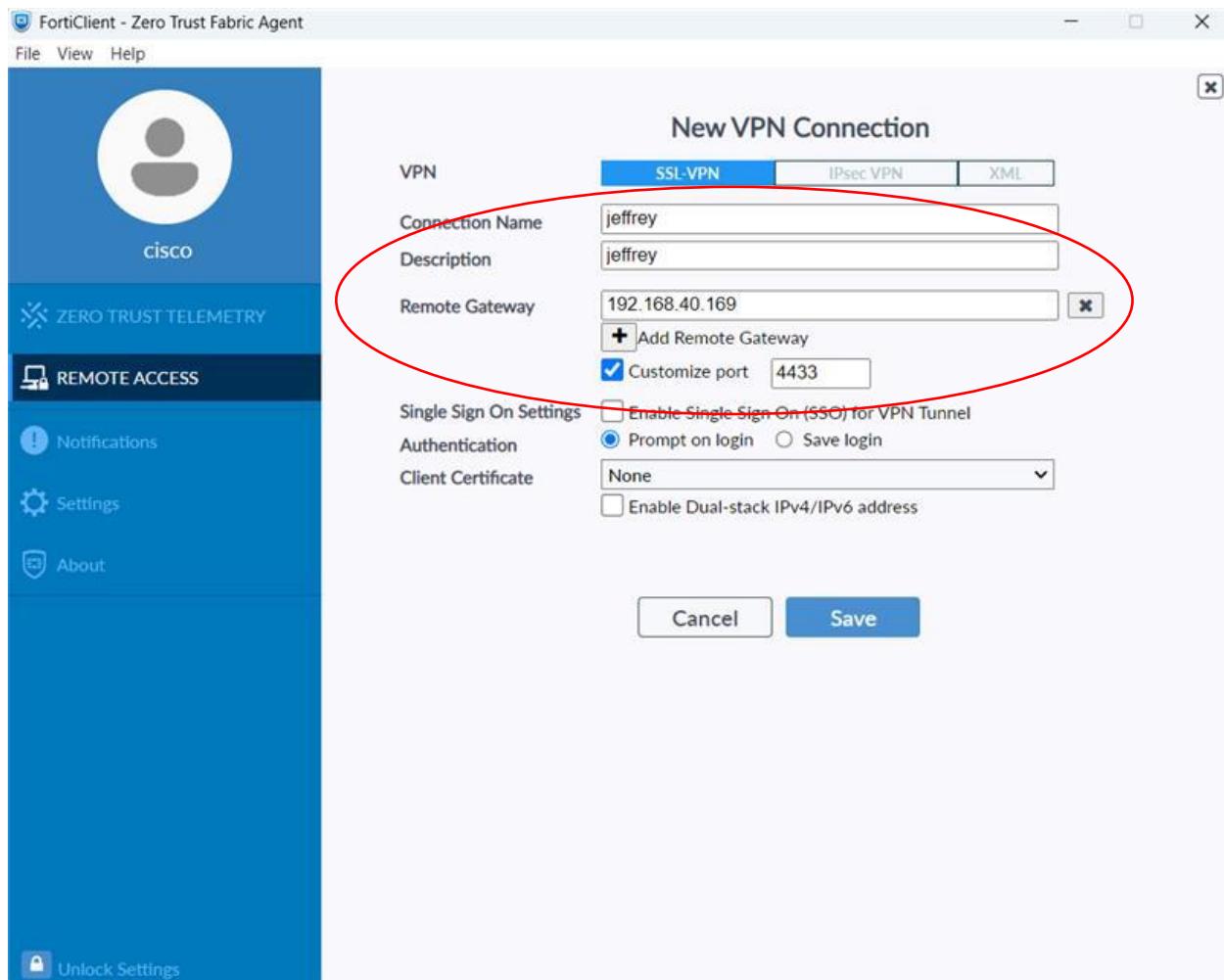
**Settings**

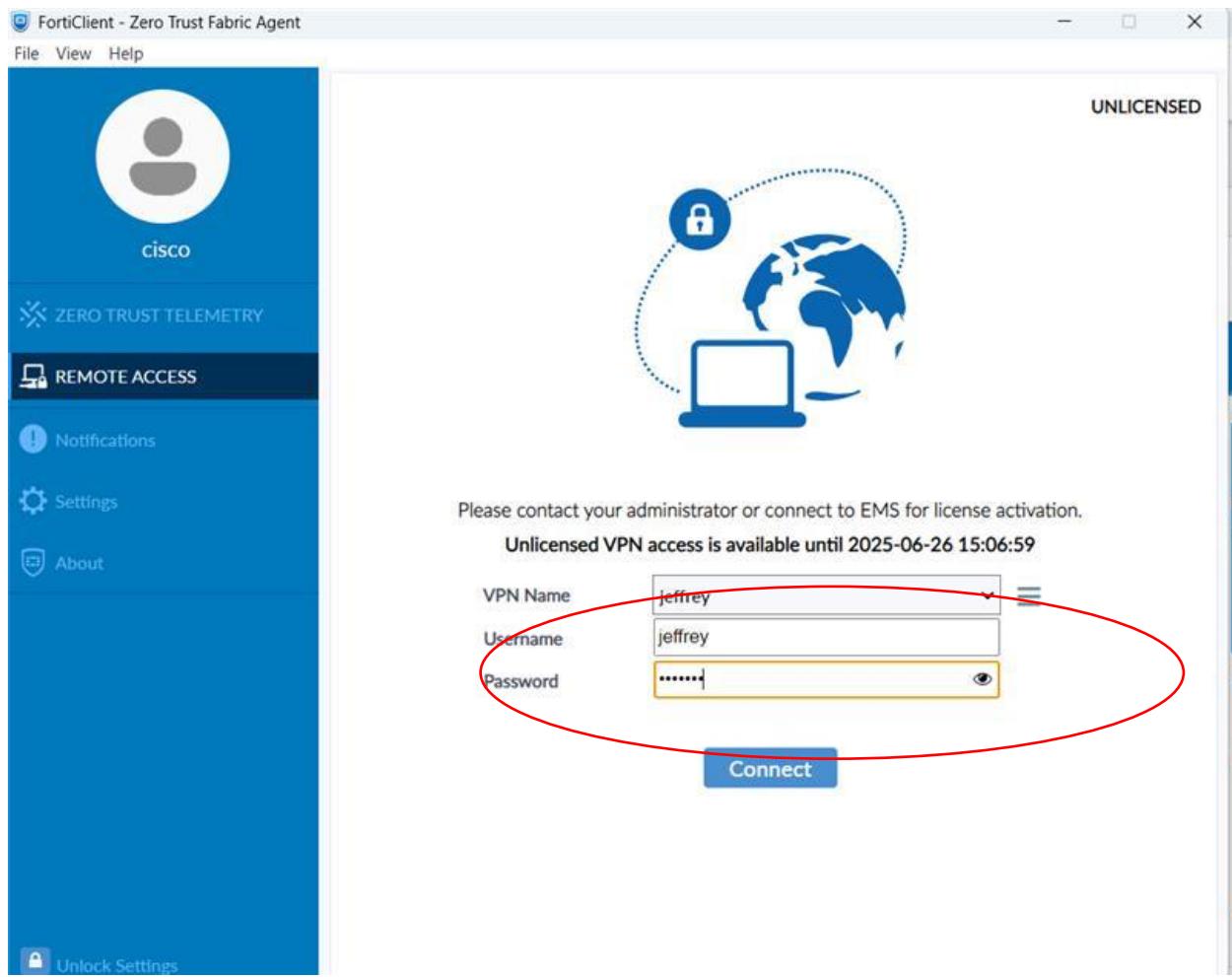
**About**

**Unlock Settings**

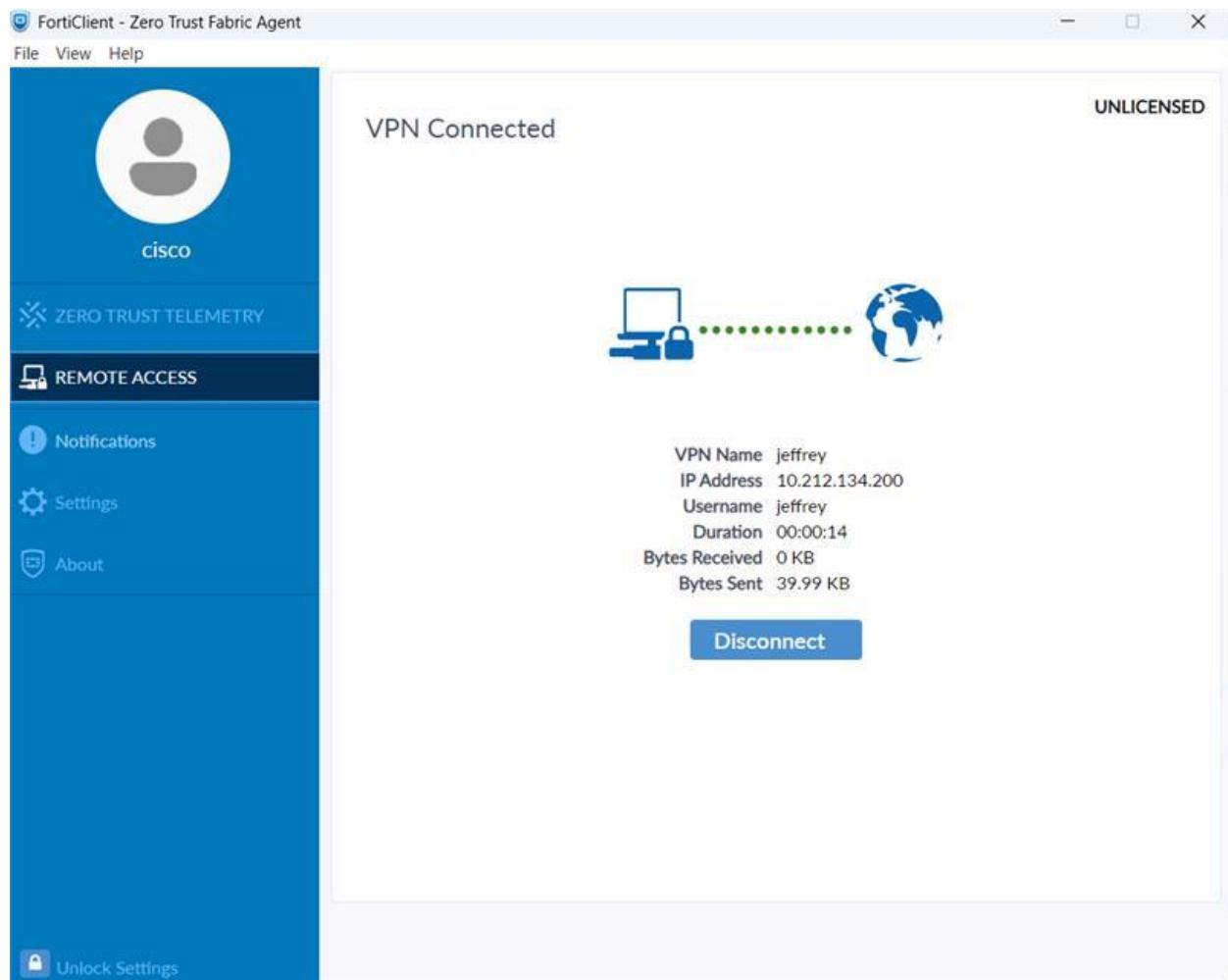
select SSL-VPN, then write whatever in Connection Name and description. In Remote Gateway, put in the IP of your LAN interface. Also, if you configured a different port in SSL-VPN settings, select customize port and the port number you chose.





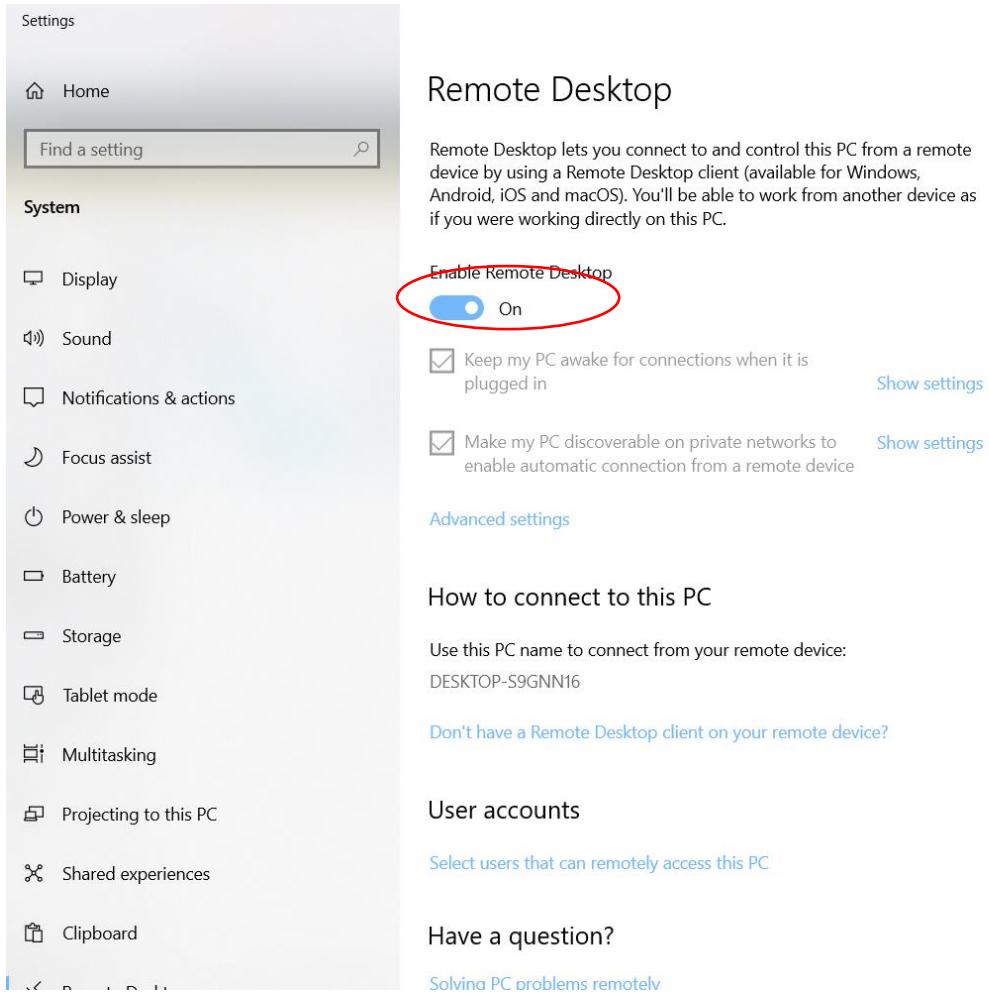


Use the username and password you set for the users enabled for access. Afterwards, it should be set to be connected.



