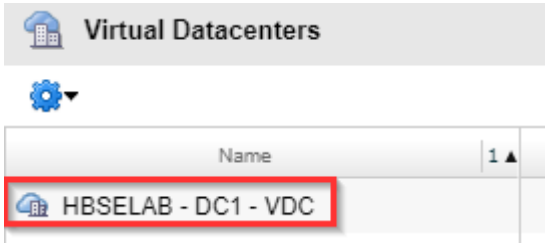
Setting Up IPSEC Site-to-Site VPN on NSX Edge Gateway

Accessing the NSX Edge Gateway

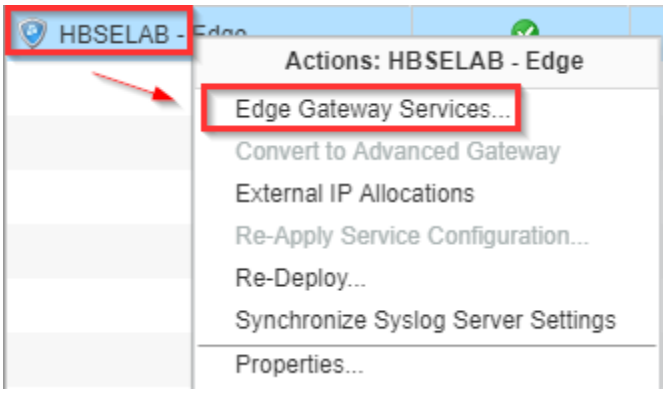
Login to vCloud and proceed to the “Administration” tab:

Select (left-click) your Organization’s Virtual Datacenter:



Select the “Edge Gateways” tab:

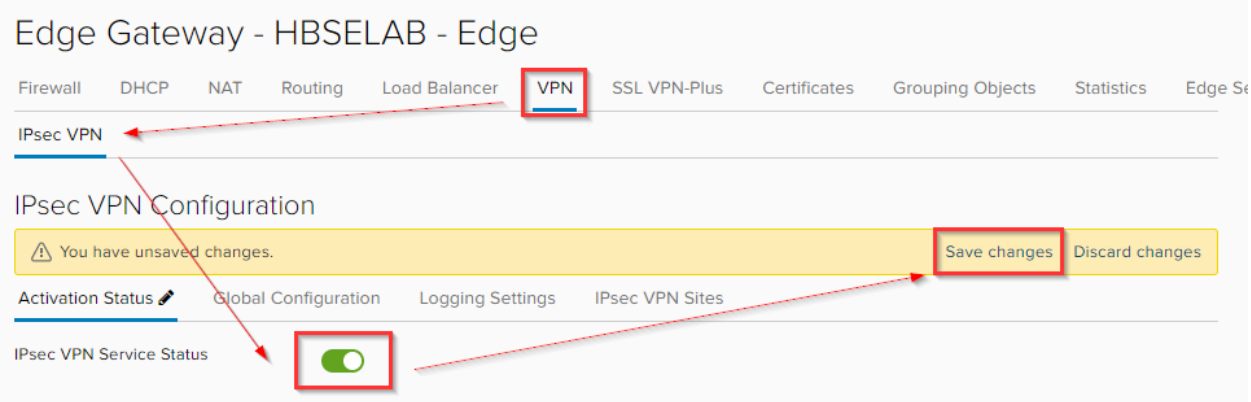
Right-click on your Edge Gateway and select “Edge Gateway Service…”



