

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

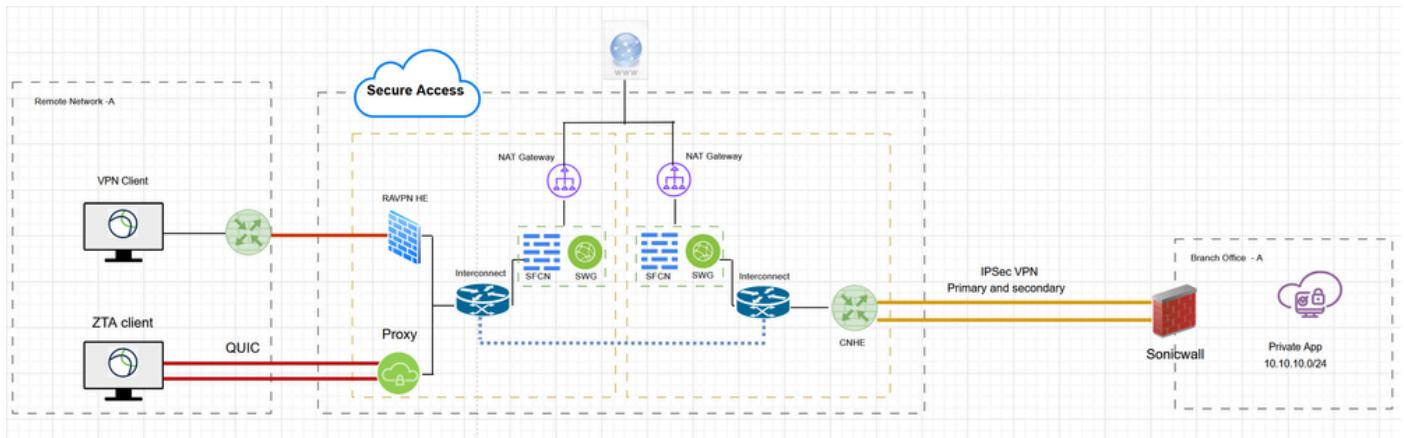


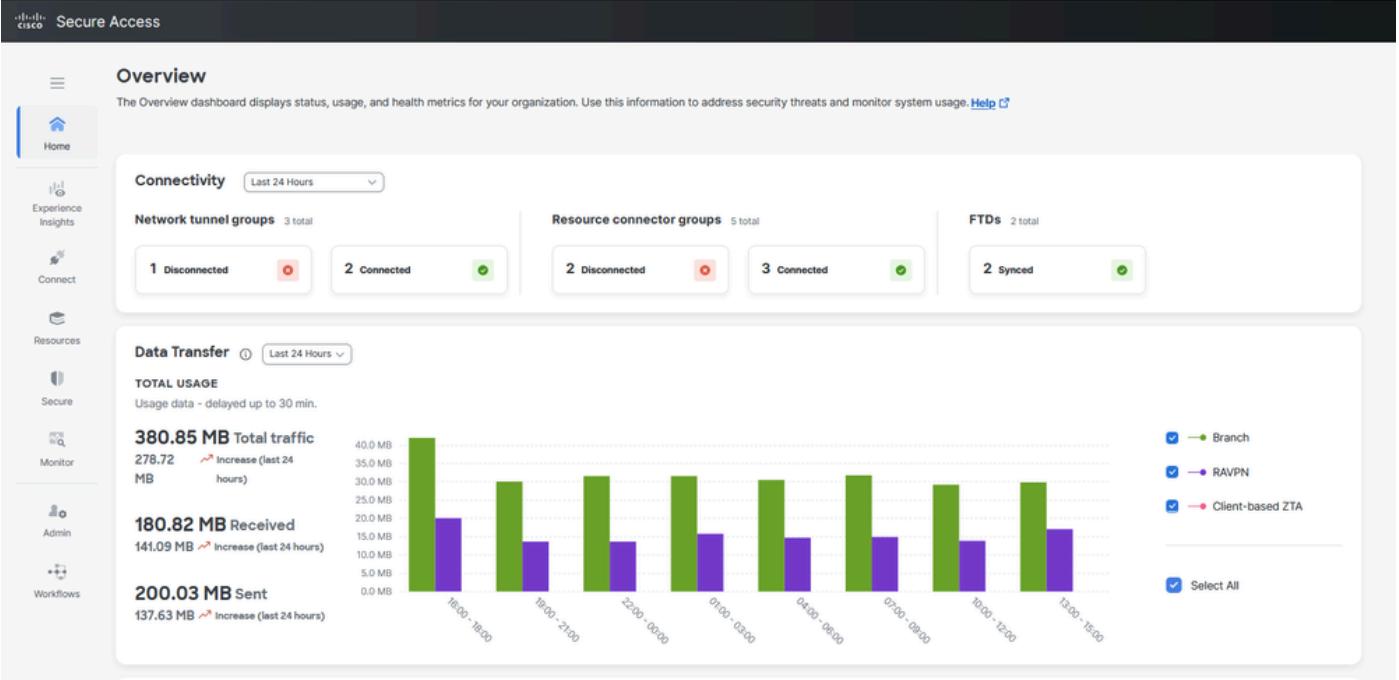
Diagramme du réseau

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

The screenshot shows the Cisco Secure Access web interface. The top navigation bar includes the Cisco logo and the title "Secure Access". On the left, there's a vertical sidebar with icons for Home, Experience Insights, Connect (which is selected and highlighted with a blue border), Resources, Secure, and Monitor. The main content area is titled "Connect" and has a sub-section titled "Essentials". Under "Essentials", there are four items: "Network Connections" (highlighted with a blue box), "Users, Groups, and Endpoint Devices", "End User Connectivity", and "DNS Forwarders".

Accès sécurisé - Connexions réseau

- Sous Network Tunnel Groups, cliquez sur + Add

The screenshot shows the "Network Tunnel Groups" page within the Cisco Secure Access interface. The left sidebar includes icons for Home, Experience Insights, Connect (selected and highlighted with a blue border), Resources, Secure, Monitor, Admin, and Workflows. The main content area displays a summary of network tunnel groups: 0 Disconnected, 0 Warning, and 2 Connected. Below this, a detailed table lists the "Network 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 of the table, there is a blue "+ Add" button. Navigation controls at the bottom right include "Rows per page" (set to 10), a previous/next page indicator, and a search bar.

Accès sécurisé - Groupes de tunnels réseau

- 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: SonicWall-NTG

Region: US (Pacific Northwest)

Device Type: Other

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

Accès sécurisé - Groupe de tunnels réseau - Paramètres généraux



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: SonicWall-VPN @<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](#) [Next](#)

