



## 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.

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

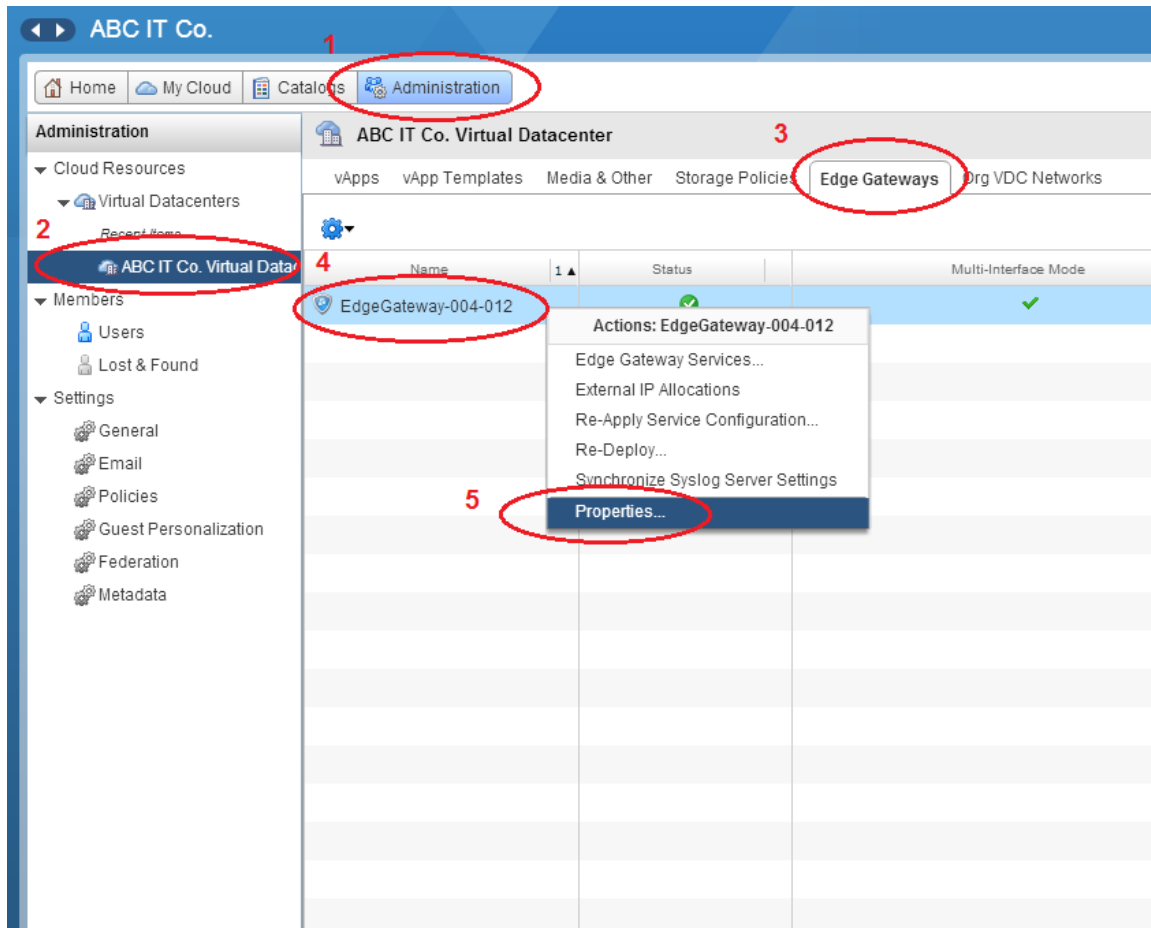
A working knowledge of TCP/IP and VPN/IPSec is necessary for the individual performing this procedure.

