Site-to-Site VPN And Log Forwarding To Splunk For TTI Network

CISA 4390 – Enterprise Network Project

Instructors: John Ali, Kirksal Icoz, Rouzbeh Keshavarz, Travis Penner, Hamid Talebi, Areeb Yasir

Scott Bandy (A01366713)
Jason Chan (A01248750)
Nicholas Dunsmuir (A01325497)
Brian Hayter (A01356751)
Thomas Jelstad (A01357395)
Harsheen Kaur (A01363090)
Joey Lam (A00967230)
Yvonne Li (A00730798)
Suraj Nand (A01240738)
Andrei Tepei (A01384863)

Table of Contents

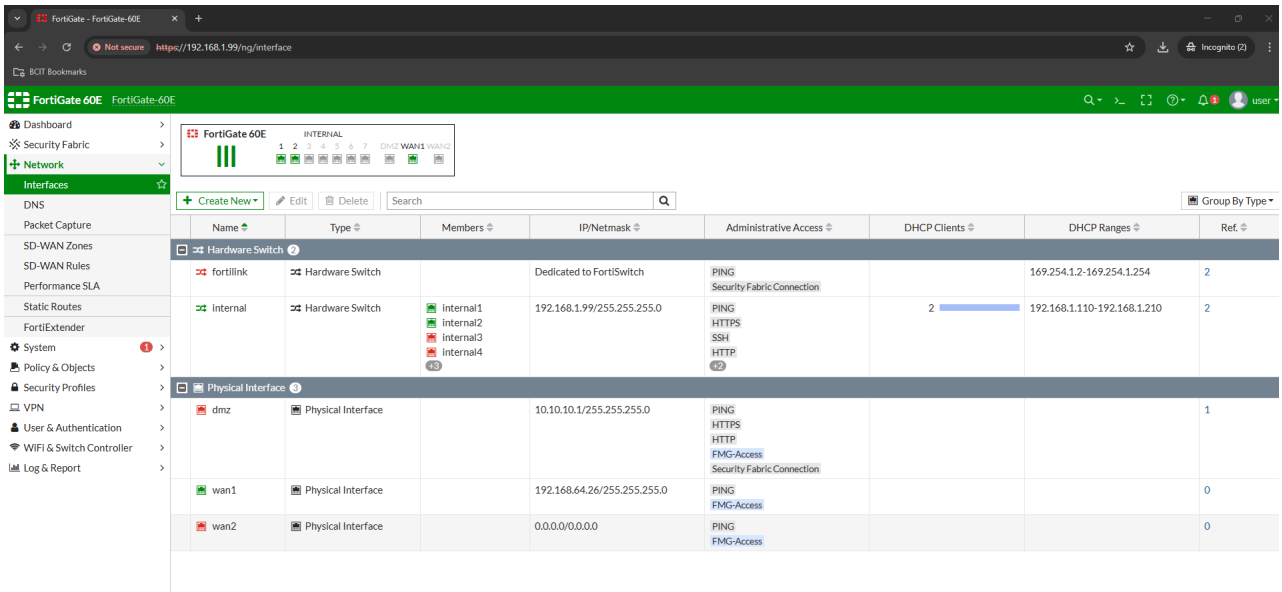
Phase 1: Site-to-Site VPN between Vancouver and Burnaby

IP Addressing Table

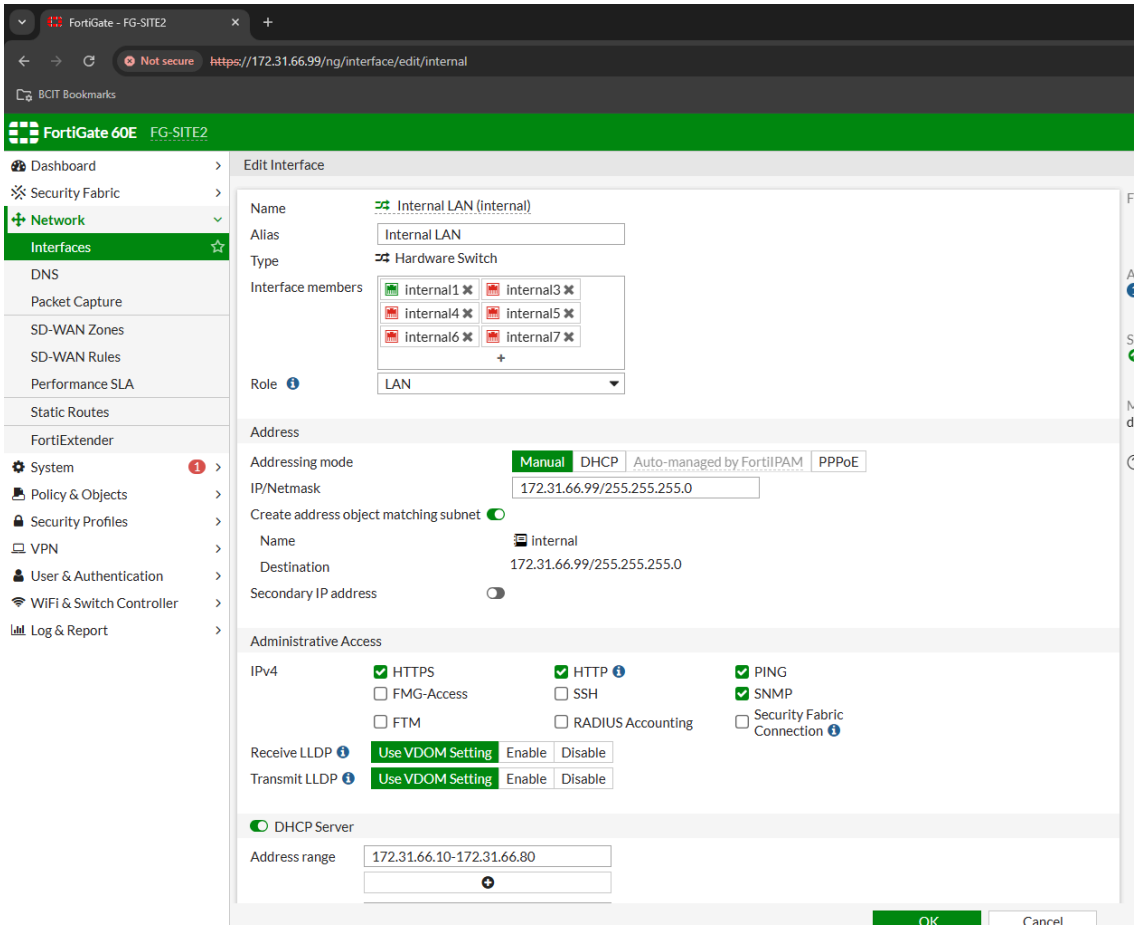
Site 2 - Vancouver	Address	172.31.64.0/20
Router WAN	To Fortigate	172.31.64.254/24
FortiGate	To Site Router	172.31.64.220/24
	To Vancouver LAN	172.31.65.10/24
	To Splunk LAN	172.31.66.99/24
	DHCP Server for Splunk LAN	172.31.66.10-80/24
Host PC	DHCP Client on Splunk LAN	
Splunk Server	Static	172.31.66.200/24
Splunk Forwarder	Static	172.31.66.201/24
Site 3 - Burnaby	Address	172.31.96.0/21
Router WAN	To Fortigate	172.31.96.254/24
FortiGate	To Site Router	172.31.96.220/24
	To Burnaby LAN	172.31.97.10/24
	To Splunk LAN	172.31.98.99/24
	DHCP Server for Splunk LAN	172.31.98.10-80/24
Host PC	DHCP Client on Splunk LAN	
Splunk Server	Static	172.31.98.200
Splunk Forwarder	Static	172.31.98.201

FortiGate Setup (configure on both sites accordingly)

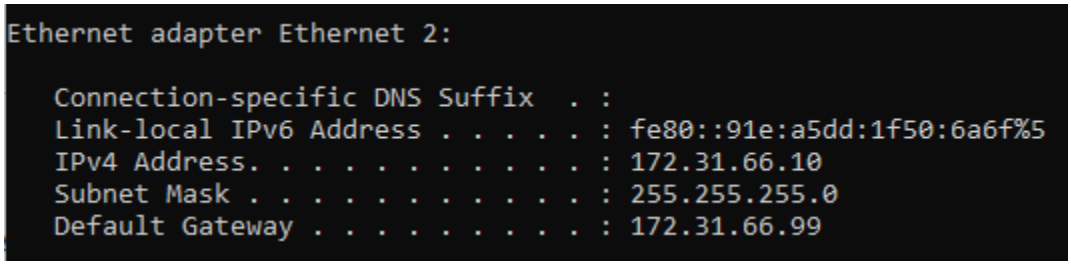
This is the baseline configuration.



Double-click the ‘Internal’, change the IP Address, and configure the DHCP Server range for your LAN.

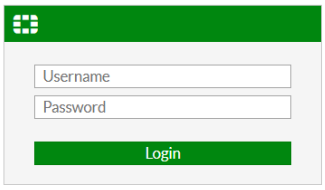


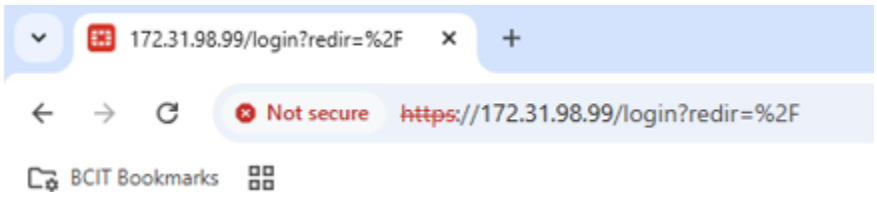
On the Host PC, shutdown and then bring up the NIC that is connected to the FortiGate. The IP should change according to the DHCP Server. (Site 2 and 3)



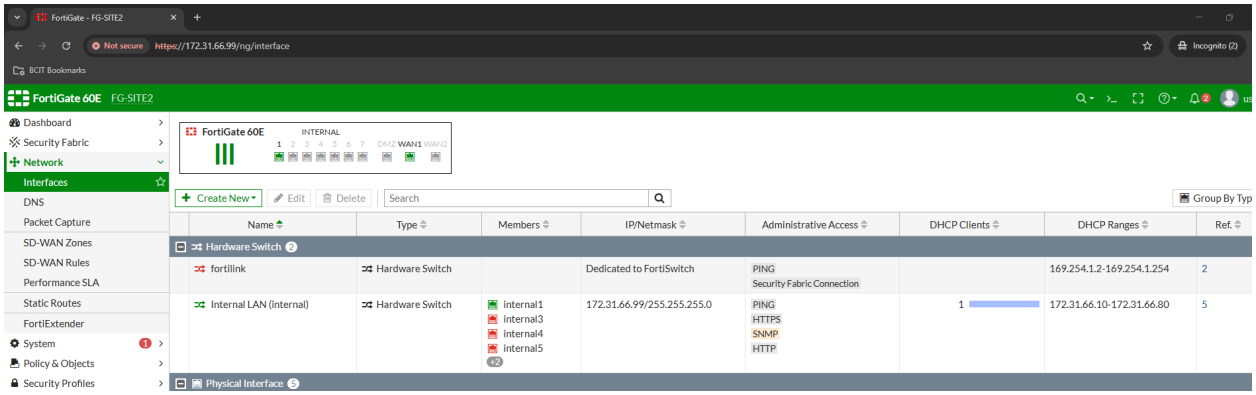
```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet 10G 2P X550-t Adapter
   Physical Address. . . . . . . . . : B4-96-91-A8-C7-F0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2de5:f71c:ea32:aaea%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.98.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, May 22, 2025 11:20:33 AM
   Lease Expires . . . . . . . . . . : Thursday, May 29, 2025 11:20:34 AM
   Default Gateway . . . . . . . . . : 172.31.98.99
   DHCP Server . . . . . . . . . . . : 172.31.98.99
   DHCPv6 IAID . . . . . . . . . . . : 129275537
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-DF-EF-01-B4-96-91-A8-C7-F0
   DNS Servers . . . . . . . . . . . : 96.45.45.45
                                       96.45.46.46
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Go to the new Management IP on the browser which is the gateway address of the FortiGate. Site2: https://172.31.66.99/ or Site3: https://172.31.98.99/. Click ‘Advanced’ and proceed to the login page then sign in with your account.

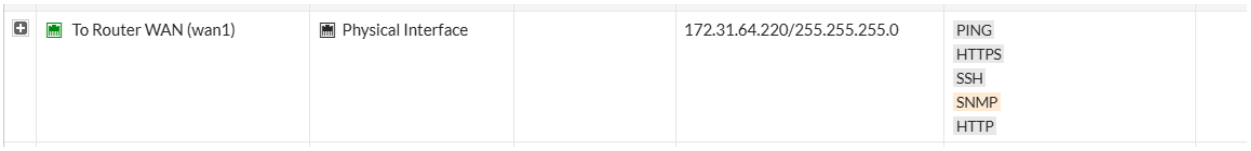




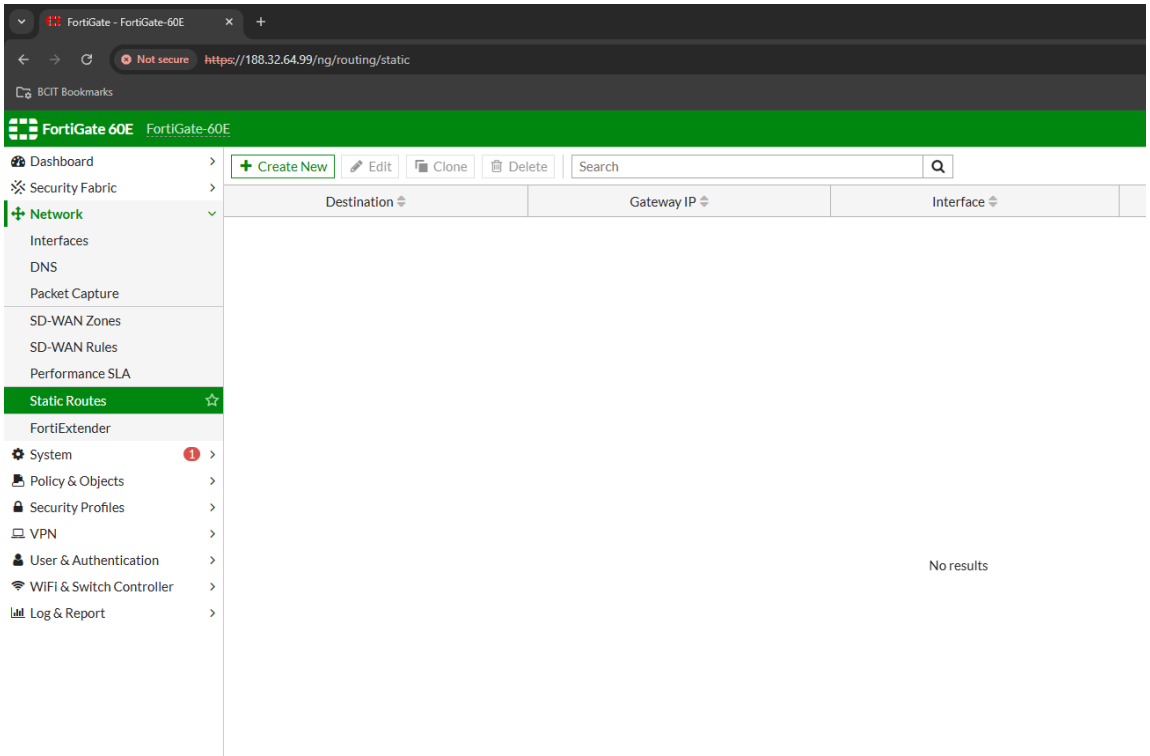
Now you should see the Internal LAN IP has changed. 172.31.98.99 for Site 3.



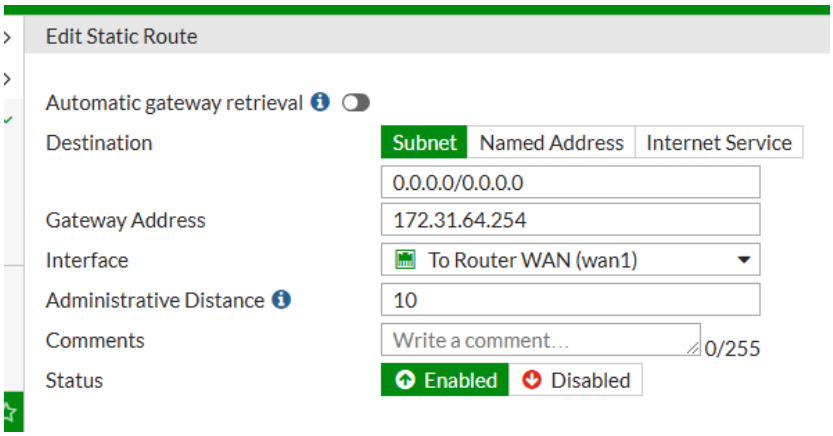
Go to the WAN port and configure an IP address on the same subnet as the Site Router to connect to the local Site Router. Here, we configured a 172.31.64.220/24 address since the Site 2 Router is 172.31.64.254/24. 172.31.96.220/24 for Site 3.



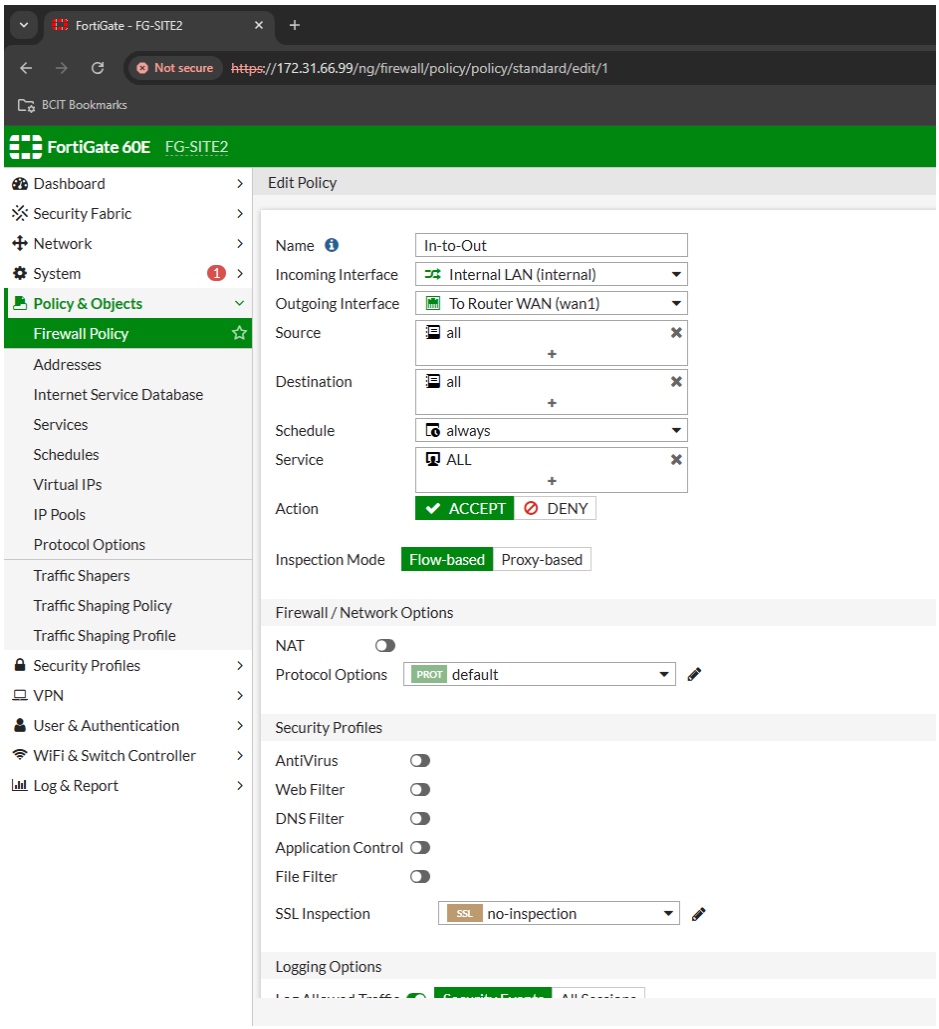
Go to ‘Network’ then ‘Static Routes’ as we will be manually defining the path the network traffic should follow to reach their destination.



Click ‘Create New’ and configure the following where Gateway Address is the WAN Router’s IP. 172.31.96.254 for Site 3.



Configure the Firewall Policy like so. Name it appropriately, specifying incoming and outgoing traffic (interface), specifying the source and destination IPs, and defining the type of protocol allowed (service).



Verify connectivity with a ping test to the local Router from Fortigate.

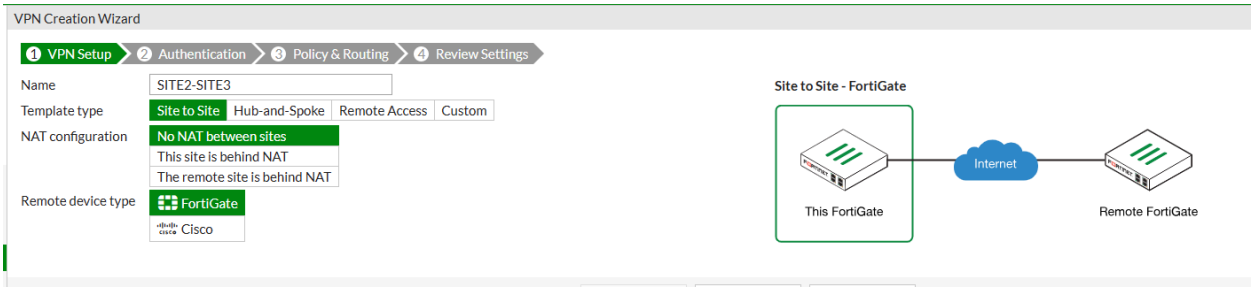
```
FG-SITE2 # execute ping 172.31.64.254
PING 172.31.64.254 (172.31.64.254): 56 data bytes
64 bytes from 172.31.64.254: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.31.64.254: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 172.31.64.254: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 172.31.64.254: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 172.31.64.254: icmp_seq=4 ttl=255 time=0.2 ms

--- 172.31.64.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.4 ms

FG-SITE2 #
```

```
FG-SITE3 # execute ping 172.31.96.254
PING 172.31.96.254 (172.31.96.254): 56 data bytes
64 bytes from 172.31.96.254: icmp_seq=0 ttl=255 time=0.4 ms
64 bytes from 172.31.96.254: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 172.31.96.254: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 172.31.96.254: icmp_seq=3 ttl=255 time=0.2 ms
64 bytes from 172.31.96.254: icmp_seq=4 ttl=255 time=0.3 ms

