

Configurer un accès sécurisé avec le pare-feu Sonicwall

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configurer le groupe de tunnels réseau \(VPN\) sur l'accès sécurisé](#)

[Configuration du tunnel sur Sonicwall](#)

[Configuration du tunnel - Règles et paramètres](#)

[Ajouter une interface de tunnel VPN](#)

[Ajouter un objet et des groupes réseau](#)

[Ajouter une route](#)

[Ajouter des règles d'accès](#)

[Vérifier](#)

[Dépannage](#)

[PC utilisateur](#)

[Accès sécurisé](#)

[Paroi Sonique](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer un tunnel IPsec VTI entre un accès sécurisé au pare-feu Sonicwall à l'aide du routage statique.

Conditions préalables

- [Configurer le provisionnement utilisateur](#)
- [Configuration de l'authentification ZTNA SSO](#)
- [Configuration de l'accès sécurisé VPN à distance](#)

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pare-feu SonicWall (NSv270 - SonicOSX 7.0.1)

- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - ZTNA
- ZTNA sans client

Composants utilisés

Les informations contenues dans ce document sont basées sur :

- Pare-feu SonicWall (NSv270 - SonicOSX 7.0.1)
- Accès sécurisé
- Client sécurisé Cisco - VPN
- Client sécurisé Cisco - 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Diagramme du réseau

