



Create a VPN Tunnel between an On Premise Network and a CloudConnect Org VDC Network

In this example we will connect to an on premise subnet of **192.168.10.0/24** with a Public Address of **123.234.123.234**. Replace these values with your on premise values and follow this procedure to setup a connection from your CloudConnect Virtual Datacenter.

This procedure may be used to create a Highly Available Site-to-Site VPN/IPsec Tunnel between an on premise network and a CloudConnect Org VDC (Client) Network using the vCloud Director HTML portal.

This procedure requires an on premise VPN capable firewall. In this example we use a SonicWALL NSA running SonicOS.

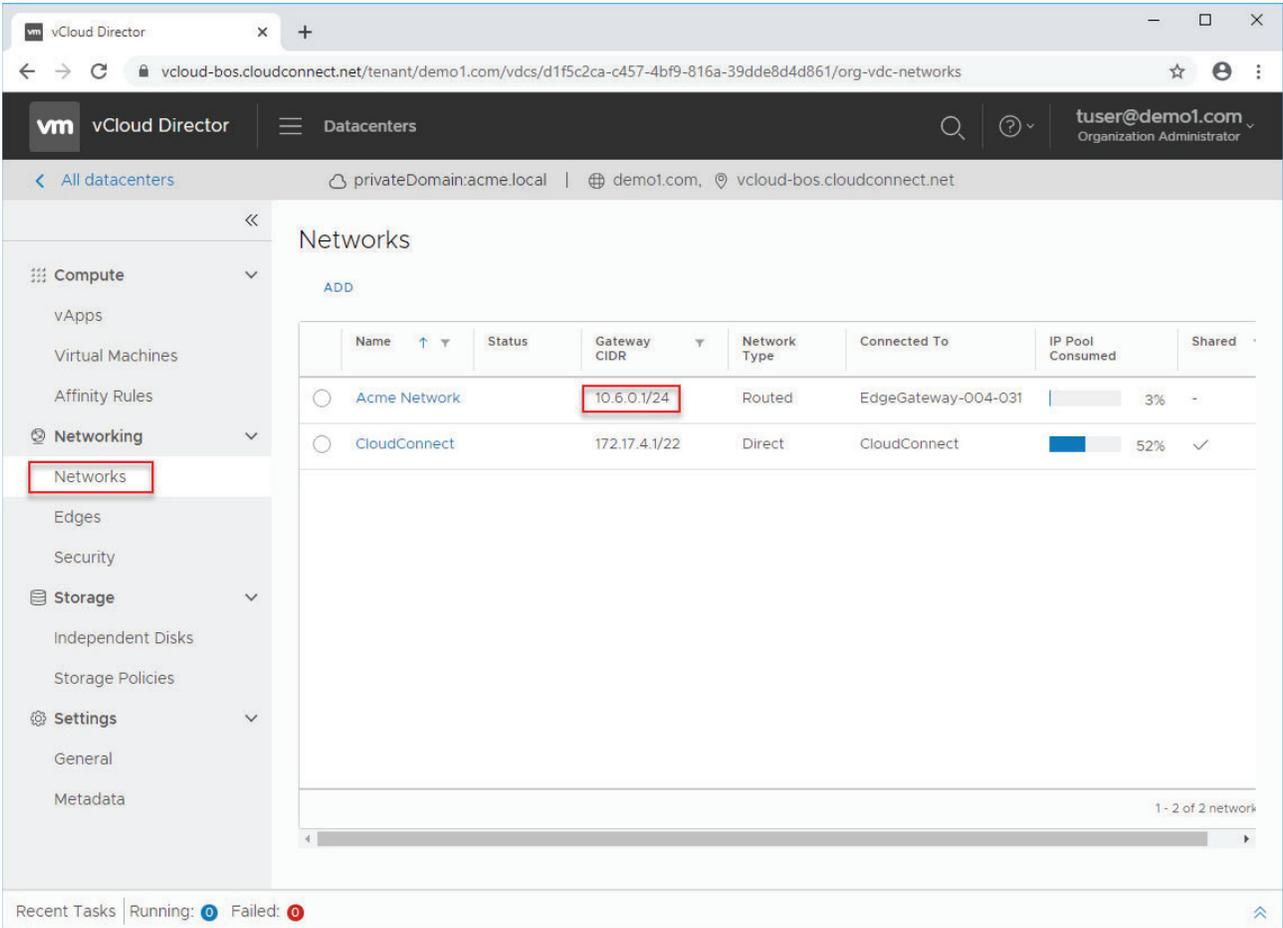
A working knowledge of TCP/IP and VPN/IPSec is necessary for the individual performing this procedure.