--- 172.31.96.254 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.4 ms

FG-SITE3 #
```

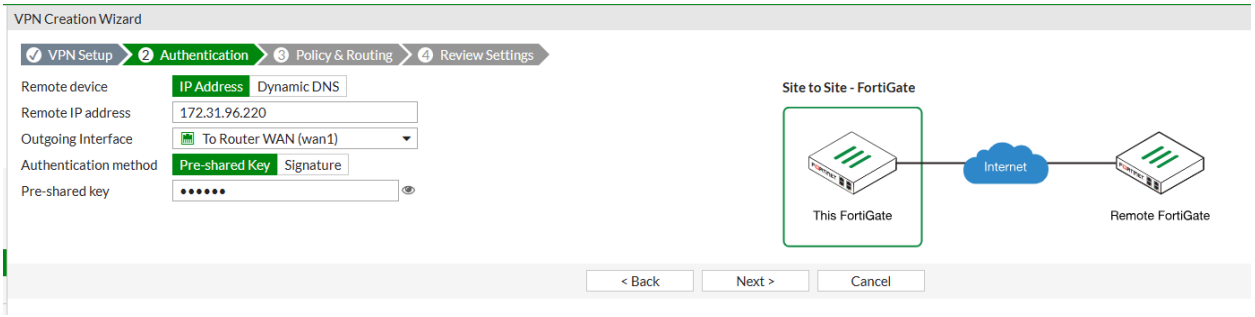
Then you will do the same on the Burnaby side but with the proper IP addressing scheme.

Configure Site-to-Site VPN From Both Routers

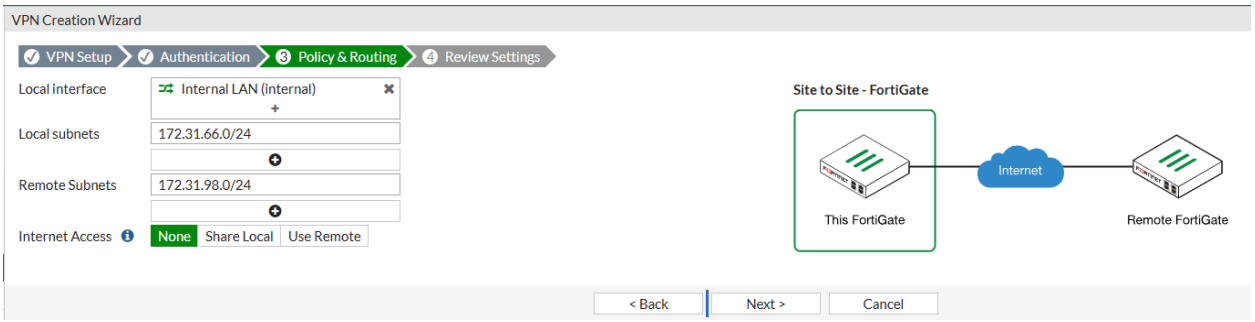
Go to ‘VPN’ on the sidebar, then click ‘IPsec Wizard’ and configure the following. Configure a policy name, select 'No NAT' to disable address translation, and apply the settings to FortiGate devices. For Site 3, name it ‘SITE3-SITE2’



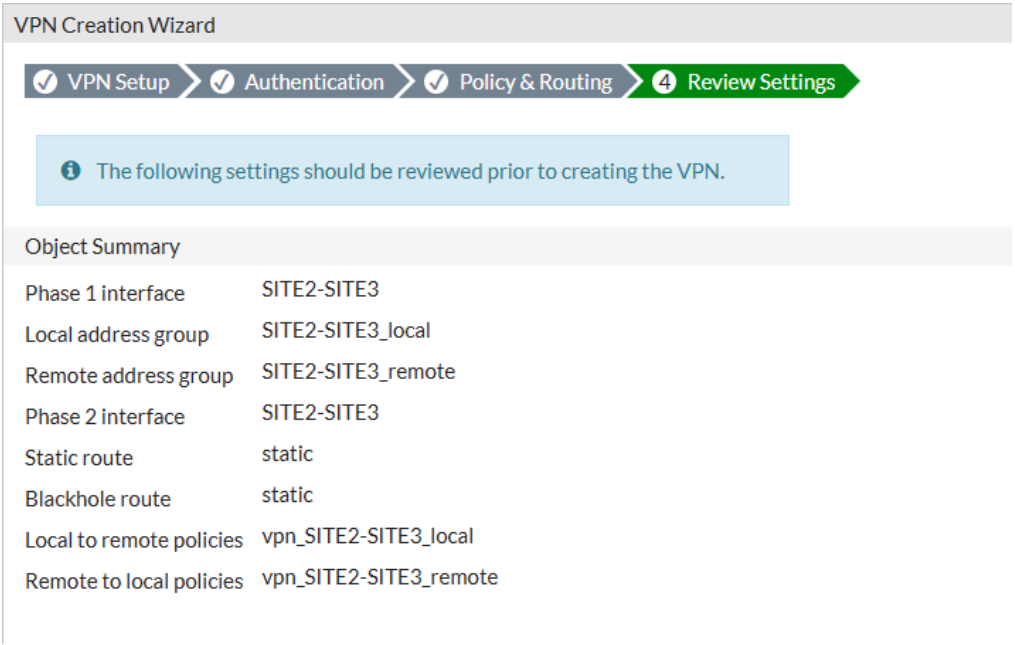
Enter the remote device's IP address, select the outgoing interface, choose "Pre-shared Key" authentication, enter the key, then click "Next." Make sure it matches on both sides. Remote IP 172.31.64.220 on Site 3 side.

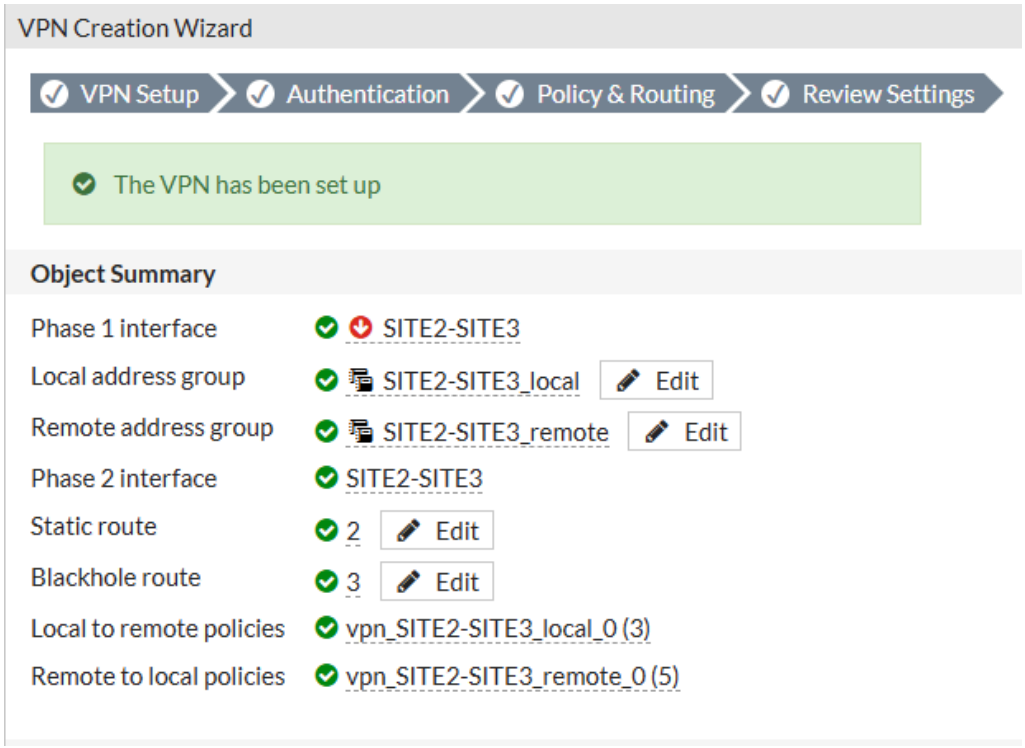


Specify the local interface and subnets, add the remote subnets, select the desired internet access option, and click "Next." Reverse it for Site 3.

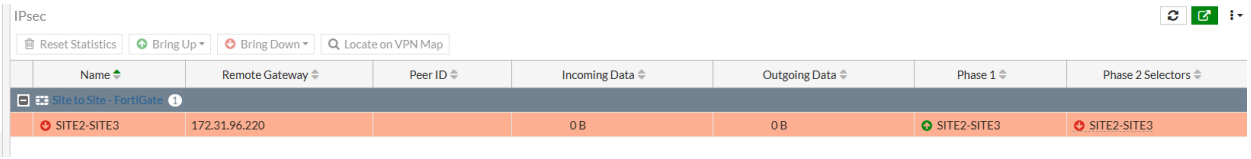


Review and confirm it.

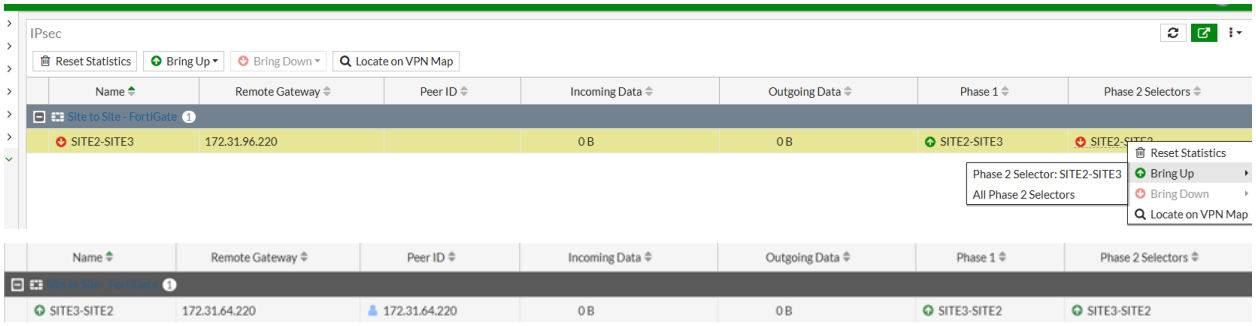




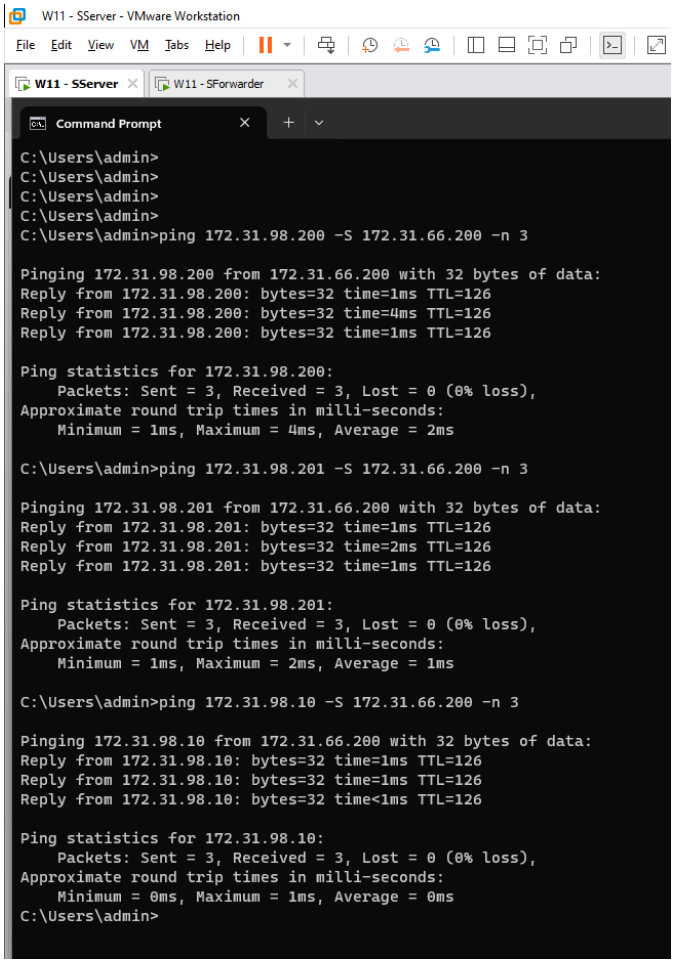
You can see it here in the tunnel list.

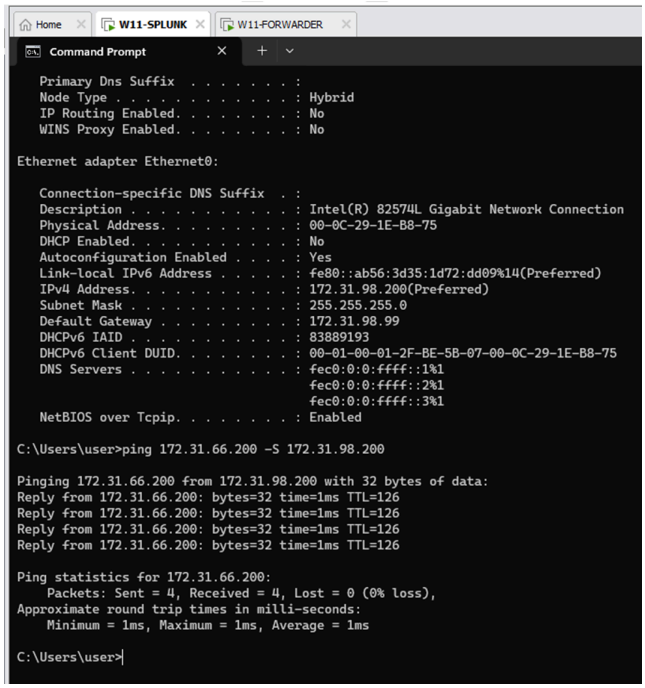


Double-click the SITE2-SITE3, then click Bring Up, then bring up All Phase 2 Selectors. You should see the tunnel is up as well as the icons being green confirming it.



Do a ping test from VM on one site to the other site to verify Site-to-Site VPN connectivity.

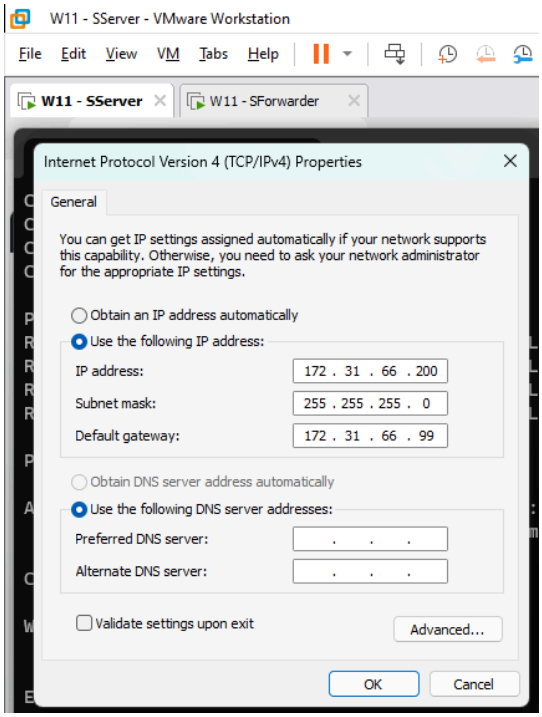




Phase 2: Splunk Configuration

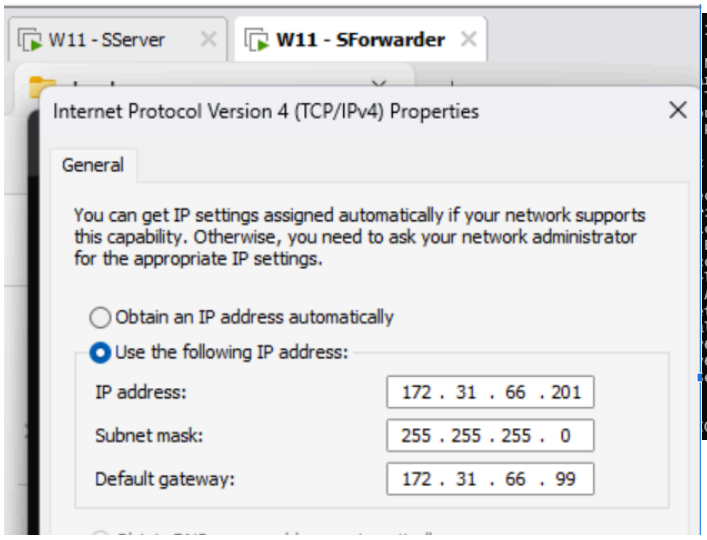
IP Configuration on Windows VM (Splunk Server and Forwarder) on **both Sites**

On the **Splunk Server VM**, we change the IP address as followed from the table. The following IP configured is for the Vancouver Site. Configure the correct IP on the other side.




```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : W11-SPLUNK
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-1E-B8-75
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::ab56:3d35:1d72:dd09%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.31.98.200(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.31.98.99
   DHCPv6 IAID . . . . . . . . . . . : 83889193
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2F-BE-5B-07-00-0C-29-1E-B8-75
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

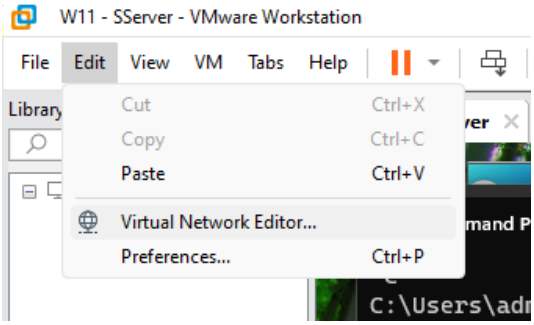
On the **Splunk Forwarder VM,** we change the IP address as followed from the table. No DNS. Configure the correct IP on the other side.



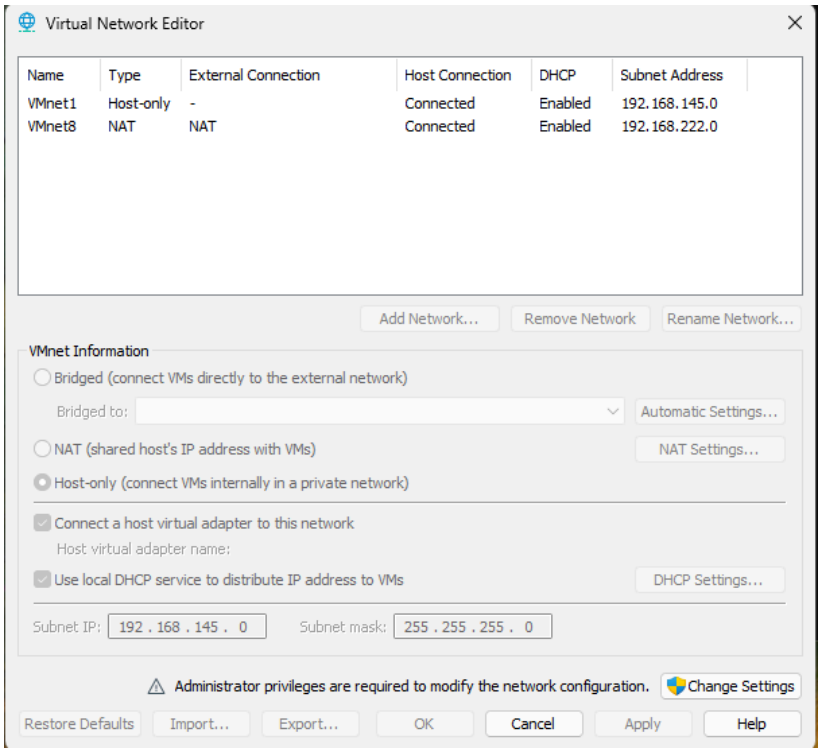

```
IP Configuration

Name . . . . . . . . . . . . : W11-FORWARDER
ry Dns Suffix  . . . . . . . :
Type . . . . . . . . . . . . : Hybrid
uting Enabled. . . . . . . . : No
Proxy Enabled. . . . . . . . : No

 adapter Ethernet0:

ction-specific DNS Suffix  . :
iption . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
cal Address. . . . . . . . . : 00-0C-29-C2-4E-67
Enabled. . . . . . . . . . . : No
onfiguration Enabled . . . . : Yes
local IPv6 Address . . . . . : fe80::13b5:fe60:d54d:83c%9(Preferred)
Address. . . . . . . . . . . : 172.31.98.201(Preferred)
t Mask . . . . . . . . . . . : 255.255.255.0
lt Gateway . . . . . . . . . : 172.31.98.99
6 IAID . . . . . . . . . . . : 100666409
6 Client DUID. . . . . . . . : 00-01-00-01-2F-BE-5F-95-00-0C-29-C2-4E-67
ervers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                              fec0:0:0:ffff::2%1
                              fec0:0:0:ffff::3%1
OS over Tcpip. . . . . . . . : Enabled
```

VMware Workstation Setup (on both Sites):

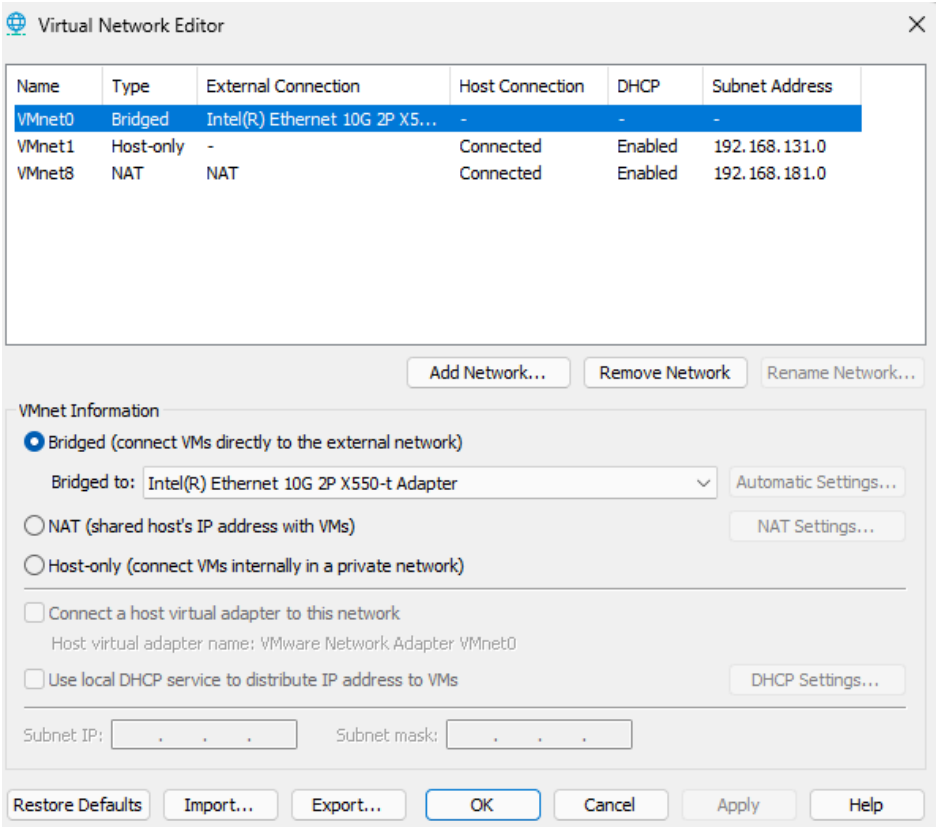
On the VMware Workstation itself, go to Virtual Network Editor. You will change the default NIC that the bridge connection will use.



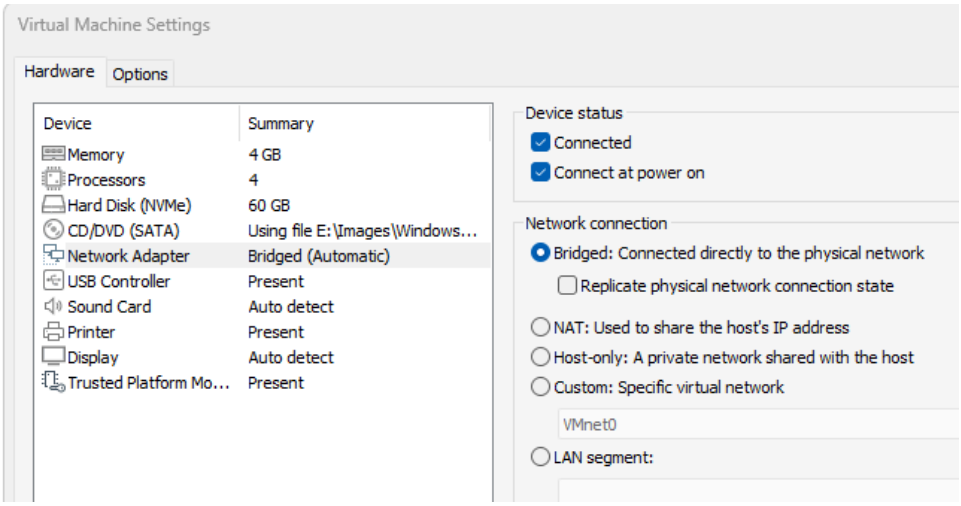
At the bottom right, click Change Settings, and accept the prompt for administrator access.



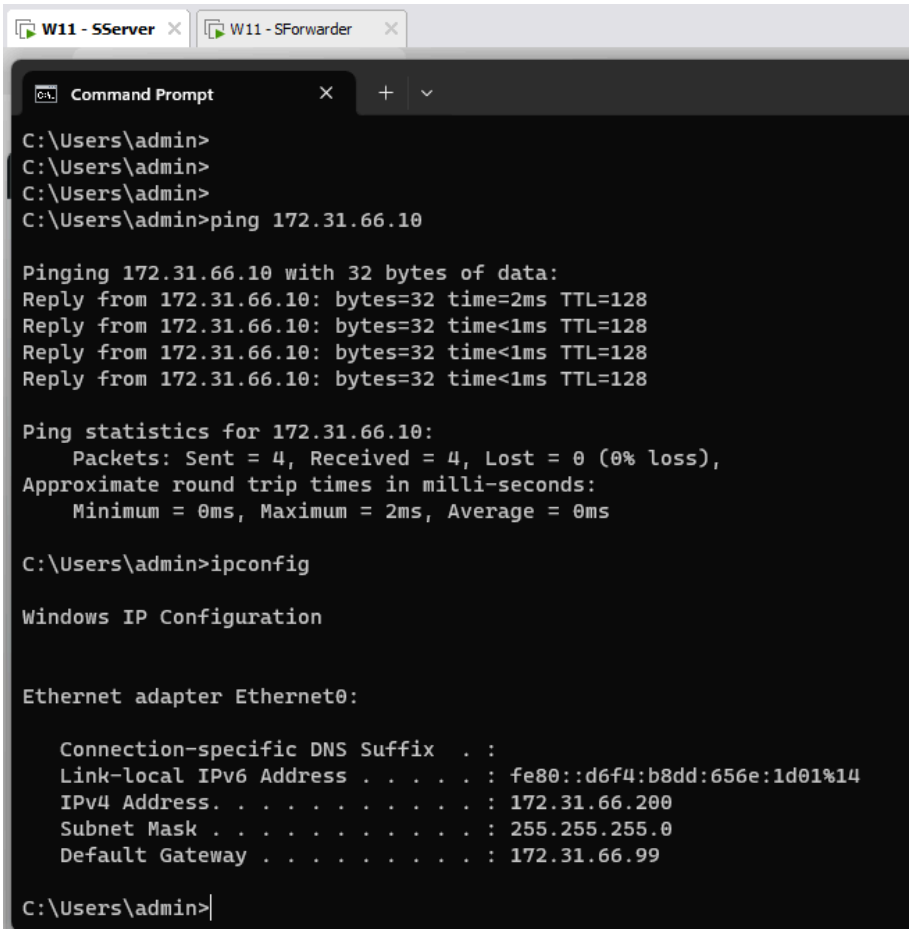
Change the Bridged Adapter from Automatic to the physical NIC on the Host



On the VMs that will connect to your physical network, in the VM Settings, change the Network Connection to Bridged allowing it to communicate directly with other devices on the network like a physical computer.