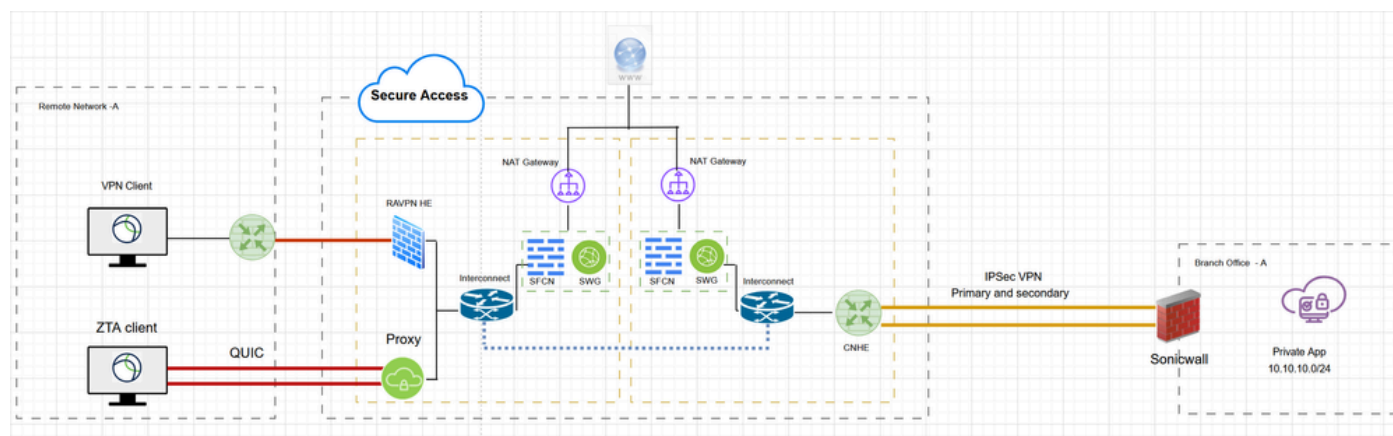


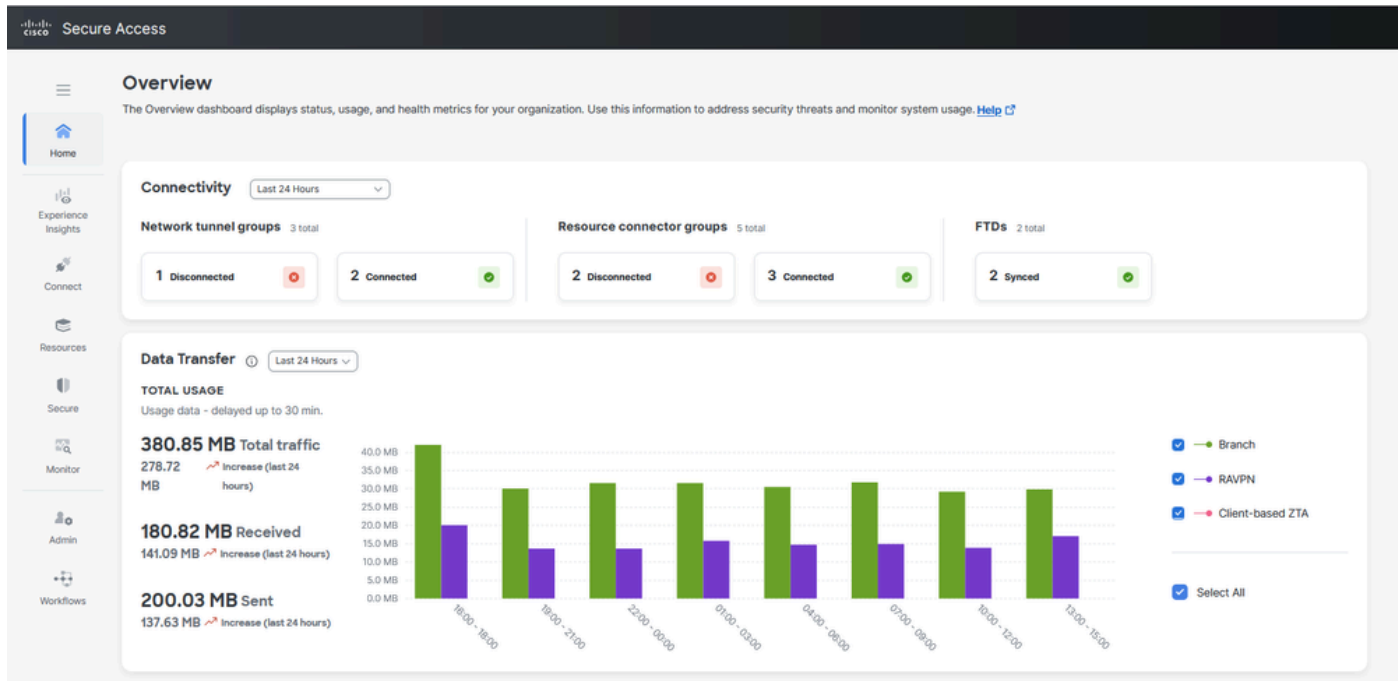
Diagramme du réseau

Configurer

Configurer le groupe de tunnels réseau (VPN) sur l'accès sécurisé

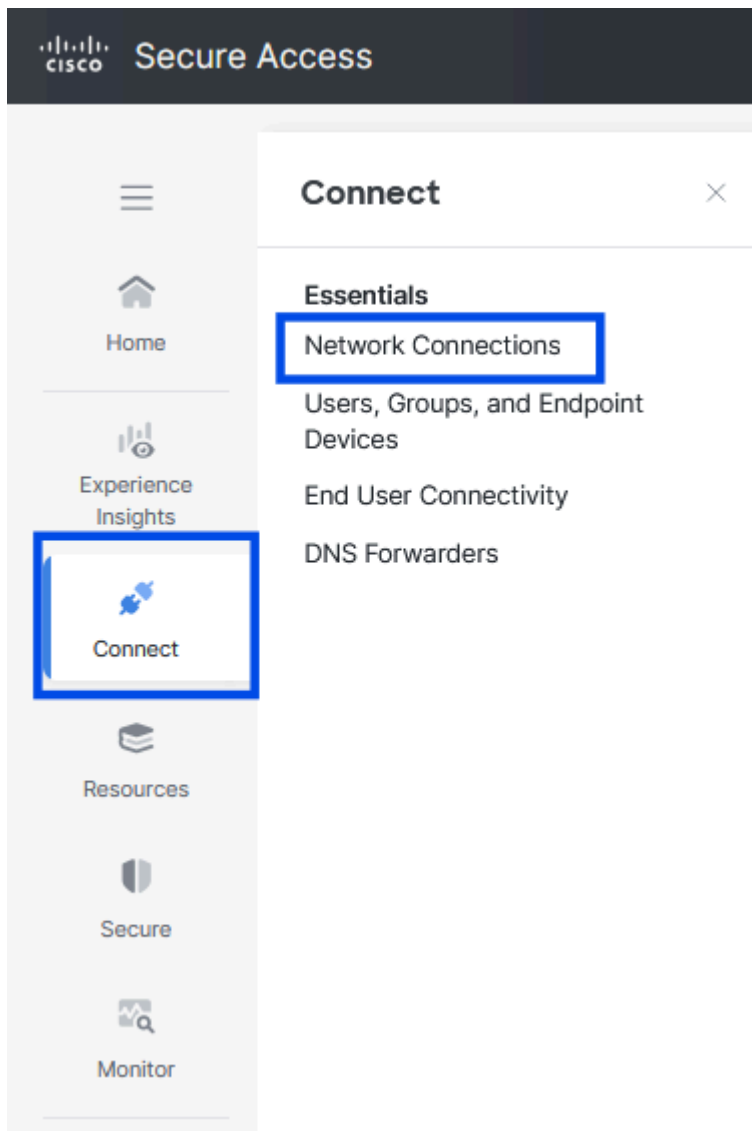
Afin de configurer un tunnel VPN entre Secure Access et Sonicwall