Note: Any setting written in **Bold Orange** is a variable and will vary depending on your environment. All other settings are standard fixed settings.

Workflow 1: Configure the Edge Gateway (vCloud Director Tasks)

Obtain your Edge Gateway properties. Locate your Edge Gateway.

- 1) Login to vCloud Director. URL: <https://vcloud-bos.cloudconnect.net/tenant/YOURDOMAIN>
- 2) Select the VDC, and navigate to "Networks"
- 3) Take note of the Gateway CIDR. This is your internal subnet for upcoming steps. In this example, the Gateway CIDR is **10.6.0.0/24**



The screenshot displays the vCloud Director web interface. The browser address bar shows the URL: vcloud-bos.cloudconnect.net/tenant/demo1.com/vdcs/d1f5c2ca-c457-4bf9-816a-39dde8d4d861/org-vdc-networks. The user is logged in as **tuser@demo1.com**, an Organization Administrator. The interface shows a navigation menu on the left with 'Networking' selected and 'Networks' highlighted. The main content area displays a table of networks:

Name	Status	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared
Acme Network		10.6.0.0/24	Routed	EdgeGateway-004-031	3%	-
CloudConnect		172.17.4.1/22	Direct	CloudConnect	52%	✓

At the bottom of the interface, there is a 'Recent Tasks' section showing 'Running: 0' and 'Failed: 0'.

Locate the Edge Gateway's Internet Access IP Address

- 1) Navigate to "Edges" and highlight the Edge Gateway you're going to use to establish a VPN connection.
- 2) The Internet Access IP Address is displayed in the right column. Ignore the CloudConnect IP Address. Take note of the **Internet Access IP Address** as you will need this in multiple later steps. In this example, the Edge Gateway Internet Access IP Address is **172.29.254.214**. This address is pre-assigned to you by CloudConnect.
- 3) Once you've taken note of both the Internet IP and Subnet, click "Configure Services" to move on.

The screenshot shows the vCloud Director interface. The left sidebar has 'Edges' selected under the 'Networking' section. The main content area shows the 'Edges' configuration page with a table of Edge Gateways. The 'Edge Gateway Settings' for 'EdgeGateway-004-031' are displayed below. The 'IP Addresses' table is as follows:

External Networks	Subnets	IP Addresses
CloudConnect	172.17.4.0/22	172.17.4.31
Internet Access	172.29.254.0/24	172.29.254.214

Access the Edge Gateway Firewall Service and create an exception to allow tunneled traffic to traverse the edge gateway.

- 1) In the Firewall tab, click the "+" button to add a new rule.
- 2) Provide a Name for the Firewall rule. This rule should clearly identify the Source of the Traffic (i.e. the On-Premise Network). For Example "Allow Acme Chicago Office"
- 3) Enter the Network address in the Source Window, **192.168.10.0/24**
- 4) Enter the Org VDC Network subnet into the Destination Window, **10.6.0.0/24**
- 5) In the Service window, choose "Any." If you want to limit only certain ports to traverse the tunnel, that is also acceptable and you can customize that on this screen.
- 6) Verify the "Action" radio window is set to "Accept"
- 7) Optionally, you can enable logging of the traffic.
- 8) Finally, click "Save changes".