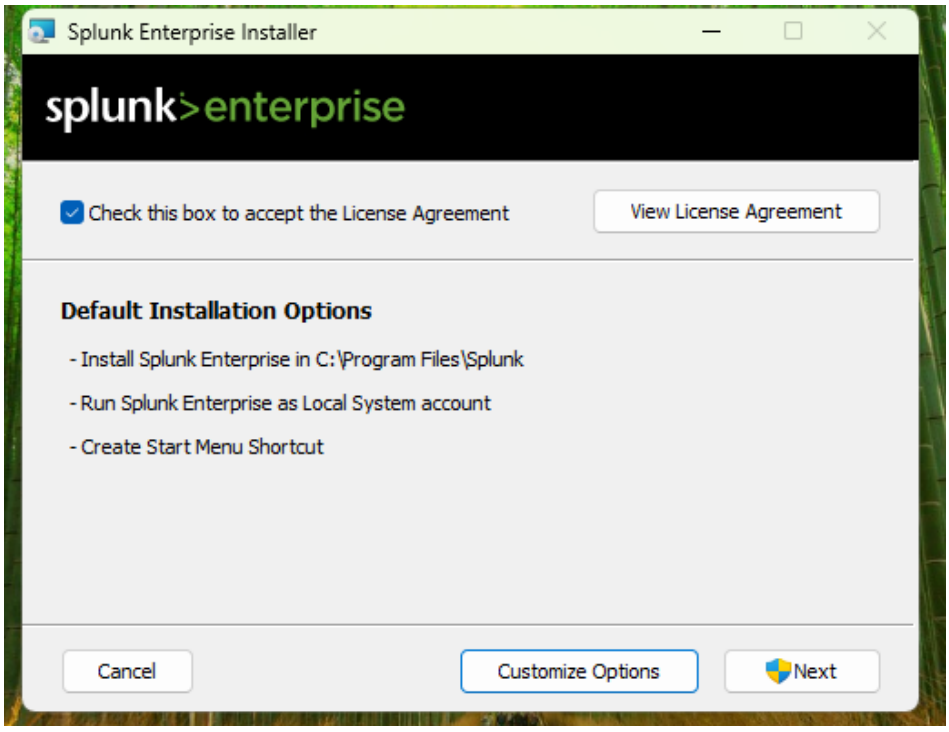
Verify connectivity with a Ping Test between VM and Host. Here, we are pinging the host (172.32.66.10) from the Splunk Server (172.32.66.200)



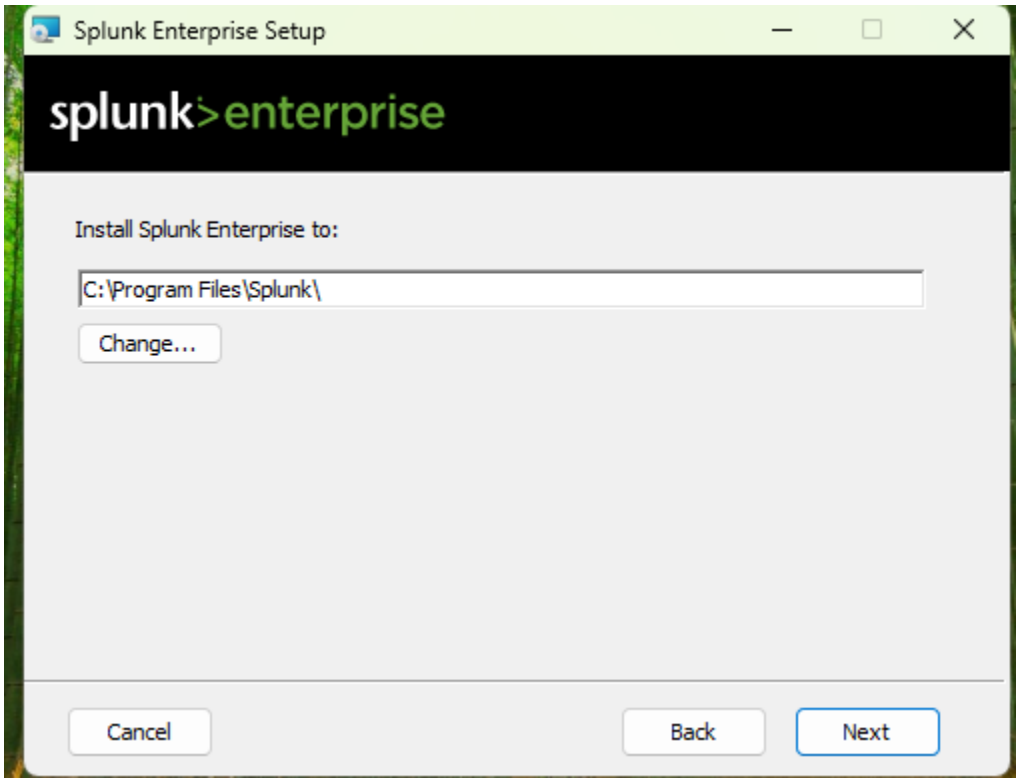
Splunk Server Setup:

You download the official Splunk application and run it located wherever you downloaded it. In this case, we saved it to the desktop for easier access.

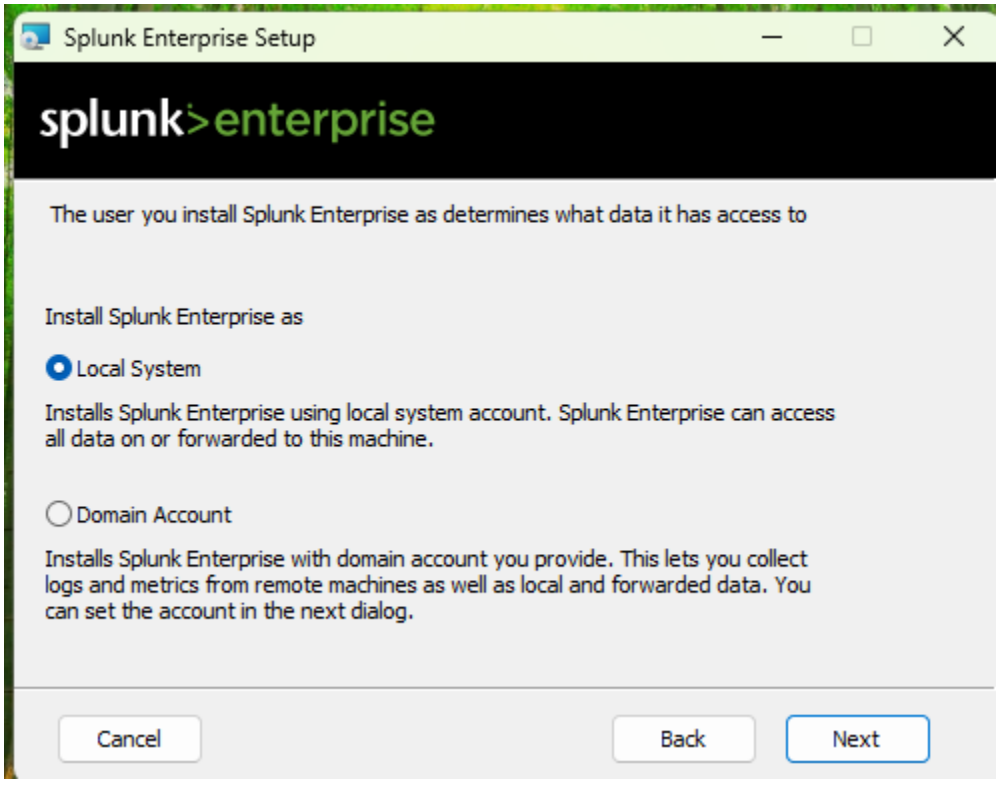
We check the box accepting the license agreement and click ‘Next’



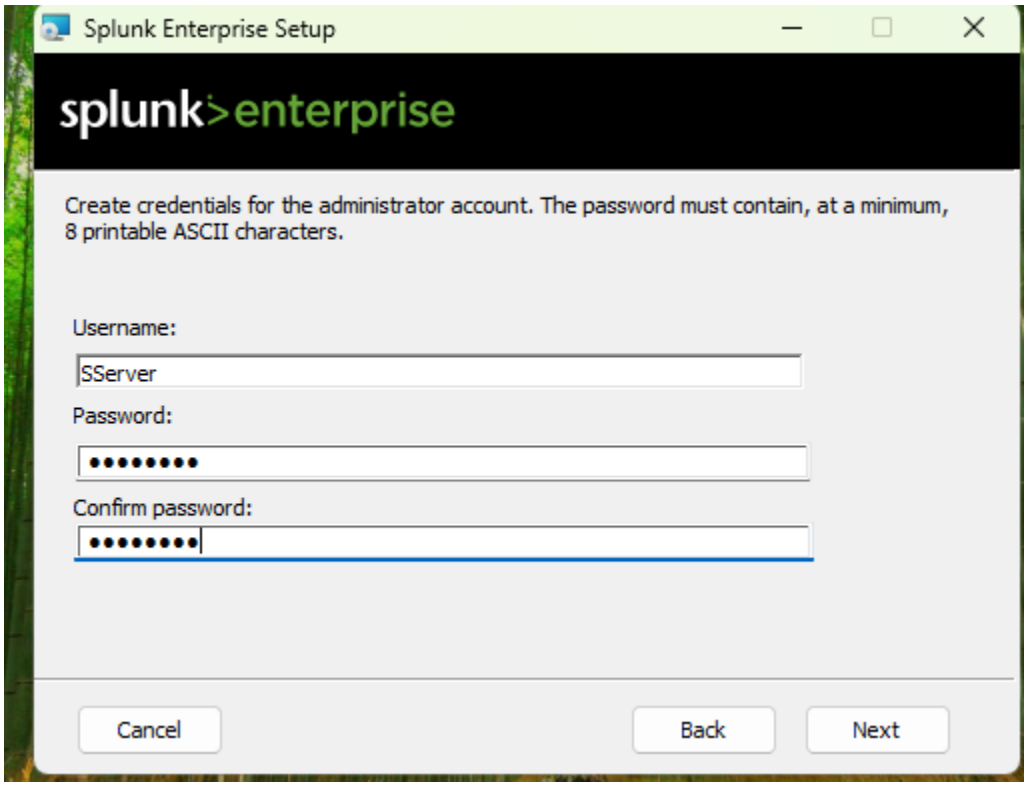
Click ‘Next’



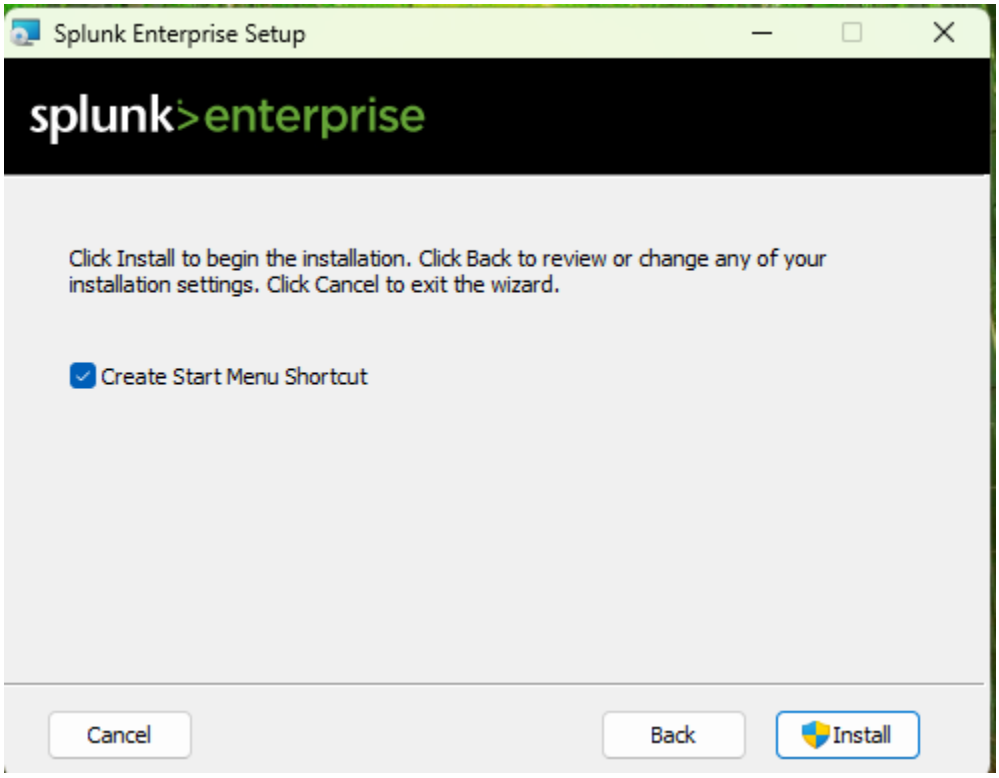
Check ‘Local System’ and click ‘Next’



Make your administrator account.

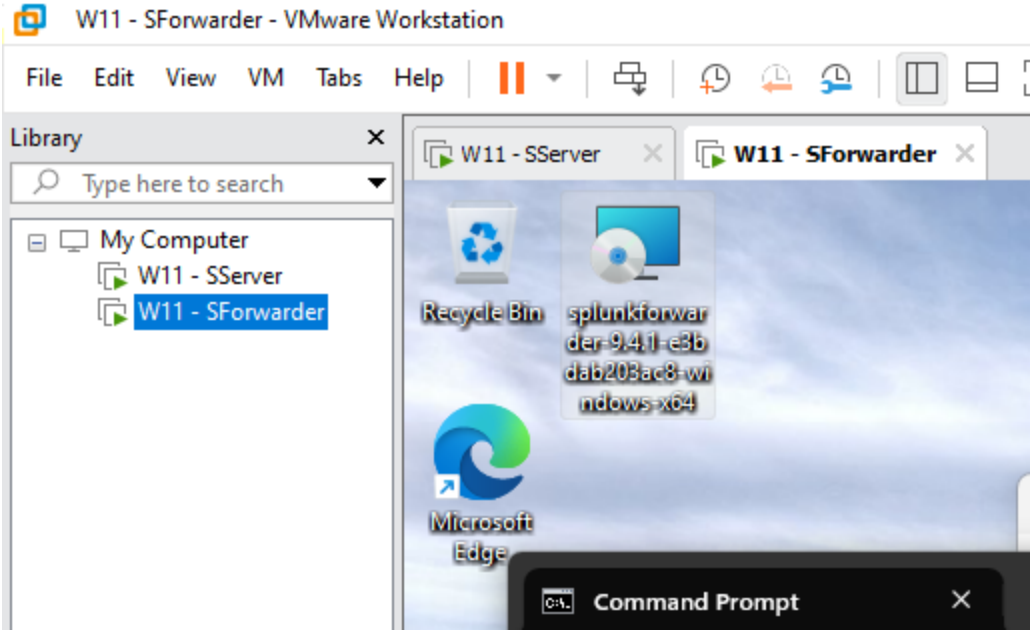


Install the Splunk Application.

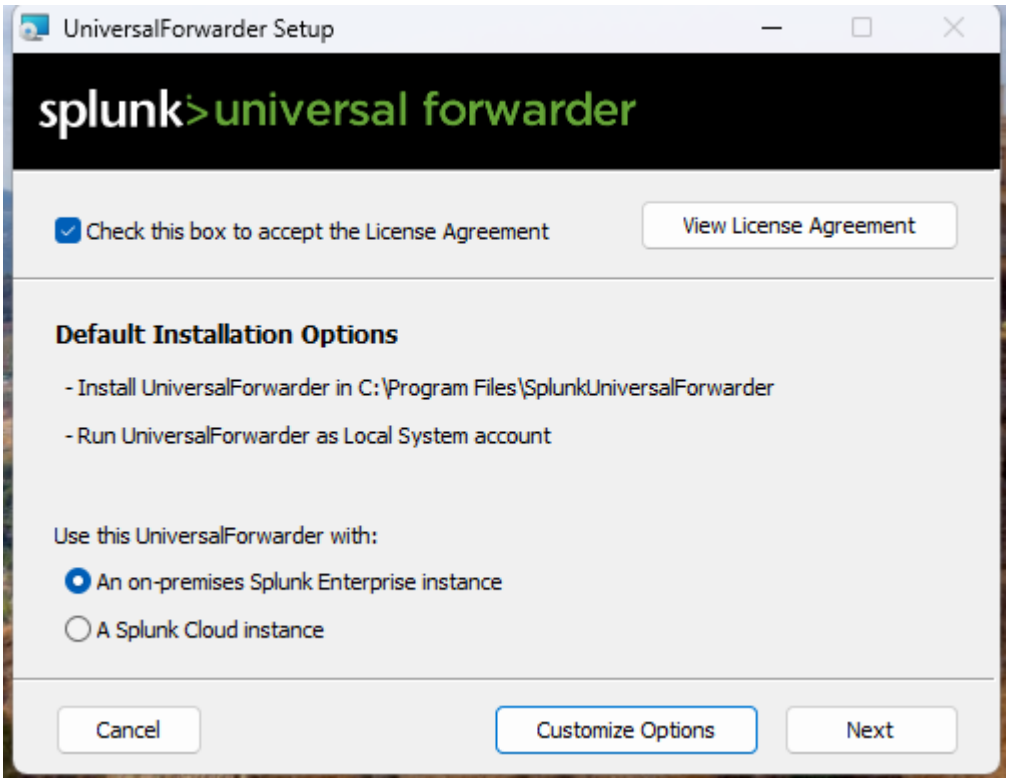


Splunk Forwarder Setup

You download the official Splunk Universal Forwarder and run the application located wherever you downloaded it. In this case, we saved it to desktop for easier access.

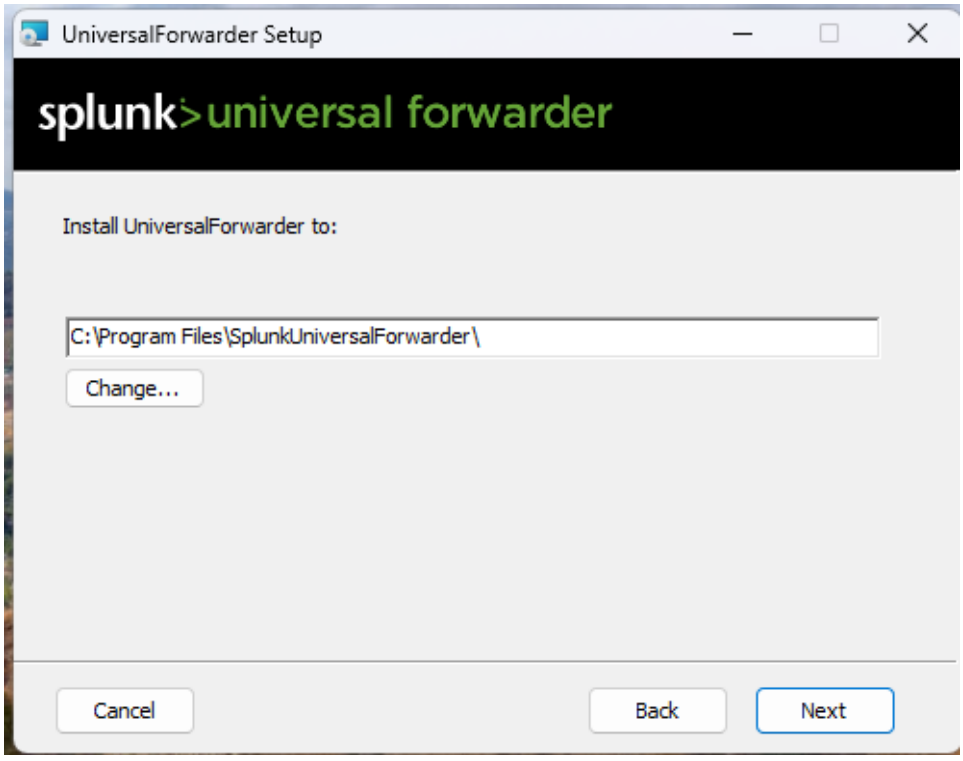


We check the box to accept the license agreement and select ‘An on-premises Splunk Enterprise Instance’

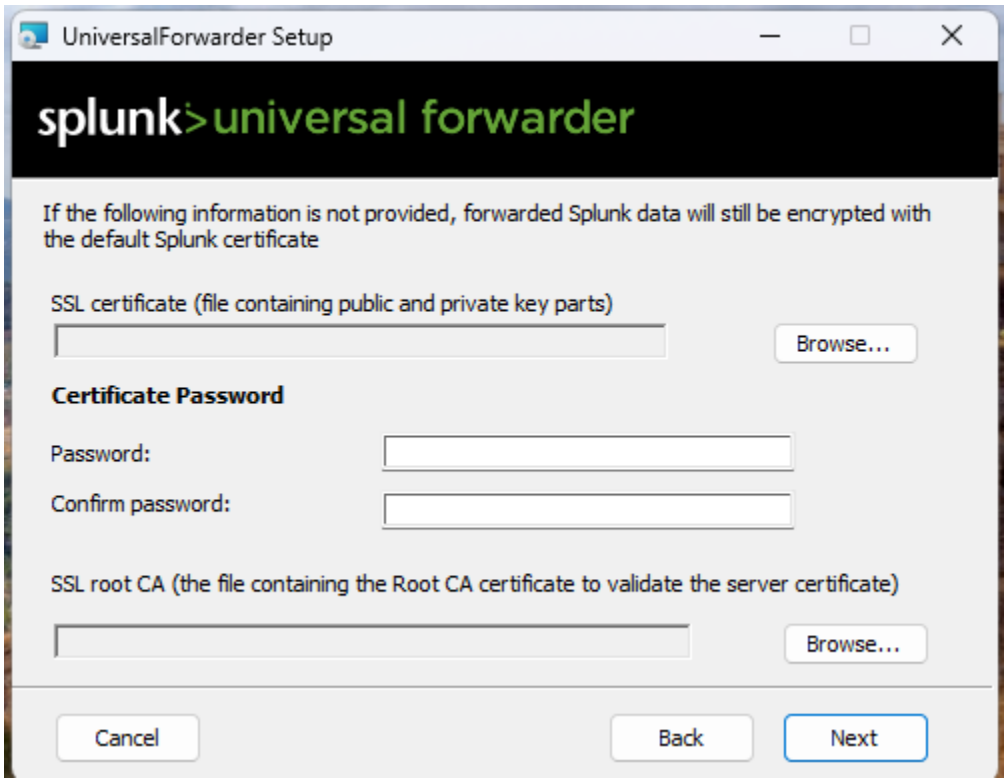


,

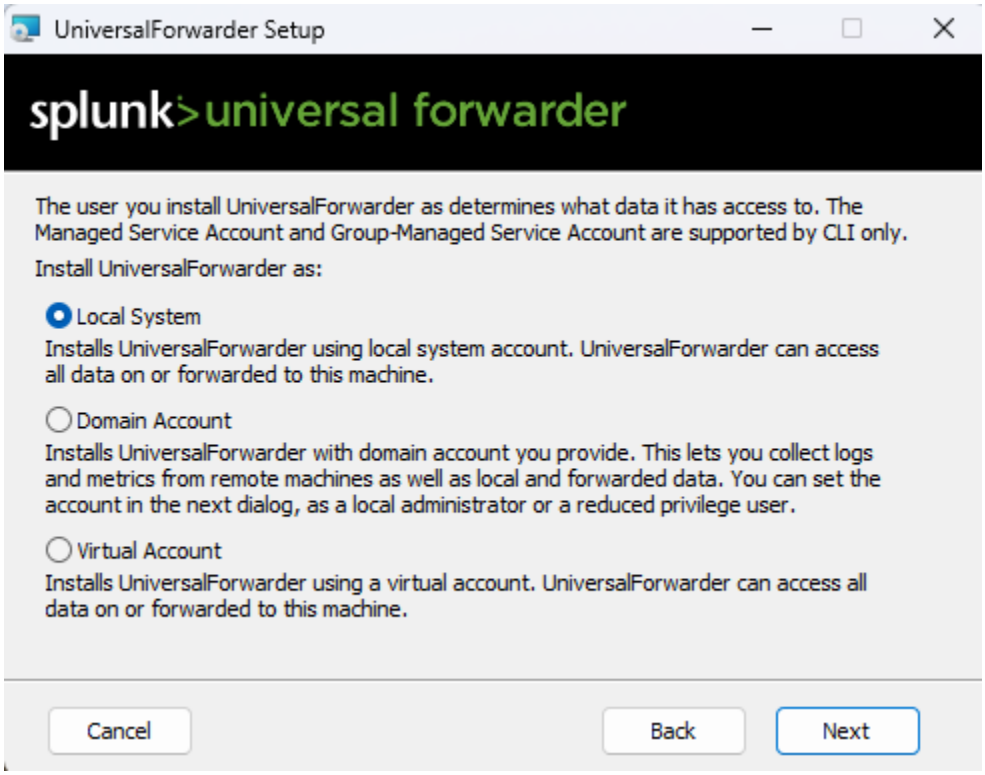
Click ‘Next’



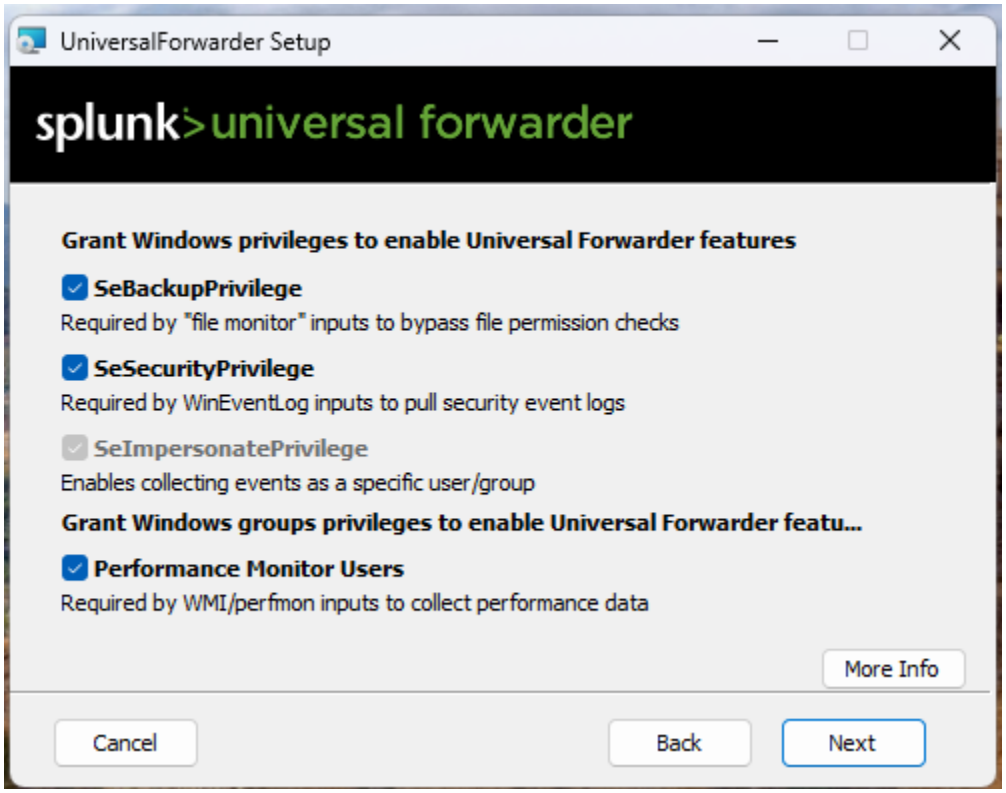
Select ‘Next’ on the SSL page.