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)

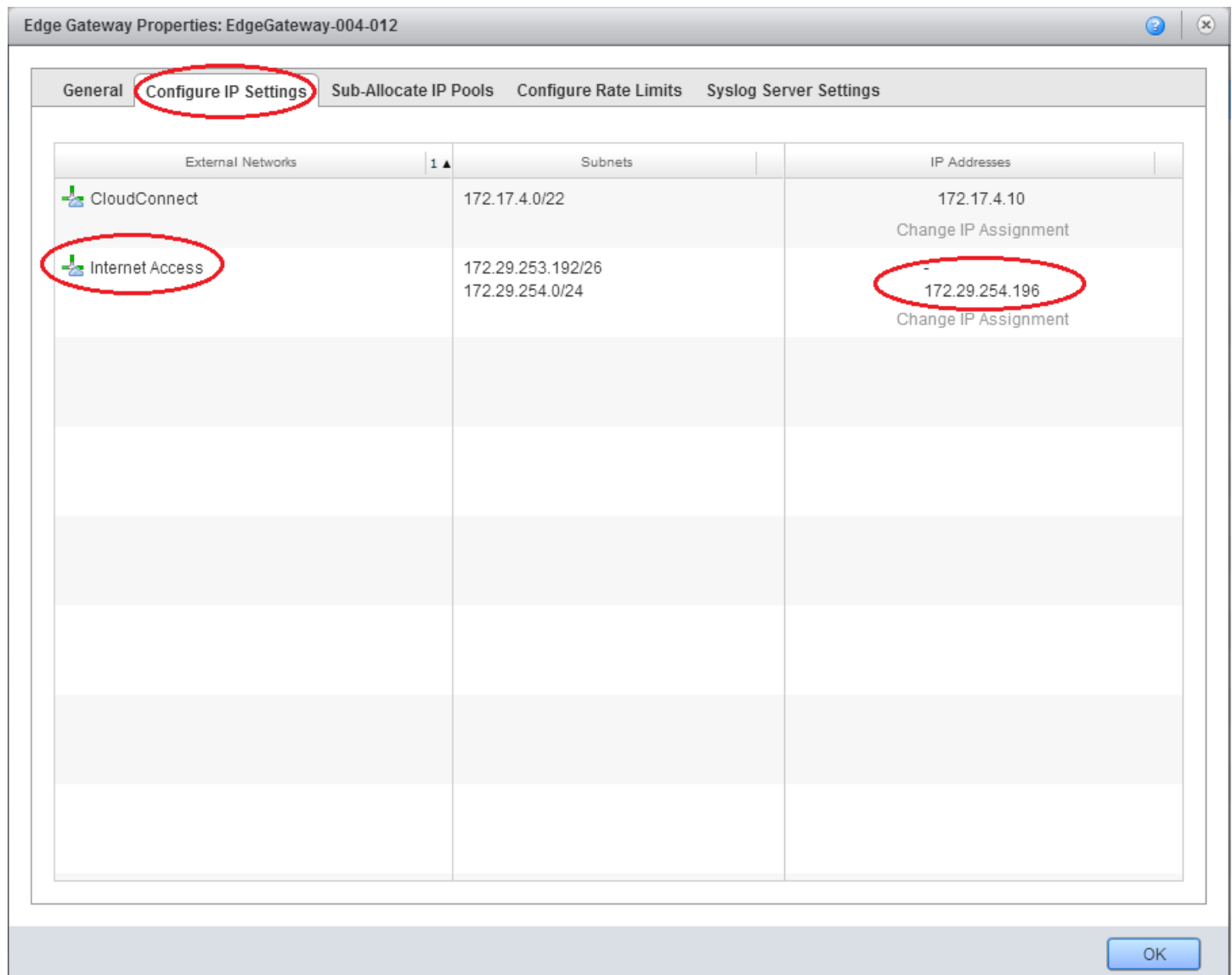
Obtain your Edge Gateway properties. Locate your Edge Gateway.

- 1) Login to vCloud Director
- 2) Select the Administration Tab
- 3) Left Click on the Virtual Datacenter to Expand the Virtual Datacenter Submenus
- 4) Choose the Edge Gateway sub menu
- 5) Right click the Edge Gateway you would like to use to create the VPN Tunnel and choose properties.