- Accédez au [portail d'administration](#) de Secure Access



Accès sécurisé - Page principale

- Cliquez sur Connect > Network Connections



Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups, cliquez sur + Add

The image shows the 'Network Connections' page in the Cisco Secure Access interface. The left navigation menu is visible with 'Connect' selected. The main content area has a header 'Network Connections' with a description and a 'Help' link. Below this are tabs for 'Connector Groups', 'Network Tunnel Groups' (selected), and 'FTDs'. A summary box for 'Network Tunnel Groups' shows 2 total groups: 0 Disconnected, 0 Warning, and 2 Connected. Below this is a section titled 'Network Tunnel Groups' with a description and a 'Help' link. It includes a search bar, filters for 'Region' and 'Status', and a '+ Add' button (highlighted with a blue box). A table lists the tunnel groups:

Network Tunnel Group	Status	Region	Primary Hub Data Center	Primary Tunnels	Secondary Hub Data Center	Secondary Tunnels
AZURE	Connected	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1 ...
LAB-BGP	Connected	US (Pacific Northwest)	sse-usw-2-1-1	1	sse-usw-2-1-0	1 ...

At the bottom right, there is a 'Rows per page' dropdown set to 10 and a page number '1'.

- Configurer le nom du groupe de tunnels , la région et le type de périphérique
- Cliquez sur Next (suivant).

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.

Tunnel Group Name

Region

US (Pacific Northwest) ▾

Device Type

Other ▾

[Cancel](#) [Next](#)



Remarque : Sélectionnez la région la plus proche de l'emplacement de votre pare-feu.

- Configuration du format ID de tunnel et de la phrase de passe
- Cliquez sur Next (suivant).

← Network Tunnel Groups

Add a Network Tunnel Group

Add a network tunnel group to Secure Access and enable secure network connections to the internet and private resources. Select one of your organization's available network devices to establish this network tunnel group connection. [Help](#)

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and passphrase that devices will use to connect to this tunnel group.

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

@<org><hub>.sse.cisco.com

Passphrase

[Show](#)

The passphrase must be between 16 and 64 characters long. It must include at least one upper case letter, one lower case letter, one number, and cannot include any special characters.

Confirm Passphrase

[Show](#)

[Cancel](#) [Back](#) [Next](#)

- Configurez les plages d'adresses IP, les hôtes ou les sous-réseaux que vous avez configurés sur votre réseau et souhaitez faire passer le trafic par un accès sécurisé
- Cliquez sur Add
- Cliquez sur Save (enregistrer)

Routing options and network overlaps
Configure routing options for this tunnel group.

Network subnet overlap

☐ 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.

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.

128.66.0.0/16, 192.0.2.0/24 Add

10.10.10.0/24 ×

☐ Dynamic routing
Use this option when you have a BGP peer for your on-premise router.

Advanced Settings ▼

Cancel Back Save

Après avoir cliqué sur Enregistrer , les informations sur le tunnel s'affichent. Enregistrez ces informations pour l'étape de configuration suivante

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.