Edge Gateway - EdgeGateway-004-031

Firewall Rules

This rule set has unsaved changes. Save to start deploying. Save changes Discard changes

Enabled

+ x ↑ ↓

Show only user-defined rules

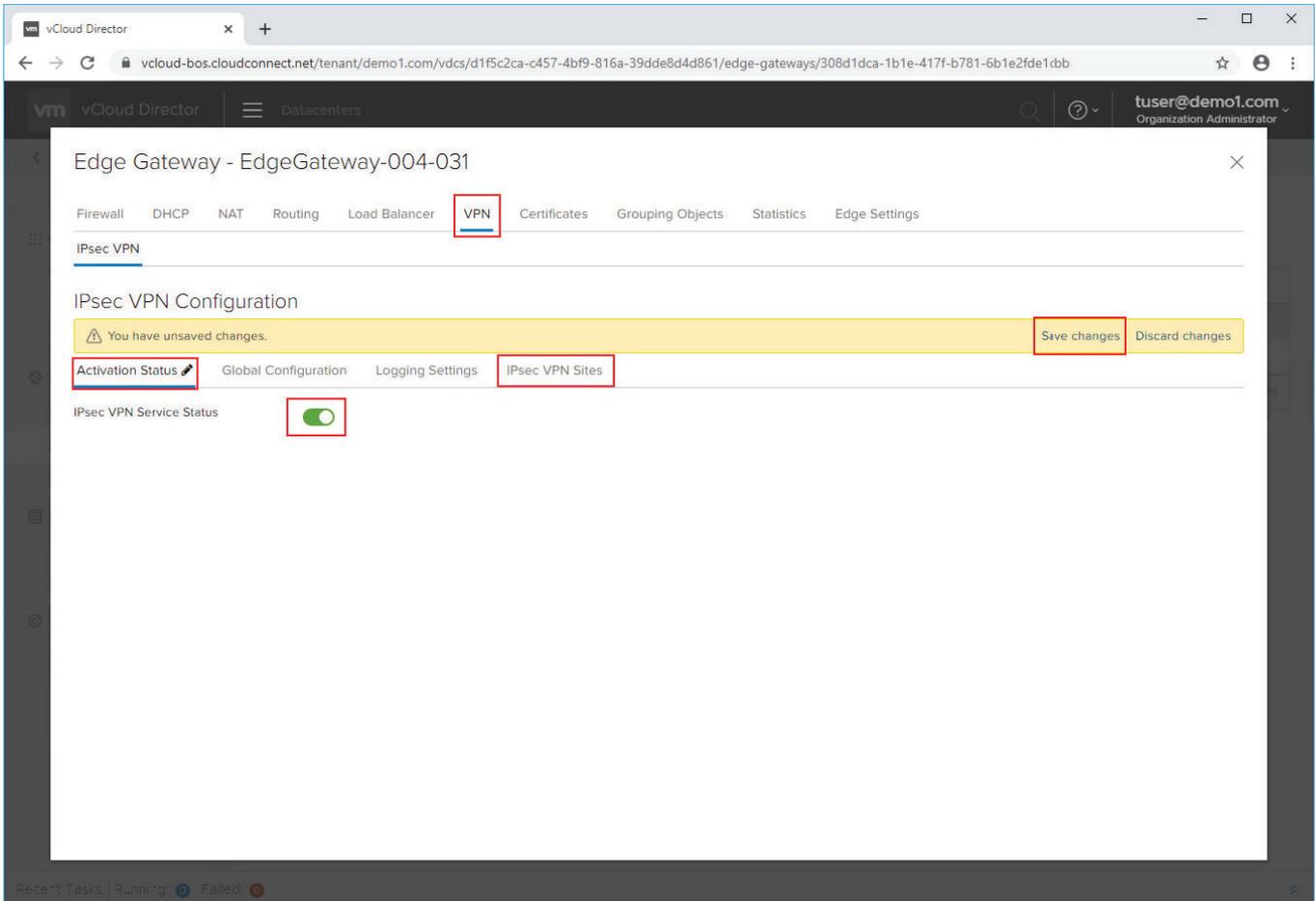
No.	Name	Type	Source	Destination	Service	Action	Enable logging
1	firewall	Internal Hi vse		Any	Any	Accept	<input type="checkbox"/>
2	Allow ACME Chicago	User	192.168.10.0/24	10.6.0.0/24	Any	Accept	<input type="checkbox"/>
3	ipsec	Internal Hi vse	172.29.254.214 192.203.253.196	172.29.254.214 192.203.253.196	udp:500:any esp:any:any	Accept	<input type="checkbox"/>
4	Default	User	internal	external	Any:any:any	Accept	<input type="checkbox"/>
5	Default	User	172.19.0.0/24	172.17.4.31	Any:any:any	Accept	<input type="checkbox"/>
6	Default	User	any	172.29.254.214	icmp:any:any	Accept	<input type="checkbox"/>