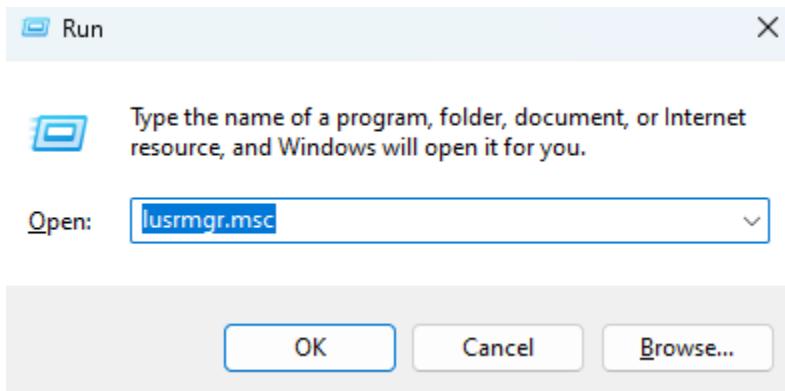
After this, it should be all set and ready to go for remote access.

To successfully remote access, you need to first turn on Remote Access in computer's settings.

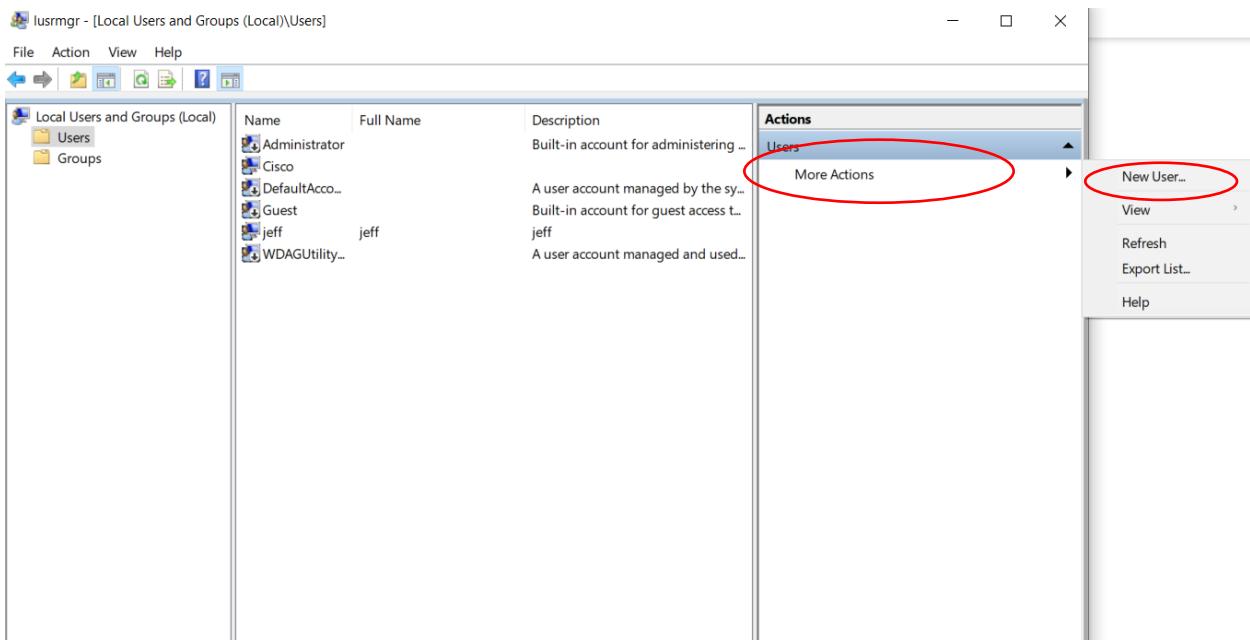


Now, for the device in the internal network, or the device in the network that you want to connect to, create a user or give an existing user permission to access Remote Desktop.

First, open Run (or Windows + r on windows, command + space on mac) and type in lusrmgr.msc.



This should pop up. Select Users and add new user (if necessary).



