Questionnaire: Site-to-Site VPN for Dedicated Region Deployments

If you select site-to-site VPN as a networking option for Messaging Connectivity between the event broker services in your Dedicated Region and your VPC, we may ask you to complete a site-to-site questionnaire to help us configure the site-to-site VPN correctly.

If you select Microsoft Azure or Google Cloud for your site-to-site VPN, you do not need to complete the site-to-site questionnaire. For information about the configuration requirements for Azure or Google Cloud site-to-site VPN, see the provider documentation listed below and then contact Solace.

- Azure VPN Gateway documentation
- Google Cloud VPN documentation

If you select AWS as the provider for your site-to-site VPN, you must complete the following questionnaire to help us configure the VPN correctly. There are two sections of questions you must answer:

- General AWS Site-to-Site VPN Details
- Tunnel Specific Details for AWS Site-to-Site VPN

For more information about configuring an AWS site-to-site VPN and to understand how you should answer the questions below, see the AWS Site-to-site VPN documentation.

General AWS Site-to-Site VPN Details

You must answer the following general questions about the configuration of your AWS site-to-site VPN.

Question	Answer	Additional Information About the Question
What datacenter do you want to connect the site-to-site VPN to? If you do not know the data-	`myfirstservice` in `eu-central-1`	We need this information to connect your VPC to the right event broker service

Question	Answer	Additional Information About the Question
center ID, you can provide an event broker service name or service ID which we will use to locate the datacenter ID.		and the region.
What is the external IP address or fully qualified domain name (FQDN) of your VPN?		We need this information to configure your gateway properly. For more information, see the Customer gateway options for your Site-to-Site VPN connection in the AWS VPN documentation.
Do you require static or dynamic routing?	Static **or** Dynamic	We recommend dynamic routing.
If you require dynamic routing, what border gateway protocol (BGP) autonomous system number (ASN) will you use?		We support an ASN in the range of 1-2,147,483,647. You can choose an existing public ASN assigned to your network. The following ASN numbers are reserved and cannot be used: • 7224—Reserved in all regions • 9059—Reserved in the eu-west-1 region • 10124—Reserved in the ap-northeast-1 region • 17934—Reserved in the ap-southeast-1 region
If you require static routing, what static route will you use?		You can provide multiple static routes if your deployment requires it. You must

Question	Answer	Additional Information About the Question
		provide the routes in CIDR format (x.x.x.x/x) and list all networks that will connect to the event broker service.
What Internet Key Exchange (IKE) version will you use?	1 **or** 2	We support IKE version 1 and 2, but recommend using IKEv2.
Will you use a VPN appliance? If so, what VPN appliance vendor and appliance platform will you be use?		We support multiple VPN appliances and appliance platforms, such as Cisco ASA 5500, Barracuda NextGen Firewall F-series, and Palo Alto PA series.
Will you use VPN software? If so, what VPN software vendor and software platform will you be use?		We support software VPNs from multiple providers, such as Cisco ASA 9.7+ VTI, Barracuda 6.2+, and Palo Alto PAN-OS 7.0+.

Tunnel Specific Details for AWS Site-to-Site VPN

You must complete the following tunnel specific configuration details about your AWS site-to-site VPN. For more information, see the AWS Site-to-site VPN documentation. For some properties, we suggest using the default values recommended in the AWS documentation.

Question	Answer	Additional Information About the Question
Tunnel 1		

Question	Answer	Additional Information About the Question
Pre-shared key (PSK)		Either party can provide the PSK. If you would like Solace to provide the PSK, leave the answer blank.
Phase 1 encryption algorithms		
Phase 2 encryption algorithms		
Phase 1 integrity algorithm		
Phase 2 integrity algorithm		
Phase 1 DH group numbers		
Phase 2 DH group numbers		
Phase 1 lifetime (in seconds)		We suggest using the default value.
Phase 2 lifetime (in seconds)		We suggest using the default value.
Rekey fuzz (as a percentage)		We suggest using the default value.
Replay window size (number of packets)		We suggest using the default value.

Question	Answer	Additional Information About the Question
Dead peer dedication (DPD) timeout action		We support Clear, Restart, and None, but recommend using Restart for self-recovery.
Startup action		We support both Add and Start, but recommend Start. Start requires IKEv2.
Tunnel 2		
Pre-shared key (PSK)		Either party can provide the PSK. If you would like Solace to provide the PSK, leave the answer blank.
Phase 1 encryption algorithms		
Phase 2 encryption algorithms		
Phase 1 integrity algorithm		
Phase 2 integrity algorithm		
Phase 1 DH group numbers		
Phase 2 DH group numbers		
Phase 1 lifetime (in seconds)		We suggest using the default value.
Phase 2 lifetime		We suggest using the default value.

Question	Answer	Additional Information About the Question
(in seconds)		
Rekey fuzz (as a percentage)		We suggest using the default value.
Replay window size (number of packets)		We suggest using the default value.
Dead peer dedication (DPD) timeout action		We support Clear, Restart, and None, but recommend using Restart for self-recovery.
Startup action		We support both Add and Start, but recommend Start. Start requires IKEv2.