Note: This rule applies to the already encapsulated traffic. There is no need to create standard IPSec port exceptions (e.g. IKE, ESP, UDP 500, UDP 4500) on the Edge Gateway Firewall as Edge Gateway will automatically determine and configure these exceptions based on the VPN configuration settings.

Customers with overlapping on-premise subnets should not be configured on the same Edge Gateway.

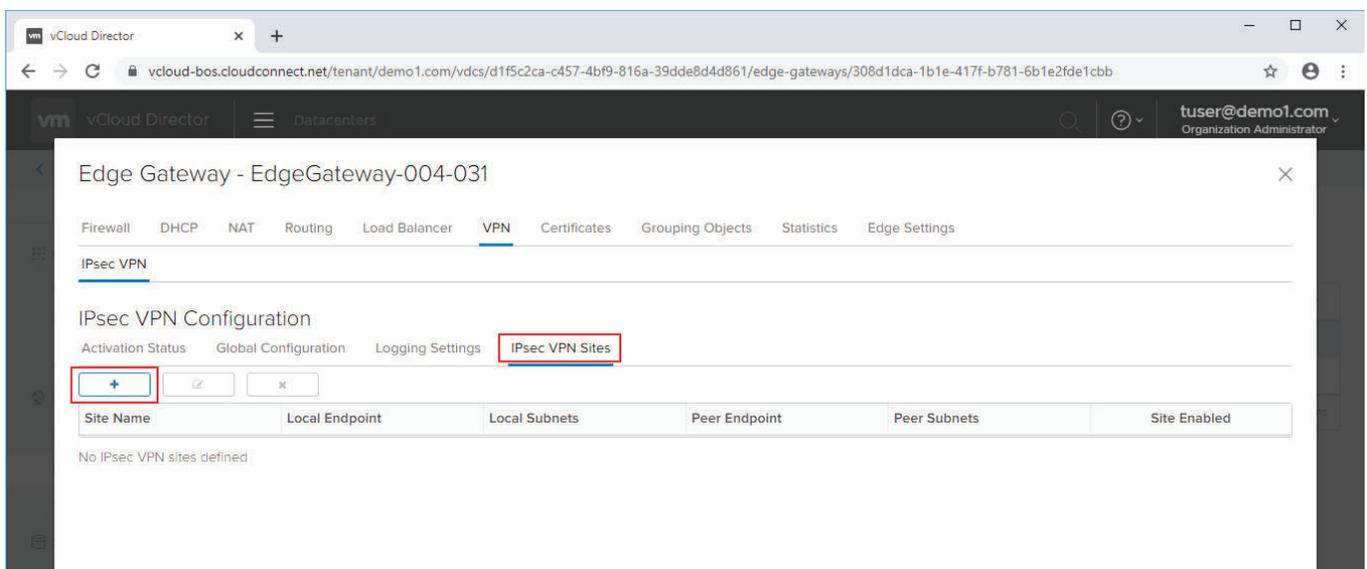
Add a New Site-to-Site VPN configuration:

- 1) Navigate to the VPN tab.
- 2) Verify the IPsec VPN Service Status is enabled.
- 3) Save changes, and navigate to the IPsec VPN Sites sub-tab.



