Configure Secure Access with Fortigate Firewall

Contents
Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
Configure the VPN on Secure Access
Tunnel Data
Configure the VPN Site to Site on Fortigate
Network
Authentication
Phase 1 Proposal
Phase 2 Proposal
Configure the Tunnel Interface
Configure Policy Route
<u>Verify</u>

Introduction

This document describes how to configure Secure Access with Fortigate Firewall.

Prerequisites

- Configure User Provisioning
- <u>ZTNA SSO Authentication Configuration</u>
- <u>Configure Remote Access VPN Secure Access</u>

Requirements

Cisco recommends that you have knowledge of these topics:

- Fortigate 7.4.x Version Firewall
- Secure Access
- Cisco Secure Client VPN
- Cisco Secure Client ZTNA
- Clientless ZTNA

Components Used

The information in this document is based on:

- Fortigate 7.4.x Version Firewall
- Secure Access

- Cisco Secure Client VPN
- Cisco Secure Client ZTNA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Secure Access BTINET

Cisco has designed Secure Access to protect and provide access to private applications, both on-premise and cloud-based. It also safeguards the connection from the network to the internet. This is achieved through the implementation of multiple security methods and layers, all aimed at preserving the information as they access it via the cloud.

Configure

Configure the VPN on Secure Access

Navigate to the admin panel of Secure Access.



Click on Connect > Network Connections > Network Tunnels Groups

82	Overview	Overview				
		The Overview dashboard displays				
**	Connect	Essentials		Manage connections between your data of	enters and SSE	
i	Resources	Network Connections Connect data centers, tunnels,		Connector Groups Network Tunn	nel Groups	
U	Secure	Users and Groups		Network Tunnel Groups 9 total	2	2
\sim	Monitor	Provision and manage users and groups for use in access rules		4 Disconnected ()	3 Warning 🔺	Z Connected Ø
20	Admin	End User Connectivity Manage traffic steering from endpoints to Secure Access				

• Under Network Tunnel Groups click on + Add

Network Tunnel Groups

A network tunnel group provide	network tunnel group provides a framework for establishing tunnel redundancy and high										
availibility. Connect tunnels to to	alibility. Connect tunnels to the hubs within a network tunnel group to securely control										
user access to the Internet and	er access to the Internet and private resources. Help C										
Q, Search	Region	✓ Status	~	9 Tunnel Groups							

+ Add

- Configure Tunnel Group Name, Region and Device Type
- Click Next

General Settings	General Settings Give your network tunnel group a good meaningful name, choose a region through
2 Tunnel ID and Passphrase	which it will connect to Secure Access, and choose the device type this tunnel group will use.
3 Routing	Tunnel Group Name Fortigate
4 Data for Tunnel Setup	Region
	Europe (Germany) ~
	Device Type
	Other ~
$\overline{\langle}$	Cancel Next



Note: Choose the region nearest to the location of your firewall.

- Configure the Tunnel ID Format and Passphrase
- ClickNext

General Settings	Tunnel ID and Passphrase	
Tunnel ID and Passphrase	Configure the tunnel ID and passphrase that devices will use to connect tunnel group. Tunnel ID Format	to this
(3) Rodding	Email IP Address	
4 Data for Tunnel Setup	Tunnel ID @ <org> fortigate (%) <hub>.sse.cisco.com</hub></org>	
	Passphrase	
	•••••	\otimes
	The passphrase must be between 16 and 64 characters long. It must include at lea upper case letter, one lower case letter, one number, and cannot include any special characters.	st one al
	Confirm Passphrase	
	•••••	\otimes
<	Cancel Bac	k Next

- Configure the IP address ranges or hosts that you have configured on your network and want to pass the traffic through Secure Access
- ClickSave

	Deuting entires and naturally evenlage
General Settings	Routing options and network overlaps
-	Configure routing options for this tunnel group.
Tunnel ID and Passphrase	Network subnet overlap
 3 Routing (4) Data for Tunnel Setup 	Enable NAT / Outbound only Select if the IP address space of the subnet behind this tunnel group overlaps with other IP address spaces in your network. When selected, private applications behind these tunnels are not accessible.
0	Routing option
	Static routing
	Use this option to manually add IP address ranges for this tunnel group.
	IP Address Ranges
	Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.
	Add
	192.168.100.0/24 ×
	O Dynamic routing
	Use this option when you have a BGP peer for your on-premise router.
$\overline{\bullet}$	Cancel Back Save

After you click on Save the information about the tunnel gets displayed, please save that information for the next step, Configure the VPN Site to Site on Fortigate.