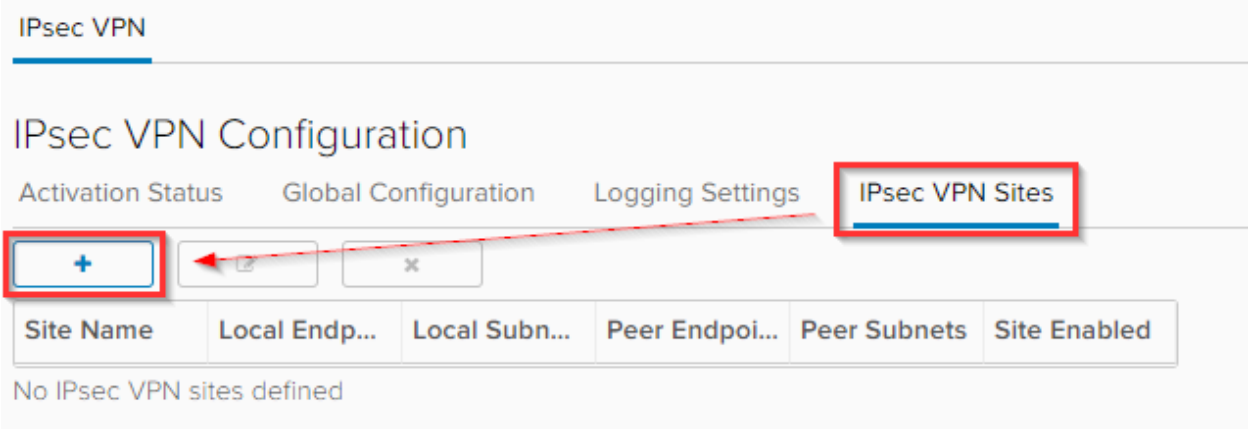
A new tab will open in your browser. You are now within the Advanced Edge Gateway.

Enabling Site-to-Site VPN

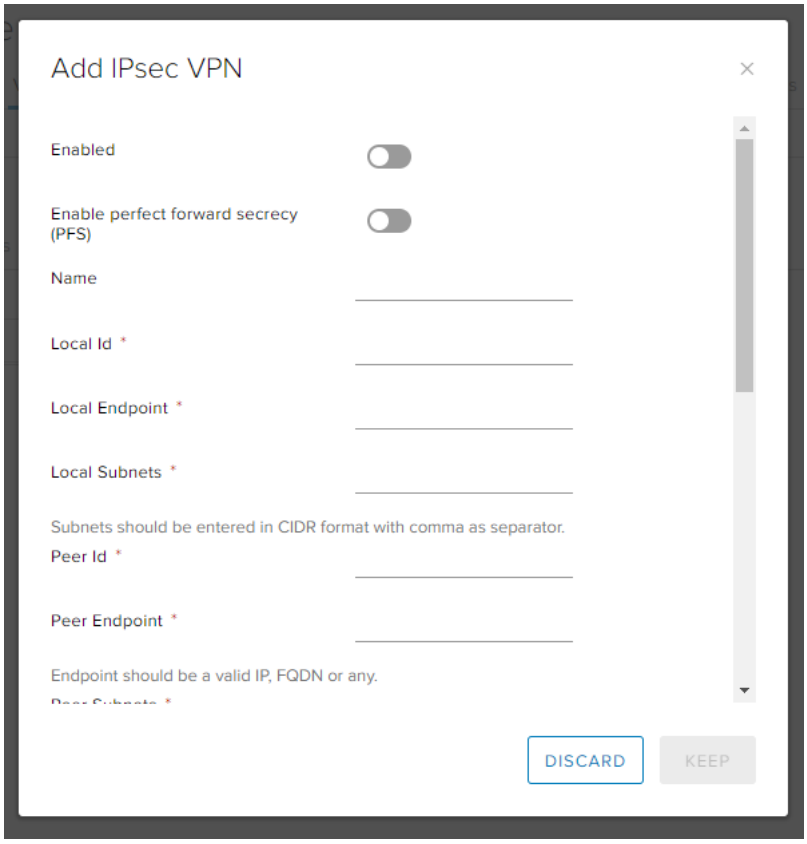
Within the Edge Gateway, select the “VPN” tab on the ribbon menu. Then within “IPsec VPN” toggle “IPsec VPN Service Status” to enable the service. Finally, save the changes:



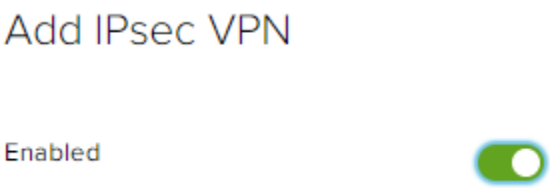
Next, select the “IPsec VPN Sites” tab. Select the plus symbol (+) to add new IPsec Tunnel:



The “Add IPsec VPN” window should appear within your browser window, this is where all the tunnel details are filled:



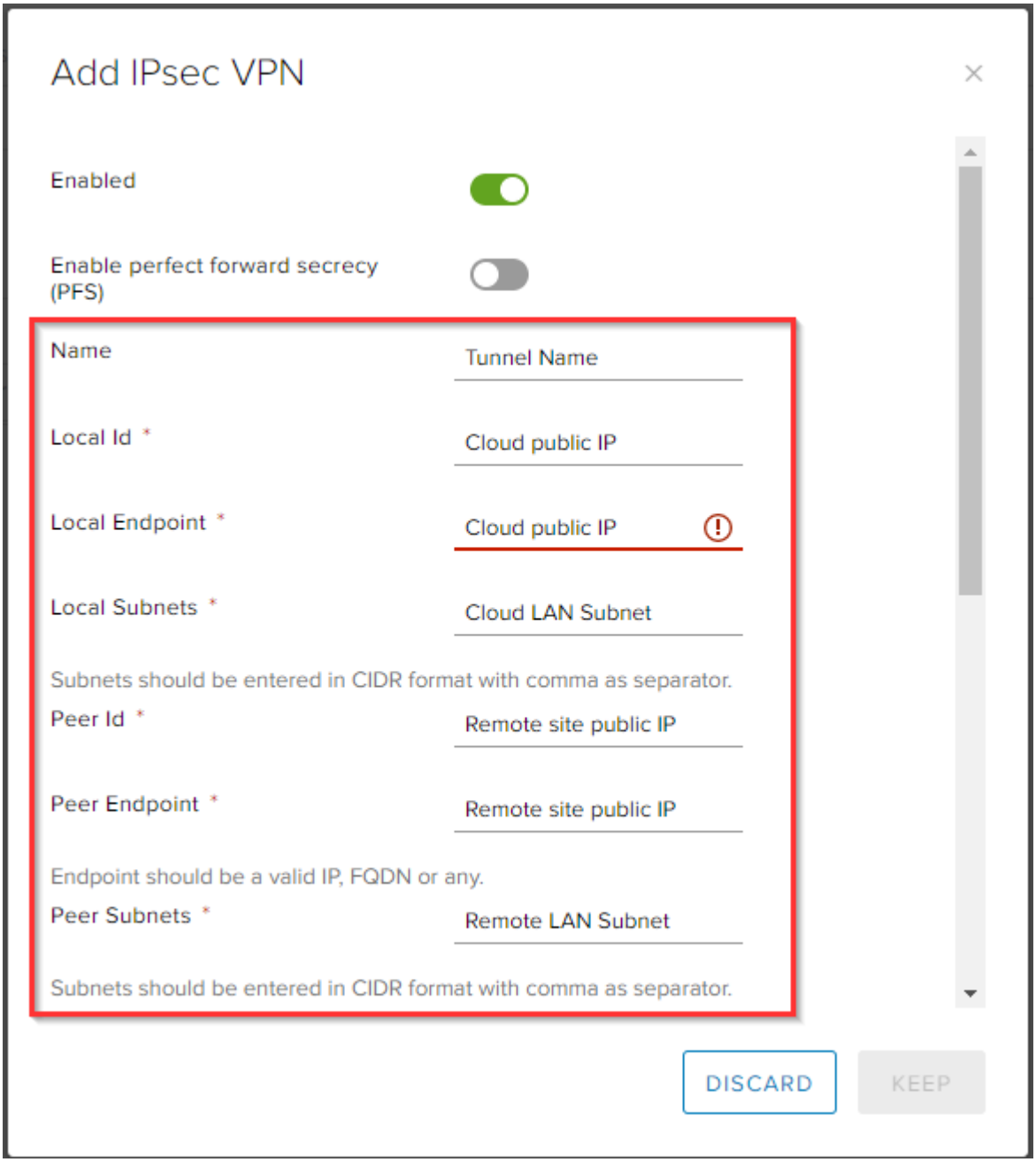
Toggle the “Enabled” switch to activate the tunnel. At this point, we are ready to enter configuration details:



To setup the IPsec VPN some information will need to be gathered ahead of time. This includes:

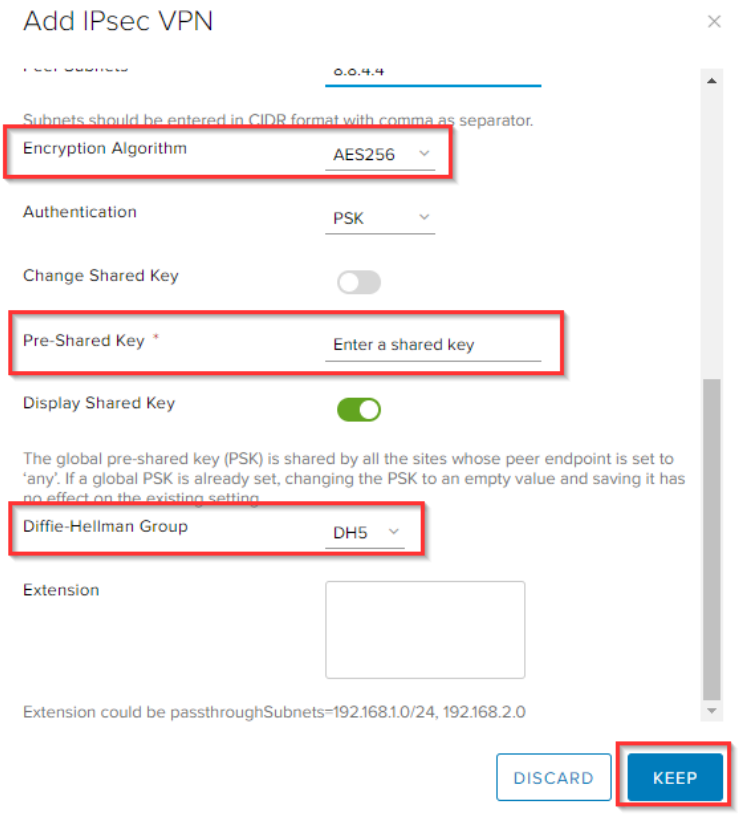
- External IP of NSX Edge Gateway (Cloud public IP)
- Internal subnet of Org VDC Network (Cloud LAN)
- External IP of remote firewall (Remote site public IP)
- Internal subnet of remote site (Remote site LAN)

Once this information is gathered enter them into the corresponding boxes:

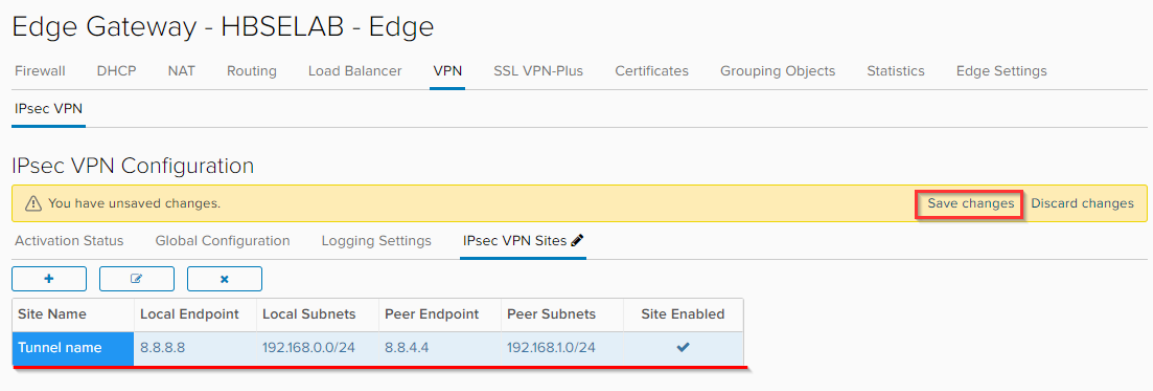


Scrolling further down within the configuration window you will find the encryption settings. Choose one of the “Encryption Algorithm” settings from the dropdown. We recommend AES256 as it is the most widely used and supported. Select “Keep” to save the configuration.

Please note, If the KEEP button is greyed out it means either settings are missing or in the incorrect format.



Your configuration should look something like this. We used Google DNS IPs to illustrate where the public IPs would go. Don’t forget to “Save changes”:

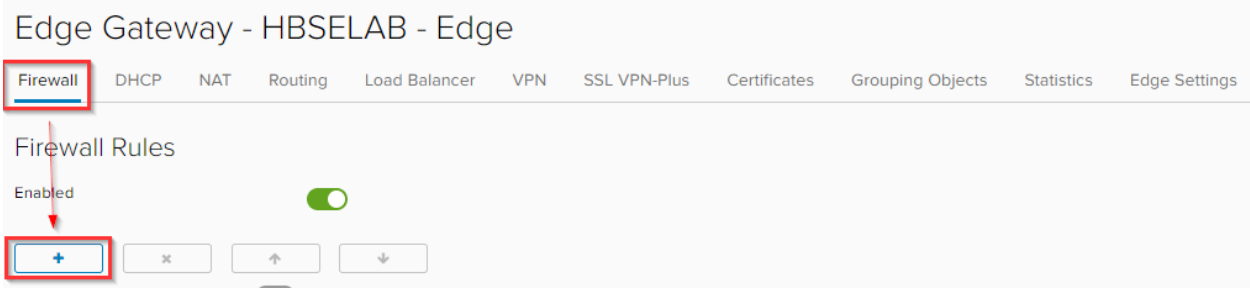


Please note, you will need to use these settings at the remote site’s firewall to establish the tunnel on that side also. Due to the complex nature of firewalls, we cannot show you the remote side configuration as it differs for every firewall.