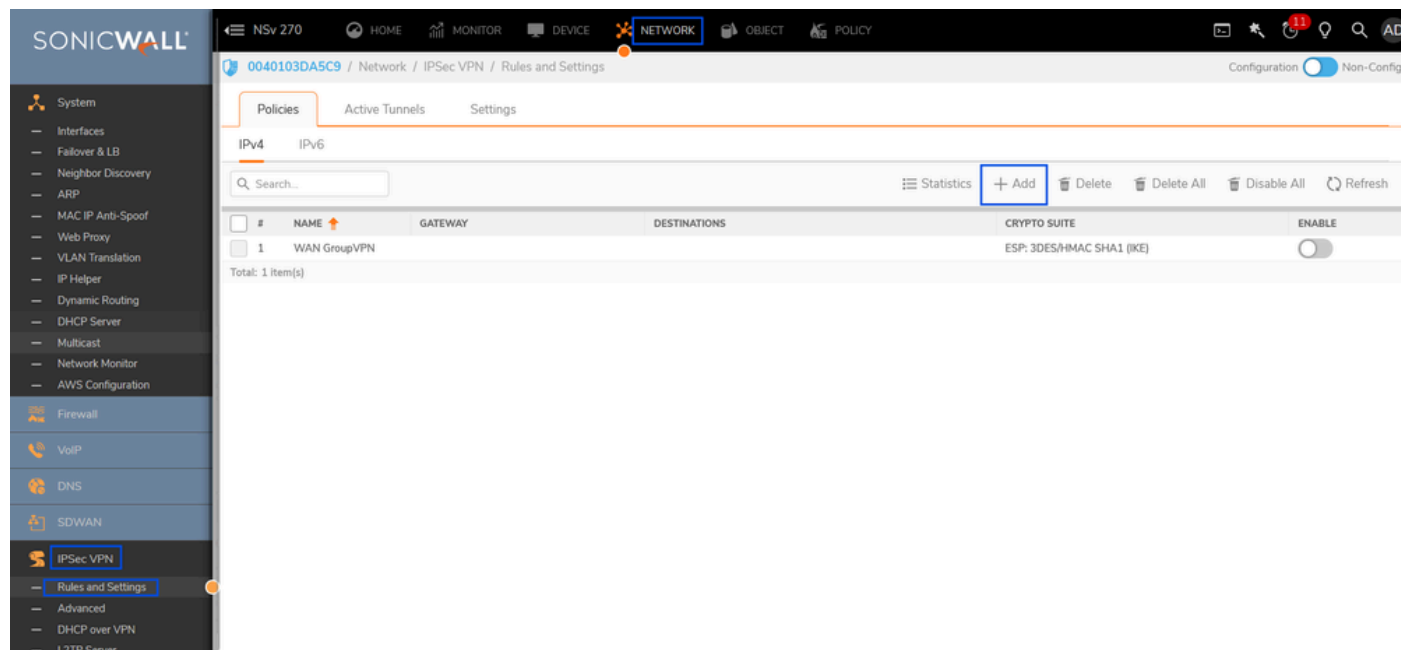
Primary Tunnel ID:	SonicWall-VPN@i	sse.cisco.com
Primary Data Center IP Address:	44.228.138.150	
Secondary Tunnel ID:	SonicWall-VPN@i	sse.cisco.com
Secondary Data Center IP Address:	52.35.201.56	
Passphrase:	sse.cisco.com	

Configuration du tunnel sur Sonicwall

Configuration du tunnel - Règles et paramètres

Accédez au tableau de bord Sonicwall.

- Réseau > VPN IPsec > Règles et paramètres
- Cliquez sur + Ajouter



Sonicwall - VPN IPsec - Règles et paramètres

- Sous VPN Policy , complétez la configuration VPN basée sur les données de tunnel de Secure Access et les [paramètres ipsec pris en charge](#)

VPN Policy

General

Proposals

Advanced

SECURITY POLICY

Policy Type

Tunnel Interface

Authentication Method

IKE Using Preshared Secret

Name

SonicWall-CSA

IPsec Primary Gateway Name or Address

44.228.138.150

IKE AUTHENTICATION

Shared Secret

Mask Shared Secret

Confirm Shared Secret

Local IKE ID

E-mail Address

SonicWall-VPN@E

7-ss

Peer IKE ID

IPv4 Address

44.228.138.150

Cancel

Save

VPN Policy

General **Proposals** Advanced

IKE (PHASE 1) PROPOSAL

Exchange	<div>IKEv2 Mode</div>
DH Group	<div>Group 14</div>
Encryption	<div>AES-256</div>
Authentication	<div>SHA256</div>
Life Time (seconds)	<div>28800</div>

IPSEC (PHASE 2) PROPOSAL

Protocol	<div>ESP</div>
Encryption	<div>AESGCM16-256</div>
Authentication	<div>None</div>
Enable Perfect Forward Secrecy	<div><input checked="" type="checkbox"/></div>
DH Group	<div>Group 14</div>
Life Time (seconds)	<div>28800</div>

