# Table of Contents

1 Introduction .......................................................................................................................... 2  
  1.1 Exemplary Site-to-Site VPN ............................................................................................ 2  

2 Configurations ..................................................................................................................... 3  
  2.1 Site 1 Controller .............................................................................................................. 3  
  2.2 Site 2 Controller .............................................................................................................. 6  
  2.3 Verifying Network Connection ....................................................................................... 8  
  2.4 Variation of the Exemplary Site-to-Site VPN ................................................................. 9  

3 Conclusion .......................................................................................................................... 13  

4 Remarks .............................................................................................................................. 13
1 Introduction

Virtual private networks (VPNs) provide a way for secure connections to be established across the public network by tunneling the traffic. VPNs generally fall into two types—remote-access VPN and site-to-site VPN. Remote-access VPNs can be used to securely connect a host to a private network. For example, companies can allow staff to remotely access the file servers or other resources on the headquarters’ intranet from an outside network using remote VPNs. With site-to-site VPNs, separate private networks could be joined for data sharing or other purposes. For example, private networks of different office branches of a company or even private networks of different companies can be joined.

In this technical guide, the Site-to-Site VPN feature on the controller is introduced, and guidance on how to build and configure an exemplary site-to-site VPN is provided through step-by-step explanations.

1.1 Exemplary Site-to-Site VPN

The exemplary site-to-site VPN is to be established between Site 1 and Site 2, and at least one controller is placed at each site for establishing the VPN. On each controller, multiple Local Sites and Remote Sites can be added to create multiple site-to-site VPNs. The terms “local” and “remote” are with respect to the current controller. Careful prior planning of the Local Subnet – Remote Subnet mapping is advised.

An important thing to keep in mind is that any of the network segments used for Local and Remote Subnets cannot overlap. For example, if a site-to-site VPN is to be established between the network segment of Service Zone 1 on controller 1 at Site 1 and the network segment of Service Zone 1 on controller 2 at Site 2, the two Service Zones cannot be assigned the same network segment. Furthermore, the network segments of Remote Subnets also cannot overlap with the network segments of any of the Service Zones on the local controller even if these Service Zones are disabled.

Here, the site-to-site VPN will be established between Service Zone 1 of the controller at Site 1 and the Default Service Zone of the controller at Site 2. See diagram below.
2 Configurations

2.1 Site 1 Controller

a. Go to Site > Service Zone > Service Zone Configuration, configure the Network Interface as desired. Here, Service Zone 1 is chosen, with its Network Interface set to 172.21.1.254/255.255.255.0.
b. Go to **Network > VPN**, click Add under Remote Sites.

![Site-to-Site VPN configuration screen]

<table>
<thead>
<tr>
<th>Local Sites</th>
<th>Remote Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. Local Host/Subnet</td>
<td>No. Name IP Address Pre-shared Key</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Remote VPN Gateway</td>
<td>Remote Host/Subnet Tunnel Status</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

c. Enter the public IP address of Site 2. 60.0.0.1 is used for this example. Enter a pre-shared key and select the Diffie-Hellman Group. Configure other settings as desired. Enter the network segments to be accessed at Site 2 into Remote Subnet. Here the entire network segment assigned to Default Service Zone of Site 2 is entered, which is 192.168.1.0/24. Click Apply.

![Remote Site Configuration details]

| Name | Site 2 |
|IP Address | 60.0.0.1 |
|Authentication Method | Pre-shared Key |
|Pre-shared Key | abcd1234 |
|Phase1 Proposal | Encryption AES256 Authentication SHA-1 |
|Diffie-Hellman Group | 1 |
|IKE Life Time | 8 |
|Dead Peer Detection | DPD Delay: 10 (second) DPD Timeout: 15 (second) |
|Remote Subnet | 1 192.168.1.0 255.255.255.0/24 2 23 255.255.255.255/32 3 |

After applying the settings, the added entry will show on the list of Remote sites.
d. Click Add under Local Sites.

e. Choose the desired WAN for Local Interface. Select Site 2 as the Remote VPN Gateway. For Local Host/Subnet, choose Subnet and enter the network segment of Service Zone 1 of Site 1 (172.21.1.0/24). For Remote Host/Subnet, choose the network segment of Default Service Zone of Site 2 (192.168.1.0/24). Configure other settings as desired. Click Apply.
After applying the settings, the added entry will show on the list of Local sites.

### 2.2 Site 2 Controller

a. Go to **System > Service Zone > Service Zone Configuration**, configure the Network Interface as desired. Here, Default Service Zone is chosen, with its Network Interface set to 192.168.1.254/24.

![Service Zone Configuration](image)

- **Service Zone Status**: Enabled
- **Service Zone Name**: Default
- **Network Interface**:
  - **IP Address**: 192.168.1.254
  - **Subnet Mask**: 255.255.255.0

a. Go to **Network > VPN**, click Add under Remote Sites and enter the public IP address of Site 1. 50.0.0.1 is used in this example. Enter the same pre-shared key as that on controller 1 and select the Diffie-Hellman Group. Configure other settings as desired. Enter the network
segments to be accessed at Site 1 into Remote Subnet. Here the entire network segment assigned to Service Zone 1 of Site 1 is entered, which is 172.21.1.0/24. Click Apply.

b. Choose the desired WAN for Local Interface. Select Site 1 as the Remote VPN Gateway. For Local Host/Subnet, choose Subnet and enter the network segment of Default Service Zone of Site 2 (192.168.1.0/24). For Remote Host/Subnet, choose the network segment of Service Zone 1 of Site 1 (172.21.1.0/24). Configure other settings as desired. Click Apply.
After applying the settings, the added entries should show on the main configuration page for Site-to-Site VPN.

2.3 Verifying Network Connection

a. Go to Network > VPN or refresh the page on both controllers to check the tunnel status. The tunnel status should show “Established”.

Site 1
b. Prepare two client devices and turn off the firewall on the devices.

c. Perform ping tests on the client devices using any ping tool to see if the two devices could ping each other.

### 2.4 Variation of the Exemplary Site-to-Site VPN

As mentioned previously, multiple Local Sites and Remote Sites can be added to create multiple site-to-site VPNs. Diagram below shows a variation of the exemplary site-to-site VPN, where an additional site-to-site VPN is to be created between the network segments of Service Zone 1 on both controllers.
2.4.1 Site 1 Controller

a. Click on the existing entry. Under Remote Subnet, add the network segment assigned to Service Zone 1 of Site 2, which is 172.21.0.0/24. Do not add a Remote Site.
b. Add a Local Site. The Remote VPN Gateway is still Site 2. For Remote Host/Subnet, select the Remote Subnet just added.

Return to the main configuration page, there should be two entries under Local Sites and one entry under Remote Site.
2.4.2 Site 2 Controller

a. Add a Local Site. For Local Host/Subnet, choose Subnet and enter the network segment of Default Service Zone of Site 2 (172.21.1.0/24). For Remote Host/Subnet, choose the network segment of Service Zone 1 of Site 1 (172.21.1.0/24).

Return to the main configuration page, there should be two entries under Local Sites and one entry under Remote Site.
3 Conclusion

In this technical guide, the Site-to-Site VPN feature on the controller is introduced, and guidance on how to build and configure an exemplary site-to-site VPN is also through step-by-step explanations.

4 Remarks

Please contact Edgecore’s Technical Support Team at ecwifi@edge-core.com for additional inquiries.