## Locate the Edge Gateway's Internet Access IP Address

- 1) In the Edge Gateway Properties Window, choose the "Configure IP Settings Tab."
- 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 **172.29.254.196**. This address is pre-assigned to you by CloudConnect.



## Access the VPN Edge Gateway Services on the CloudConnect Edge Gateway

- 1) Similar to above, from the Edge Gateway View, right click the Edge Gateway, and this time select “Edge Gateway Services” from the context menu.

The screenshot displays the ABC IT Co. Administration console. The top navigation bar includes links for Home, My Cloud, Catalog, and Administration (circled in red). The left sidebar shows the Administration menu with options like Cloud Resources, Virtual Datacenters, Members, and Settings. The main content area is titled "ABC IT Co. Virtual Datacenter" and features tabs for vApps, vApp Templates, Media & Other, Storage Policies, Edge Gateways (circled in red), and Org VDC Netw... Below the tabs is a table of Edge Gateways. The first row, "EdgeGateway-004-012", is selected (circled in red). A context menu is open over this row, listing actions: "Edge Gateway Services..." (circled in red), "External IP Allocations", "Re-Apply Service Configuration...", "Re-Deploy...", "Synchronize Syslog Server Settings", and "Properties...".

Name	Status	Multi-Interface Mode	# Used NICs	# External Networks
EdgeGateway-004-012	✓	✓	9	2

- 2) In the resultant window, select the “Firewall” tab.
- 3) Click Add in the bottom right hand corner.

Configure Services: EdgeGateway-004-012

DHCP NAT **Firewall** Static Routing VPN Load Balancer

Rules can be added to the Firewall to allow or deny specific network traffic. The order of these rules can be changed by selecting one or more rules, dragging and dropping them at the desired location in the list. The order of any selected rules is preserved after dropping them into a different location within the list.

☒ Enable firewall

Default action ☒ Deny ☐ Allow ☒ Log

Applicable to traffic that does not match the rules in the list.

Rule Id	Name	Source	Destination	Protocol	Action	Log	Enabled
1	AD Clients	10.5.0.0/16:Any	10.5.0.0/24:Any	ANY	Allow	-	✓
3	AD Clients	10.5.0.0/24:Any	internal:Any	ANY	Allow	-	✓
4	AD CloudConnect	172.19.0.0/24:Any	172.17.4.10:Any	ANY	Allow	-	✓
2	Default Internet Access	internal:Any	external:Any	ANY	Allow	-	✓
5	External to Client One DMZ	external:Any	192.168.1.0/24:80	TCP	Allow	-	✓
6	Allow ICMP	0.0.0.0/0	172.29.254.0/24	ICMP	Allow	-	✓

Add... Edit... Delete

OK Cancel

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

- 4) 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”
- 5) Enter the Network address in the **Source Window**, **192.168.10.0/24**
- 6) Enter the Org VDC Network subnet into the **Destination Window**, **10.5.0.0/24**
- 7) In the protocol dropdown menu select “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.
- 8) Verify the “Action” radio button is set to “Allow”
- 9) Optionally, you can enable logging of the traffic.

**Edit Firewall Rule**

☒ Enabled

Name:  \*

Source:  \*

Valid values can be IP address, CIDR, IP range, "any", "internal" and "external".

Source port:

Destination:  \*

Valid values can be IP address, CIDR, IP range, "any", "internal" and "external".

Destination port:

Protocol:

Action: ☒ Allow ☐ Deny

☐ Log network traffic for firewall rule

OK Cancel

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. These automatically determined exceptions will not be visible in the Firewall configuration window.

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

Add a New Site-to-Site VPN configuration:

- 1) In the Configure Services Window, select the VPN Tab.
- 2) Verify the Enable VPN checkbox is checked.
- 3) Click "Add" in the bottom right hand corner of the Window.

Configure Services: EdgeGateway-004-012

DHCP NAT Firewall Static Routing **VPN** Load Balancer

IPSec VPN service helps you create secure VPNs between gateways. Site-to-Site VPN can be configured between edge gateways in this organization, across organizations and even to third party VPN gateways.