Cancel

Save

VPN Policy

General

Proposals

Advanced

ADVANCED SETTINGS

Enable Keep Alive

☒

ⓘ

Disable IPsec Anti-Replay

☐

ⓘ

Allow Advanced Routing

☐

Enable Windows Networking (NetBIOS) Broadcast

☐

Enable Multicast

☐

Display Suite B Compliant Algorithms Only

☐

Apply NAT Policies

☐

MANAGEMENT VIA THIS SA

HTTPS

☐

SSH

☐

SNMP

☐

USER LOGIN VIA THIS SA

HTTP

☐

HTTPS

☐

VPN Policy bound to

Interface X1

IKEV2 SETTINGS

Do not send trigger packet during IKE SA negotiation

☐

ⓘ

Accept Hash & URL Certificate Type

☐

Accept Hash & URL Certificate Type Send Hash & URL Certificate Type

☐

Cancel

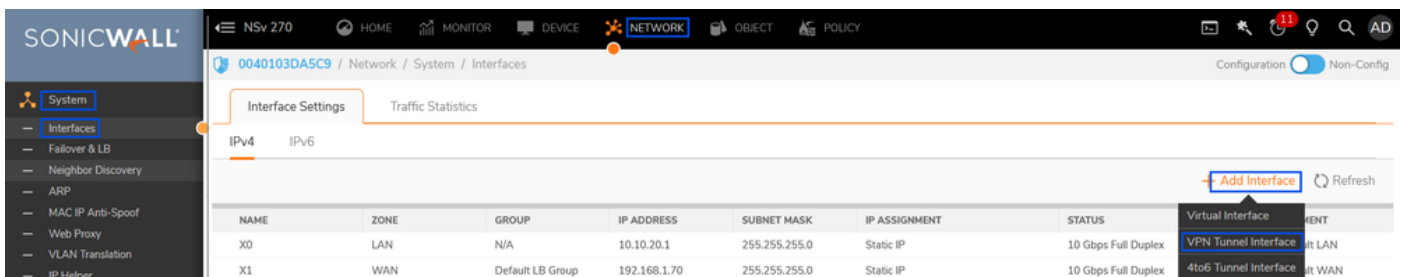
Save

- Cliquez sur Enregistrer

Ajouter une interface de tunnel VPN

Accédez au tableau de bord Sonicwall.

- Réseau > Système > Interface
- Cliquez sur + Ajouter une interface
- Sélectionner une interface de tunnel VPN



Add VPN Tunnel Interface

General

Advanced

INTERFACE SETTINGS

Zone

VPN

VPN Policy

SonicWall-CSA

Name

CSA_Tunnel1

Mode / IP Assignment

Static IP Mode

IP Address

169.254.0.6

Subnet Mask

255.255.255.252

Interface MTU

Configured automatically via VPN policy

Comment

Tunnel 1 interface - With CSA Primary DC

Domain Name



MANAGEMENT

USER LOGIN

HTTPS



Pina



HTTP



HTTPS



Cancel

OK

- Click OK

The screenshot shows the SonicWall management console interface. The left sidebar contains a menu with categories like System, Firewall, and DNS. The main content area displays the 'Interfaces' configuration page for device 0040103DA5C9. The 'Interface Settings' tab is active, showing a table of interfaces. The 'CSA_Tunnel1' interface has been added and is highlighted with a blue box. The table columns include NAME, ZONE, GROUP, IP ADDRESS, SUBNET MASK, IP ASSIGNMENT, STATUS, ENABLED, and COMMENT.

NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS	ENABLED	COMMENT
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex		Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex		Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X3	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X4	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X5	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X6	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
X7	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex		N/A
CSA_Tunnel1	VPN	N/A	169.254.0.6	255.255.255.252	Static IP	Interface Up		Tunnel 1 interface - With CSA Primary DC

Sonicwall - Interfaces - Interface de tunnel VPN

Ajouter un objet et des groupes réseau

Accédez au tableau de bord Sonicwall.

- Objet > Correspondance d'objets >Adresses
- Objets d'adressage
- Cliquez sur +Ajouter

0040103DA5C9 / Object / Match Objects / Addresses

Configuration ☒ Non-Config

Address Objects Address Groups

Search... View: All IPv4 & IPv6 + Add Delete Resolve Purge Refresh Column Selection

#	OBJECT NAME	DETAILS	TYPE	IP VERSION	ZONE	REFERENCES	CLASS
1	CSA_Tunnel1 IP	169.254.0.6/255.255.255.255	host	ipv4	VPN		Default
2	CSA_Tunnel1 Subnet	169.254.0.4/255.255.255.252	network	ipv4	VPN		Default
3	Default Active WAN IP	192.168.1.70/255.255.255.255	host	ipv4	WAN		Default