Tunnel Data

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	Ø		-sse.cisco.com	٦
Primary Data Center IP Address:	18.156.145.74 🗇			
Secondary Tunnel ID:	@		-sse.cisco.com	
Secondary Data Center IP Address:	3.120.45.23 🗇			
Passphrase:		CP	D	

Configure the VPN Site to Site on Fortigate

Navigate to your Fortigate dashboard.

• Click VPN > IPsec Tunnels

₽	VPN	~
	IPsec Tunnels	삷
	IPsec Wizard	
	IPsec Tunnel Template	
	VPN Location Map	



• Click Custom , configure a Name and click Next.

1 VPN Setup						
Name 2	Cisco Secure	e	1			
Template type	Site to Site	Hub-and-Spoke	Remote Access Custom			
					2	
				< Back	Next >	Cancel

In the next image, you see how you need to configure the settings for the Network part.

Network



- Network
 - IP Version : IPv4
 - Remote Gateway : Static IP Address
 - IP Address: Use the IP of Primary IP Datacenter IP Address, given in the step <u>Tunnel Data</u>
 - Interface : Choose the WAN interface that you have planned to use to establish the tunnel
 - Local Gateway : Disable as default
 - Mode Config : Disable as default
 - NAT Traversal : Enable
 - Keepalive Frequency : 10
 - Dead Peer Detection : On Demand
 - **DPD retry count** : 3
 - **DPD retry interval** : 10
 - Forward Error Correction : Do not check any box.
 - Advanced...: Configure it as the image.

Now configure the IKE Authentication.

Authentication

Authentication		Authentication	Authentication			
Method	Pre-shared Key 🗸	Method	Pre-shared Key 👻			
Pre-shared Key		Pre-shared Key	•••••			
IKE		IKE				
Version	1 2	Version	1 2			
Mode	Aggressive Main (ID protection)					

Authentication

- Method : Pre-Shared Key as default
- Pre-shared Key : Use the Passphrasegiven in the step Tunnel Data
- IKE
- Version : Choose version 2.



Note: Secure Access only supports IKEv2

Now configure the Phase 1 Proposal.

Phase 1 Proposal

Phase 1 Proposal	O Add					
Encryption	AES128	•	Authentication	SHA256	-	×
Encryption	AES256	-	Authentication	SHA256	-	×
Encryption	AES128	•	Authentication	SHA1	•	×
Encryption	AES256	•	Authentication	SHA1	•	×
		32	31 30 :	29 🗌 28 🗌	27	
Diffie-Hellman Gro	oups	21			16	
Kaul ifatima (seconds)		86400	V 14 V J .	2 [] 1		
Key Lifetime (seconds)		00400				
Local ID						

- Phase 1 Proposal
 - Encryption : Choose AES256

- Authentication : Choose SHA256
- Diffie-Hellman Groups : Check the box 19 and 20
- Key Lifetime (seconds) : 86400 as default
- Local ID : Use the Primary Tunnel ID, given in the step <u>Tunnel Data</u>

Now configure the Phase 2 Proposal.

Phase 2 Proposal

New Phase 2							ø	5					
Name		CSA											
Comments		Comments											
Local Address	addr_s	subnet 👻	0.0.0.0	0/0.0.0/0									
Remote Address		addr_s	subnet 👻	0.0.0.0	0/0.0.0.0								
Advanced									New Phase 2				
Phase 2 Proposal	O Add								Name		CSA		_
Encryption	AES128	•	Authenti	cation	SHA1	•	×		Comments		Comments		11
Encryption	AES256	-	Authenti	cation	SHA1	•	×		Local Address		addr_subnet 🔻	0.0.0/0.0.0.0	
Encryption	AES128	-	Authenti	cation	SHA256	•	×		Remote Address		addr_subnet 🔻	0.0.0.0/0.0.0.0	
Encryption	AES256	•	Authenti	cation	SHA256	•	×		Advanced				
Encryption	AES128GCM - X								Phase 2 Proposal	O Add			
Encryption	AES256G	CM 👻	×						Encryption	AES128	 Authentic 	cation SHA256	•
Encryption	CHACHA2	20POLY	1305 👻	×					Enable Replay Det	tection 🔽			
Enable Replay Det	ection 🗹								Enable Perfect Forward Secrecy (PFS)				
Enable Perfect For	ward Secree	y (PFS)							Local Port		All 🔽		
		32	31	30 🗆 3	29 🗌 28 🔲 3	27			Remote Port		All 🔽		
Diffie-Hellman Gro	oup	2115	20 □214 ✓	19 🔲 : 5 🔲 :	18 🔲 17 🔲 1 2 📄 1	16			Protocol		All 🔽		
Local Part									Auto-negotiate				
Bomoto Port	, i								Autokey Keep Aliv	/e			
Remote Port									Key Lifetime		Seconds		•
Auto pogotisto									Seconds		43200		
Koulifotime			ls		-								
Seconds		43200			•								