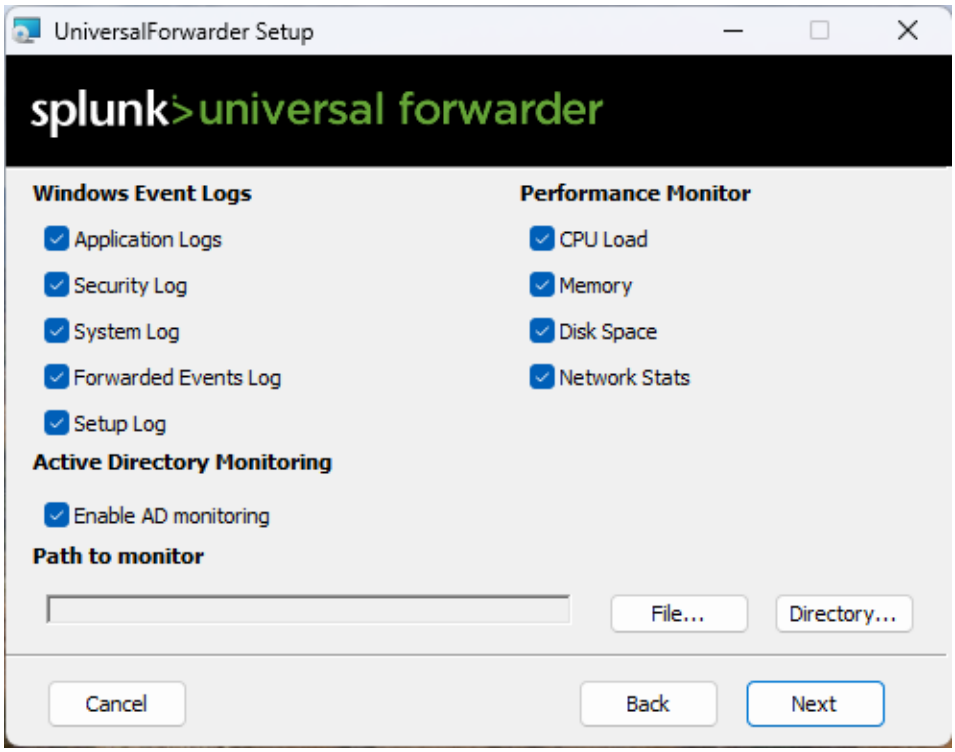
Select ‘Local System’



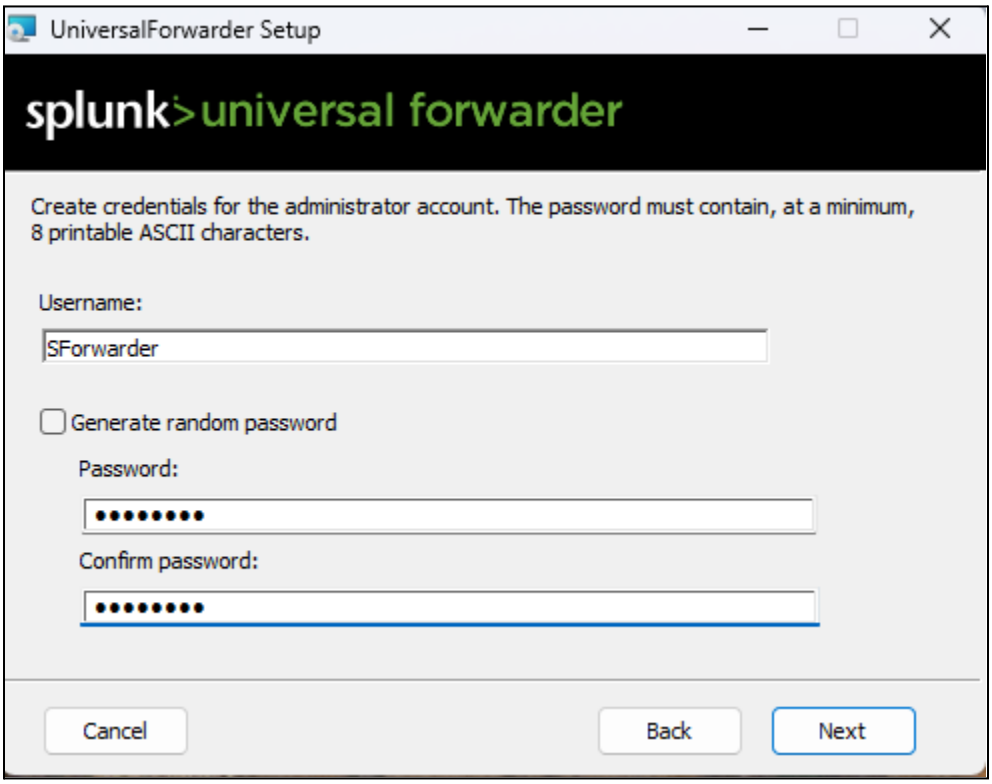
The default is fine. Click ‘Next’



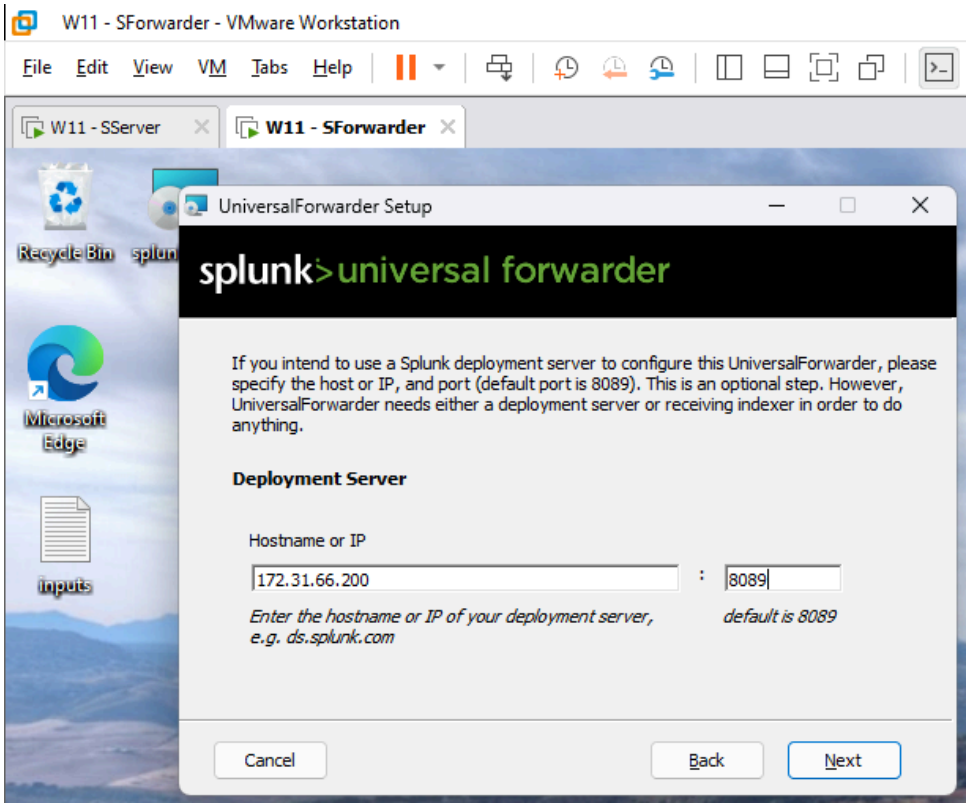
Check all the boxes to get all the logs to forward.



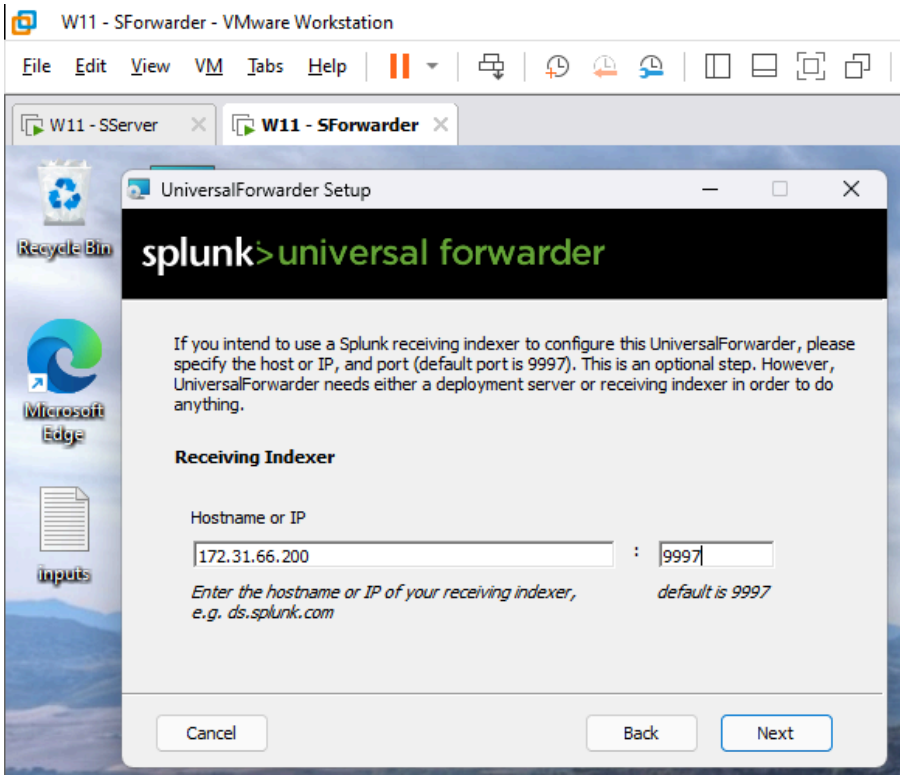
Make your administrator account.



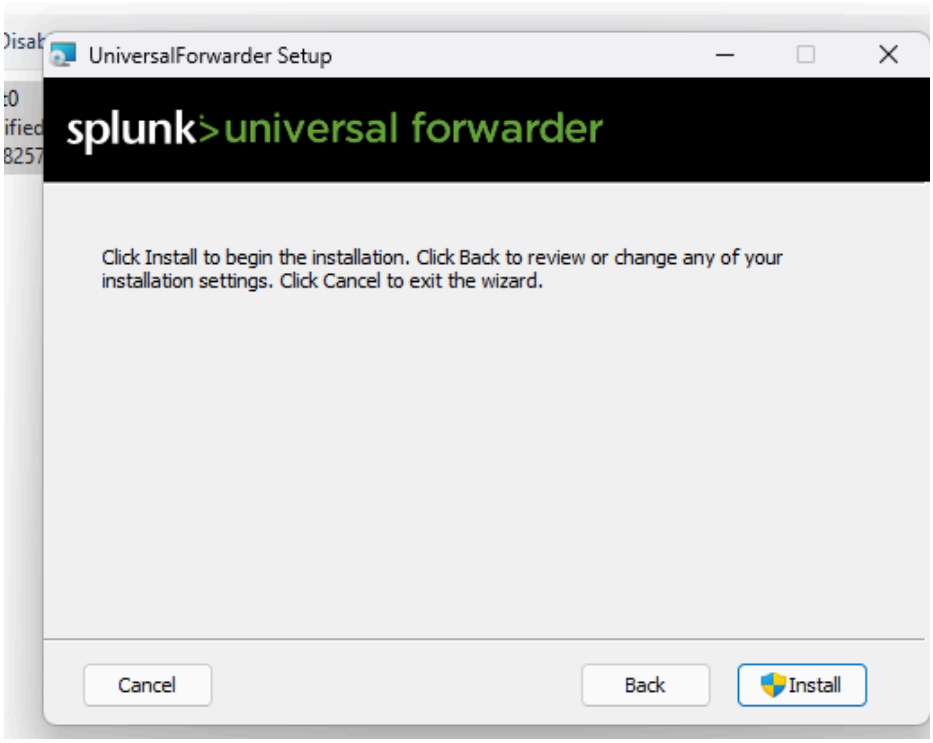
Specify the IP of the Splunk Server at 8089.172.31.98.200 for Burnaby.



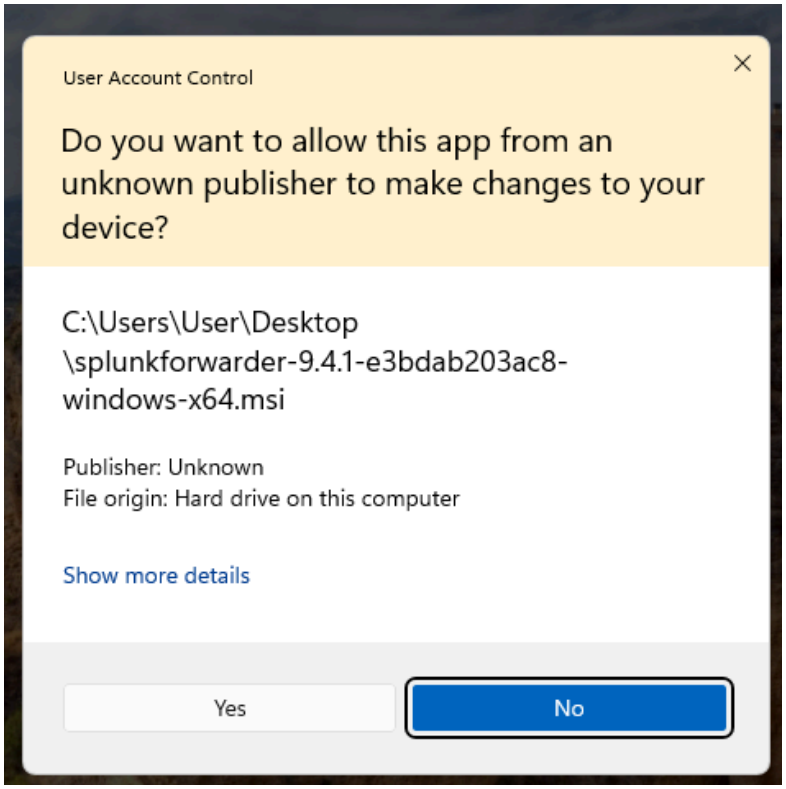
Specify the IP of the Splunk Server at 9997. 172.31.98.200 for Burnaby.



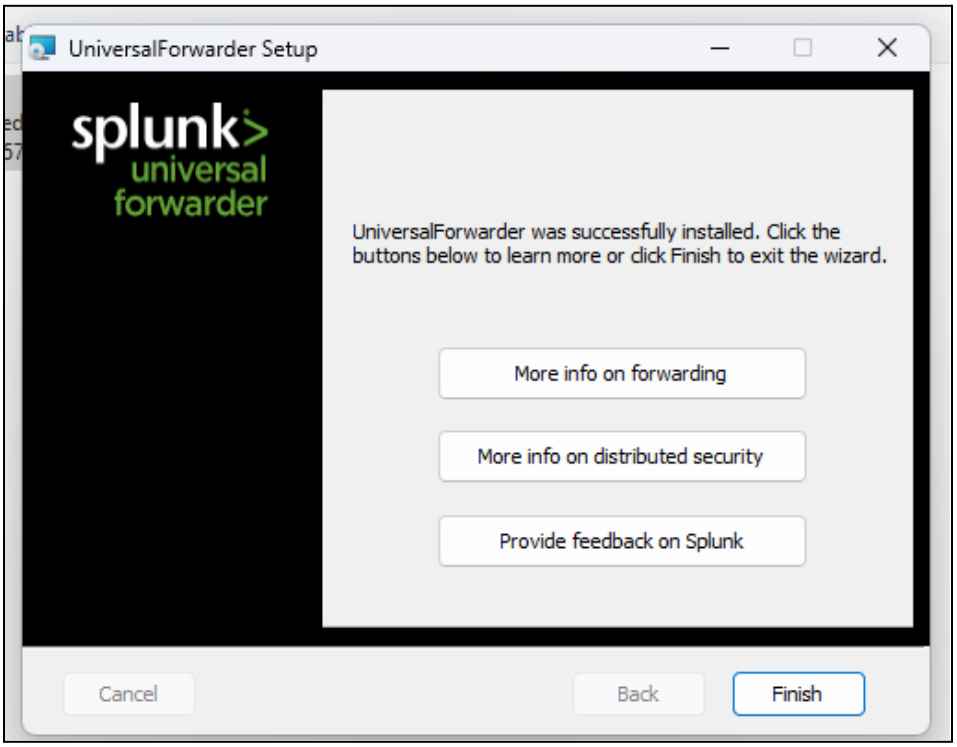
Click ‘Install.’



Click ‘Yes’ on the prompt.

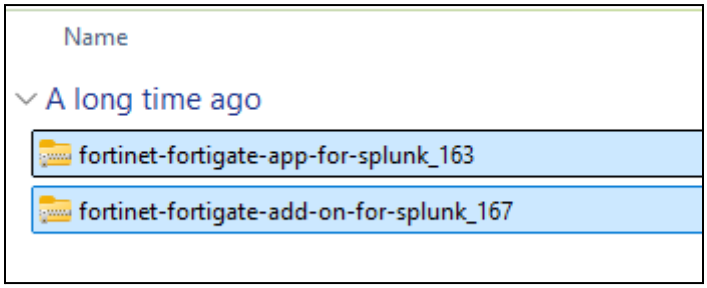


Click ‘Finish’

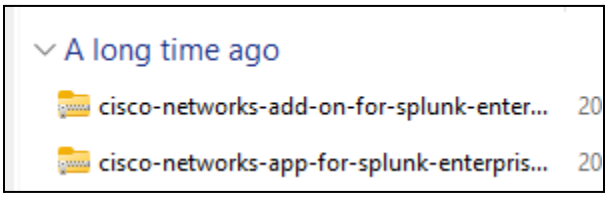


Splunk Server FG & Cisco, UDP & Index Setup on both Site VM

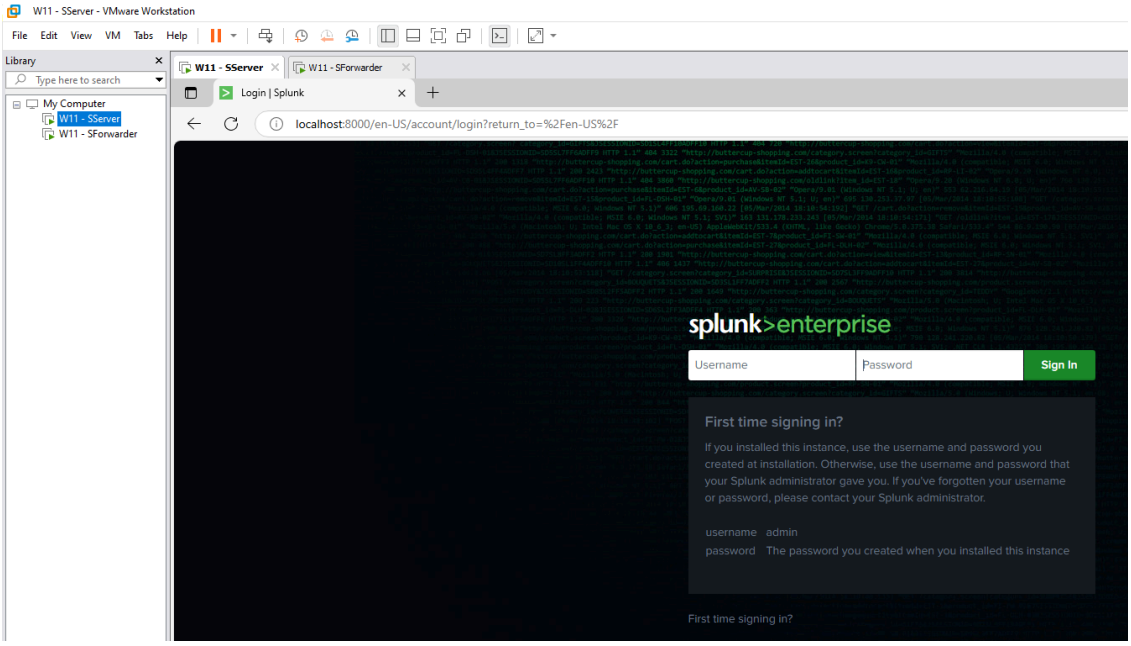
Download your own FortiGate Apps and Add-On and save it to your Server



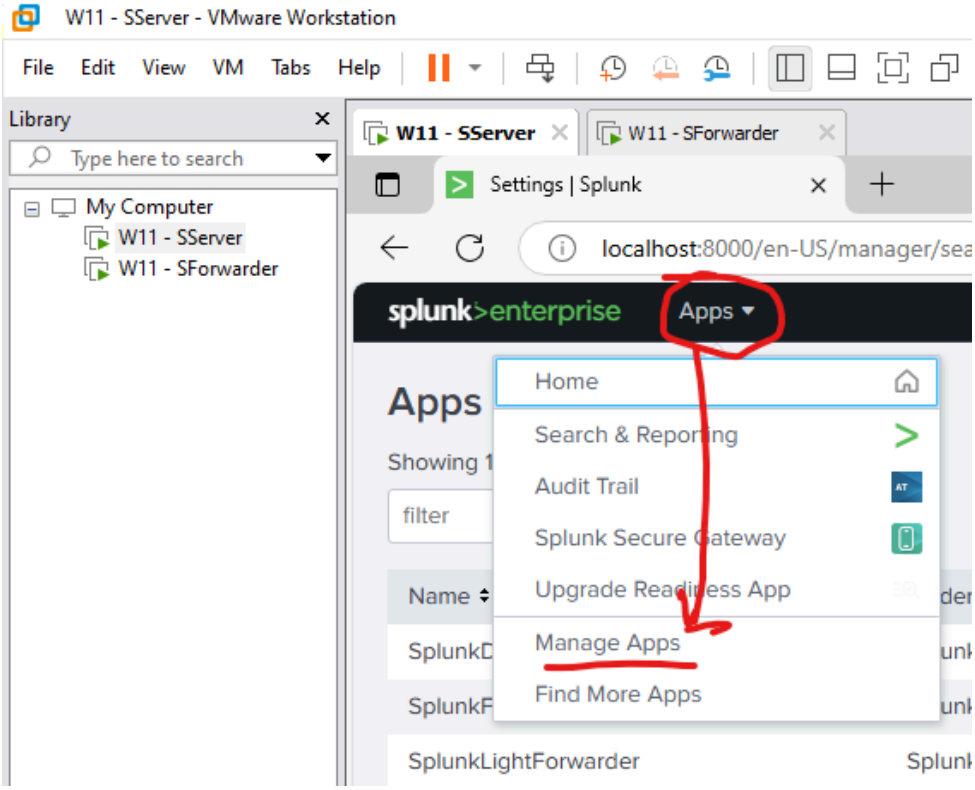
Download Cisco Network Apps and Add-On as well.



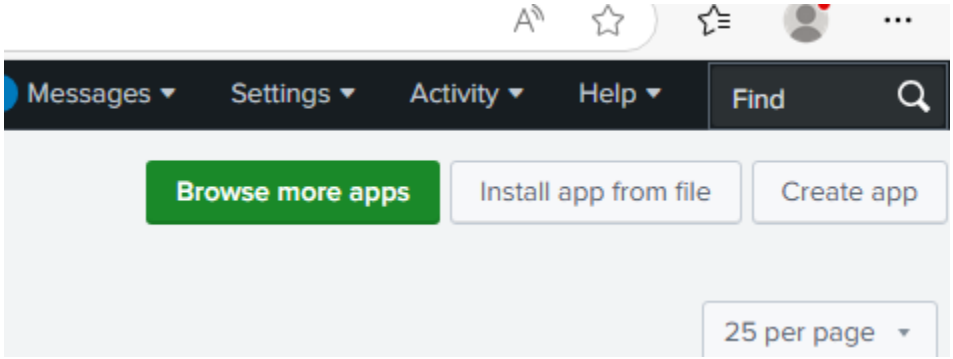
Go to either ‘localhost:8000’ or ‘127.0.0.1:8000’ which will bring you to the Splunk Login page. Sign in.