Sonicwall - Objets d'objet-adresse

Address Object Settings

Name ⓘ

Zone Assignment ▼


Type ▼

Network

Netmask / Prefix Length


- Cliquez sur Save (enregistrer)

Address Object Settings

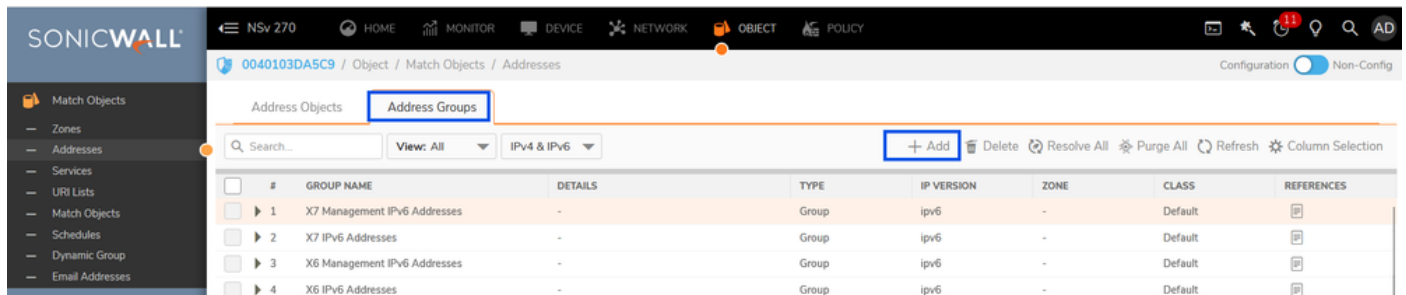
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	
Type	<input type="text" value="Network"/>	
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

- Cliquez sur Save (enregistrer)

Address Object Settings

Name	<input type="text" value="RAVPNUser-Pool"/>	
Zone Assignment	<input type="text" value="VPN"/>	
Type	<input type="text" value="Network"/>	
Network	<input type="text" value="10.10.50.0"/>	
Netmask / Prefix Length	<input type="text" value="255.255.255.0"/>	
<input type="button" value="Cancel"/>		<input type="button" value="Save"/>

- Cliquez sur Save (enregistrer)
- Créer des groupes d'adresses
- Cliquez sur +Ajouter
- Sélectionnez l'objet d'adresse et ajoutez-les aux groupes d'adresses



Sonicwall - Objet - Groupes d'adresses

Add Address Groups

Name CSA-Subnets

SHOW AVAILABLE

☒ All (136) ☒ Hosts (37) ☒ Ranges (0) ☒ Networks (32) ☒ MAC (0) ☒ FQDN (0) ☒ Groups (67)

Not in Group 134 items

Q RAV

No Data

In Group 2 items

Q

CgNAT[NW]

RAVPNUser-Pool[NW]

Cancel

Save

- Cliquez sur Save (enregistrer)

Ajouter une route

Accédez au tableau de bord Sonicwall.

- Stratégie > Règles et stratégies > Règles de routage
- Cliquez sur + Ajouter

SONICWALL

Rules and Policies

Access Rules

NAT Rules

Routing Rules

Content Filter Rules

App Rules

Endpoint Rules

DPI-SSL

DPI-SSH

Security Services

Capture ATP

Endpoint Security

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Default & Custom

IPv4

Active & Inactive

Used & Unused

GENERAL			LOOKUP				NEXT HOP					
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH
<input type="checkbox"/>	2	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard	
<input type="checkbox"/>	3	0	Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standard	
<input type="checkbox"/>	4	0	Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standard	
<input type="checkbox"/>	7	0	Route Policy_4	Any	X0 Subnet	Any	Any	X0	0.0.0.0	20	Standard	
<input type="checkbox"/>	8	24.9k	Route Policy_6	Any	X1 Subnet	Any	Any	X1	0.0.0.0	20	Standard	
<input type="checkbox"/>	9	3.4k	Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standard	
<input type="checkbox"/>	10	2.1k	Route Policy_9	Any	0.0.0.0/0	Any	Any	X1	192.168.1.1	20	Standard	

+ Add

Delete

Delete All

Edit

Live Counters

Reset Counters

Sonicwall - Règles de routage

- Ajouter une règle de routage

Adding Rule

Name

LAN-CSA

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your route...

Type

☒ IPv4 ☐ IPv6

Lookup

Next Hop

Advanced

Probe

Source

LAN

Destination

CSA-Subnets

☒ Service ☐ App

Service

Any

Show Diagram

☐

Cancel

Add

Adding Rule

Name

LAN-CSA

Tags

add upto 3 tags, use comma as separator...