Next, add a user, give it a username and password (if necessary). You can check off requiring changing password next logon (optional).

New User

User name:

Full name:

Description:

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

---

**Help** **Create** **Close**

A screenshot of the 'New User' dialog box. It contains fields for 'User name', 'Full name', and 'Description'. Below these are fields for 'Password' and 'Confirm password'. A group of checkboxes at the bottom includes 'User must change password at next logon' (which is checked), 'User cannot change password', 'Password never expires', and 'Account is disabled'. At the bottom are 'Help', 'Create', and 'Close' buttons.

It should look like this.

Name	Full Name	Description
Administrator		Built-in account for administering ...
Cisco		
DefaultAcco...		A user account managed by the sy...
Guest		Built-in account for guest access t...
jeff	jeff	jeff
WDAGUtility...		A user account managed and used...

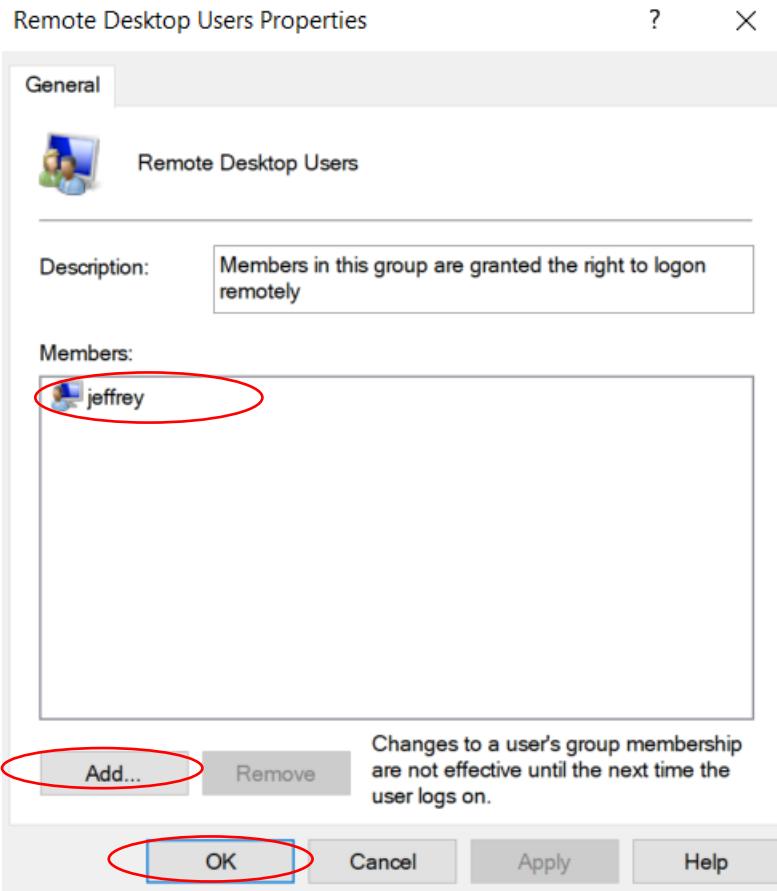
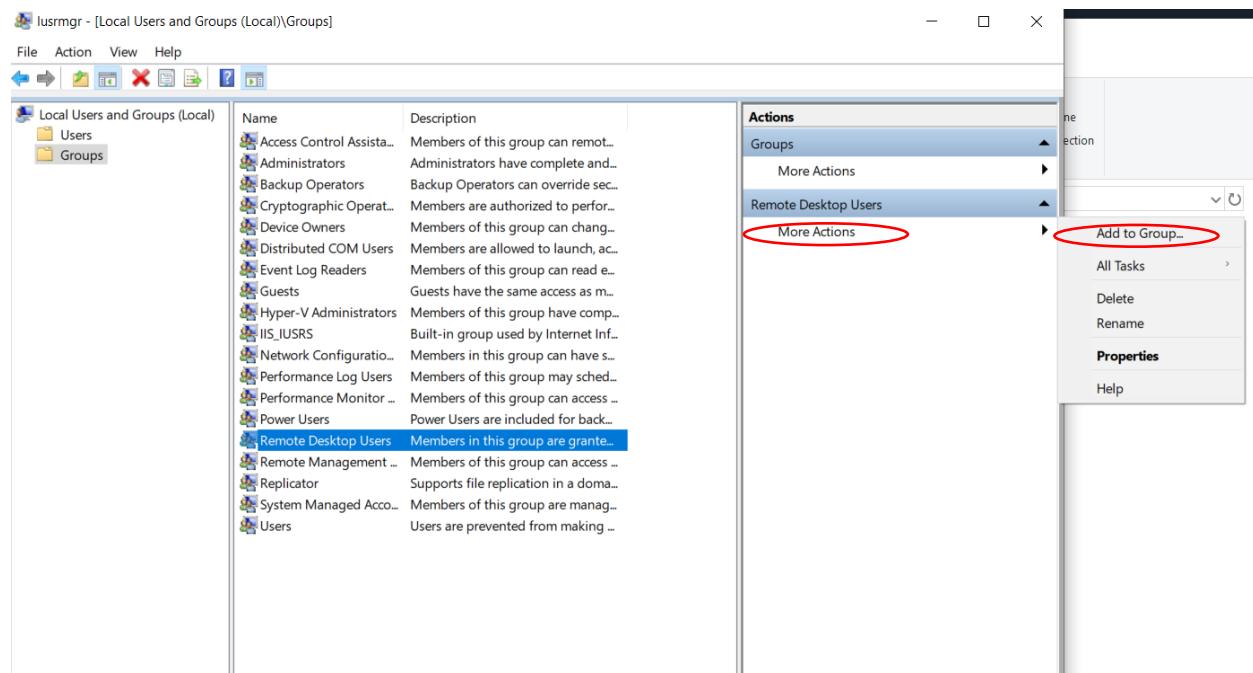
Next, go to groups. There should be a group named Remote Desktop Users.

The screenshot shows the Windows Local Users and Groups snap-in. The left pane displays a tree view with 'Local Users and Groups (Local)' expanded, showing 'Users' and 'Groups'. The 'Groups' node is highlighted with a red oval. The right pane lists the available groups:

Name	Description
Access Control Assista...	Members of this group can remot...
Administrators	Administrators have complete and...
Backup Operators	Backup Operators can override sec...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, ac...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have comp...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sched...
Performance Monitor ...	Members of this group can access ...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management ...	Members of this group can access ...
Replicator	Supports file replication in a doma...
System Managed Acco...	Members of this group are manag...
Users	Users are prevented from making ...

The 'Remote Desktop Users' group is highlighted with a blue oval. The 'Actions' pane on the right shows 'Groups' selected under 'More Actions'.

Next, add the user you've made, or an existing user, into the group to give them permission.



If you have reset password on next logon enabled, you have to reset the password before you can use the user.

Next, using the other device, remote access into the desired device via Remote Desktop Connection.

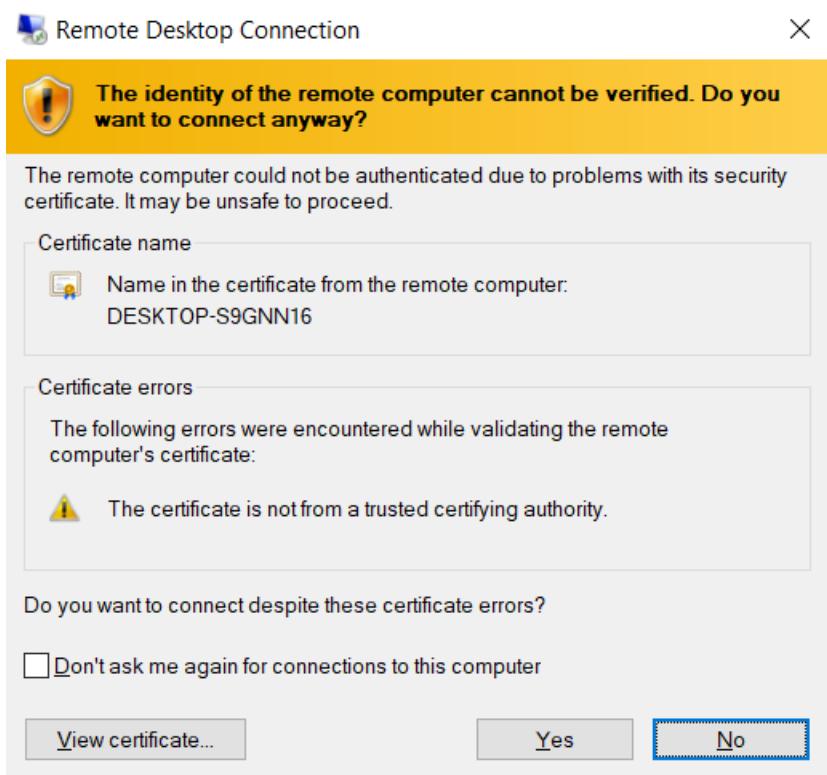


In computer, you will need to input the desired device's IP address. This can be found in Command Prompt with the command “ipconfig /all”.

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . :
Description . . . . . : Intel(R) Ethernet Connection (3) I218-LM
Physical Address. . . . . : 54-EE-75-75-94-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, January 6, 2025 3:06:37 PM
Lease Expires . . . . . : Tuesday, January 7, 2025 3:06:36 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 206892661
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
DNS Servers . . . . . : 9.9.9.9
                           1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

If successful, you should be prompted with this:



Just click Yes, and then you're all set.