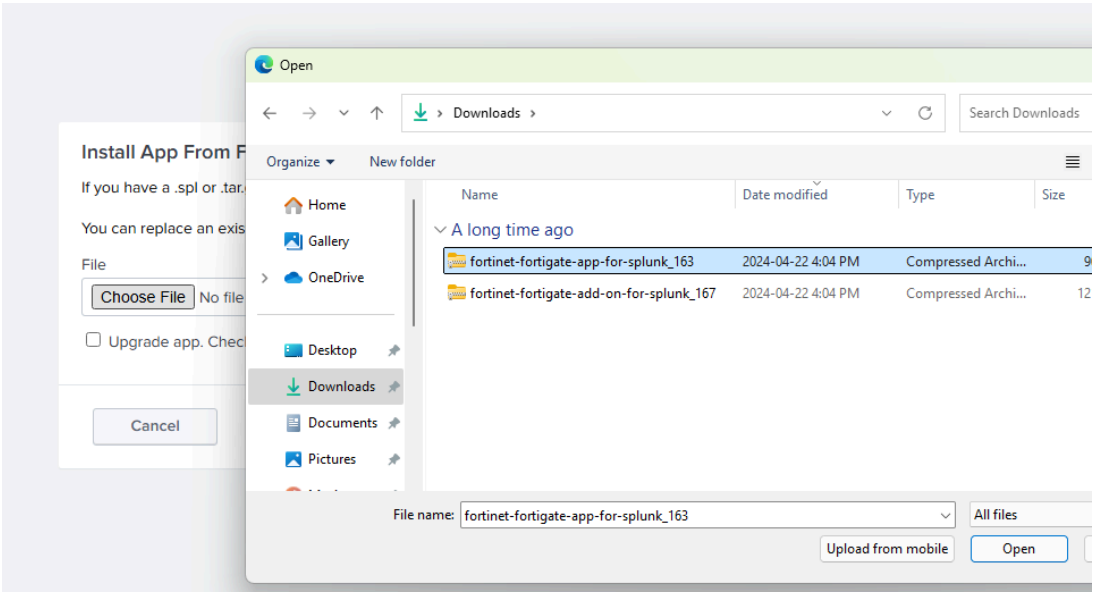
Go to ‘Apps’ and then ‘Manage Apps’

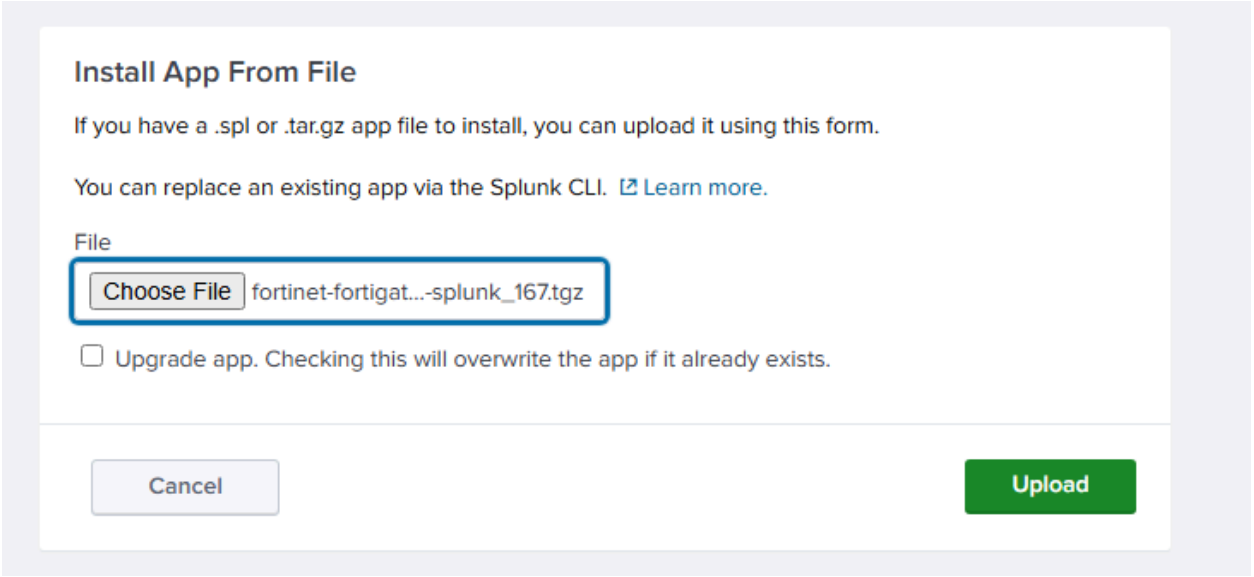


Then click on ‘Install app from file’



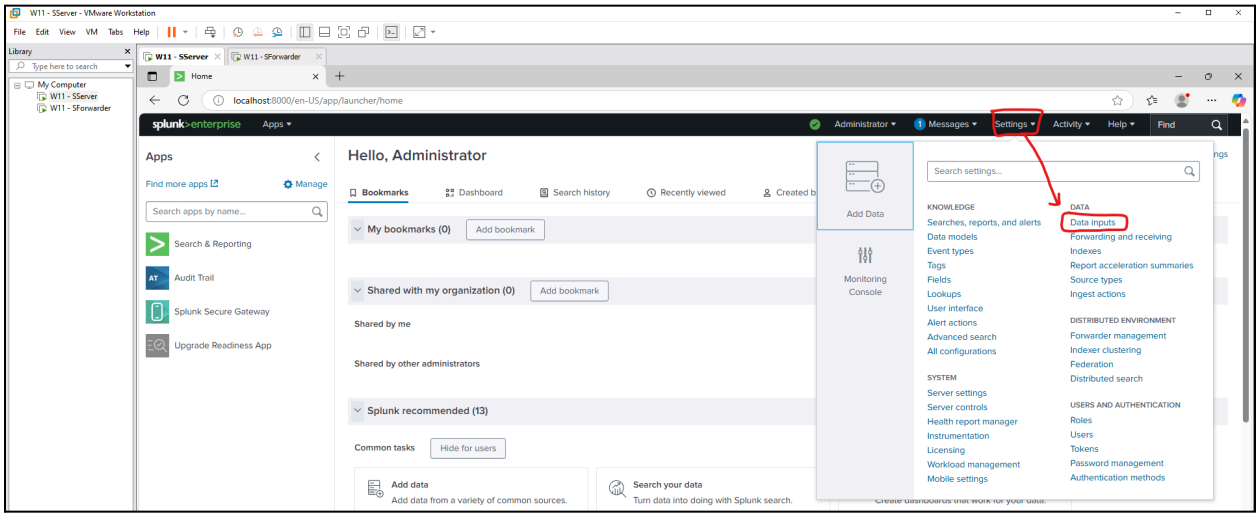
Click ‘Choose File’ and select the **FortiGate App ZIP** file then Upload. You will then do the same for the **Add-On ZIP** file **after**.



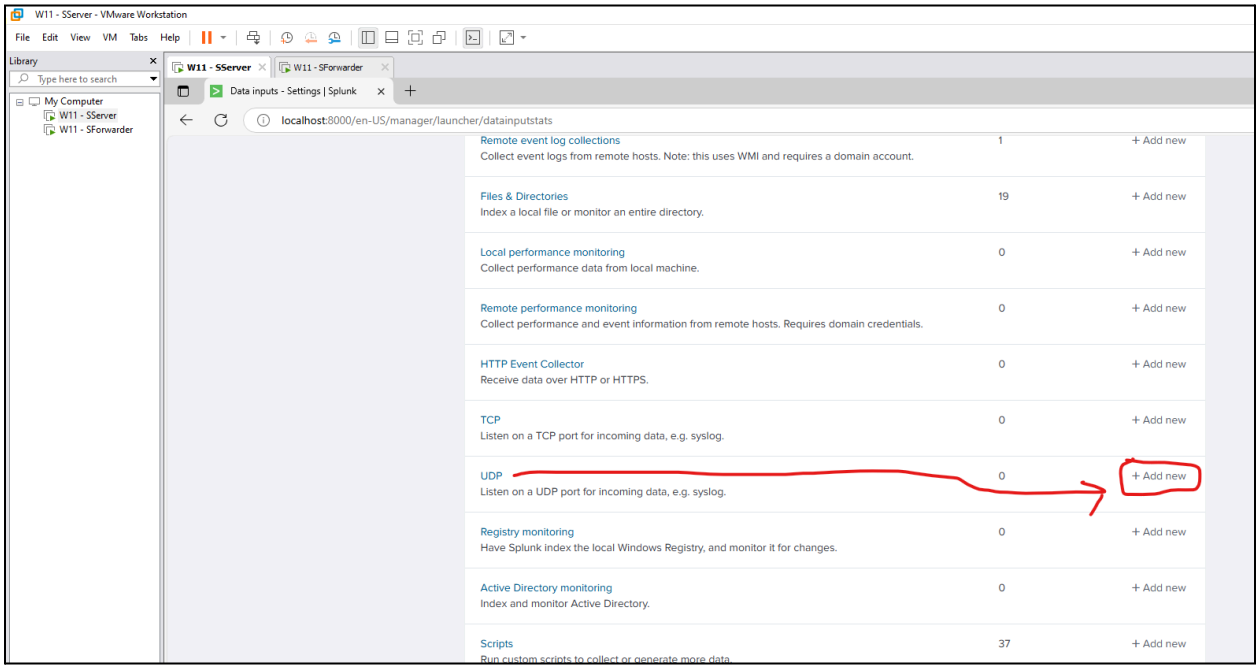


Do the same previous steps but this time for **Cisco Network Apps and Add-On.**

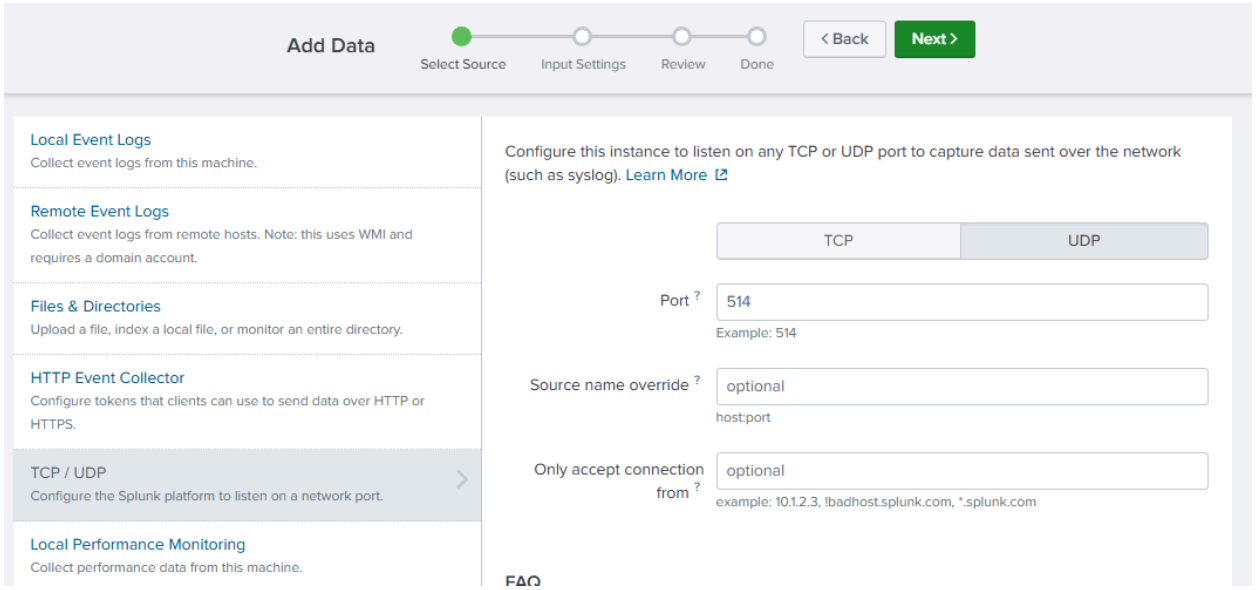
Go to ‘Settings’ then ‘Data Inputs’



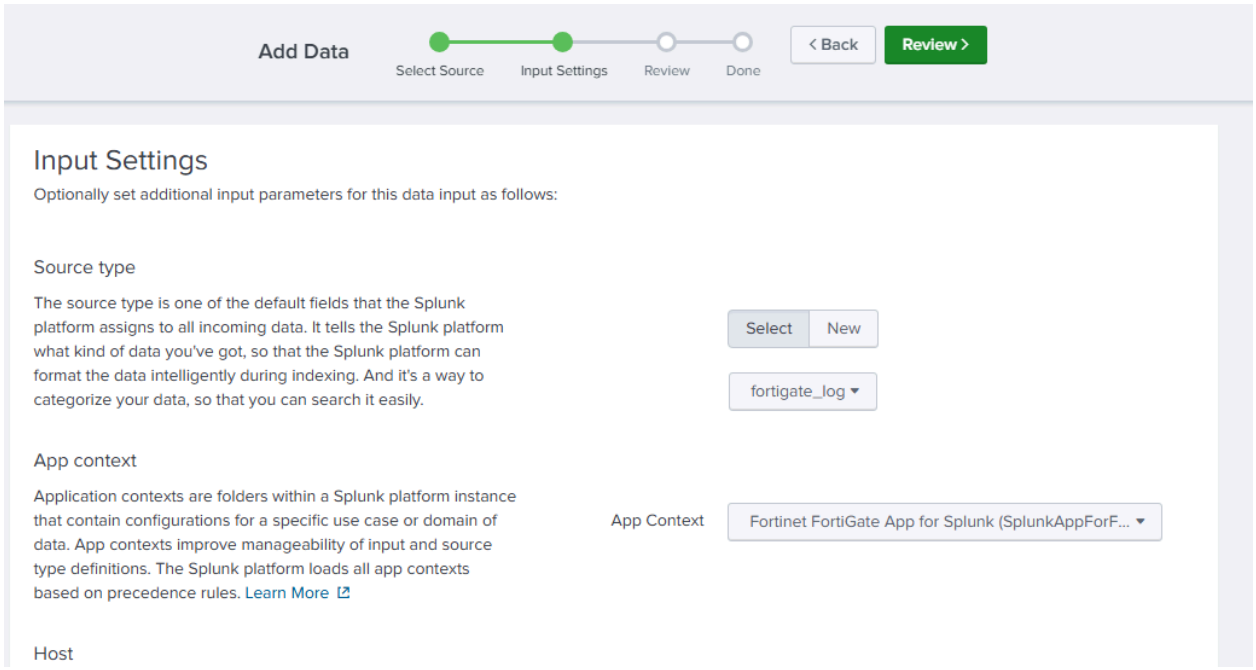
Then scroll down and click ‘Add New’ at the UDP section.



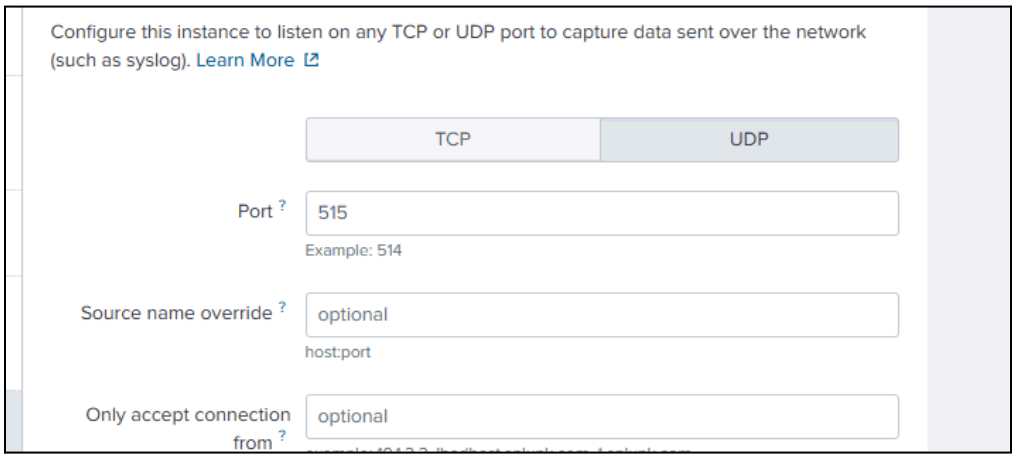
Then for ‘Port’, enter a custom Port number for your Apps, so, in our case, we do 514 for the FortiGate. Click ‘Next.’



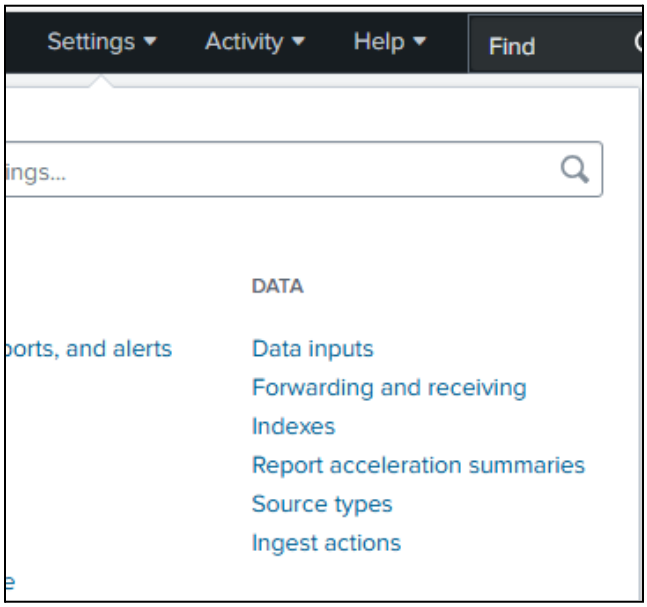
For Source Type, type “fgt_log”. For App Context, select the FortiGate App. Review and Submit.



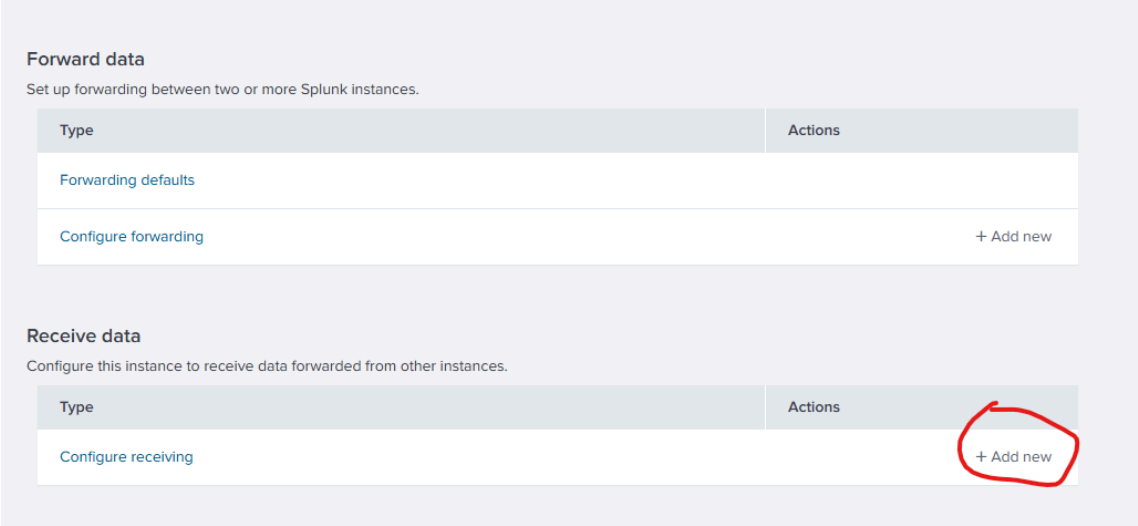
We will do the same previous steps again but this time for **port 515**, **sourcetype: cisco:ios**, and **App Context: Cisco Network**s. Complete the steps.



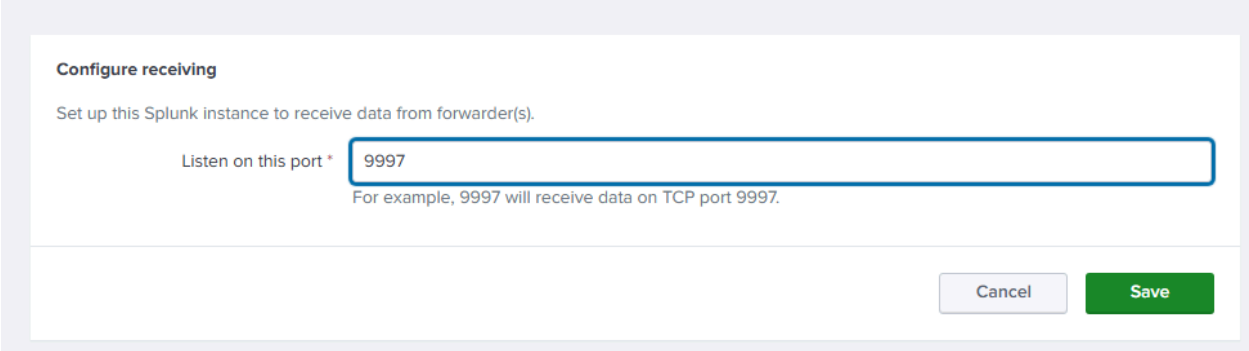
After, go to ‘Settings’ then ‘Forwarding and Receiving.’



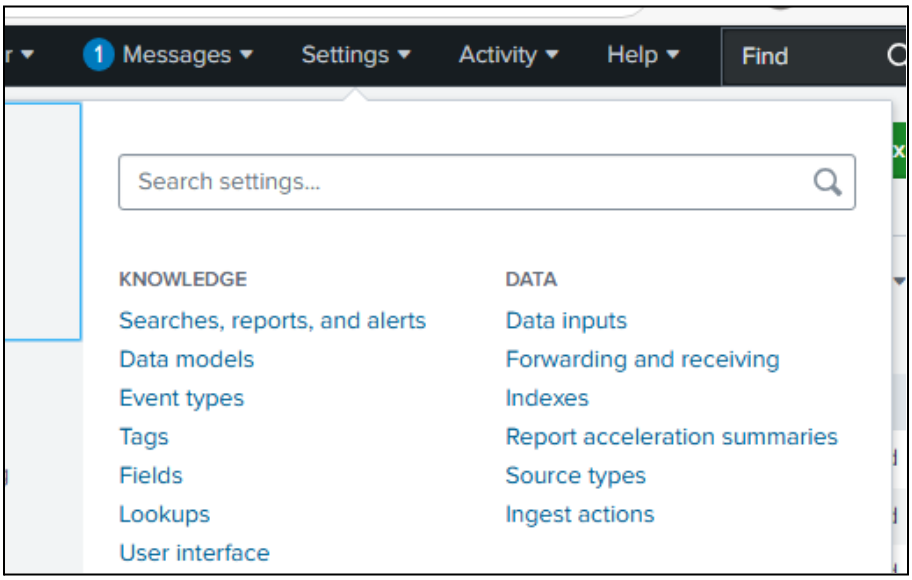
Under ‘Receive Data‘, for ‘Configure Receiving‘, click ‘+Add New.‘



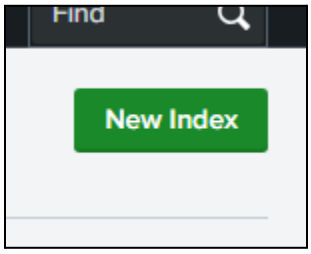
Type in ‘9997’ as we set it up earlier in the initial Splunk Forwarder setup.