Accès sécurisé - ID de tunnel et phrase de passe

- 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)

General Settings

Tunnel ID and Passphrase

Routing

4 Data for Tunnel Setup

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 **X**

Dynamic routing

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

Advanced Settings

Cancel **Back** **Save**

Accès sécurisé - Groupes de tunnels - Options de routage

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

← 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

Routing

Data for Tunnel Setup

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@1 **sse.cisco.com**

Primary Data Center IP Address: 44.228.138.150

Secondary Tunnel ID: SonicWall-VPN@1 **sse.cisco.com**

Secondary Data Center IP Address: 52.35.201.56

Passphrase: **(Redacted)**

Accès sécurisé - Données pour la configuration du tunnel

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

The screenshot shows the SonicWall NSv 270 interface. In the top navigation bar, the 'NETWORK' tab is selected. Below it, the path '0040103DA5C9 / Network / IPsec VPN / Rules and Settings' is visible. On the left, a sidebar menu includes 'System', 'Firewall', 'VoIP', 'DNS', 'SDWAN', and 'IPSec VPN' (which is currently selected). Under 'IPSec VPN', 'Rules and Settings' is also selected. The main pane displays a table of rules:

#	NAME	GATEWAY	DESTINATIONS	CRYPTO SUITE	ENABLE
1	WAN GroupVPN			ESP: 3DES/HMAC SHA1 (IKE)	<input type="checkbox"/>

Total: 1 item(s)

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

The screenshot shows the 'IKE AUTHENTICATION' section of the VPN Policy configuration. It includes fields for Shared Secret (a masked password), Mask Shared Secret (a green toggle switch), Confirm Shared Secret (another masked password), Local IKE ID (E-mail Address: SonicWall-VPN@E, 7-ss), and Peer IKE ID (IPv4 Address: 44.228.138.150). At the bottom are 'Cancel' and 'Save' buttons.