Configure the Site-to-Site VPN Configuration:

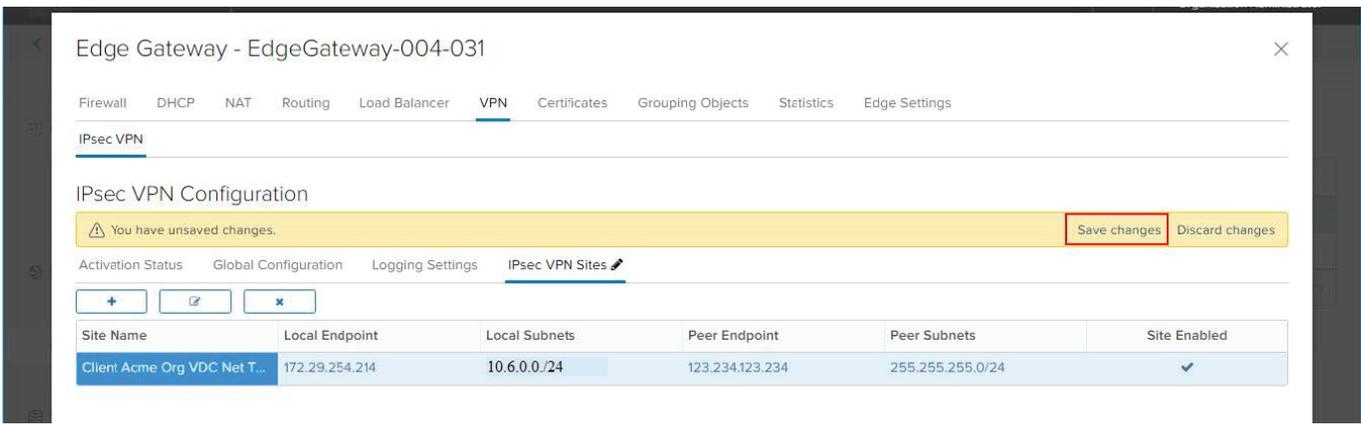
- 1) Enter a Name for the Tunnel. Because you may have multiple Tunnels, it is best to use a naming convention that clearly describes both the On-Premise Network you are connecting to as well as the Org VDC Network. For example, From "Client Acme Org VDC Net TO Acme Chicago"
Note: At a minimum you will want to clearly describe the On-Premise Network as the Configuration is ORG VDC Network Aware.
- 2) The Local ID is the Edge Gateway IKE Identifier (Internet Access IP Address from Above). In this example, it is **172.29.254.214** Add this to the "Local ID" and "Local Endpoint" window.
Note: Depending on the router that is being used on-premise, as well as your FQDN, the "Local ID" **might** be your FQDN. Only attempt to use your FQDN in this window if you have exhausted all other troubleshooting steps.
- 3) The Local Subnets are the subnets associated with this OrgVDC network, noted previously. In this example, it is **10.6.0.0/24**
- 4) The Peer ID is **generally** the statically assigned Internet IP Address of the On-Premise firewall. In this example, it is **123.234.123.234**.
- 5) The Peer Endpoint is **always** the statically assigned Internet IP Address of the On-Premise firewall. In this example, it is also the Peer ID, **123.234.123.234**.
- 6) The Peer Subnets are the subnets associated with the on-prem network. In this example, it is **192.168.10.0/24**
- 7) Choose AES-256 as the encryption protocol. If your on premise firewall does not support AES encryption, consider upgrading that device.
- 8) Choose "PSK" (Pre-shared Key) as the authentication method.
- 9) Choose a Pre-shared Key that is between 32 and 128 alphanumeric characters. This key must have at least one lowercase letter, one uppercase letter, and one number. **Make note of this key.**
- 10) Choose the Diffie-Hellman Group. DH2 and DH14 are supported.
- 11) Make note of other settings: the VPN established from the on-premise network must have the same settings.
- 12) Click "Keep", and save changes.