## Problems

This is a fairly straightforward lab that shouldn't come with any hitches. However, there are some minor tweaks that may need to be made.

In SSL-VPN portal, the default port used is 443, which is also the port number for HTTPS. While this shouldn't interfere with anything, it can be a good habit to change the port number. FYI, you'd also need to tick custom port number and change the port number to the corresponding port number in FortiClient when establishing the connection.

Our lab is a basic demonstration of how this lab can be set up. More changes need to be made if you want a more secure connection, such as custom certificates...

## Conclusion

In conclusion, Fortinet is a useful tool that can mitigate threats and risks while providing secure remote access to users. It allows users to remote access desktop and bypass geographical limitations while securely encrypting data. Fortinet VPN can benefit wide range of uses, from individual use to corporate management.



# FortiGate FortiGate-40F

**Setting up Site to Site VPN and Remote Access  
with Fortigate-40F**



**Jeffrey Yiu Cheung**

## Purpose

This lab report demonstrates a way to set up Site to Site VPN with two Fortinet FortiGate-40F firewalls and enable remote access.

## Background information

In the modern age, being able to securely access private network remotely is important for work and organizations. With cybersecurity threats constantly evolving, hackers can utilize new knowledge to breach sensitive data. To prevent sensitive information from being risked, Fortinet designed and offers its own VPN to its customers.

Remote Access technology enables users to connect to a computer, network, or system regardless of geographical barriers. This technology can enable the ease of accessing files, managing systems, and running applications. While not all businesses may benefit from this, this technology is a staple to telecommuters (those who work from home), business travels, or those needing to work offsite due to distance or other barriers. While this technology is convenient, it requires a lot of security to maintain.

Fortinet, Inc. is a cybersecurity company headquartered in Sunnyvale, CA. It is a leader in the Cybersecurity industry, securing over 700,000 enterprises and organizations worldwide. It leads the industry in training individuals and has made innovations to incorporate AI into their business. Fortinet made it their mission to educate 1,000,000 people by 2026.

With new technologies constantly enabling the ease of interaction with the web, more information is being uploaded every second. There is useless information, educational information, but there are also sensitive, personal information in the web. To prevent these cybersecurity threats, Fortinet offers cybersecurity devices and programs like firewalls malware prevention programs.

GUI or Graphics Users Interface, is a really nice aspect of the Fortinet Firewalls. Compared to other firewalls like for example the Palo Alto firewalls' GUI, Fortinet firewall GUI is clean and user-friendly, and an overall great upgrade. GUI is an underrated and important aspect of firewalls and their configurability. It can have a big impact on efficiency, reduced errors, and improved user experiences.

VPNs, or virtual private networks, is a technology that allows users to securely connect to private networks over the internet. By creating a tunnel and encrypting data with advanced protocols like IPsec and SSL/TLS to ensure protection against eavesdropping attacks and other threats. VPNs provides stronger privacy and security online, and on top of this, it also allows users to bypass geographical limitations.

SSL, or Secure Sockets Layer, is a protocol that encrypts data through the application layer. Compared to IPsec, or internet protocol security, it is easier to set up, and completes the same goal if users use web-based applications. However, unlike IPsec, it does not provide end-to-end

encryption for all network traffic and is less broad. While SSL VPN is good for this demonstration, one should consider IPsec to be the better option.

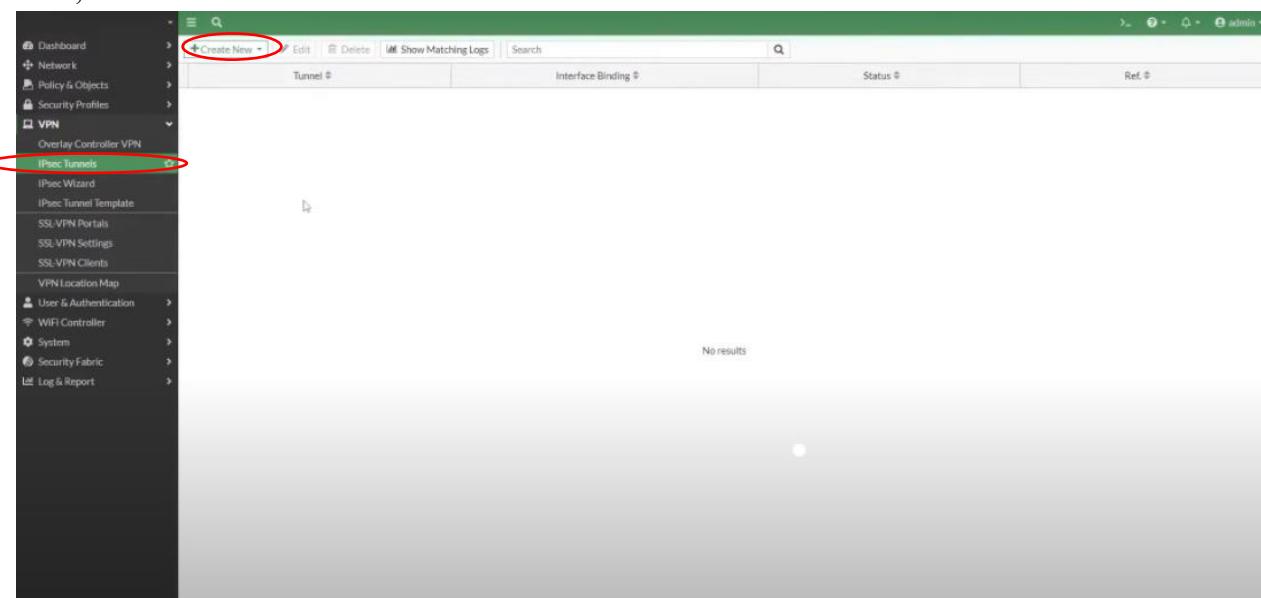
IPsec, an encryption protocol used by GlobalProtect, is a combination of other security protocols to create a protocol that ensures security, integrity, and authentication. It uses protocols like Authentication Header and Encapsulation Security Payload. IPsec follows AES (Advanced Encryption Standard), a highly secure and efficient encrypting algorithm. Although IPsec is secure, it is resource intensive and may drop performance.

Remote Desktop Protocol is a service provided by Microsoft which allows users to connect and control another device via IP (or domain name if applicable). This technology allows users to work, access files, using the computer despite not physically having the machine they need. However, RDP needs the devices to be on the same network, and RDP is vulnerable to cyberattacks, with unrestricted port access and other exploits like BlueKeep, and thus is necessary to run it within a VPN.

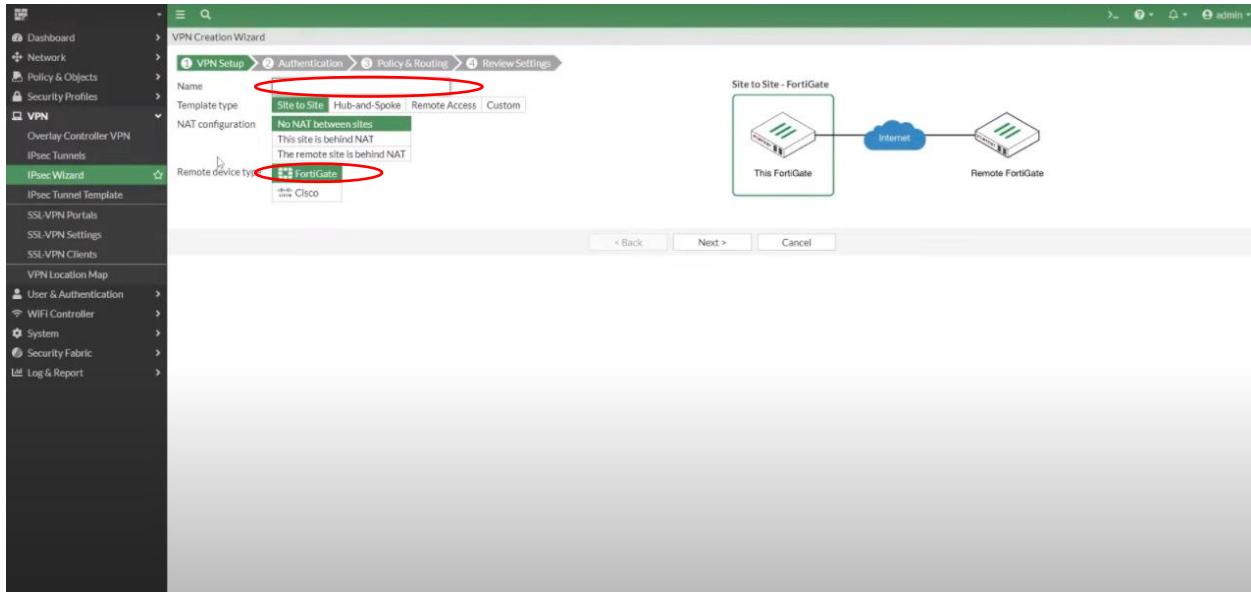
Microsoft is one of the largest and most influential technology company to have exist. Founded in 1975, Microsoft developed and revolutionize how commercial computers are built. Their products range from Operating Systems (windows), computers, software (Microsoft Office), cloud services, and videogames. Today, Microsoft is a technology giant that shape ongoing technology development.