Shared Secret	*****
Mask Shared Secret	<input checked="" type="checkbox"/>
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	IKEv2 Mode
DH Group	Group 14
Encryption	AES-256
Authentication	SHA256
Life Time (seconds)	28800

IPSEC (PHASE 2) PROPOSAL

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

[Cancel](#) [Save](#)

VPN Policy

General Proposals Advanced

ADVANCED SETTINGS

Enable Keep Alive <input checked="" type="checkbox"/>	Display Suite B Compliant Algorithms Only <input type="checkbox"/>
Disable IPsec Anti-Replay <input type="checkbox"/>	Apply NAT Policies <input type="checkbox"/>
Allow Advanced Routing <input type="checkbox"/>	
Enable Windows Networking (NetBIOS) Broadcast <input type="checkbox"/>	
Enable Multicast <input type="checkbox"/>	

MANAGEMENT VIA THIS SA

HTTPS <input type="checkbox"/>	SNMP <input type="checkbox"/>
SSH <input type="checkbox"/>	

USER LOGIN VIA THIS SA

HTTP <input type="checkbox"/>	HTTPS <input type="checkbox"/>
VPN Policy bound to <input type="button" value="Interface X1"/>	

IKEV2 SETTINGS

Do not send trigger packet during IKE SA negotiation <input type="checkbox"/>	Accept Hash & URL Certificate Type <input type="checkbox"/>
Accept Hash & URL Certificate Type Send Hash & URL Certificate Type <input type="checkbox"/>	

- 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

The screenshot shows the SonicWall interface under the 'NETWORK' tab. In the left sidebar, 'Interfaces' is selected. On the main screen, there is a table of existing interfaces (X0, X1) and a 'Virtual Interface' section. A blue box highlights the '+ Add Interface' button in the 'Virtual Interface' section.

Sonicwall - Interfaces

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

HTTPS

Ping

USER LOGIN

HTTP

HTTPS

- Click OK

SONICWALL

NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY

0040103DASC9 / Network / System / Interfaces

Configuration 11

Interface Settings Traffic Statistics

IPv4 IPv6

+ Add Interface Refresh

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	<input checked="" type="checkbox"/>	Default LAN
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex	<input checked="" type="checkbox"/>	Default WAN
X2	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X3	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X4	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X5	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X6	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
X7	Unassigned	N/A	0.0.0.0	0.0.0.0		10 Gbps Full Duplex	<input checked="" type="checkbox"/>	N/A
CSA_Tunnel1	VPN	N/A	169.254.0.6	255.255.255.252	Static IP	Interface Up	<input checked="" type="checkbox"/>	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

#	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

i

Zone Assignment

LAN

Type

Network

Network

Netmask / Prefix Length

Cancel
Save

- Cliquez sur Save (enregistrer)

Address Object Settings

Name ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

- Cliquez sur Save (enregistrer)

Address Object Settings

Name ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

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

#	GROUP NAME	DETAILS	TYPE	IP VERSION	ZONE	CLASS	REFERENCES
1	X7 Management IPv6 Addresses	-	Group	ipv6	-	Default	
2	X7 IPv6 Addresses	-	Group	ipv6	-	Default	
3	X6 Management IPv6 Addresses	-	Group	ipv6	-	Default	
4	X6 IPv6 Addresses	-	Group	ipv6	-	Default	

Sonicwall - Objet - Groupes d'adresses

Add Address Groups

Name

SHOW AVAILABLE

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

Not in Group 134 items

No Data

In Group 2 items

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

	GENERAL		LOOKUP				NEXT HOP					
	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH
			Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standar	d
			Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standar	d
			Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standar	d
			Route Policy_4	X0 Subnet	Any	Any	Any	X0	0.0.0.0	20	Standar	d
			Route Policy_6	X1 Subnet	Any	Any	Any	X1	0.0.0.0	20	Standar	d
			Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standar	d
			Route Policy_9	0.0.0.0/0	Any	Any	Any	X1	192.168.1.1	20	Standar	d

[+ Add](#)
Delete
Delete All
Edit
Live Counters
Reset Counters

Sonicwall - Règles de routage

- Ajouter une règle de routage

Adding Rule

Name	<input type="text" value="LAN-CSA"/>	Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Tags	add upto 3 tags, use comma as separator...		
Description	provide a short description of your route...		