Firewall Rules

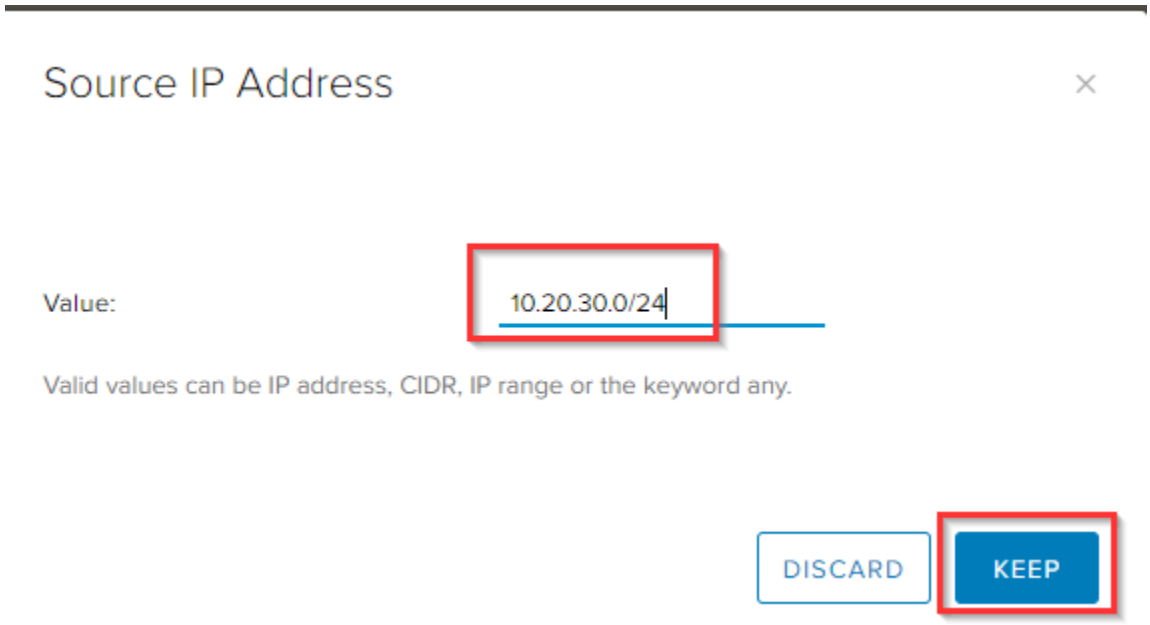
Now that the IPsec VPN Tunnel is established firewall rules will need to be created to allow traffic to pass through the tunnel.

Navigate to the “Firewall” tab of the Edge Gateway, and select the “+” symbol to create a new rule:

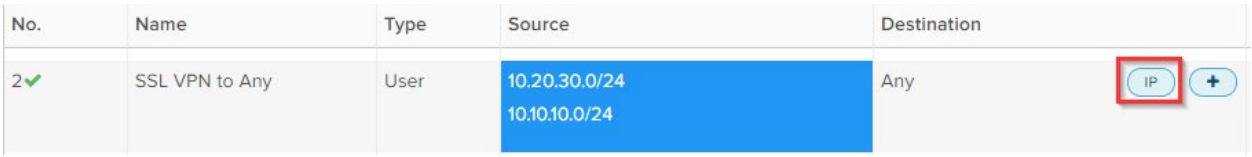


Name the rule, and under “Source” select “IP”

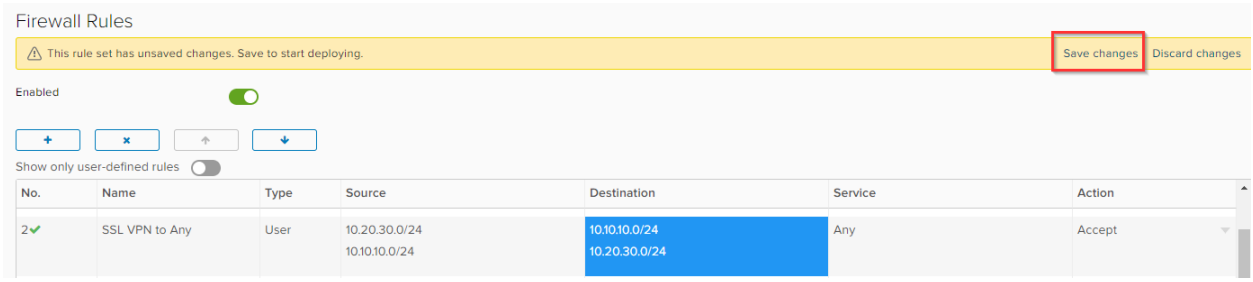
Input your remote site IP range here, and select “Keep”:



Repeat this step and add the Org VDC Network IP pool (Cloud LAN). It should look like the below (except for your IPs of course). Next do the same for “Destination”:



You can restrict the port to those on your cloud server, or leave it open so any port can be accesses by an SSL VPN user. In the below example, we’ve left it as “Any”. “Save changes” once your rule is complete.



You now have established an IPsec VPN tunnel between the sites and have allowed all traffic to pass between the two sites.