Add IPsec VPN



Enabled	<input checked="" type="checkbox"/>
Enable perfect forward secrecy (PFS)	<input checked="" type="checkbox"/>
Name	Client Acme Org VDC Net TO Acme Chicago
Local Id *	172.29.254.214
Local Endpoint *	172.29.254.214
Local Subnets *	10.6.0.0/24
Subnets should be entered in CIDR format with comma as separator.	
Peer Id *	123.234.123.234
Peer Endpoint *	123.234.123.234
Peer Subnets *	192.168.10.0/24
Subnets should be entered in CIDR format with comma as separator.	
Encryption Algorithm	AES256
Authentication	PSK
Change Shared Key	<input type="checkbox"/>
Pre-Shared Key *	ThisIsAnExampleKey123
Display Shared Key	<input checked="" type="checkbox"/>
The global pre-shared key (PSK) is shared by all the sites whose peer endpoint is set to 'any'. If a global PSK is already set, changing the PSK to an empty value and saving it has no effect on the existing setting.	
Diffie-Hellman Group	DH14
Extension	<div style="border: 1px solid #ccc; height: 40px;"></div>
Extension could be passthroughSubnets=192.168.1.0/24, 192.168.2.0	
Digest Algorithm	Sha1
IKE Option	IKEv1
IKE Responder Only	<input type="checkbox"/>
Session Type	Policy Based Session



Workflow 2: Configure the SonicWALL (On Premise Tasks)

Create a Network Object defining the CloudConnect Org VDC Network:

- 1) From the On-Premise Network, access the SonicWALL device and **verify you are running the latest firmware.** At a minimum, the device should be running SonicOS 5.1.
- 2) Create a Network Object, which identifies the Org VDC Network (“Client Acme Network” CloudConnect subnet) that you are connecting to.
- 3) Provide a Name, which clearly identifies the CloudConnect Org VDC Network as such.
- 4) Choose type “Network”
- 5) In the “Zone Assignment” window, choose “LAN.” For sophisticated deployments, you may have a dedicated zone for this traffic, or you may use the VPN zone. Generally, the Zone will define what On-Premise resources traffic coming from the VPN tunnel has access to.
- 6) Enter the Network address of the Org VDC Network, **10.6.0.0/24**
- 7) Enter the Netmask **255.255.255.0**

Create a New VPN Policy:

- 1) From the main menu, choose, VPN, Settings.
- 2) In the results pane, under “VPN Policies” click “Add”

The screenshot shows the SonicWALL Network Security Appliance web interface. The left sidebar has 'Settings' highlighted. The main content area is titled 'VPN / Settings'. Under 'VPN Global Settings', 'Enable VPN' is checked, and the 'Unique Firewall Identifier' is 'C0EAE45EB870'. Below this is the 'VPN Policies' table with two rows: '1: WAN Group/VPN' and '2: WLAN Group/VPN'. An 'Add...' button is circled in red. At the bottom, there is a section for 'Currently Active VPN Tunnels' which is currently empty.

Before configuring the VPN policy, we must first derive the Primary Gateway Address and the Secondary Gateway Address.

CloudConnect assigns two Public IP Addresses to each Internet Access IP Address of your Edge Gateway. The Primary Public IP Address is used during normal operation and is the Primary Gateway Address for any on premise SonicWALL or other VPN firewall appliance. The Standby Public IP Address is used if a serious disaster event occurs, which requires CloudConnect to invoke a Geographic Site failover. Additional use of this Standby Public IP Address may occur during a planned migration or planned CloudConnect infrastructure maintenance. The Standby Public IP Address should be used as your Secondary Gateway Address in any On-Premise SonicWALL or other VPN firewall appliance. More information about this configuration is available in this KB Article:

<https://support.cloudconnect.net/solution/articles/1000199548-cct-20150817-configuring-a-cloudconnect-statically-assigned-internet-ip-address-to-be-highly-availa>

As mentioned in the above referenced KB Article, the following table provides a mapping between your Edge Gateway’s Internet Access IP Address(es) and the Primary and Standby Public IP Addresses

Edge Gateway Address	Primary Public IP Address	Standby Public IP Address
172.29.253.XYZ	216.93.253.XYZ	96.233.53.XYZ
172.29.254.XYZ	192.203.253.XYZ	108.26.236.XYZ

In this example, the Edge Gateway Internet Access IP Address (from Workflow 1, above) is **172.29.254.214**. The corresponding **Primary Public IP Address** is **192.203.253.214** and the corresponding **Standby Public IP Address** is **108.26.236.214**.