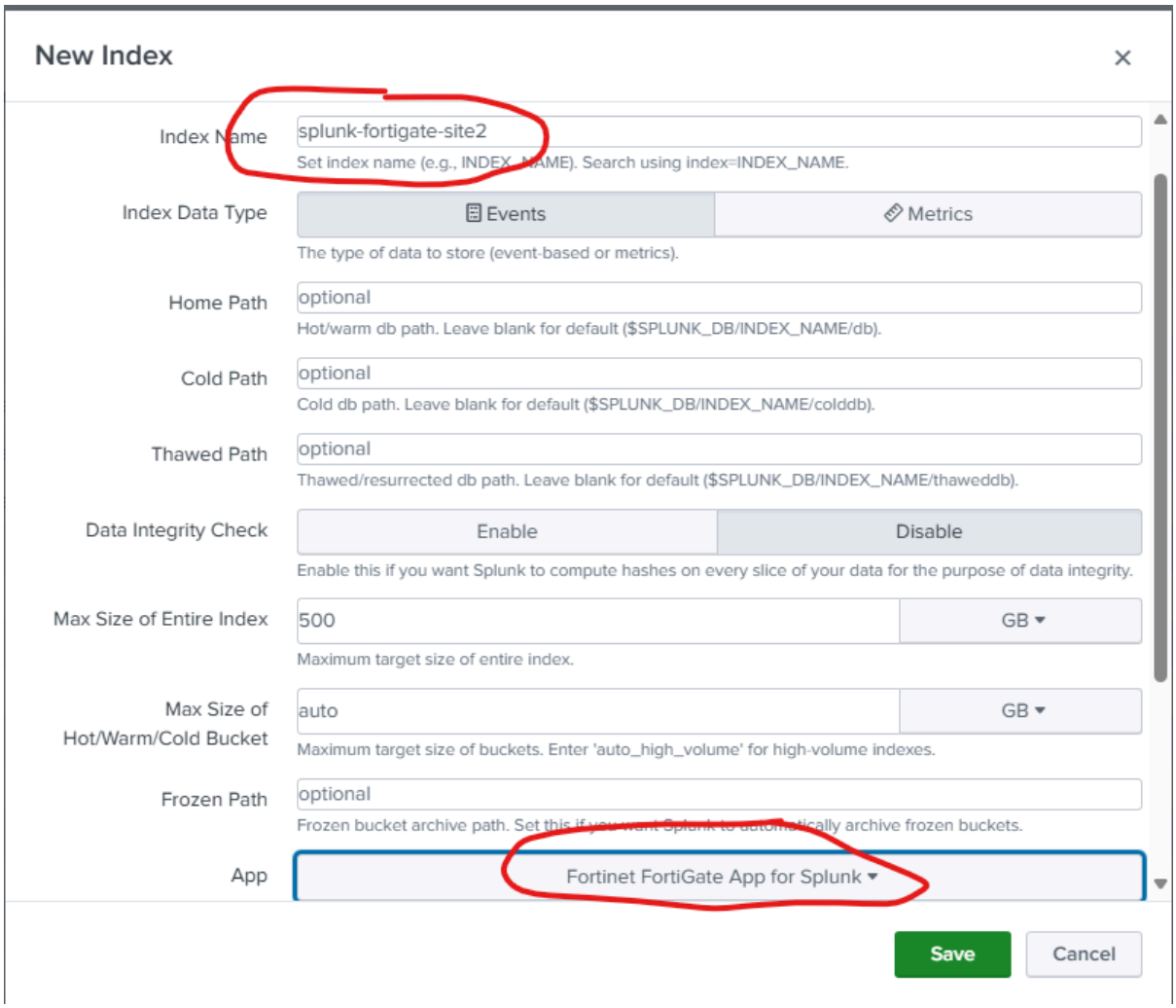
Then go to ‘Settings‘, ‘Indexes‘

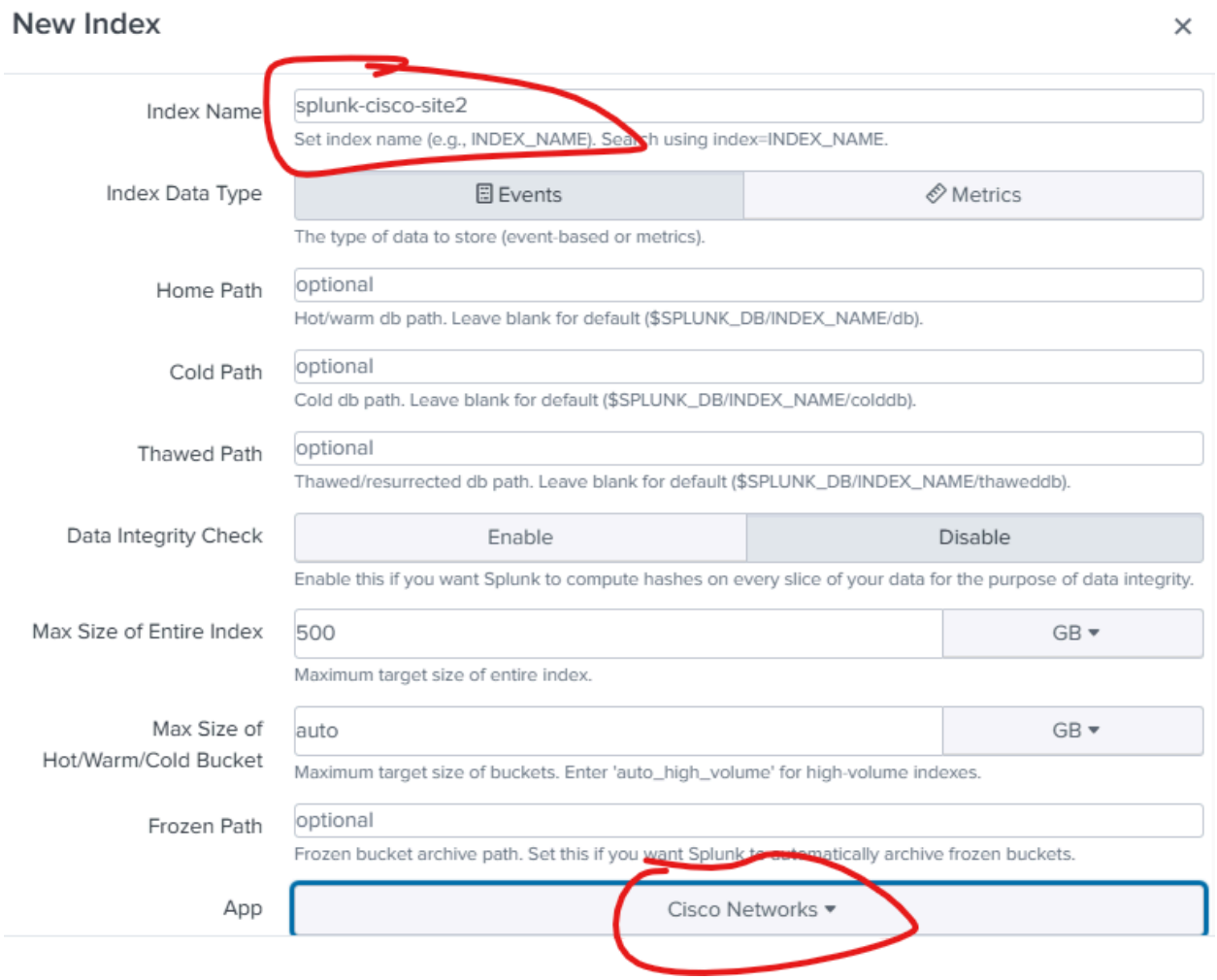


Click ‘New Index’

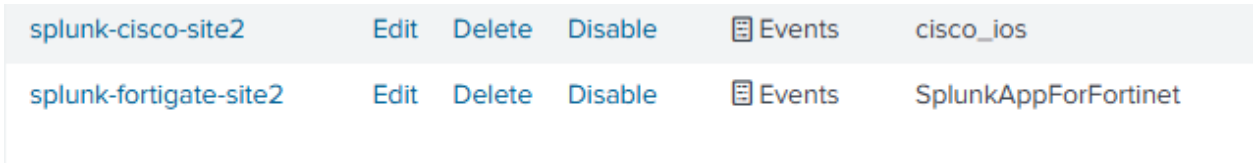


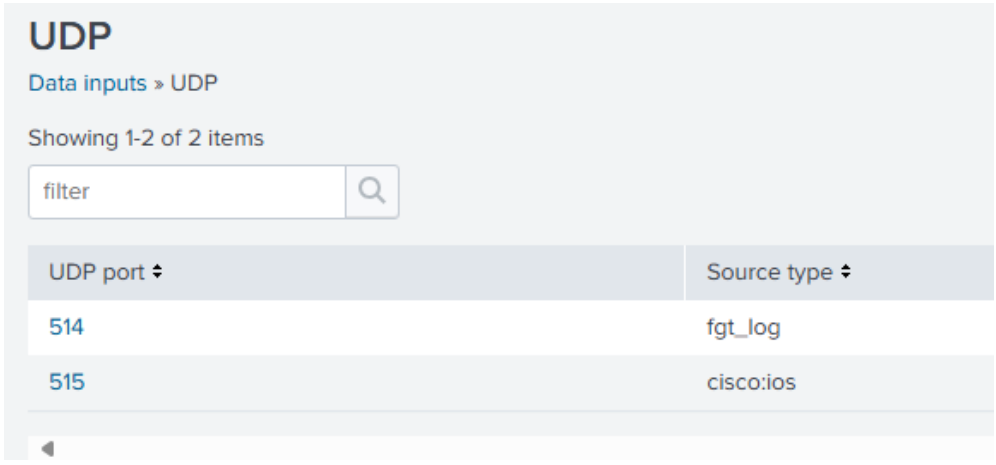
Configure the ‘Index Name‘ and ‘App‘ like so accordingly. We use the index name ‘**splunk-FortiGate-site2‘** and ‘**splunk-cisco-site2‘** for our Index name and App Fortinet and Cisco Networks respectively. **Change the ‘site2’ to ‘site3’ for Burnaby.**





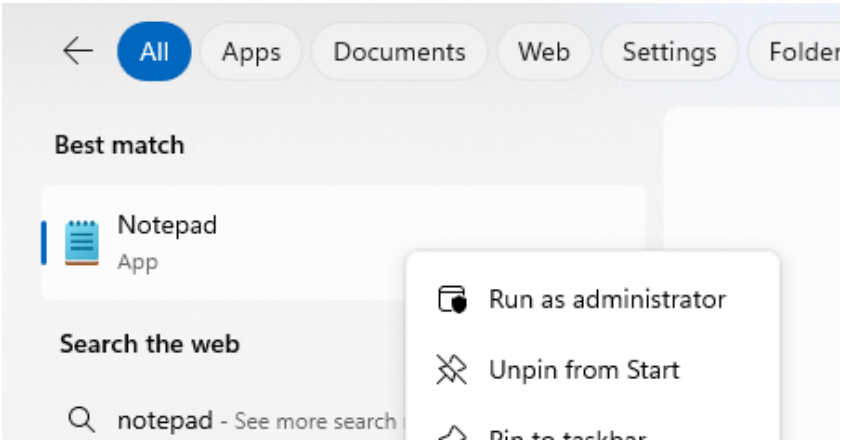
You should see this in **Indexes** and **UDP** if done correctly. Site3 for Burnaby.



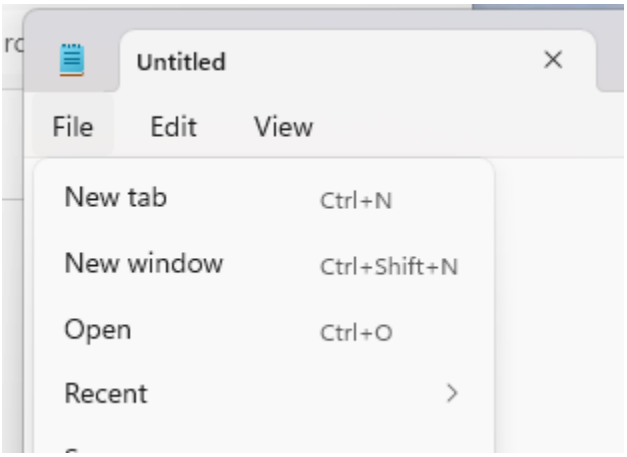


Splunk Forwarder Conf File Configuration

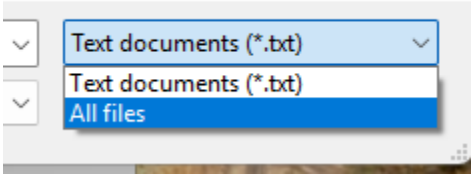
Open Notepad in Administrator Mode

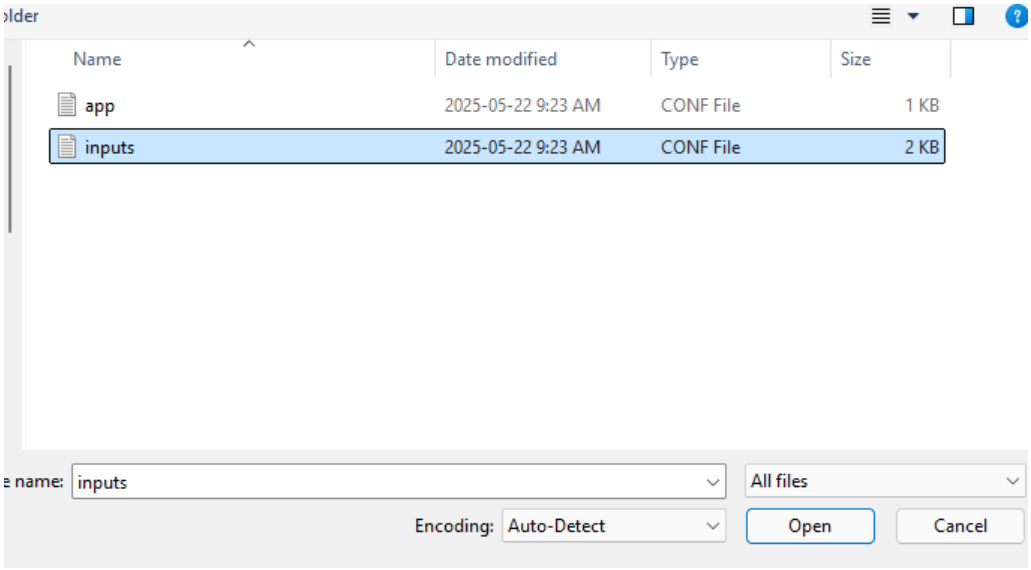


Go to ‘Files‘ then ‘Open‘

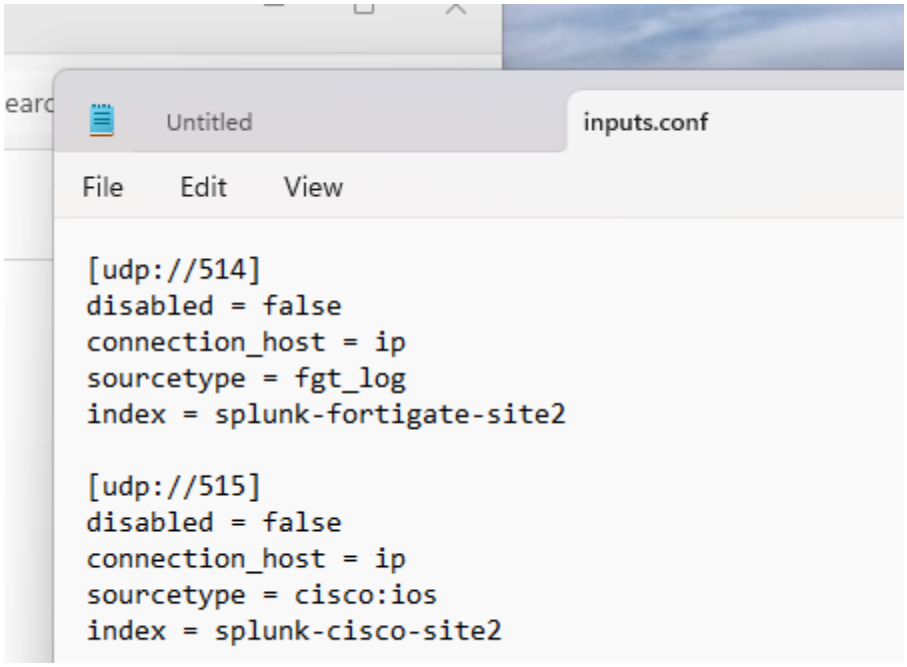


Go to **C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local**. Change the ‘.txt‘ to ‘All Files‘ then select the ‘inputs.conf‘ file.

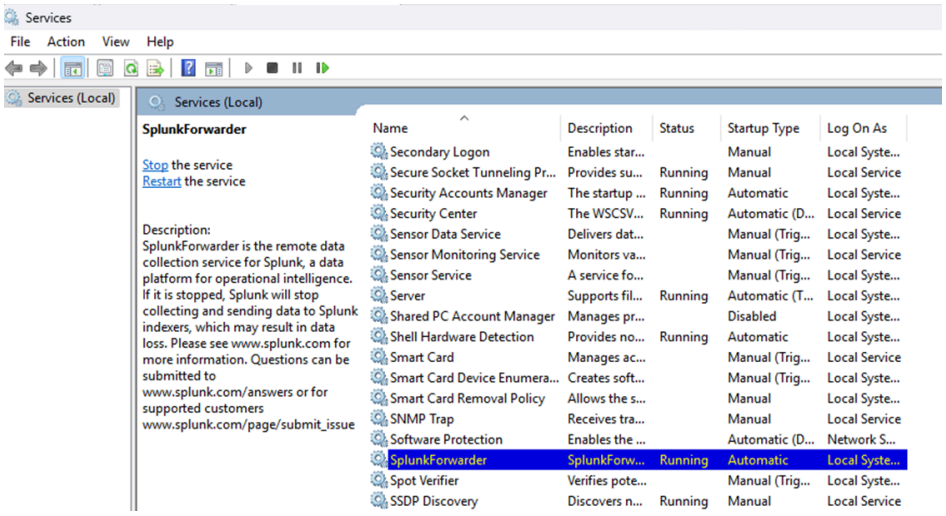




Add the following at the top with proper spacing and save. This will allow the forwarder to listen and send logs at the specified ports to the proper index on Splunk Server with appropriate sourcetypes for each log source.

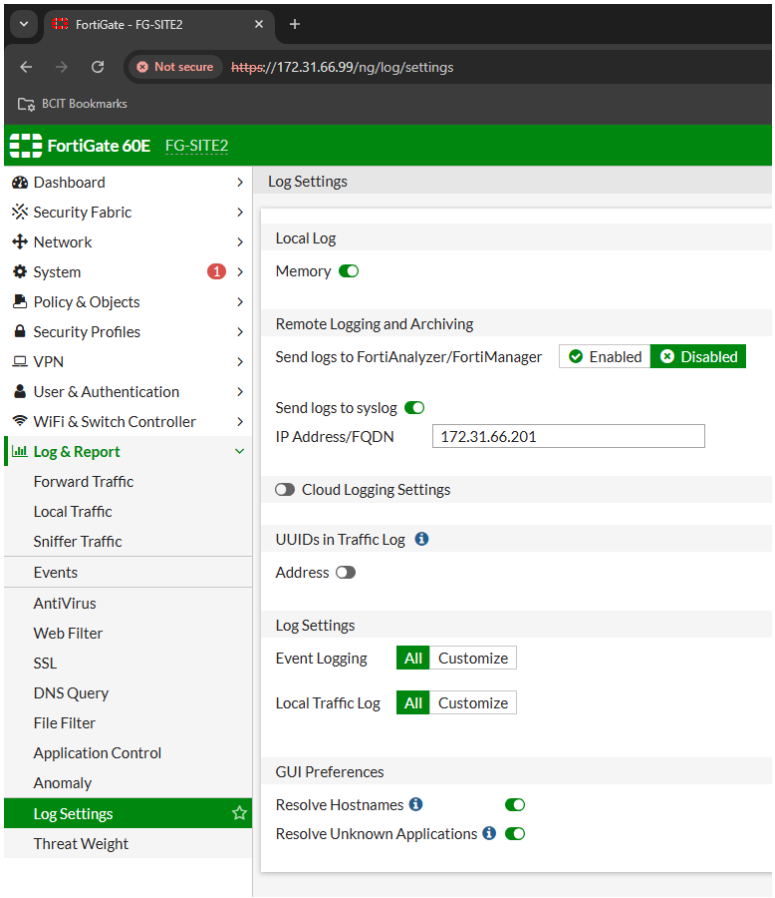


We need to restart the SplunkForwarder service because we configured the inputs.conf file.



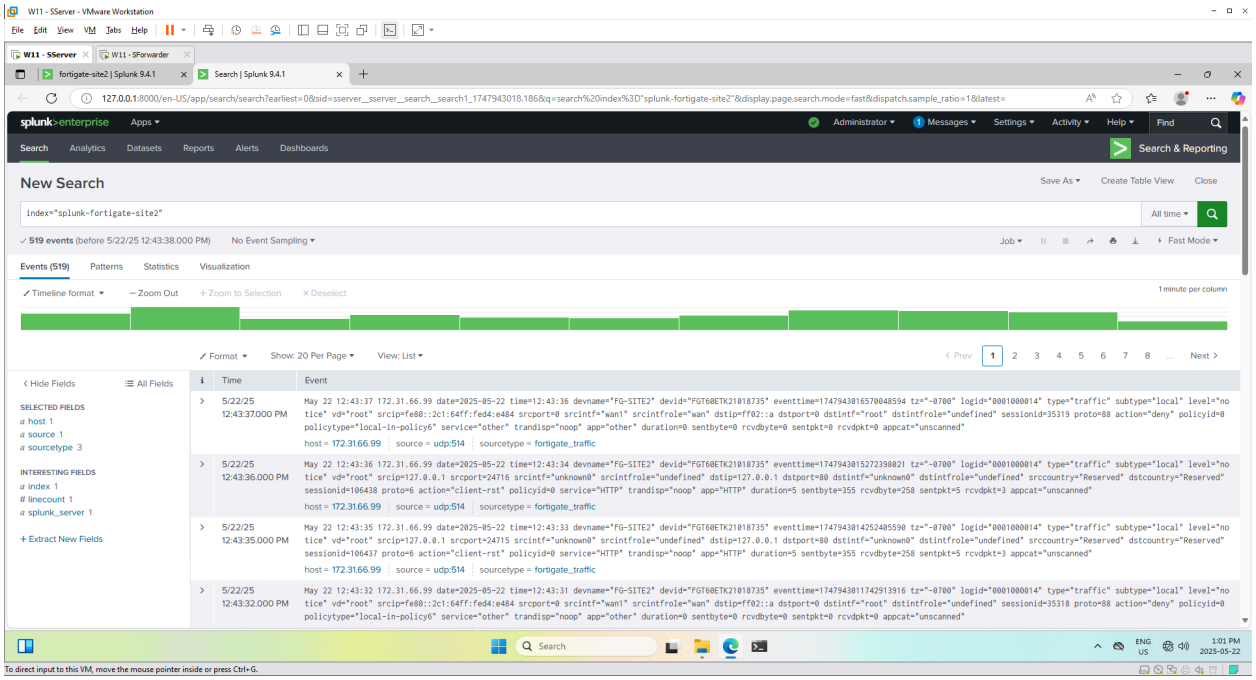
FortiGate Logging Setting Setup

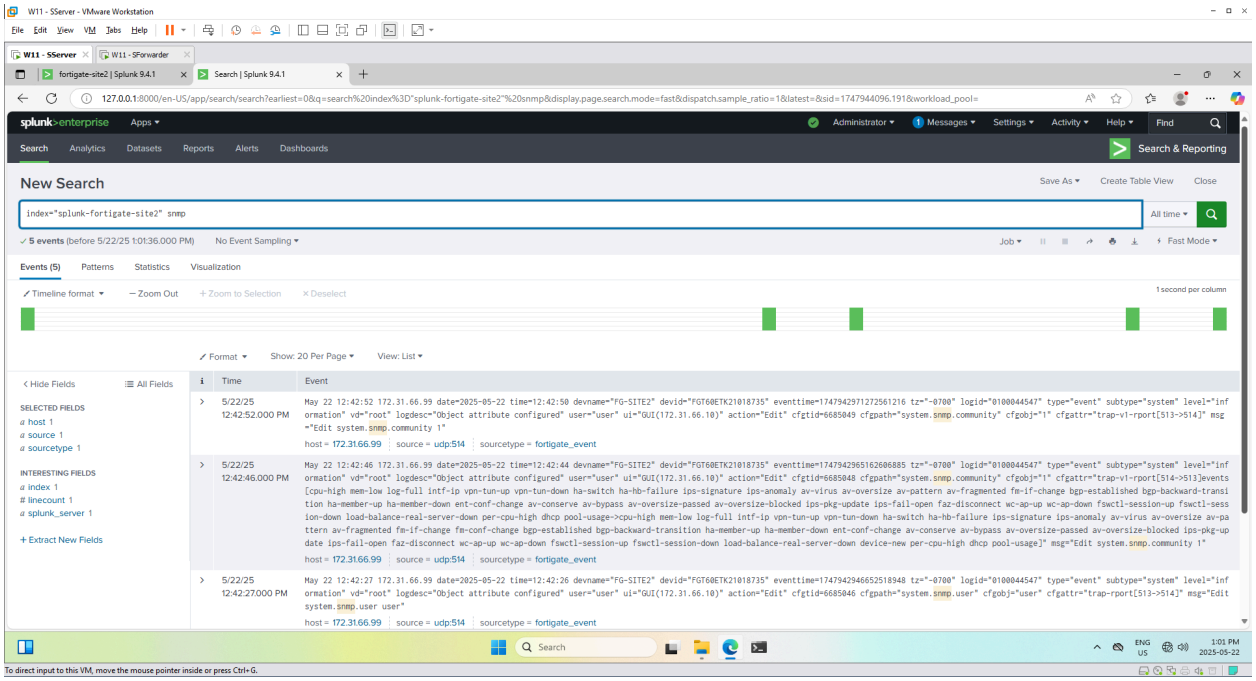
Go to ‘Log & Report’ then ‘Log Settings’. Enable the ‘Send logs to syslog’ and enter the IP address of the Splunk Forwarder which will then forward the logs to the Splunk Server. We also change ‘Local Traffic Log’ to ‘All’ so that all traffic logs are logged.