## Lab summary

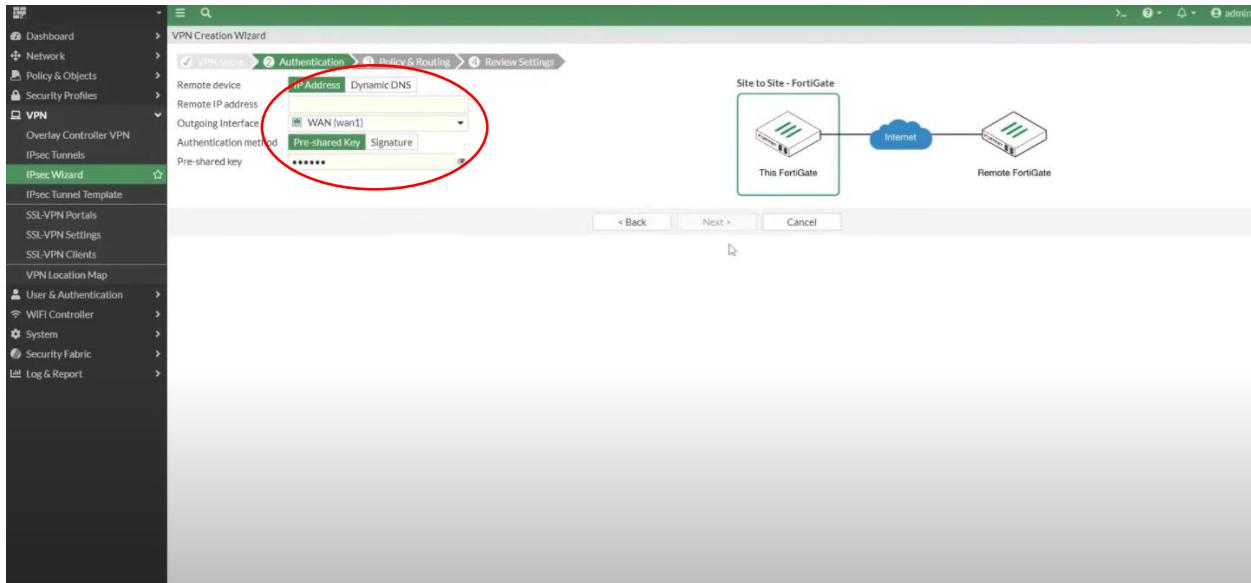
First, create a new IPsec Tunnel in the VPN tab.



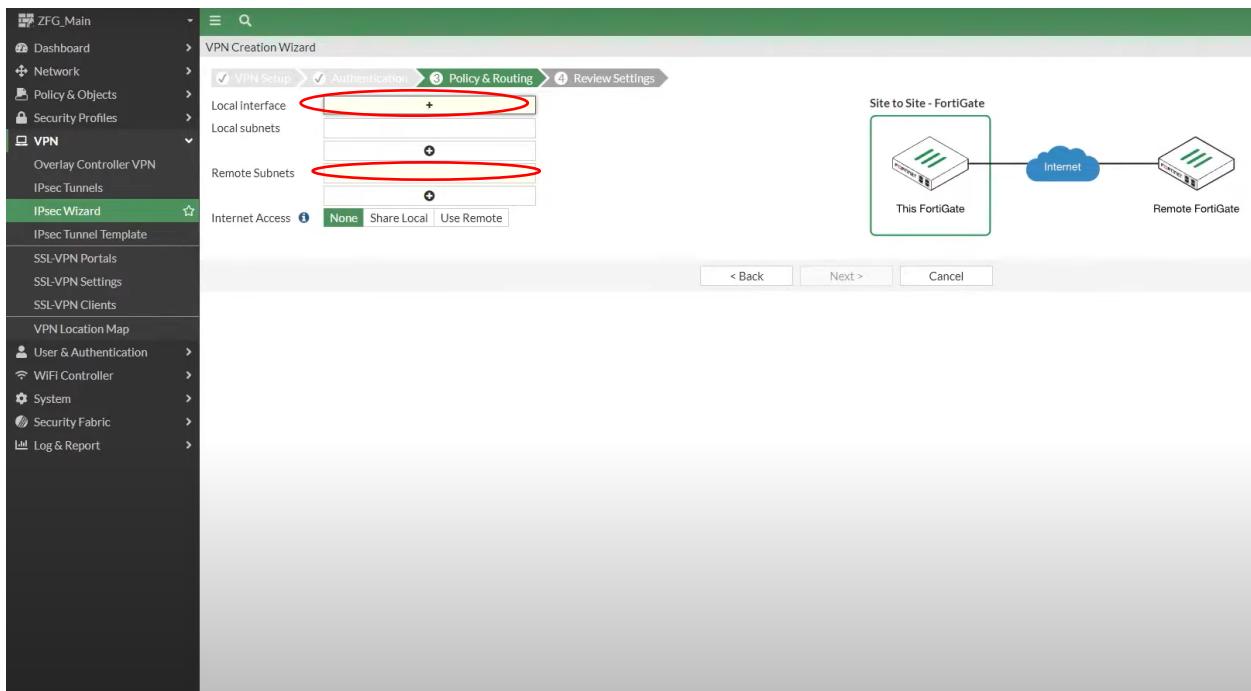
Through the VPN creation Wizard, choose the template type as Site to Site, set the remote device type as FortiGate, and finally, give it a name.



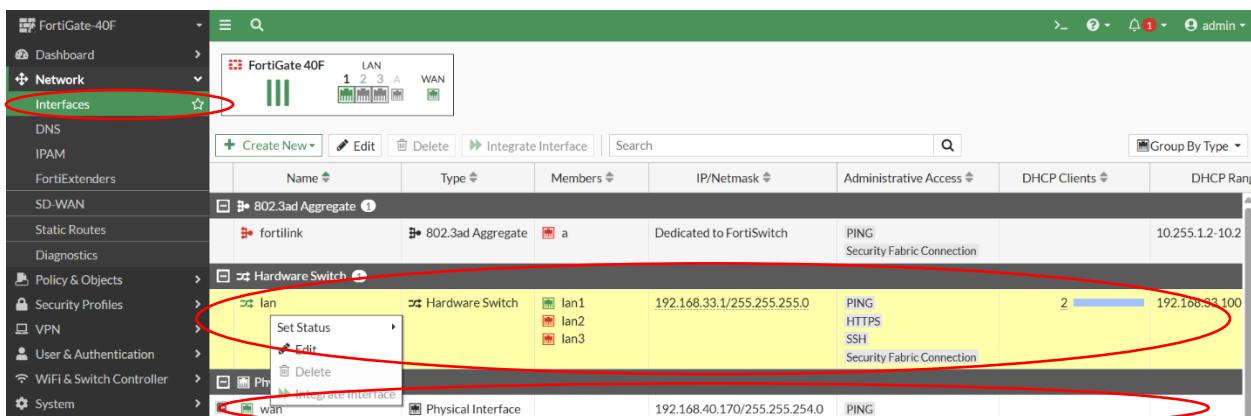
Next, set the outgoing interface as your WAN, and put the Remote IP address as the other device's WAN's IP address. The PSK needs to be the same on both devices.



Next, in Policy & Routing, use your LAN as the Local Interface. For the local subnet, use the subnet of your LAN network, and for the Remote local address, use the other device's LAN address.



You can check the device's LAN's or WAN's IP address in the Network tab.



Next, review your configuration and finalize, then create. Afterwards, you should have this in your IPsec Tunnel tab.

The screenshot shows the FortiGate-40F IPsec Tunnel configuration page. The left sidebar includes sections for Dashboard, Network, Policy & Objects, VPN, IPsec Tunnels (selected), IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings, SSL-VPN Clients, VPN Location Map, User & Authentication, WiFi & Switch Controller, System, Security Fabric, and Log & Report. The main pane displays a table of tunnels with columns for Name, Tunnel, Interface Binding, Status, and Ref. A red circle highlights the 'jamesTUNNEL' row, which has a context menu open with options: View Template, Delete, and Show Matching Logs.

This process should automatically create the firewall policies that allows traffic from the VPN to the LAN, and from LAN to VPN. But if not, you can create through the Firewall Policies Tab.

The screenshot shows the FortiGate-40F Firewall Policy configuration page. The left sidebar includes sections for Dashboard, Network, Policy & Objects (selected), Firewall Policy (highlighted with a star), Addresses, Internet Service, Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, WiFi & Switch Controller, System, and Security Fabric. The main pane displays a table of firewall policies with columns for Name, Source, Destination, Schedule, Service, Action, NAT, Security Profiles, Log, and Bytes. A red circle highlights the 'jeffreyTUNNEL' policy entry in the list.

Next, in the other firewall device, create a tunnel with the same configurations aside from the name (optional).

If you want to be sure, you can edit a tunnel to compare the tunnels.

The screenshot shows the FortiGate 40F web interface. The left sidebar navigation includes: Dashboard, Network, Policy & Objects, Security Profiles, VPN (selected), Overlay Controller VPN, IPsec Tunnels (selected), IPsec Wizard, IPsec Tunnel Template, SSL-VPN Portals, SSL-VPN Settings, SSL-VPN Clients, VPN Location Map, User & Authentication, WiFi & Switch Controller, System, Security Fabric (with a red notification dot), and Log & Report. The main content area displays a table of IPsec Tunnels. A context menu is open over the first row, which has a yellow background. The menu items are: Edit (circled in red), View Template, Delete, and Show Matching Logs.