- New Phase 2
 - Name : Let as default (This is taken from the name of your VPN)
 - Local Address : Let as default (0.0.0/0.0.0)
 - Remote Address : Let as default (0.0.0.0/0.0.0.0)
- Advanced
 - Encryption : Choose AES128
 - Authentication : Choose SHA256
 - Enable Replay Detection : Let as default (Enabled)
 - Enable Perfect Forward Secrecy (PFS) : Unmark the checkbox
 - Local Port : Let as default (Enabled)
 - Remote Port: Let as default (Enabled)
 - Protocol : Let as default (Enabled)
 - Auto-negotiate : Let as default (Unmarked)
 - Autokey Keep Alive : Let as default (Unmarked)
 - Key Lifetime : Let as default (Seconds)
 - Seconds : Let as default (43200)

After that, click OK. You see after some minutes that the VPN was established with Secure Access, and you can continue with the next step, Configure the Tunnel Interface.

CSA

🛗 WAN (port1)

🕜 Up

Configure the Tunnel Interface

After the tunnel is created, you notice that you have a new interface behind the port that you are using as a WAN interface to communicate with Secure Acces.

In order to check that, please navigate to Network > Interfaces.

Network Interfaces DNS IDAM	≻	FortiGate VM64-AZURE	1 3 5 7 9 11 13 15 2 4 6 8 10 12 14 10 2 Delate	17 19 21 23 18 19 19 19 18 20 22 24	arch		
SD-WAN		+ Create New + Fort	B Delete Frintegra	te interrace Se	dicii	Q	
Static Routes		Name Ŧ	Тур	. ₽	Members ₹	IP/Netmask ₹	Administrative Access ₹
Dalia: Dautas	6	🗄 🗜 802.3ad Aggregate 🕦					
RIP		₽• fortilink	₽ 802.3ad Ag	gregate		Dedicated to FortiSwitch	PING Security Fabric Connection
OSPF	l.	🖃 🔛 Physical Interface 👍					
BGP Routing Objects Multicast		LAN (port2)	Physical Int	erface		192.168.100.5/255.255.255.0	PING HTTPS SSH
Diagnostics	1	WAN (port1)	Physical Int	erface		10.3.4.4/255.255.255.192	PING
💄 Policy & Objects	>						SSH
Security Profiles	> [🗉 💿 Tunnel Interface 🕦					
VPN User & Authentication	> >	NAT interface (naf.root)	Tunnel Inte	rface		0.0.0.0/0.0.0.0	
	>						

Expand the port you use to communicate with Secure Access; in this case, the WAN interface.

	🔚 WAN (port1)	Physical Interface
• • • • •		Tunnel Interface

• Click on your Tunnel Interface and click Edit

+ Cr	eate New 🔻 🖋 Edit 🛍 Delete	► Integrate Interface Searce					
	Name 🗢	Type 🗢					
= *	🖃 💤 802.3ad Aggregate 🔟						
	}● fortilink	 802.3ad Aggregate 					
	Physical Interface 4						
	🖬 LAN (port2)	Physical Interface					
	WAN (port1)	Physical Interface					
• • • • •	CSA CSA	Tunnel Interface					