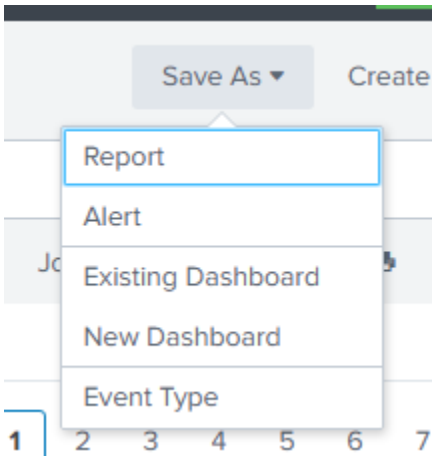
Verification of Fortigate Logs Received

Now, we go search for some FortiGate Logs like shown using queries like **index=”splunk-fortigate-site2”** and keywords with ‘***snmp***’, replacing site2 for site3 on Burnaby

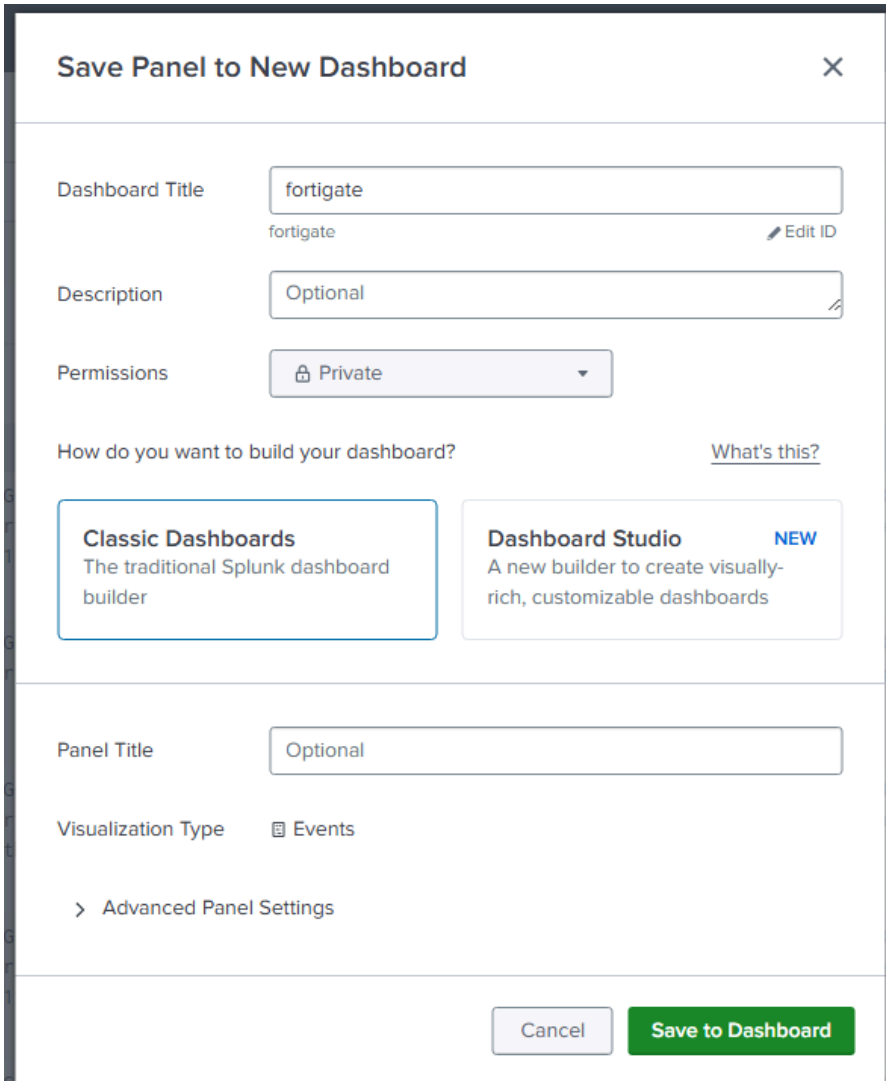




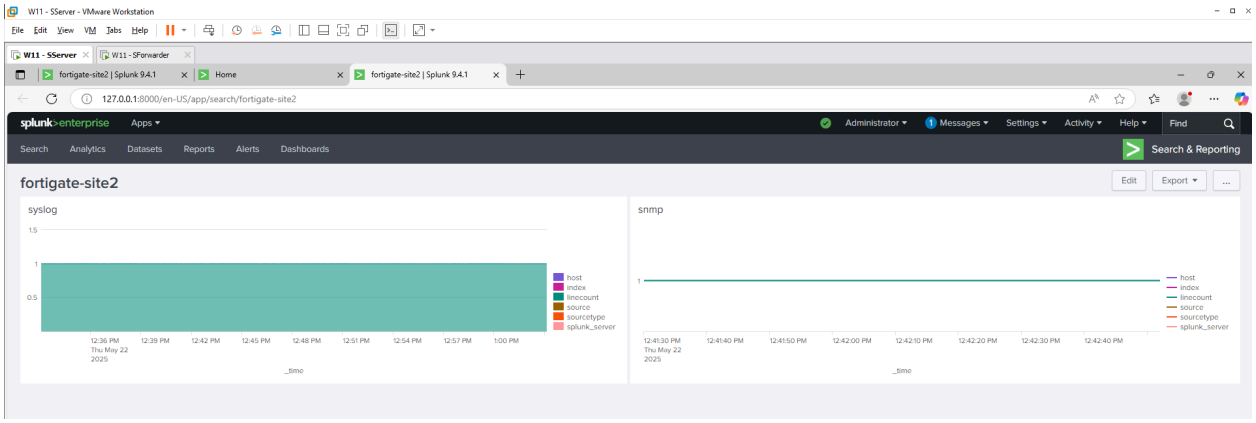
We can see that we are correctly receiving logs. Add this to a dashboard by going ‘Save As’, then ‘New Dashboard’.



Give a Dashboard Title, and select Classic Dashboards, then Save to Dashboard.

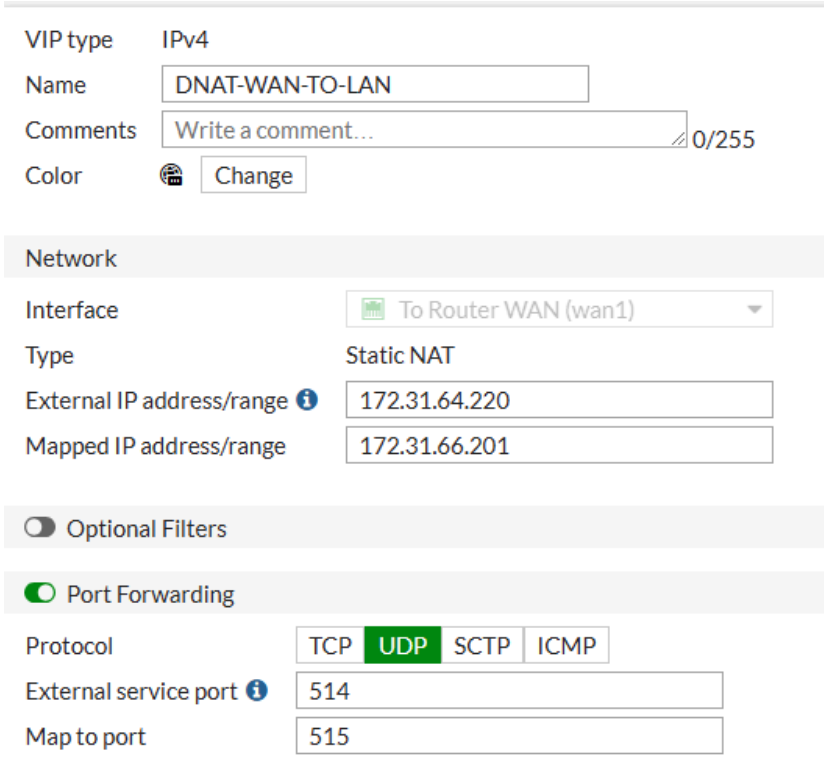


Repeat like so with the corresponding searches. Then you can view your dashboard with your custom queries in one place for easy viewing.

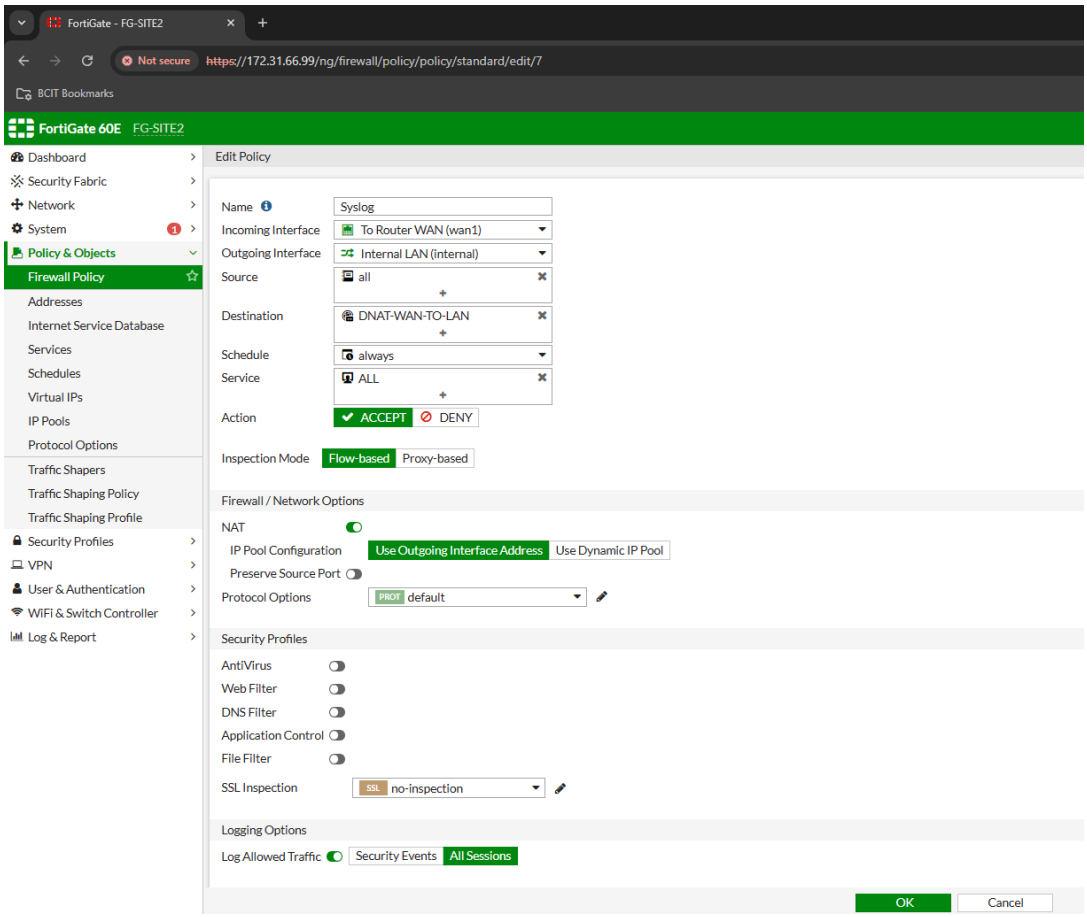


Cisco Logging Configuration

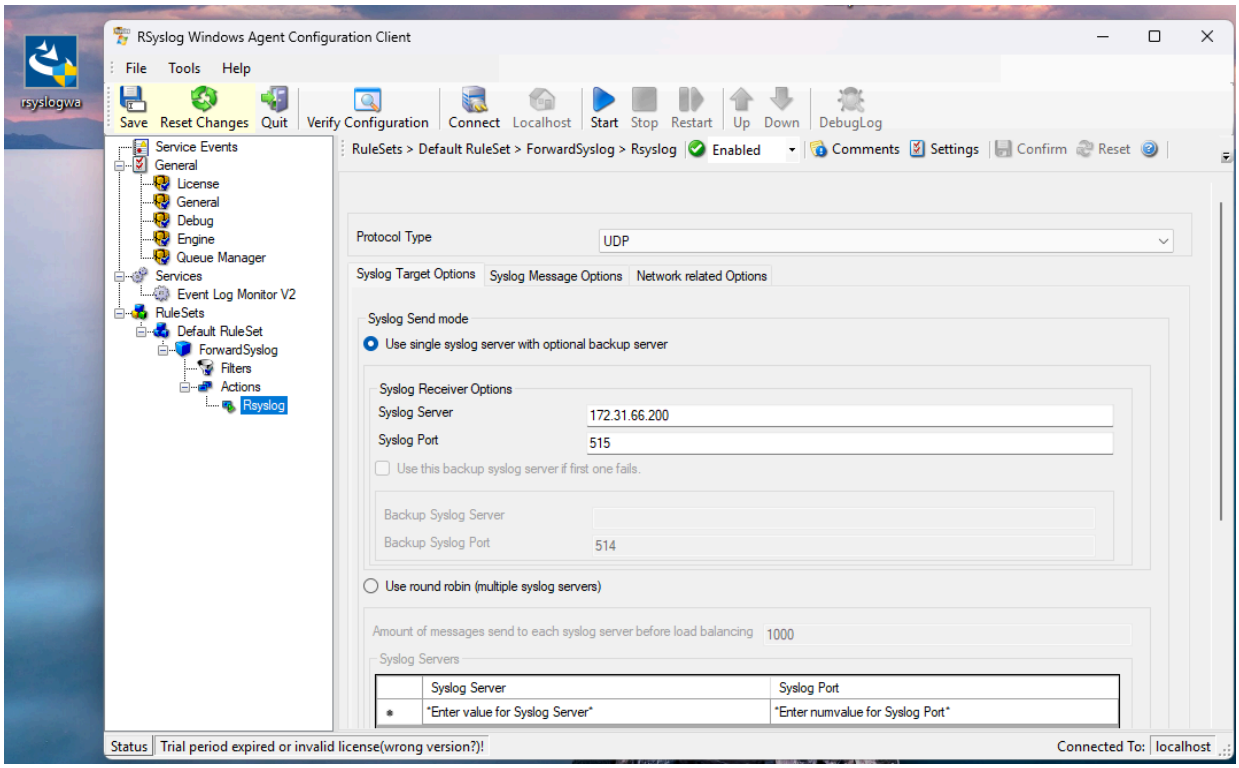
Configure a Virtual IP DNAT as followed. Give it a name, External IP is the Fortigate's WAN-facing interface IP, Mapped IP address is the Splunk Server IP, enable Port Forwarding for protocol UDP at External Service Port 514 to Mapped Port 515. Change the IP as accordingly.



Configure a Firewall Policy for the Cisco to Server with NAT enabled. The Destination is the Nat we created above. Follow it like so. You will do the same on the **other Site.**



On the SForwarder, we will need to download **rsyslog**, an open source log processing system which will collect and forward log messages over the network to listen on port 515 (coming from the Cisco Routers) and forwarding to the Splunk Server. Once you execute and install **rsyslog** from accepting the default configurations, open the program, and expand the path: RuleSets→Default RuleSet→ForwardSyslog→Actions→Rsyslog, then change the Syslog Server IP to the Splunk Server IP, and Syslog Port to 515 because of our inputs.conf configuration.

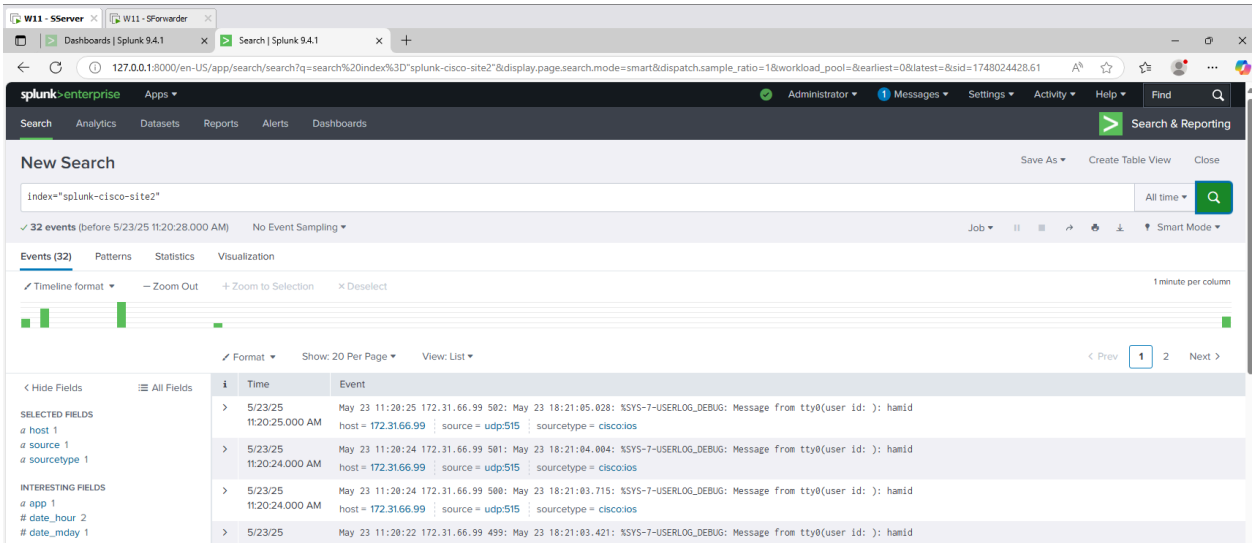


Verification of Cisco Logging

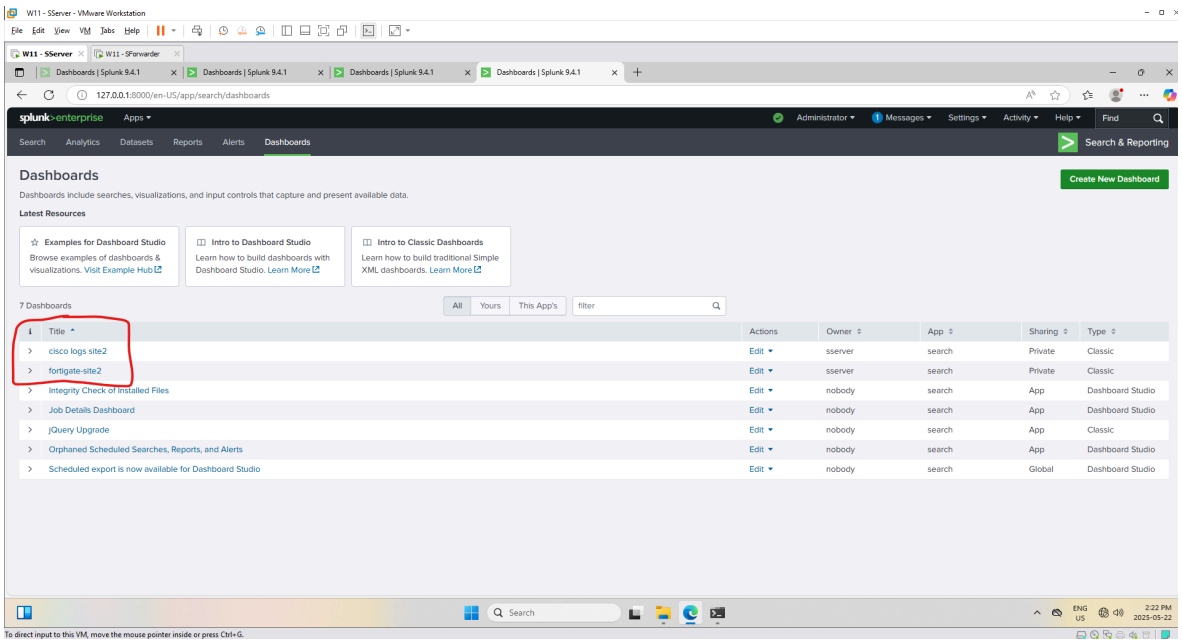
Generate some logs from the Cisco Router using:
logging host *FirewallIPtowardsRouter* transport udp port *CustomPort*
send log *yourtestmessage*
In our case:

- logging host 172.31.64.220 transport udp port 514
- send log hamid

Below is the proof that it works. We searched for **index="splunk-cisco-site2"** as we configured earlier for Cisco. Change the name ‘site2’ for ‘site3’ for Burnaby.

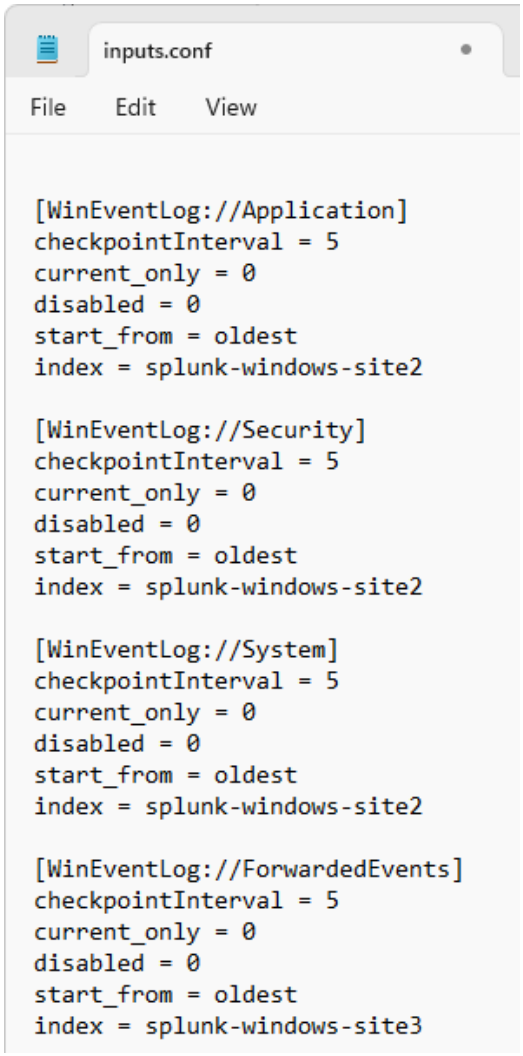


Dashboard Proof of Cisco and Fortigate logs



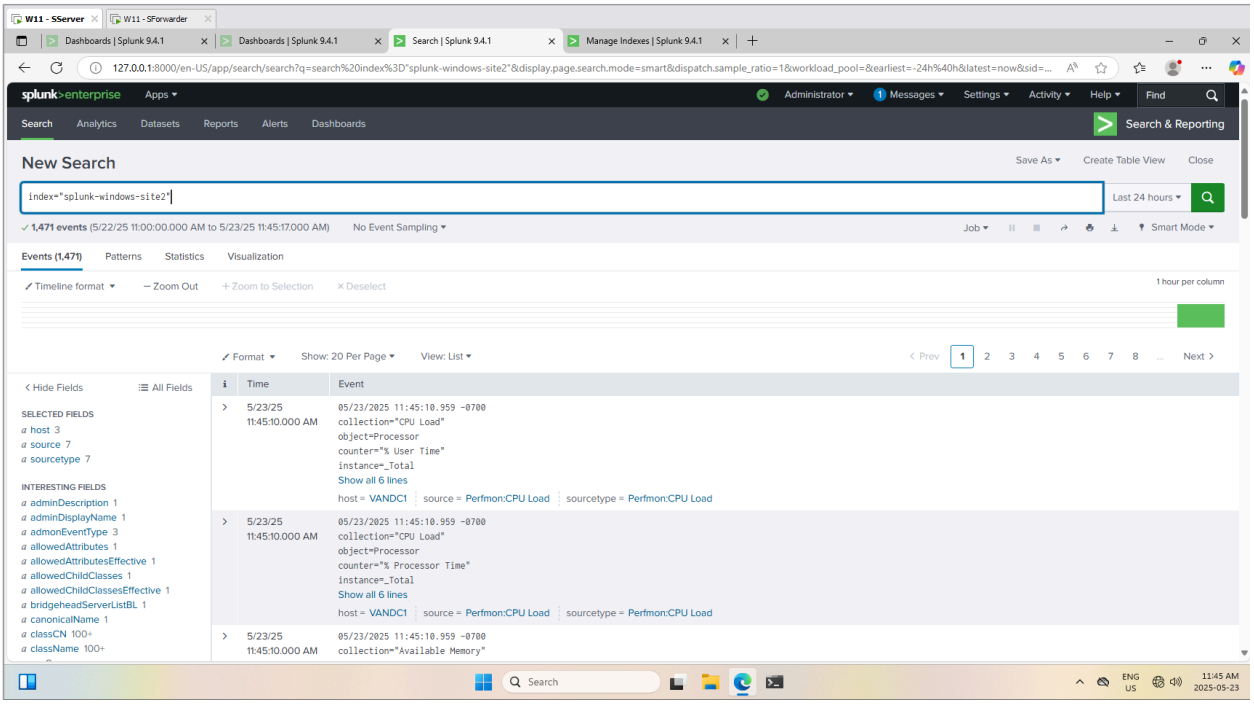
Active Directory Configuration

On the domain controllers, follow the same above listed steps under Splunk Forwarder Setup as well as the Splunk Forwarder Conf File Configuration. Make sure you restart the SplunkForwarder service after changing the inputs.conf file.

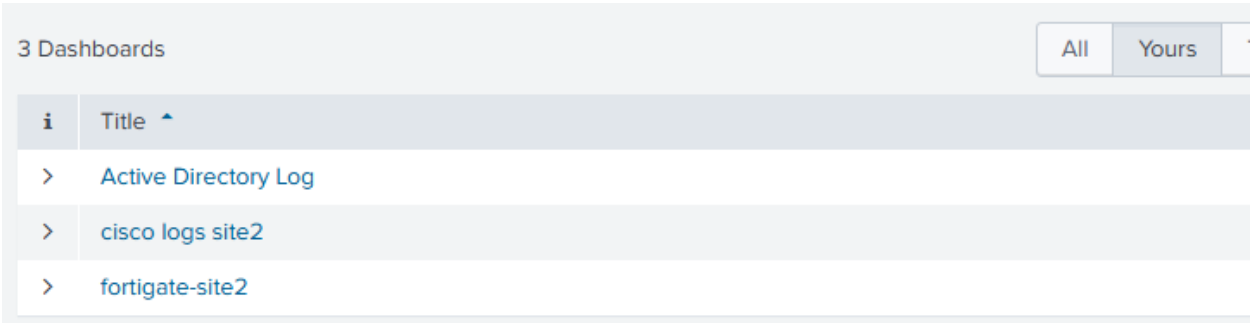


Verification of Active Directory Logs

Following the same steps as listed under the Index Setup, create an index and call it “splunk-windows-site2” (site3 for Burnaby), and search the **index=”splunk-windows-site2”** You should be receiving logs from the domain controllers if configured properly.

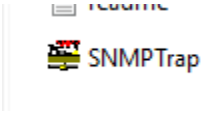


Save the dashboard following the steps listed under the Verifications steps and save it to a new dashboard with a name of your choice. In Vancouver’s Site case, we simply named it **Active Directory Logs**.