Description

provide a short description of your route...

Type

☒ IPv4 ☐ IPv6

Lookup

Next Hop

Advanced

Probe

☒ Standard Route

☐ Multi-Path Route

☐ SD-WAN Rule

Interface

CSA_Tunnel1

Gateway

0.0.0.0/::

Metric

5

Show Diagram

☐

Cancel

Add

- Cliquez sur + Ajouter

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Configuration Non-Config

Rules and Policies

Access Rules

NAT Rules

Routing Rules

Content Filter Rules

App Rules

Default & Custom

IPv4

Active & Inactive

Used & Unused

Settings

GENERAL				LOOKUP				NEXT HOP				PROBE	OPERATION	
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M	TYPE	PATH PROFILE	PROBE	CLASS
<input type="checkbox"/>	1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard			Custom
<input type="checkbox"/>	3	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standard			Default

Sonicwall - Règles de routage

Ajouter des règles d'accès

Accédez au tableau de bord Sonicwall.

- Stratégie > Règles et stratégies > Règles d'accès
- Cliquez sur + Ajouter

SONICWALL												
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY												
0040103DA5C9 / Policy / Rules and Policies / Access Rules Configuration Non-Config												
Rules and Policies												
Access Rules												
NAT Rules												
Routing Rules												
Content Filter Rules												
App Rules												
Endpoint Rules												
DPI-SSL												
DPI-SSH												
Security Services												
Capture ATP												
Endpoint Security												
GENERAL												
ZONE												
ADDRESS												
SERVICE												
USER												
SCHEDULE												
PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE	
1 (M)	0	Default Access Rule_2	Allow	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always	
2 (M)	0	Default Access Rule_3	Allow	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always	
3 (M)	0	Default Access Rule_4	Allow	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always	
4 (M)	0	Default Access Rule_5	Allow	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always	
5 (M)	0	Default Access Rule_6	Allow	LAN	LAN	Any	Any	Any	All	None	Always	
6 (M)	0	Default Access Rule_9	Allow	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always	
7 (M)	0	Default Access Rule_124	Allow	LAN	VPN	obj_10.10.20.0.24	CSA-Subnets	Any	All	None	Always	
8 (M)	0	Default Access Rule_12	Allow	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always	
9 (M)	0	Default Access Rule_13	Allow	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always	
10 (M)	11.4k	Default Access Rule_14	Allow	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always	
11 (M)	0	Default Access Rule_15	Allow	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always	
12 (M)	2	Default Access Rule_123	Allow	WAN	WAN	X1 IP	Any	Any	All	None	Always	
13 (A)	0	Default Access Rule_122	Allow	WAN	WAN	Any	X1 IP	Any	All	None	Always	
14 (M)	0	Default Access Rule_22	Allow	DMZ	DMZ	Any	Any	Any	All	None	Always	
15 (M)	0	Default Access Rule_23	Allow	DMZ	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always	

Sonicwall - Règles d'accès

Adding Rule

Name

CSA-Inbound-Allow

Description

Access rule to allow CSA subnets (RAVPN and CgNAT) to access the internal network/s

Action

☒ Allow
 ☐ Deny
 ☐ Discard

Type

☒ IPv4
 ☐ IPv6

Priority

Manual 1

Schedule

Always

Enable

☒

Source / Destination

User & TCP/UDP

Security Profiles

Traffic Shaping

Logging

Optional Settings

SOURCE

Zone/Interface

VPN

Address

CSA-Subnets

Port/Services

Any

DESTINATION

Zone/Interface

LAN

Address

LAN

Port/Services

Any

Show Diagram

☐

Cancel

Add

- Cliquez sur +Ajouter

SONICWALL												
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY												
0040103DA5C9 / Policy / Rules and Policies / Access Rules Configuration Non-Config												
Rules and Policies												
Access Rules												
NAT Rules												
Routing Rules												
Content Filter Rules												
App Rules												
Endpoint Rules												
DPI-SSL												
DPI-SSH												
Security Services												
Capture ATP												
Endpoint Security												
GENERAL												
ZONE												
ADDRESS												
SERVICE												
USER												
SCHEDULE												
PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE	
1 (M)	0	CSA-Inbound-Allow_127	Allow	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always	

Sonicwall - Règles d'accès

Vérifier

- État du tunnel sur accès sécurisé

← Network Tunnel Groups

SonicWall-NTG

Review and edit this network tunnel group. Details for each IPsec tunnel added to this group are listed including which tunnel hub it is a member of. [Help](#)

Summary

Warning

Primary and secondary hubs mismatch in number of tunnels.