☒ **Enable VPN**

[Configure Public IPs...](#)

Public IPs can be configured for each of the external networks, this is useful if you are using NAT in your environment.

Name	Local End Point	Peer End Point	Enabled	Status	Local Network	Peer Network	Peer Organization

[Add...](#) [Edit...](#) [Delete](#) [Peer settings...](#)

[OK](#) [Cancel](#)

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 Office"

Note: At a minimum you will want to clearly describe the On-Premise Network as the Configuration is ORG VDC Network Aware.

- 2) Verify that the "Enable this VPN configuration" checkbox is checked.
- 3) In the "Establish VPN to" dropdown menu, choose "A Remote Network."
- 4) In the "Local Networks" window, choose the Org VDC Network (Cloud Network) you would like to have access to the VPN Tunnel. In this example, the Network name is **Client Acme Network**.
- 5) In the "Peer Networks" Window, enter the network address in CIDR format of the On-Premise Network. In this example, **192.168.10.0/24**.
- 6) Scroll Down and Select "Internet Access" from the "Local Endpoint" dropdown menu.
- 7) The Local ID is the Edge Gateway IKE Identifier (Internet Access IP Address from Above). In this example, it is **172.29.254.196**. Add this to the "Local ID" window.
- 8) 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**.
- 9) The Peer IP 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**.
- 10) Choose AES-256 as the encryption protocol. If your on premise firewall does not support AES encryption, consider upgrading that device.
- 11) Scroll down and Click the "Show key" checkbox. Take note of this key, or copy it to your clipboard. You will need to copy the randomly generated Pre Shared Key into your SonicWALL.

Add a Site-to-Site VPN configuration

Name:

To Acme Chicago Office \*

Description:

☒ Enable this VPN configuration

Establish VPN to:

a remote network ▼

Local & Peer Networks

Local Networks:

Client Acme Network (10.5.0.0/24)

Client Network (10.5.9.0/24)

Client One Network (10.5.1.0/24)

Client AXGlobal Network (10.5.6.0/24)

Peer Networks:

192.168.10.0/24 \*

Enter network address in CIDR format. For example:  
192.168.2.0/24, 192.168.3.0/24.

VPN connection settings

Local Endpoint:

Internet Access ▼

Local ID:

172.29.254.196 \*

Peer ID:

123.234.123.234 \*

An ID to uniquely identify the peer. If the peer address is on this or another organization VDC network, this should be peer's native IP address. If peer is NAT'd, this should be the private peer IP address.

Peer IP:

123.234.123.234 \*

IP address to reach the peer. If the Peer is NAT'd, this should be the public side address of NAT.

Encryption protocol:

AES-256 ▼

Shared Key:

9oPxli96NbxmsFIF2enndr6MkhpN7dghdfg  
hdt54yt6|

The shared secret must be an alphanumeric string between 32 and 128 characters in length. It must include at least one uppercase letter, one lowercase letter, and one number.

☒ Show key

MTU

1500 \*

OK

Cancel



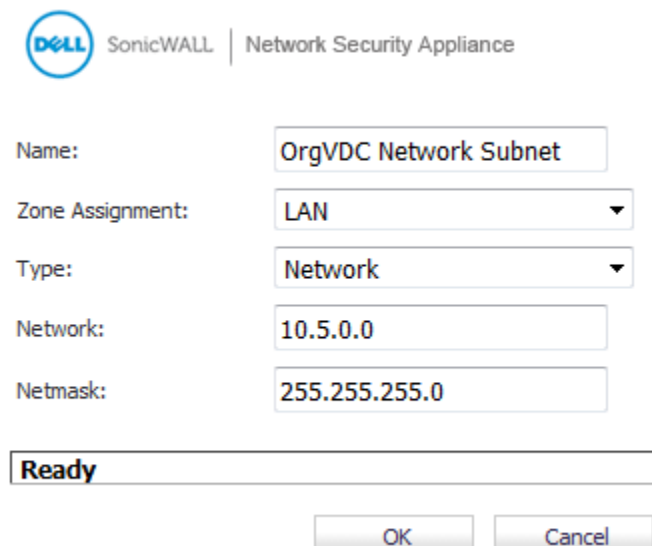
Note: The Shared Key can be retrieved later on if you do not have your SonicWALL (On-Premise device) readily accessible during this step.

