

# **Technical Guide**

# Site-to-Site VPN

Released: 2018-01-10 Doc Rev No: R2

#### **Copyright Notification**

#### **Edgecore Networks Corporation**

© Copyright 2019 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

## Table of Contents

1	Introd	uction	2
	1.1	Exemplary Site-to-Site VPN	
2	Config	rurations	
	2.1	Site 1 Controller	
	2.2	Site 2 Controller	
	2.3	Verifying Network Connection	
	2.4	Variation of the Exemplary Site-to-Site VPN	
3	Conclu	ision	
4	Remar	<sup>.</sup> ks	

## 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

 Go to System > 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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Main > System > Servio	c <mark>e Zone</mark> > Service Zone C	onfiguration			
WAN						
IPv6	Basic Sett	ings				
LAN Ports						
High Availability						
Service Zones	Service Zon	e Status	Enabled Oisabled	1		
Port Location Mapping	Service Zon	e Name	SZ1			
PMS Interface	Network Int	terface	VLAN Tag	1 * (Range: 1 ~ 40	94)	
			Tag-based Isolation	Inter-VLAN Isolation	on 🔍 Clients Isolation	None
			Note: When set to "None" gateway's LAN port may b the switch and there are 2	, the port on a switch conne be shut down if 'Loop Protec 2 VLANs belonging to this Se	cting to the tion' is enabled on rvice Zone.	
			Operation Mode	NAT OR Router		
			IP Address 172.21.1.254	* Subnet Mask 25	5.255.255.0 *	
			Network Alias List	Configure		
			This list defines other IP A Zone.	ddresses (range) that are ro	utable in this Service	
	DHCP		Enabled	Configure		

b. Go to N	letwork > VI	PN, click	Add under	Remote Sites.
------------	--------------	-----------	-----------	---------------

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
NAT				CONTRACTOR OF THE		
Monitor List	Site-to-Sit	e VPN				
Walled Garden	Site-to-Sit	CVIN				
VPN						
Proxy Server	Local Sites					
Local DNS Records						
Dynamic Routing	_	dd Delete				
DDNS			Local Local	Remote	Remote	
Client Mobility		No. Hos	st/Subnet Interface	VPN Gateway	Host/Subnet	Tunnel Status
	Remote Site	s				
	A	dd ] Delete				
		No.	Name	IP Address	Pre-sl	hared Key
			_ <b>A</b>	pply 🖸 🖸 Ca	ncel	

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.

Name	Site 2			
IP Address	60.0.0.1			
Authentication Method	Pre-shared Key ▼			
Pre-shared Key	abcd1234			
Phase1 Proposal	Encryption Authentication	AES256 ▼ SHA-1 ▼		
Diffie-Hellman Group	🗹 Group 1 🔲 Gro	up 2 Group 5		
Diffie-Hellman Group IKE Life Time	Ø Group 1 □ Gro 8	up 2 Group 5	; e.g. 36h stands for 1 d.	ay and 12 hours)
Diffie-Hellman Group IKE Life Time Dead Peer Detection	Group 1 □ Gro     Group 1 □ Gro     DPD Delay	up 2 Group 5 time is a 5-digit number	; e.g. 36h stands for 1 d	ay and 12 hours)
Diffie-Hellman Group IKE Life Time Dead Peer Detection	<ul> <li>✓ Group 1 □ Gro</li> <li>8 □ h ▼ (The</li> <li>DPD Delay</li> <li>DPD Timeout</li> </ul>	up 2 Group 5 time is a 5-digit number 10 15	; e.g. 36h stands for 1 d (second) (second)	ay and 12 hours)
Diffie-Hellman Group IKE Life Time Dead Peer Detection Remote Subnet	Group 1 Gro Group 1 Gro The DPD Delay DPD Timeout No.	up 2 Group 5 time is a 5-digit number 10 15 Network	; e.g. 36h stands for 1 d (second) (second)	ay and 12 hours) Mask

After applying the settings, the added entry will show on the list of Remote sites.

ote Sites				
Add D	elete			
	No.	Name	IP Address	Pre-shared Key
	1	Site 2	60.0.0.1	abcd1234

d. Click Add under Local Sites.