Tunnel	Interface Binding	Status	Ref.
Custom 1 jamesTUNNEL	wan	Inactive	5

This is the settings for JeffTunnel

## Edit VPN Tunnel

Name	jeffreyTUNNEL
Comments	Comments
<b>Network</b>	
IP Version	IPv4
Remote Gateway	Static IP Address
IP Address	192.168.40.170
Interface	wan
Local Gateway	<input checked="" type="checkbox"/>
Mode Config	<input type="checkbox"/>
NAT Traversal	<input checked="" type="button"/> Enable <input type="button"/> Disable <input type="button"/> Forced
Keepalive Frequency	10
Dead Peer Detection	<input type="button"/> Disable <input type="button"/> On Idle <input checked="" type="button"/> On Demand
DPD retry count	3
DPD retry interval	20 s
Forward Error Correction	Egress <input type="checkbox"/> Ingress <input type="checkbox"/>
<a href="#">+ Advanced...</a>	
<b>Authentication</b>	
Method	Pre-shared Key
Pre-shared Key	*****
<b>IKE</b>	
Version	<input checked="" type="button"/> 1 <input type="button"/> 2
Mode	<input type="button"/> Aggressive <input checked="" type="button"/> Main (ID protection)

**Phase 1 Proposal** + Add

Encryption <span style="border: 1px solid black; padding: 2px 5px;">AES128</span> <span style="border: 1px solid black; padding: 2px 5px;">▼</span>	Authentication <span style="border: 1px solid black; padding: 2px 5px;">SHA256</span> <span style="border: 1px solid black; padding: 2px 5px;">▼</span>
<input type="checkbox"/> 32 <input type="checkbox"/> 31 <input type="checkbox"/> 30 <input type="checkbox"/> 29 <input type="checkbox"/> 28 <input type="checkbox"/> 27 <input type="checkbox"/> 21 <input type="checkbox"/> 20 <input type="checkbox"/> 19 <input type="checkbox"/> 18 <input type="checkbox"/> 17 <input type="checkbox"/> 16 <input type="checkbox"/> 15 <input checked="" type="checkbox"/> 14 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 2 <input type="checkbox"/> 1	
Diffie-Hellman Groups	
Key Lifetime (seconds)	86400
Local ID	

#### Phase 2 Selectors

Name	Local Address	Remote Address	✎
jeffrey	192.168.60.0/255.255.255.0	192.168.33.0/255.255.255.0	✎

#### Edit Phase 2

Name <span style="border: 1px solid black; padding: 2px 5px;">jeffrey</span>	Comments <span style="border: 1px solid black; padding: 2px 5px;">Comments</span>
Local Address <span style="border: 1px solid black; padding: 2px 5px;">Subnet</span> <span style="border: 1px solid black; padding: 2px 5px;">▼</span>	192.168.60.0/255.255.2
Remote Address <span style="border: 1px solid black; padding: 2px 5px;">Subnet</span> <span style="border: 1px solid black; padding: 2px 5px;">▼</span>	192.168.33.0/255.255.2
<span style="border: 1px solid black; padding: 2px 5px;">+ Advanced...</span>	

And this is the settings for JamesTunnel

## Edit VPN Tunnel

Name jamesTUNNEL

Comments

### Network



IP Version IPv4

Remote Gateway

192.168.40.169

IP Address

Interface

Local Gateway

Mode Config

NAT Traversal

Keepalive Frequency 10

Dead Peer Detection

DPD retry count 3

DPD retry interval 20 s

Forward Error Correction Egress  Ingress

[+ Advanced...](#)

### Authentication



## Phase 2 Selectors

Name	Local Address	Remote Address	
jamesTUNNEL	192.168.33.0/255.255.255.0	192.168.60.0/255.255.255.0	

## Edit Phase 2



Name	jamesTUNNEL		
Comments	<input type="text"/> <small>A text area for comments.</small>		
Local Address	Subnet	▼	192.168.33.0/255.255.2
Remote Address	Subnet	▼	192.168.60.0/255.255.2
<input checked="" type="checkbox"/> <b>Advanced...</b>			

## Phase 1 Proposal

Add



Encryption	AES128	▼	Authentication	SHA256	▼	
Encryption	AES256	▼	Authentication	SHA256	▼	
Encryption	AES128	▼	Authentication	SHA1	▼	
Encryption	AES256	▼	Authentication	SHA1	▼	

Diffie-Hellman Groups

<input type="checkbox"/> 32	<input type="checkbox"/> 31	<input type="checkbox"/> 30	<input type="checkbox"/> 29	<input type="checkbox"/> 28	<input type="checkbox"/> 27
<input type="checkbox"/> 21	<input type="checkbox"/> 20	<input type="checkbox"/> 19	<input type="checkbox"/> 18	<input type="checkbox"/> 17	<input type="checkbox"/> 16
<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 14	<input checked="" type="checkbox"/> 5	<input type="checkbox"/> 2	<input type="checkbox"/> 1	

Key Lifetime (seconds)

86400

Local ID

## Authentication



Method

Pre-shared Key

Pre-shared Key

•••••••

## IKE

Version

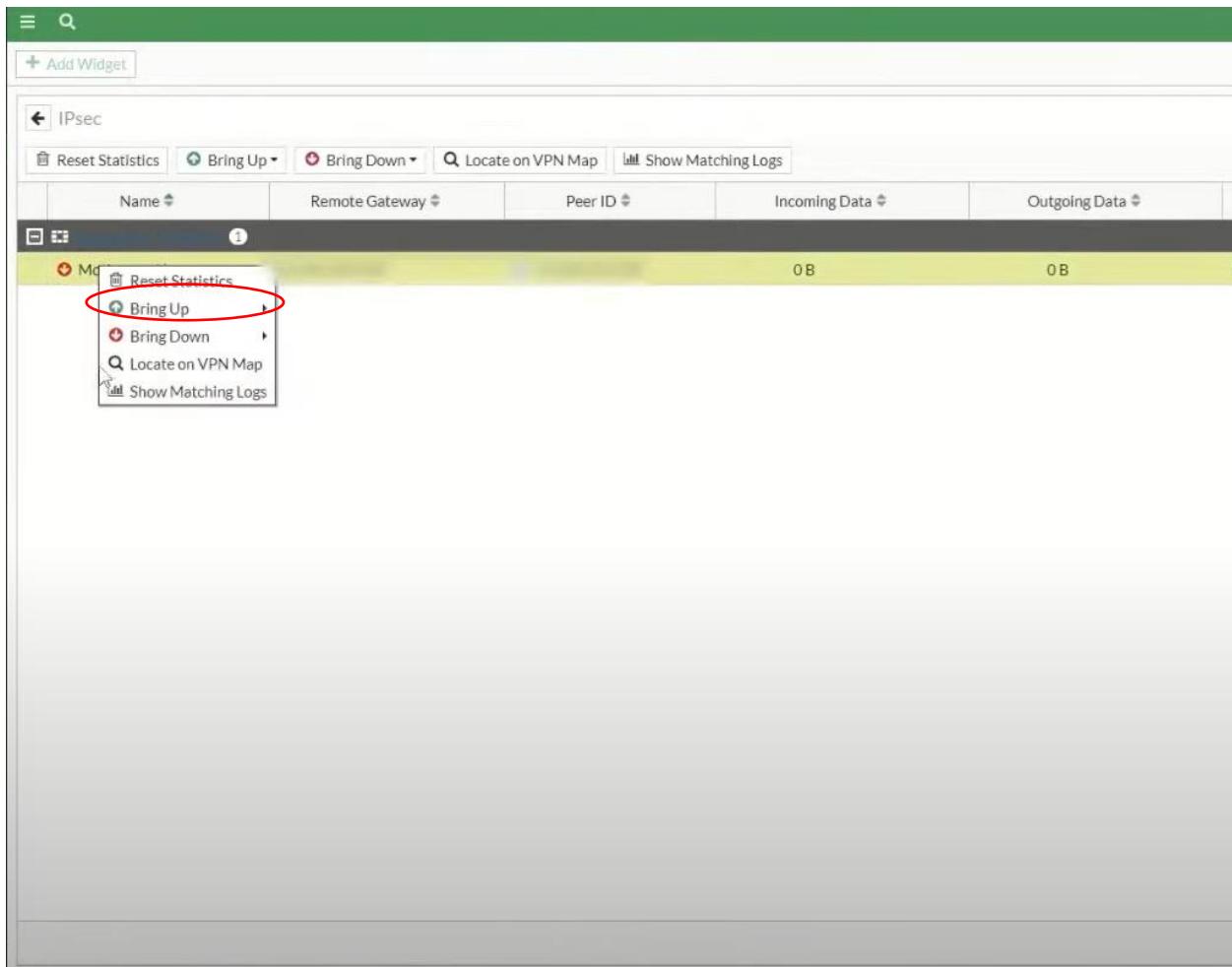
1 2

Mode

Aggressive Main (ID protection)

Again, the Pre-shared Keys NEEDS to be the same.

After this, there should be an option to Bring Up the tunnel.



Afterwards, the tunnel is all set.

To set up Remote Access, you need to first turn on Remote Access in computer's settings.