- 12) Click OK to close the Site-to-Site VPN configuration
- 13) CLICK OK to close the Edge Gateway Services Configuration Window. The Edge Gateway will update itself with the new configuration.

## **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, **10.5.0.0**
- 7) Enter the Netmask **255.255.255.0**



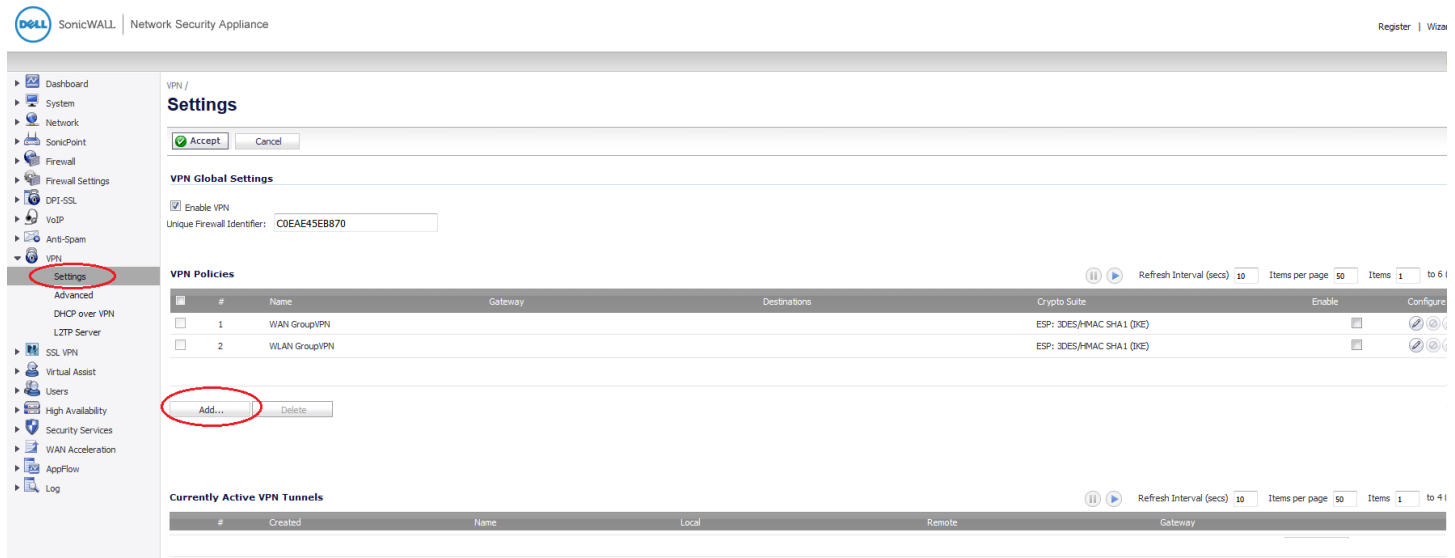
The screenshot shows the SonicWALL Network Security Appliance configuration interface. At the top, there is a header with the Dell logo, the text "SonicWALL", and "Network Security Appliance". Below this, there are five configuration fields:

- Name:** A text box containing "OrgVDC Network Subnet".
- Zone Assignment:** A dropdown menu with "LAN" selected.
- Type:** A dropdown menu with "Network" selected.
- Network:** A text box containing "10.5.0.0".
- Netmask:** A text box containing "255.255.255.0".

Below these fields is a status bar that says "Ready". At the bottom right, there are two buttons: "OK" and "Cancel".

## Create a New VPN Policy:

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



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 **172.29.254.196**. The corresponding **Primary Public IP Address** is **192.203.253.196** and the corresponding **Standby Public IP Address** is **108.26.236.196**.