	SYSTEM	USERS	DEVIC	ES	NETWORK	UTILITIES	STATUS
NAT							
Monitor List	Site-to-Sit	e v P N					
Walled Garden							
VPN	Local Sites						
Proxy Server	Local Sites						
Local DNS Records	A	dd Delete					
Dynamic Routing							
DDNS		No.	Local Host/Subnet	Local	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
Client Mobility							
	Remote Site	5					
	A	dd Delete					
		<b>•</b> N	lo. Nan	ne	IP Address	Pre-sh	ared Key
			1 Site	2	60.0.0.1	abo	d1234
				🖉 Ap	ply 🖸 Cance	N	

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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
NAT						
Monitor List	Local Site	Configurat	ion			
Walled Garden						
VPN						
Proxy Server	Local Interfa	ice	WAN1 V			
Local DNS Records	Remote VPN	l Gateway	Site 2 ▼ Edit Host	Add a New Host		
Dynamic Routing	Least Liest/C	whenet	🔍 Host 💿 Subnet			
DDNS	LOCAL HOSU'S	oubnet	172.21.1.0/24	(in prefix notation: x.x.x.x	(уу)	
Client Mobility	Remote Hos	t/Subnet	192.168.1.0/24 🔻			
	Phase2 Prop	oosal	Encryption AES	5256 ▼		
			Authentication SH/	A-1 ▼		
	Key Life Tim	e	24 h 🔻 (1~	99999; e.g. 36h stands for 1 da	ay and 12 hours)	
	Rekey		Enable Rekey			
			Rekey Margin 9	m ▼ (1 ~ 99999; e.g.	36h stands for 1 day and 12 ho	ours)
				Apply Ca	ancel	

	es					
	Add Del	ete				
	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
	1	172.21.1.0/24	WAN1	60.0.0.1	192.168.1.0/24	Not established
Remote	Sites	ete				
Remote	Sites	ete No.	Name	IP Address	Pre-	shared Key

After applying the settings, the added entry will show on the list of Local sites.

#### 2.2 Site 2 Controller

 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.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
General	Main > System > Servio	<b>ce Zone</b> > Service Zone (	Configuration			
WAN						
IPv6	Basic Sett	ings				
LAN Ports						
Service Zones						
Port Location Mapping	Service Zon	e Status	Enabled			
PMS Interface	Service Zon	e Name	Default			
	Network Int	terface	Tag-based Isolation	Inter-VLAN Isolatio	n 🔍 Clients Isolation 🤇	None
			Note: When set to "None", t gateway's LAN port may be the switch and there are 2 V	he port on a switch connec shut down if 'Loop Protecti /LANs belonging to this Sen	ting to the ion' is enabled on vice Zone.	
			Operation Mode	🖲 NAT 🔍 Router		
			IP Address 192.168.1.254	* Subnet Mask 255	5.255.255.0 *	
			Network Alias List	Configure		
			This list defines other IP Ado Zone,	dresses (range) that are rou	utable in this Service	
				Craftering		

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.

Name	Site 1			
IP Address	50.0.0.1			
Authentication Method	Pre-shared Key 🔻			
Pre-shared Key	abcd1234			
Phase1 Proposal	Encryption Authentication	AES256 ▼ SHA-1 ▼		
Diffie-Hellman Group	🗹 Group 1 🔲 Grou	in 2 🗐 Group 5		
		ap z = droup s		
IKE Life Time	8 h ▼ (The	time is a 5-digit number	r; e.g. 36h stands for 1	day and 12 hours)
IKE Life Time Dead Peer Detection	8 h 🔻 (The DPD Delay	time is a 5-digit number	r; e.g. 36h stands for 1 (second)	day and 12 hours)
r IKE Life Time Dead Peer Detection	8 h 🔻 (The DPD Delay DPD Timeout	time is a 5-digit number	r; e.g. 36h stands for 1 (second) (second)	day and 12 hours)
IKE Life Time Dead Peer Detection Remote Subnet	8 h ▼ (The DPD Delay DPD Timeout No.	time is a 5-digit number 10 15 Network	r; e.g. 36h stands for 1 (second) (second)	day and 12 hours) Mask
IKE Life Time Dead Peer Detection Remote Subnet	8 h ▼ (The DPD Delay DPD Timeout No.	time is a 5-digit number 10 15 Network 172.21.1.0	r; e.g. 36h stands for 1 (second) (second)	day and 12 hours) Mask 255.255.255.0 (/24)
IKE Life Time Dead Peer Detection Remote Subnet	8 h ▼ (The DPD Delay DPD Timeout No. 1 2	time is a 5-digit number 10 15 Network 172.21.1.0	r; e.g. 36h stands for 1 (second) (second)	day and 12 hours) Mask 255.255.255.0 (/24)

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.