Region

US (Pacific Northwest)

Routing Type

Static Routing

Device Type

Other

IP Address Range

10.10.10.0/24

Last Status Update

Jul 06, 2025 4:13 PM

Primary Hub

Hub Up

1

Active Tunnels

Tunnel Group ID

SonicWall-VPN@

Data Center

sse-usw-2-1-1

IP Address

44.228.138.150

Secondary Hub

Hub Down

0

Active Tunnels

Tunnel Group ID

SonicWall-VPN@

Data Center

sse-usw-2-1-0

IP Address

52.35.201.56

Network Tunnels

Review this network tunnel group's IPsec tunnels. [Help](#)

Tunnels	Peer ID	Peer Device IP Address	Data Center Name	Data Center IP Address	Status	Last Status Update
Primary 1	131073	76.39.159.129	sse-usw-2-1-1	44.228.138.150	Connected	Jul 06, 2025 4:11 PM

Accès sécurisé - Groupe de tunnels réseau - État VPN

- État du tunnel sur le pare-feu Sonicwall

SONICWALL

NSv 270

HOME

MONITOR

DEVICE

NETWORK

OBJECT

POLICY

0040103DA5C9 / Network / IPsec VPN / Rules and Settings

Configuration Non-Config

Policies

Active Tunnels

Settings

IPv4

IPv6

Search

Refresh

#	CREATED	NAME	LOCAL	REMOTE	GATEWAY	COMMENT
1	07/06/2025 08:42:48	SonicWall-CSA	0.0.0.0 - 255.255.255.255	0.0.0.0 - 255.255.255.255	44.228.138.150	

Total: 1 item(s)

Sonicwall - État VPN IPsec

Vous pouvez effectuer le même processus pour configurer le tunnel entre le data center secondaire Secure Access et Sonicwall

Maintenant , le tunnel est UP sur Secure Access et Sonicwall, vous pouvez continuer à configurer l'accès aux ressources privées via RA-VPN , Browser Based ZTA ou Client Based ZTA sur Secure Access Dashboard

Dépannage

PC utilisateur

- Vérifiez que l'utilisateur peut se connecter/s'inscrire à RAVPN/ZTNA correctement ou non. Si ce n'est pas le cas, identifiez les raisons de la défaillance de la connexion du plan de contrôle.
- Vérifiez que le réseau auquel l'utilisateur tente d'accéder est supposé passer par le tunnel RAVPN ou ZTNA . Sinon, vérifiez la configuration sur la tête de réseau .

Accès sécurisé

- Vérifiez la configuration du pilotage du trafic sur le profil de connexion RAVPN pour confirmer que le réseau de destination est configuré pour envoyer le tunnel vers l'accès sécurisé.
- Vérifiez que la ressource privée est définie avec un protocole/des ports valides et que les mécanismes de connexion ZTNA/RAVPN sont vérifiés.
- Vérifiez que la stratégie d'accès est configurée pour autoriser l'utilisateur RAVPN/ZTNA à accéder au réseau de ressources privées et que son est placé dans un ordre où aucune autre règle n'est prioritaire pour bloquer le trafic.
- Vérifiez que le tunnel IPSec est activé et que l'accès sécurisé indique des routes client valides via le routage statique qui couvre la ressource privée à laquelle l'utilisateur tente d'accéder.

Paroi Sonique

- Vérifiez que le tunnel IPSec est activé ou non (IKE & IPSec SA).
- Vérifiez que la ou les routes client(s) sont correctement annoncées.
- Vérifiez que les sources de trafic de l'utilisateur RAVPN/ZTNA destinées à une ressource privée derrière Sonicwall atteignent le pare-feu Sonicwall via un tunnel en effectuant une capture de paquets sur Sonicwall.
- Vérifiez que le trafic a atteint la ressource privée et répondez au client RAVPN/ZTNA ou non. Si oui, vérifiez que ces paquets atteignent l'interface Sonical X0 (LAN).
- Vérifiez que Sonicwall transfère le trafic de retour via le tunnel IPSec vers Secure Access.

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Centre d'aide Cisco Secure Access](#)
- [Module d'accès Zero Trust](#)
- [Dépannez L'Erreur D'Accès Sécurisé « Le Service D'Inscription Ne Répond Pas. Contactez votre service d'assistance informatique"](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.