General Tab

- 1) Policy Type: **Site to Site**
- 2) Authentication Method: **IKE using Preshared Secret**
- 3) Name: Choose a Name that clearly describes the Tunnel's destination Network. For example, "**To CloudConnect Acme Network**"
- 4) IPsec Primary Gateway Address: Enter the **Primary Public IP Address** of your Edge Gateway. In this example, **192.203.253.214**
- 5) IPsec Secondary Gateway Address: Enter the **Standby Public IP Address** of your Edge Gateway. In this example, **108.26.236.214**
- 6) Shared Secret: Enter the Shared Secret from your Edge Gateway Site-to-Site Configuration.
- 7) Local IKE ID: IP Address - This is generally the Public IP Address of the SonicWALL. In this example, **123.234.123.234**.
- 8) Peer IKE ID: IP Address - This is the *Edge Gateway's Internet Access IP Address (NOT THE PUBLIC IP ADDRESS)*. In this example, it is **172.29.254.214**.



General | Network | Proposals | Advanced

Security Policy

Policy Type:	Site to Site	
Authentication Method:	IKE using Preshared Secret	
Name:	To CloudConnect OrgVDC Network	
IPsec Primary Gateway Name or Address:	192.203.253.214	
IPsec Secondary Gateway Name or Address:	108.26.236.214	

IKE Authentication

Shared Secret:	<input type="text" value="ThisIsAnExampleKey123"/>	
Confirm Shared Secret:	<input type="text" value="ThisIsAnExampleKey123"/>	<input type="checkbox"/> Mask Shared Secret
Local IKE ID:	IP Address	<input type="text" value="123.234.123.234"/>
Peer IKE ID:	IP Address	<input type="text" value="172.29.254.214"/>

Ready

OK Cancel Help

Network Tab

- 1) In the Network Tab, choose the On-Premise Network which will have access to the VPN Tunnel. In this example, we are using, "LAN Subnets"
- 2) For Remote Networks, choose the Network Object we created as our first SonicWALL configuration task. In this example, we are using Org VDC Network Subnet ("Client Acme Network").

The screenshot shows the configuration interface for a SonicWALL Network Security Appliance. At the top left is the Dell SonicWALL logo and the text "SonicWALL | Network Security Appliance". Below this is a navigation bar with four tabs: "General", "Network", "Proposals", and "Advanced". The "Network" tab is selected. The interface is divided into two sections: "Local Networks" and "Remote Networks".

Local Networks

- Choose local network from list (Dropdown menu: LAN Subnets)
- Local network obtains IP addresses using DHCP through this VPN Tunnel
- Any address

Remote Networks

- Use this VPN Tunnel as default route for all Internet traffic
- Destination network obtains IP addresses using DHCP through this VPN Tunnel
- Choose destination network from list (Dropdown menu: OrgVDC Network Subnet)

At the bottom of the window, there is a status bar that says "Ready" and three buttons: "OK", "Cancel", and "Help".

Proposals Tab

IKE (Phase 1) Proposal

- | | |
|-------------------------|-----------|
| 1) Exchange: | Main Mode |
| 2) DH Group: | Group 14 |
| 3) Encryption: | AES-256 |
| 4) Authentication: | SHA1 |
| 5) Life Time (seconds): | 28800 |

Ipssec (Phase 2) Proposal

- | | |
|------------------------------------|-----------------|
| 1) Protocol: | ESP |
| 2) Encryption: | AES-256 |
| 3) Authentication: | SHA1 |
| 4) Enable Perfect Forward Secrecy: | Checked/Enabled |
| a. DH Group: | Group 14 |
| 5) Life Time (seconds): | 3600 |



General Network Proposals Advanced

IKE (Phase 1) Proposal

Exchange:	Main Mode
DH Group:	Group 14
Encryption:	AES-256
Authentication:	SHA1
Life Time (seconds):	28800

Ipssec (Phase 2) Proposal

Protocol:	ESP
Encryption:	AES-256
Authentication:	SHA1
<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy	
DH Group:	Group 14 *
Life Time (seconds):	3600

*The DH group might default to either Group 2 or Group 14. If you get the message "No Proposal Chosen" in the logs, try switching between the two.