## 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, **192.203.253.196**
- 5) IPsec Secondary Gateway Address: Enter the **Standby Public IP Address** of your Edge Gateway. In this example, **108.26.236.196**
- 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 **172.29.254.196**.

 SonicWALL | Network Security Appliance

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: 192.203.253.196

IPsec Secondary Gateway Name or Address: 108.26.236.196

---

### IKE Authentication

Shared Secret: 9oPxI96NbxmsFIF2enndr6MkhpN7

Confirm Shared Secret: 9oPxI96NbxmsFIF2enndr6MkhpN7 ☐ Mask Shared Secret

Local IKE ID: IP Address 123.234.123.234

Peer IKE ID: IP Address 172.29.254.196

---

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").



SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

### Local Networks

- ☒ Choose local network from list 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 OrgVDC Network Subnet ▼

Ready

OK

Cancel

Help

## Proposals Tab

### IKE (Phase 1) Proposal

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

### Ipsec (Phase 2) Proposal

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



SonicWALL | Network Security Appliance

General

Network

Proposals

Advanced

### IKE (Phase 1) Proposal

Exchange:	Main Mode
DH Group:	Group 2
Encryption:	AES-256
Authentication:	SHA1
Life Time (seconds):	28800

### Ipsec (Phase 2) Proposal

Protocol:	ESP
Encryption:	AES-256
Authentication:	SHA1
<input checked="" type="checkbox"/> Enable Perfect Forward Secrecy	
DH Group:	Group 2 *
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.

 SonicWALL | Network Security Appliance Register | Wiza

---

Dashboard

System

Network

SonicPoint

Firewall

Firewall Settings

DPI-SSL

VoIP

Anti-Spam

VPN

Settings

Advanced

DHCP over VPN

L2TP Server

SSL VPN

Virtual Assist

Users

High Availability

Security Services

WAN Acceleration

AppFlow

Log

VPN /

Settings

Accept

Cancel

VPN Global Settings

☒ Enable VPN

Unique Firewall Identifier: C0EAE45EB870

VPN Policies

Refresh Interval (secs) 30

Items per page 50

Items 1 to 61

#	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	192.203.253.196 108.26.236.196	10.5.0.0 - 10.5.0.255	ESP: AES-256/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>

Add...

Delete

Site To Site Policies: 4 Policies Defined, 3 Policies Enabled, 75 Maximum Policies Allowed

Group/VPN Policies: 2 Policies Defined, 0 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels

Refresh Interval (secs) 30

Items per page 50

Items 1 to 41

#	Created	Name	Local	Remote	Gateway	
4	11/11/2015 09:23:45	To CloudConnect Org/DC Network	192.168.10.0 - 192.168.10.255	10.5.0.0 - 10.5.0.255	192.203.253.196	<div>Renegotiate</div>

In the vCloud Director Control Panel, verify the Tunnel Status in Edge Gateway VPN Services configuration.

Configure Services: EdgeGateway-004-012 ? ✕

DHCP NAT Firewall Static Routing VPN Load Balancer

IPSec VPN service helps you create secure VPNs between gateways. Site-to-Site VPN can be configured between edge gateways in this organization, across organizations and even to third party VPN gateways.

☒ Enable VPN

Configure Public IPs...

Public IPs can be configured for each of the external networks, this is useful if you are using NAT in your environment.

Name	Local End Point	Peer End Point	Enabled	Status	Local Network	Peer Network	Peer Organization
To Acme Chicago Offi	123.234.123.234	71.162.115.4	✓	✓	10.5.0.1/24	192.168.10.0/24	-

Add...

Edit...

Delete

Peer settings...

OK

Cancel

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 10.5.0.10

Pinging 10.5.0.10 with 32 bytes of data:
Reply from 10.5.0.10: bytes=32 time=13ms TTL=127
Reply from 10.5.0.10: bytes=32 time=13ms TTL=127
Reply from 10.5.0.10: bytes=32 time=11ms TTL=127
Reply from 10.5.0.10: bytes=32 time=13ms TTL=127

Ping statistics for 10.5.0.10:
    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!