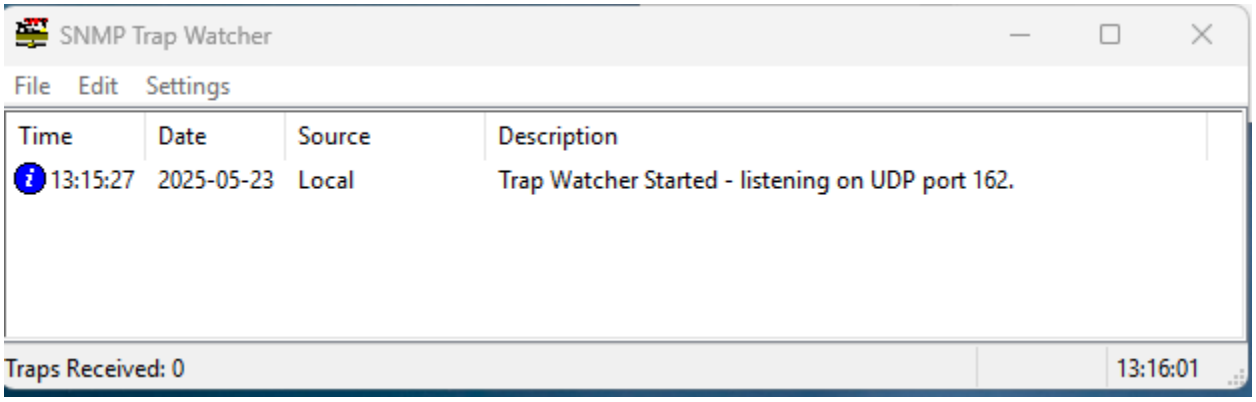


SNMP Trap Configuration

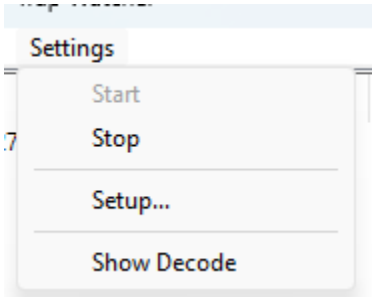
On the domain controllers, you will download a program called SNMP Trap Watcher and run it.



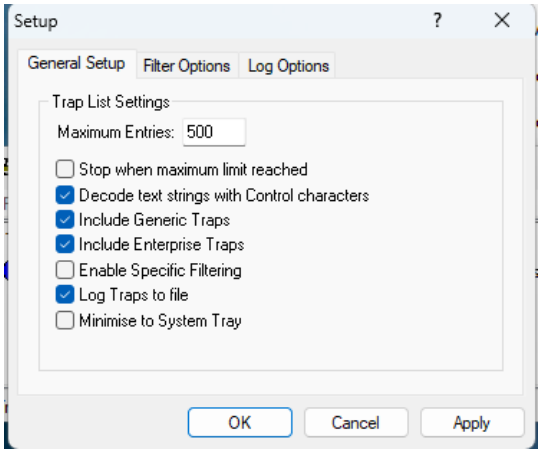
It will automatically start listening to UDP port 162. We will need to configure some settings to properly forward it.



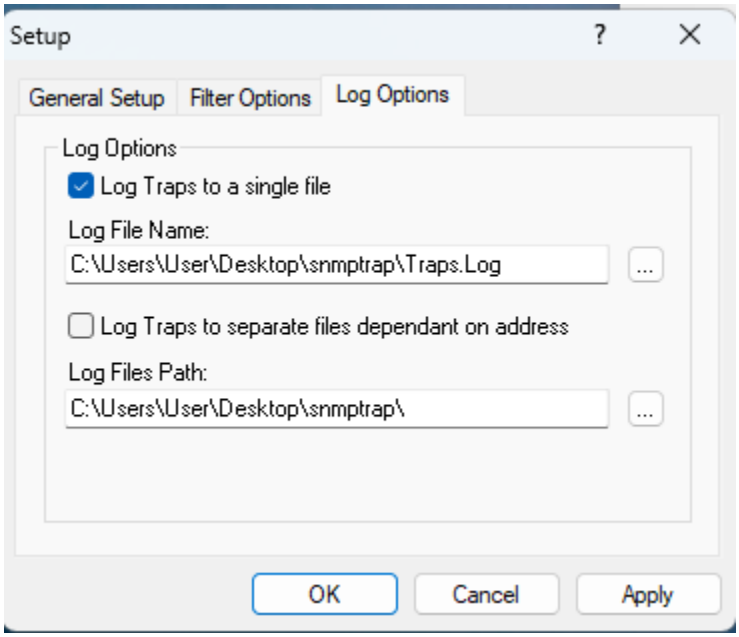
Open the Settings → Setup



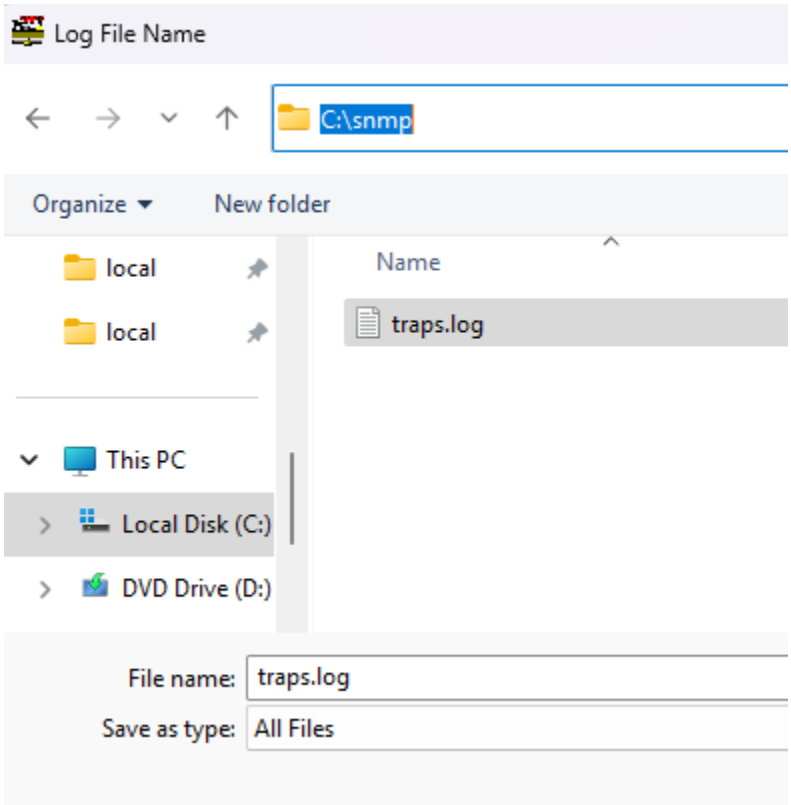
Check Log Traps to file

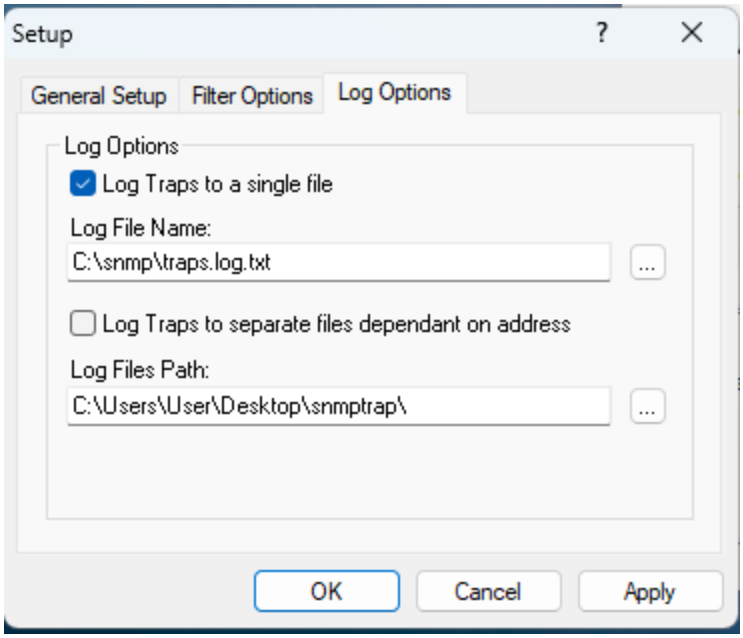


Click Log Options, and check the Log Traps to a single file.



Click the … and point it a new file/folder location. In our case, I created a **snmp** folder located on C:\ and create a new text file called **traps.log**. Point to that and click Ok.



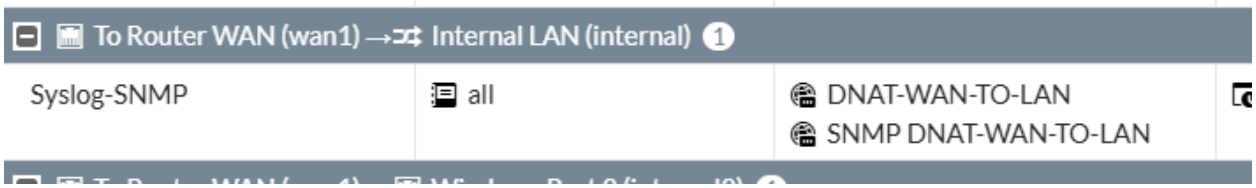


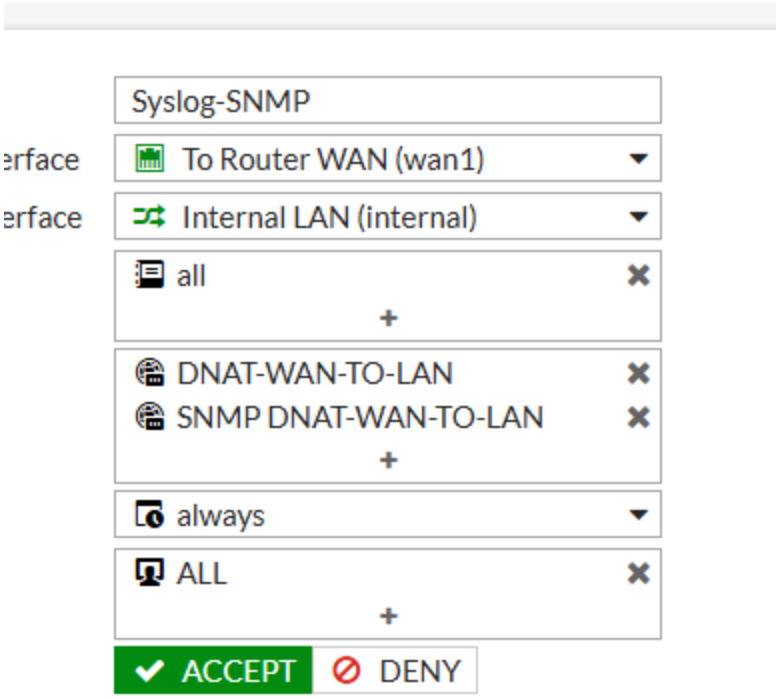
Apply it and OK.

On the Fortigate, we also need to configure a new DNAT rule so that the Cisco Router can route to Splunk Forwarder on UDP 162 (unchangeable)

Name	Details	Interfaces
IPv4 Virtual IP 2		
DNAT-WAN-TO-LAN	172.31.64.220 → 172.31.66.201 (UDP: 514 → 515)	To Router WAN (wan1)
SNMP DNAT-WAN-TO-LAN	172.31.64.220 → 172.31.66.201 (UDP: 162 → 162)	To Router WAN (wan1)

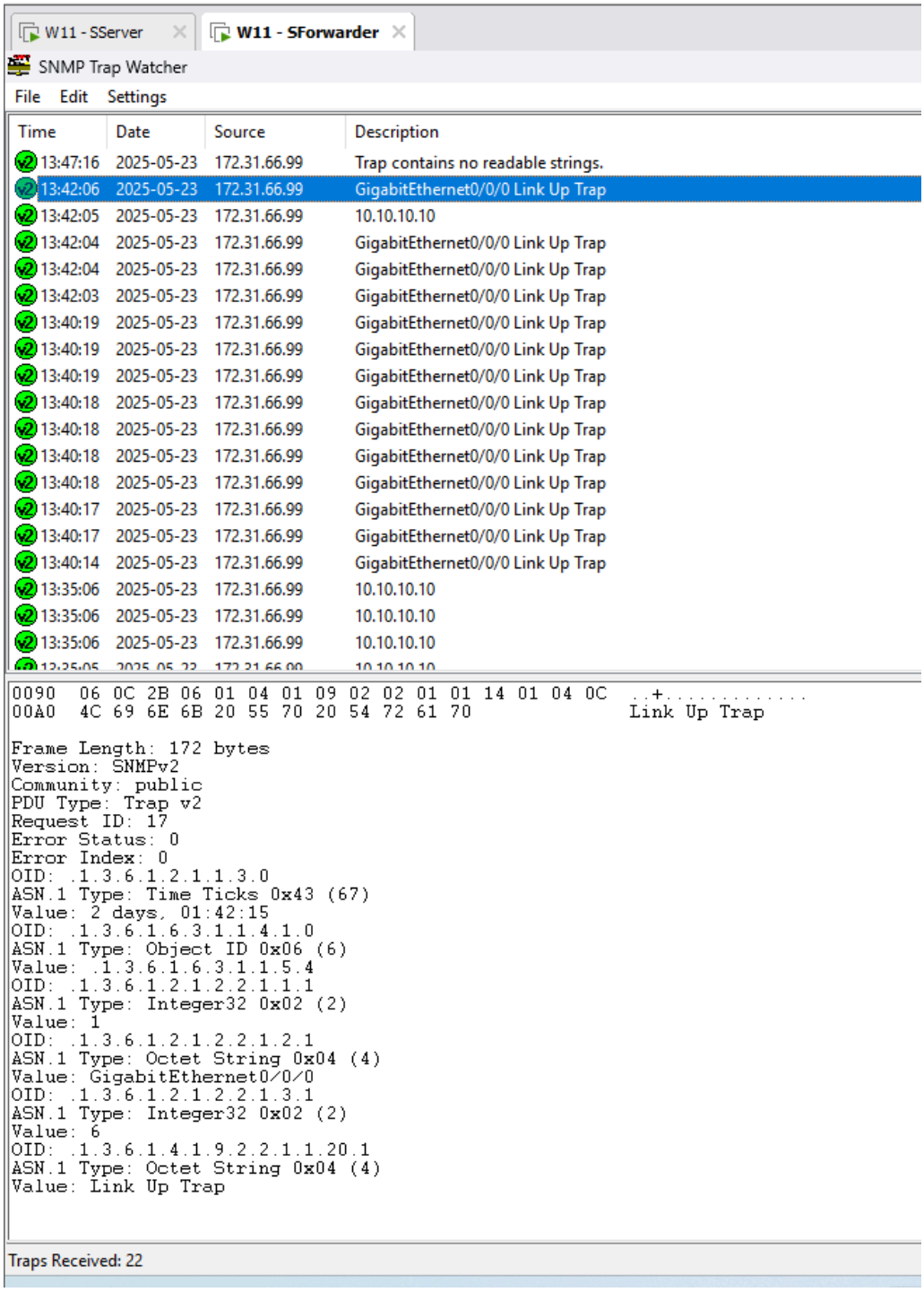
Then you need to add the SNMP NAT to the Syslog Service configured earlier. We renamed it for better naming.





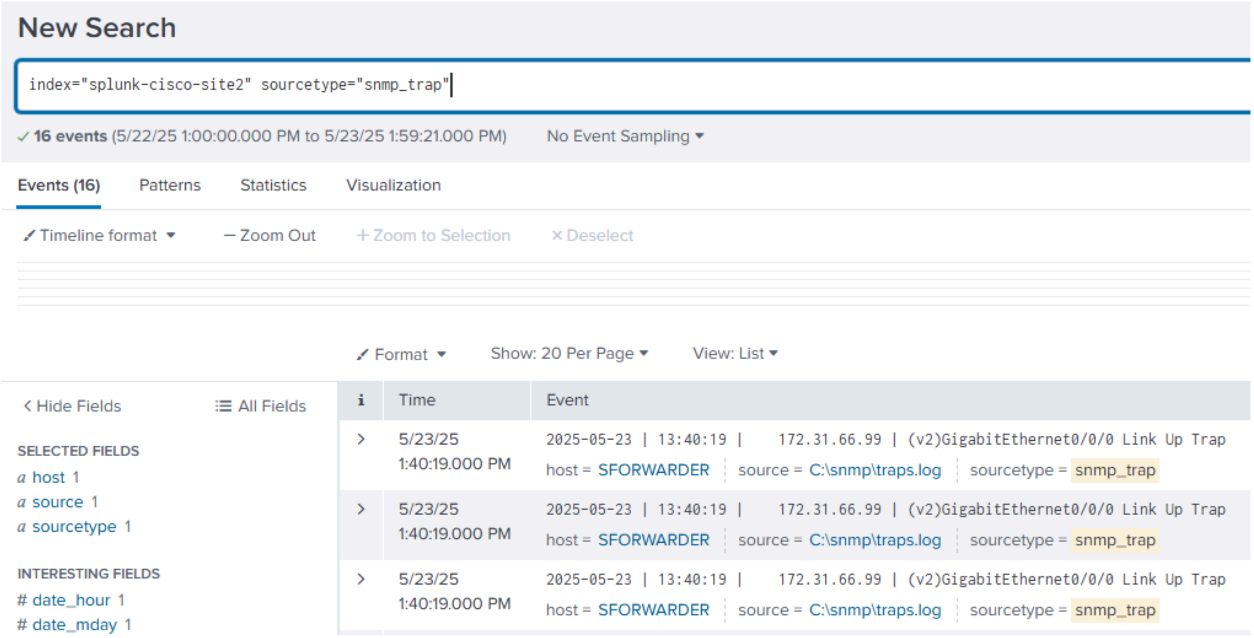
On the Cisco Router, configure the following:
snmp-server community public RO
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps config
snmp-server enable traps memory bufferpeak
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server host 172.31.64.220 version 2c public
Then you can test using: **test snmp trap snmp linkup**
On the Forwarder VM, you can see that we successfully got the SNMP Test. Add this into the inputs.conf and restart SplunkForwarder service.

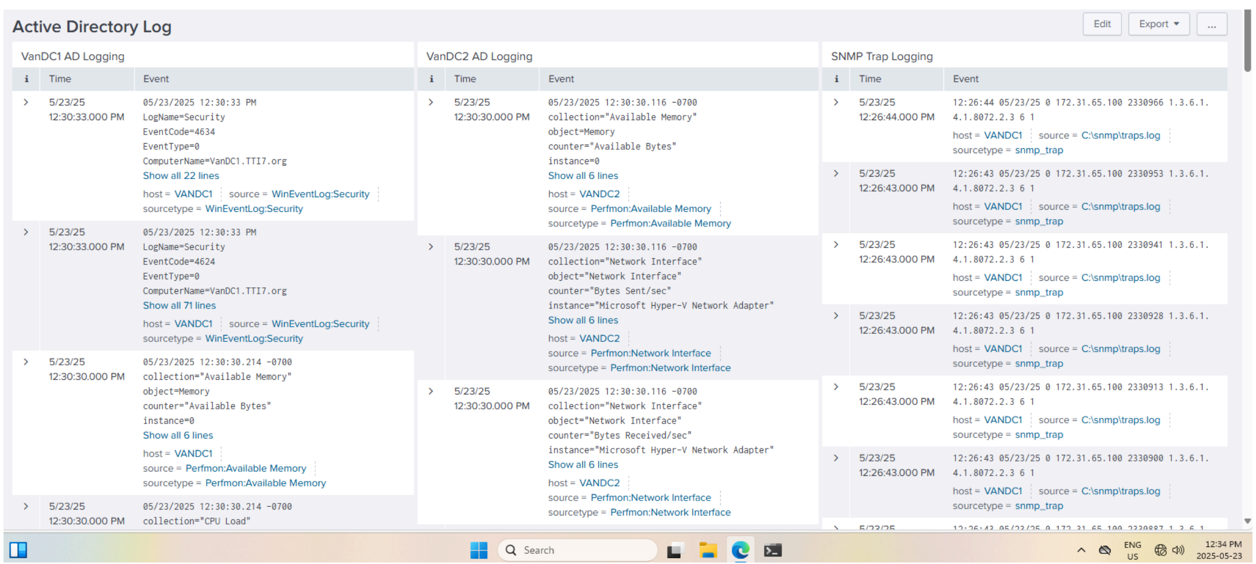
```
[monitor://C:\snmp\traps.log]
disabled = 0
sourcetype = snmp_trap
index = splunk-cisco-site2
```

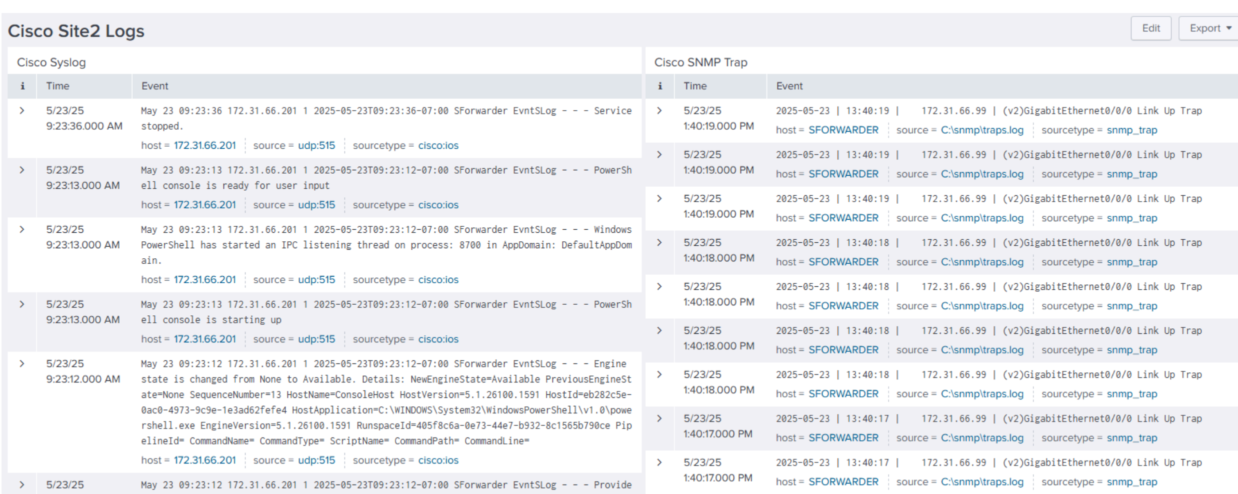


Verification of SNMP Trap Logging

Do a search on the **index=”splunk-windows-site2” sourcetype=”snmp_trap”** to filter to the SNMP logs under the index. Replace ‘site2’ with ‘site3’ for Burnaby.


New Search
index="splunk-cisco-site2" sourcetype="snmp_trap"
✓ 16 events (5/22/25 1:00:00.000 PM to 5/23/25 1:59:21.000 PM)
No Event Sampling
Events (16)
Patterns
Statistics
Visualization
Timeline format
— Zoom Out
+ Zoom to Selection
× Deselect
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
Time
Event
5/23/25 1:40:19.000 PM
2025-05-23 | 13:40:19 | 172.31.66.99 | (v2)GigabitEthernet0/0/0 Link Up Trap
host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap


Active Directory Log
Edit
Export
VanDC1 AD Logging
VanDC2 AD Logging
SNMP Trap Logging
Time
Event
5/23/25 12:30:33.000 PM
05/23/2025 12:30:33 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=VanDC1.TTI7.org
Show all 22 lines
host = VANDC1 source = WinEventLog:Security
sourcetype = WinEventLog:Security
Show all 71 lines
05/23/2025 12:30:30.214 -0700
collection="Available Memory"
object=Memory
counter="Available Bytes"
instance=0
Show all 6 lines
source = Perfmon:Available Memory
sourcetype = Perfmon:Available Memory
collection="CPU Load"
05/23/2025 12:30:30.116 -0700
host = VANDC2
collection="Network Interface"
object="Network Interface"
counter="Bytes Sent/sec"
counter="Bytes Received/sec"
instance="Microsoft Hyper-V Network Adapter"
source = Perfmon:Network Interface
sourcetype = Perfmon:Network Interface
5/23/25 12:26:43.000 PM
host = VANDC1 source = C:\snmp\traps.log
sourcetype = snmp_trap
Search
12:34 PM
2025-05-23


Cisco Site2 Logs
Edit
Export
Cisco Syslog
Cisco SNMP Trap
Time
Event
5/23/25 9:23:36.000 AM
May 23 09:23:36 172.31.66.201 1 2025-05-23T09:23:36-07:00 SForwarder EvntSLog - - - Service stopped.
host = 172.31.66.201 source = udp:515 sourcetype = cisco:ios
5/23/25 9:23:13.000 AM
May 23 09:23:13 172.31.66.201 1 2025-05-23T09:23:12-07:00 SForwarder EvntSLog - - - PowerShell console is ready for user input
May 23 09:23:13 172.31.66.201 1 2025-05-23T09:23:12-07:00 SForwarder EvntSLog - - - PowerShell console is starting up
5/23/25 1:40:19.000 PM
2025-05-23 | 13:40:19 | 172.31.66.99 | (v2)GigabitEthernet0/0/0 Link Up Trap
host = SFORWARDER source = C:\snmp\traps.log sourcetype = snmp_trap
5/23/25 1:40:18.000 PM
2025-05-23 | 13:40:18 | 172.31.66.99 | (v2)GigabitEthernet0/0/0 Link Up Trap
5/23/25 1:40:17.000 PM
2025-05-23 | 13:40:17 | 172.31.66.99 | (v2)GigabitEthernet0/0/0 Link Up Trap