Local Interface	WAN1 V
Remote VPN Gateway	Site 1 🔻 Edit Host Add a New Host
Local Host/Subnet	<ul> <li>Host Subnet</li> <li>192.168.1.0/24</li> <li>(in prefix notation: x.x.x.x/yy)</li> </ul>
Remote Host/Subnet	172.21.1.0/24 🔻
Phase2 Proposal	Encryption AES256 V
	Authentication SHA-1 •
Key Life Time	24 h ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Rekey	Enable Rekey
	Rekey Margin 9 m ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)

After applying the settings, the added entries should show on the main configuration page for Site-to-Site VPN.

	les						
	Add De	lete					
	No.	Loca Host/Sul	l bnet l	Local nterface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
	1	192 168 1	.0/24	WAN1	50.0.0.1	172.21.1.0/24	Not established
Remote	Sites	ete					
Remote	Sites	lete No.	Name		IP Address	Pre-s	hared Key

#### 2.3 Verifying Network Connection

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

	Add De	lete				
	No.	Loca Host/Sul	l Loc onet Inter	al Remote face VPN Gateway	Remote Host/Subnet	Tunnel Status
	0 1	172.21.1.	0/24 WA	N1 60.0.0.1	192.168.1.0/24	Established
Remote	Sites	ete	Name	10 Addrose	Pro	shared Vey
Remote	Sites	ete No.	Name	IP Address	Pre	-shared Key

Site 1

	Add De	lete				
	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
		in ossi babilet				
	1	192.168.1.0/24	WAN1	50.0.0.1	172.21.1.0/24	Established
Remote S	ittes	192.168.1.0/24	WAN1	50.0.0.1	172.21.1.0/24	Established
Remote S	ittes	192.168.1.0/24 ete	WAN1	50.0.0.1 IP Address	172.21.1.0/24	Established

- 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 siteto-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.

Name	Site 2			
IP Address	60.0.0.1			
Authentication Method	Pre-shared Key 🔻	]		
Pre-shared Key	abcd1234			
Phase1 Proposal	Encryption Authentication	AES256 ▼ SHA-1 ▼		
Diffie-Hellman Group	🗷 Group 1 🔲 Gro	oup 2 🔲 Group 5		
IKE Life Time	8 h 🔻 (Th	e time is a 5-digit numbe	r; e.g. 36h stands for 1	day and 12 hours)
Dead Peer Detection	DPD Delay	10	(second)	
Dead Peer Detection	DPD Delay DPD Timeout	10 15	(second) (second)	
Dead Peer Detection Remote Subnet	DPD Delay DPD Timeout <b>No.</b>	10 15 Network	(second) (second)	Mask
Dead Peer Detection Remote Subnet	DPD Delay DPD Timeout <b>No.</b> 1	10 15 Network 192.168.1.0	(second) (second)	Mask 255.255.255.0 (/24)
Dead Peer Detection Remote Subnet	DPD Delay DPD Timeout <b>No.</b> 1 2	10 15 Network 192.168.1.0 172.21.0.0	(second) (second)	Mask 255.255.255.0 (/24) ▼ 255.255.255.0 (/24) ▼

b. Add a Local Site. The Remote VPN Gateway is still Site 2. For Remote Host/Subnet, select the Remote Subnet just added.

Local Interface	WAN1 T
Remote VPN Gateway	Site 2 🔻 Edit Host Add a New Host
Local Host/Subnet	Host Subnet 172.21.1.254/24 (in prefix notation: x.x.x.x/yy)
Remote Host/Subnet	172.21.0.0/24 🔻
Phase2 Proposal	Encryption AES256  Authentication SHA-1
Key Life Time	24  [h ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Rekey	Enable Rekey
	Rekey Margin 9 m ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)

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

	Add	Delete					
	-	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
		1	172.21.1.0/24	WAN1	60.0.0. <mark>1</mark>	192.168.1.0/24	Not established
	-		172 21 1 0/24		100 101 101		
		2	172.21.1.0724	WANT	60.0.0.1	1/2.21.0.0/24	Not established
Remote	Sites	) Delete	No.	Name	60.0.0.1 IP Address	172.21.0.0/24	Not established

#### 2.4.2 Site 2 Controller

 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).

Local Interface	WAN1 V
Remote VPN Gateway	Site 1 🔻 Edit Host Add a New Host
Local Host/Subnet	Host Subnet 172.21.0.0/24 (in prefix notation: x.x.x.x/yy)
Remote Host/Subnet	172.21.1.0/24 🔻
Phase2 Proposal	Encryption AES256 V
	Authentication SHA-1 🔻
Key Life Time	24 h ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hours)
Rekey	Enable Rekey
	Rekey Margin 9 m ▼ (1 ~ 99999; e.g. 36h stands for 1 day and 12 hour

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

	les						
	Add	Delete					
	-	No.	Local Host/Subnet	Local Interface	Remote VPN Gateway	Remote Host/Subnet	Tunnel Status
		1	192.168.1.0/24	WAN1	50.0.0.1	172.21.1.0/24	Not established
				1000000			
		2	172.21.0.0/24	WAN1	50.0.0.1	172.21.1.0/24	Not established
Remote	Sites	2 Delete	No. Na	me	IP Address	172.21.1.0/24	Not established

## 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 <u>ecwifi@edge-core.com</u> for additional inquiries.