Settings

Home

Find a setting

System

Display

Sound

Notifications & actions

Focus assist

Power & sleep

Battery

Storage

Tablet mode

Multitasking

Projecting to this PC

Shared experiences

Clipboard

Remote Desktop

Enable Remote Desktop

On

Keep my PC awake for connections when it is plugged in [Show settings](#)

Make my PC discoverable on private networks to enable automatic connection from a remote device [Show settings](#)

[Advanced settings](#)

How to connect to this PC

Use this PC name to connect from your remote device:  
DESKTOP-S9GNN16

[Don't have a Remote Desktop client on your remote device?](#)

User accounts

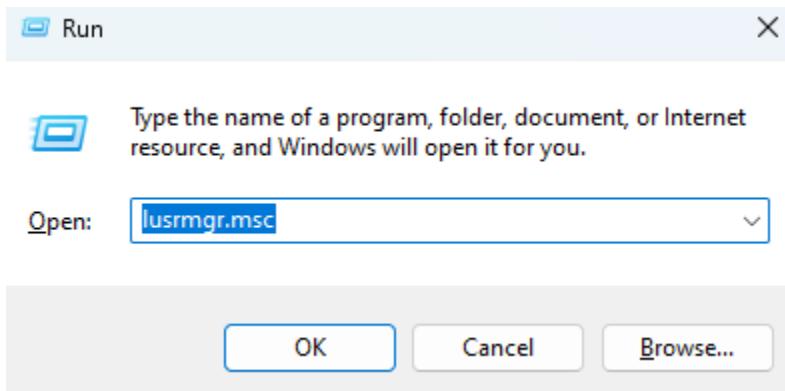
[Select users that can remotely access this PC](#)

Have a question?

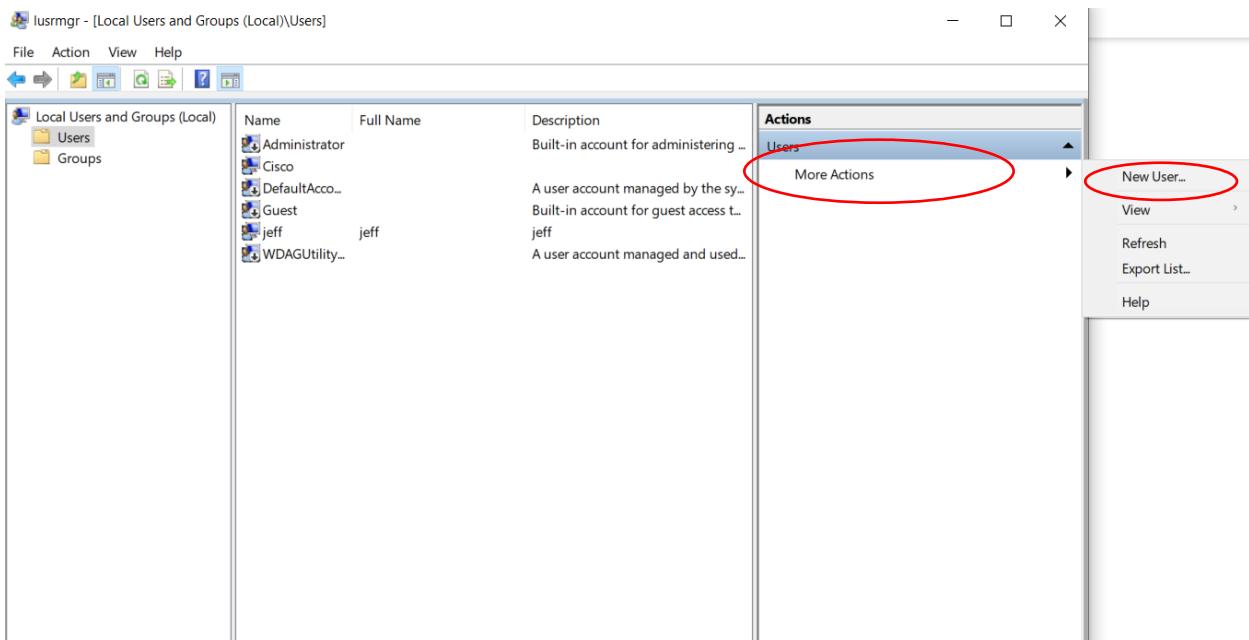
[Solving PC problems remotely](#)

Now, for the device in the internal network, or the device in the network that you want to connect to, create a user or give an existing user permission to access Remote Desktop.

Then, open Run (or Windows + r on windows, command + space on mac) and type in lusrmgr.msc.



This should pop up. Select Users and add new user (if necessary).



Next, add a user, give it a username and password (if necessary). You can check off requiring changing password next logon (optional).

New User

User name:

Full name:

Description:

---

Password:

Confirm password:

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

---

**Help**      **Create**      **Close**

It should look like this.

Name	Full Name	Description
Administrator		Built-in account for administering ...
Cisco		
DefaultAcco...		A user account managed by the sy...
Guest		Built-in account for guest access t...
jeff	jeff	jeff
WDAGUtility...		A user account managed and used...

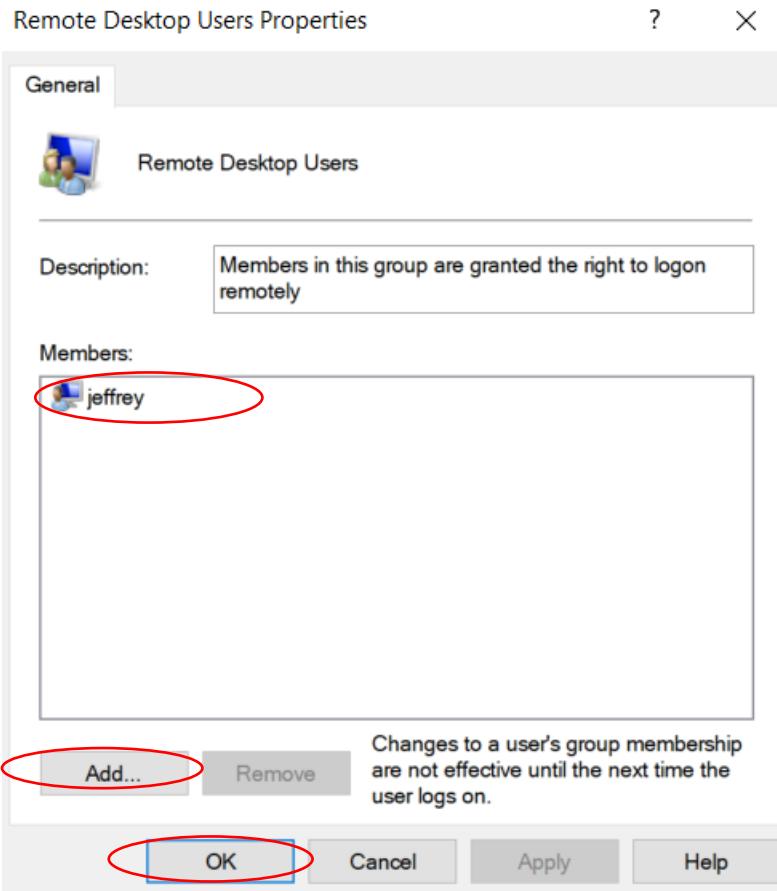
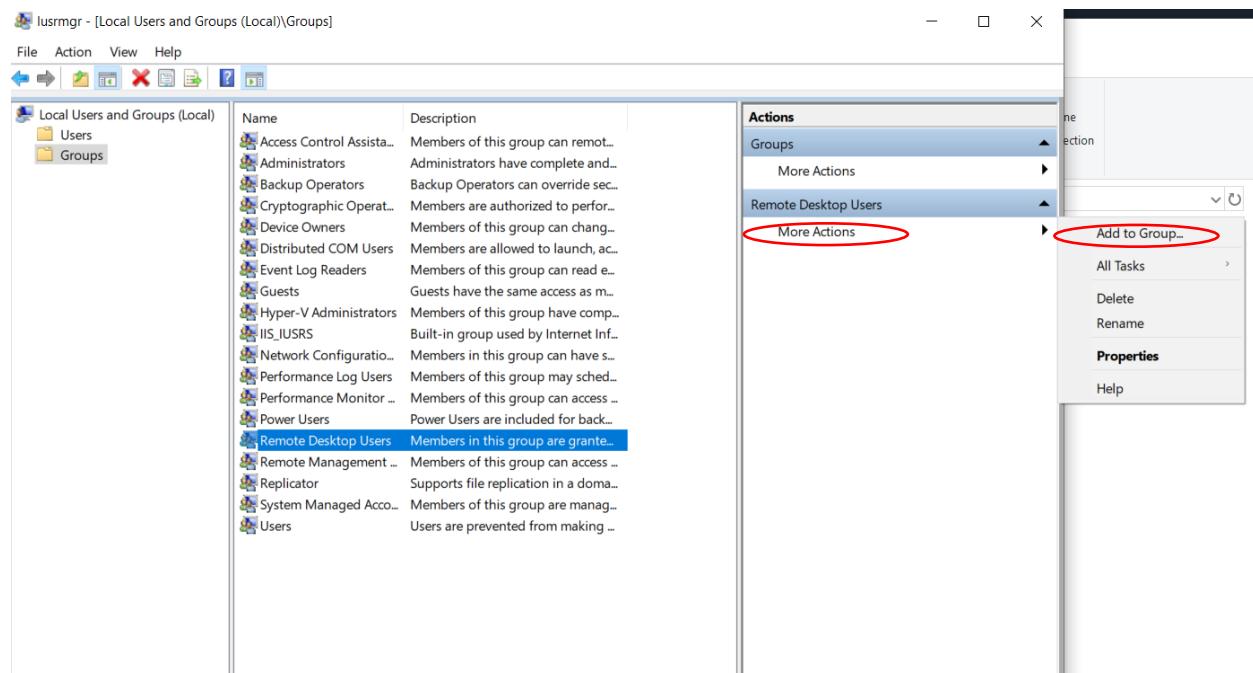
Next, go to groups. There should be a group named Remote Desktop Users.