• You have the next image that you need to configure

Name Alias Type Interface VRF ID (1) Role (1)	CSA CSA Tunn WAN O Undefi	el Interface (port1) ned -	Name Alias Type Interface VRF ID (Role ()	Name Image: CSA Alias Image: CSA Type Tunnel Interface Interface Image: WAN (port 1) /RF ID 0 Role Undefined	
Address			Address		
Addressing m IP	ode	Manual 0.0.0.0	Addressing IP	g mode	Manual 169.254.0.1
Netmask Remote IP/Ne	etmask	255.255.255.255	Netmask Remote IP	/Netmask	255.255.255.255 169.254.0.2 255.255.255.252

- Interface Configuration
- IP : Configure a non-routable IP that you do not have in your network (169.254.0.1)
- Remote IP/Netmask : Configure the Remote IP as the next IP of your interface IP and with a Netmask of 30 (169.254.0.2 255.255.255.252)

After that, click \mathbf{OK} to save the configuration and proceed with the next step, Configure Policy Route (Origin-based routing).



Warning: After this part, you must configure the Firewall Policies on your FortiGate in order to permit or allow the traffic from your device to Secure Access and from Secure Access to the networks that you want to route the traffic.

Configure Policy Route

At this point, you have your VPN configured and established to Secure Access; now, you must re-route the traffic to Secure Access to protect your traffic or access to your private applications behind your FortiGate firewall.

• Navigate to Network > Policy Routes

Ð	Dashboard	>		+ Creat	e New
÷	Network	~	F		Sec. #
	Interfaces		ŀ		Seq.#
	DNS			1	
	IPAM			2	
	SD-WAN			2	
	Static Routes				
	Policy Routes	<u></u>			

• Configure the policy

If incoming traffic mate	hes:	If incoming traffic matches:		
Incoming interface	+	Incoming interface	🖮 LAN (port2) 🗙 +	
IP/Netmask		Source Address		
	O	IP/Netmask	192.168.100.0/255.255.255.0	
Addresses	+		0	
Destination Address		Addresses	+	
IP/Netmask		Destination Address		
	0	IP/Netmask		
Addresses	+		0	
Internet service	+	Addresses	🗐 all 🛛 🗙	
Protocol	TCP UDP SCTP ANY Specify	Internet service	+	
Type of service	0 0x00 Bit Mask 0x00	Protocol	TCP UDP SCTP ANY Specify 0	
Then:		Type of service	0x00 Bit Mask 0x00	
Action	Forward Traffic Stop Policy Routing	Then:		
Outgoing interface 🌑	CSA 🔻	Action	Forward Traffic Stop Policy Routing	
Gateway address		Outgoing interface		
Comments	Write a comment # 0/255	Gateway address	169.254.0.2	
Status	Enabled Disabled	Comments	Write a comment	
		Status	• Enabled • Disabled	

- If Incoming traffic matches
 - Incoming Interface : Choose the interface from where you planned to re-route the traffic to Secure Access (Origin of traffic)
- Source Address
 - IP/Netmask : Use this option if you only route a subnet of an interface
 - Addresses : Use this option if you have the object created and the source of the traffic comes from multiple interfaces and multiple subnets
- Destination Addresses
 - Addresses: Choose all
 - Protocol: Choose ANY
- Then
 - Action: Choose Forward Traffic
- Outgoing Interface : Choose the Tunnel Interface that you modified on the step, <u>Configure Tunnel</u> <u>Interface</u>
- Gateway Address: Configure the Remote IP configured on the step, <u>RemoteIPNetmask</u>
- Status : Choose Enabled

Click **OK** to save the configuration, you are now ready to verify if your devices traffic was re-routed to Secure Access.

Verify

In order to verify if the traffic of your machine was re-routed to Secure Access, you have two options; you can check on the internet and check for your public IP, or you can run the next command with curl:

```
C:\Windows\system32>curl ipinfo.io
{
    "ip": "151.186.197.1",
    "city": "Frankfurt am Main",
    "region": "Hesse",
    "country": "DE",
    "loc": "50.1112,8.6831",
    "org": "AS16509 Amazon.com, Inc.",
    "postal": "60311",
    "timezone": "Europe/Berlin",
    "readme": "https://ipinfo.io/missingauth"
}
```

The public range from where you can see your traffic is from:

Min Host: 151.186.176.1

Max Host: 151.186.207.254



Note: These IPs are subject to change, which means that Cisco probably extend this range in the future.

If you see the change of your public IP, that means you are being protected by Secure Access, and now you can configure your private application on the Secure Access dashboard to access your applications from VPNaaS or ZTNA.