Ready

OK Cancel Help

Advanced Tab

- 1) Preempt Secondary Gateway: Checked/Enabled
 - a. Primary Gateway Detection Inter: 28800
- 2) Management via this SA: Optional

Note: It is recommended to keep all other Advanced Settings disabled/unchecked. Enabling these features can cause the Tunnel to stop functioning.

Click OK in the bottom right hand corner.



SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

Advanced Settings

- Enable Keep Alive
- Suppress automatic Access Rules creation for VPN Policy
- Disable IPsec Anti-Replay
- Require authentication of VPN clients by XAUTH
- Enable Windows Networking (NetBIOS) Broadcast
- Enable Multicast
- Permit Acceleration
- Apply NAT Policies

Management via this SA:

- HTTP
- HTTPS
- SSH
- SNMP

User login via this SA:

- HTTP
- HTTPS

Default LAN Gateway (optional):

0.0.0.0

VPN Policy bound to:

Zone WAN

- Preempt Secondary Gateway

Primary Gateway Detection Interval (seconds)

28800

Ready

OK

Cancel

Help

The tunnel should show as up.

VPN / Settings

Accept Cancel

VPN Global Settings

Enable VPN
 Unique Firewall Identifier: COEAE45EB870

VPN Policies

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/>	1	WAN GroupVPN		ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/>	2	WLAN GroupVPN		ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	6	To CloudConnect Org/DC Network	192.203.253.214 108.26.236.214	ESP: AES-256/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Site To Site Policies: 4 Policies Defined, 3 Policies Enabled, 75 Maximum Policies Allowed
 GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels

#	Created	Name	Local	Remote	Gateway	Renegotiate
4	12/17/2019 9:23:45	To CloudConnect Org/DC Network	192.168.10.0 - 192.168.10.255	10.6.0.1 - 10.6.0.255	192.203.253.214	<input type="button" value="Renegotiate"/>

In the the Edge Gateway Configuration Window, navigate to the Statistics tab.
 Navigate to the IPsec VPN sub-tab.
 Ensure the Channel and Tunnel status are checked.

Edge Gateway - EdgeGateway-004-031

Firewall DHCP NAT Routing Load Balancer VPN Certificates Grouping Objects **Statistics** Edge Settings

Connections **IPsec VPN**

IPsec Statistics
 Last refreshed at Dec 17, 2019

IPsec VPN Statistics & Status

Peer ID	Local IP Address	Peer IP Address	Last Message	Channel Status
123.234.123.234	172.29.254.214	123.234.123.234	None	<input checked="" type="checkbox"/>

IPsec VPN Tunnel Statistics & Status

Local Subnet	Peer Subnet	Last Message	Tunnel Status
10.6.0.0/24	255.255.255.0/24	None	<input checked="" type="checkbox"/>

Test the tunnel by pinging across to verify connectivity:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\administrator>ping 10.6.0.10

Pinging 10.6.0.10 with 32 bytes of data:
Reply from 10.6.0.10: bytes=32 time=13ms TTL=127
Reply from 10.6.0.10: bytes=32 time=13ms TTL=127
Reply from 10.6.0.10: bytes=32 time=11ms TTL=127
Reply from 10.6.0.10: bytes=32 time=13ms TTL=127

Ping statistics for 10.6.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 13ms, Average = 12ms

C:\Users\administrator>
```

Note: If the tunnels shows as Up, but you are unable to ping across, check your firewall configurations on both sides as these may be dropping traffic in either or both directions.

Congratulations!!! If you can ping through, you have successfully linked your on premise network to the customer's Org VDC Network on CloudConnect!