The screenshot shows the Windows Local Users and Groups snap-in. The left pane displays a tree view with 'Local Users and Groups (Local)' expanded, showing 'Users' and 'Groups'. The 'Groups' node is highlighted with a red oval. The right pane lists the available groups:

Name	Description
Access Control Assista...	Members of this group can remot...
Administrators	Administrators have complete and...
Backup Operators	Backup Operators can override sec...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, ac...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have comp...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sched...
Performance Monitor ...	Members of this group can access ...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management ...	Members of this group can access ...
Replicator	Supports file replication in a doma...
System Managed Acco...	Members of this group are manag...
Users	Users are prevented from making ...

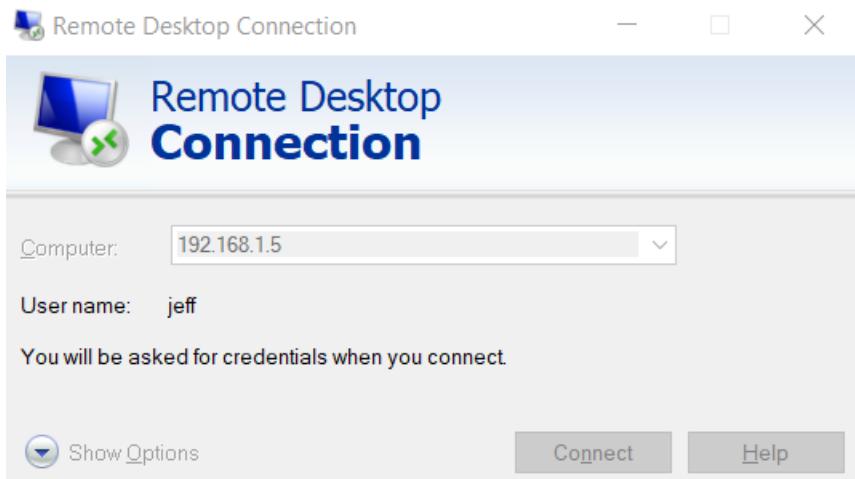
The 'Remote Desktop Users' group is highlighted with a blue oval. The 'Actions' pane on the right shows 'Groups' selected under 'More Actions'.

Next, add the user you've made, or an existing user, into the group to give them permission.



If you have reset password on next logon enabled, you have to reset the password before you can use the user.

Next, using the other device, remote access into the desired device via Remote Desktop Connection.

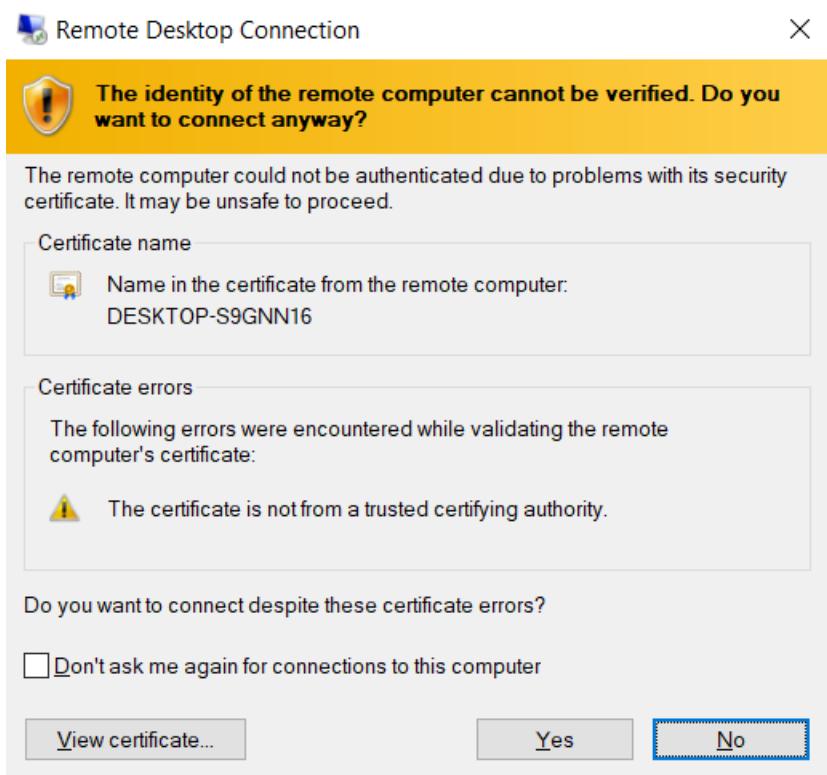


In computer, you will need to input the desired device's IP address. This can be found in Command Prompt with the command “ipconfig /all”.

```
Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . :
Description . . . . . : Intel(R) Ethernet Connection (3) I218-LM
Physical Address. . . . . : 54-EE-75-75-94-1D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::75ec:339b:9a6f:c202%20(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, January 6, 2025 3:06:37 PM
Lease Expires . . . . . : Tuesday, January 7, 2025 3:06:36 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 206892661
DHCPv6 Client DUID. . . . . : 00-01-00-01-2A-C6-6E-3F-54-EE-75-75-94-1D
DNS Servers . . . . . : 9.9.9.9
                           1.1.1.1
NetBIOS over Tcpip. . . . . : Enabled
```

If successful, you should be prompted with this:

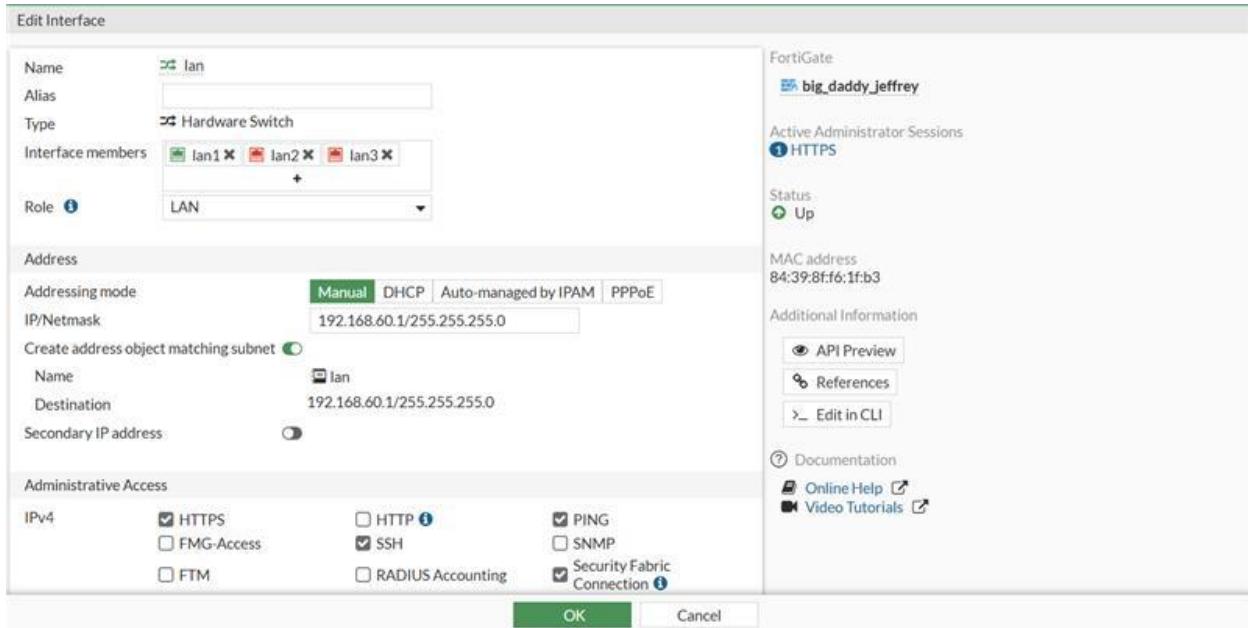


Just click Yes, and then you're all set.

## Problems

This is a lab that shouldn't prove to be too difficult. However, we still ran into some encounters with obstacles. In our lab setting, since everybody had the same default LAN at first, we had to change it before getting into the lab.

The screenshot shows the FortiGate 40F management interface. The left sidebar has a tree view with 'Interfaces' selected. The main pane displays the 'Interfaces' configuration for the 'fortigate' device. It shows a summary of 'FortiGate 40F' with 'LAN' and 'WAN' ports. Below this is a table with columns: Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, and DHCP Ranges. The table lists several interfaces: '802.3ad Aggregate' (Type: 802.3ad Aggregate, Members: 'a'), 'fortilink' (Type: 802.3ad Aggregate, Members: 'a', Dedicated to FortiSwitch), 'Hardware Switch' (Type: Hardware Switch, Members: 'lan1', 'lan2', 'lan3'), 'Physical Interface' (Type: Physical Interface, Members: 'wan'), 'Software Switch' (Type: Software Switch, Members: 'wqt.root', 'wqtn.12jeffrey'), and 'Tunnel Interface' (Type: Tunnel Interface). The 'lan' interface is highlighted in yellow. A context menu for 'lan' is open, showing options: Set Status, Edit, Delete, and Integrate Interface. The bottom status bar shows 'FORTINET v7.0.17' and '0% Updated: 12:09:21'.



On top of this, me and my partner were stuck for a little bit when we created the tunnel but couldn't find the option to bring it up. After a while, we found out that it was an option on the other device.

While these were minor nuisances, they can still be annoying to deal with, and there are probably many more that we haven't discovered.

## Conclusion

In conclusion, Fortinet Firewalls are useful tools that can mitigate threats and risks while providing secure remote access to users. It can allow users to remote access desktop and bypass geographical limitations while securely encrypting data.