Lookup
Next Hop
Advanced
Probe

Source	<input type="text" value="LAN"/>	▼	✎	 ⓘ
Destination	<input type="text" value="CSA-Subnets"/>			
<input checked="" type="radio"/> Service <input type="radio"/> App				
Service	<input type="text" value="Any"/>	▼	✎	 ⓘ

Show Diagram
[Cancel](#)
[Add](#)

Adding Rule

Name: LAN-CSA Type: IPv4 IPv6

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

Description: provide a short description of your route...

Lookup Next Hop Advanced Probe

Standard Route
 Multi-Path Route
 SD-WAN Rule

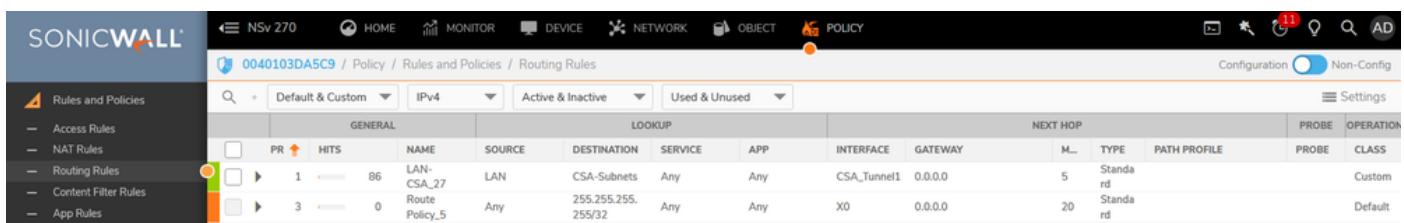
Interface: CSA_Tunnel1

Gateway: 0.0.0.0/0

Metric: 5

Show Diagram Cancel Add

- Cliquez sur + Ajouter



The screenshot shows the SonicWall NSv 270 interface with the following details:

- Header:** NSv 270, HOME, MONITOR, DEVICE, NETWORK, OBJECT, POLICY.
- Breadcrumbs:** 0040103DA5C9 / Policy / Rules and Policies / Routing Rules.
- Filter:** Default & Custom, IPv4, Active & Inactive, Used & Unused.
- Table Headers:** GENERAL, LOOKUP, NEXT HOP, PROBE, OPERATION.
- Table Data:**

	PR ↑	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	M...	TYPE	PATH PROFILE	PROBE	OPERATION
<input type="checkbox"/>	1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standar...		Custom	
<input type="checkbox"/>	3	0	Route Policy_5	Any	255.255.255.255/32	Any	Any	X0	0.0.0.0	20	Standar...		Default	
- Buttons:** Configuration (Non-Config), Settings.

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 - Règles d'accès

Access Rules												
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
			Default Access Rule_2	Allow	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
			Default Access Rule_3	Allow	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
			Default Access Rule_4	Allow	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
			Default Access Rule_5	Allow	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
			Default Access Rule_6	Allow	LAN	LAN	Any	Any	Any	All	None	Always
			Default Access Rule_9	Allow	LAN	VPN	RemoteAccess Networks	Any	Any	All	None	Always
			Default Access Rule_124	Allow	LAN	VPN	obj_10.10.20.0_24	CSA-Subnets	Any	All	None	Always
			Default Access Rule_12	Allow	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
			Default Access Rule_13	Allow	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
			Default Access Rule_14	Allow	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
			Default Access Rule_15	Allow	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
			Default Access Rule_13	Allow	WAN	WAN	Any	IKE	All	All	None	Always
			Default Access Rule_123	Allow	WAN	WAN	X1 IP	IKE	All	All	None	Always
			Default Access Rule_122	Allow	WAN	WAN	Any	X1 IP	IKE	All	None	Always
			Default Access Rule_22	Allow	DMZ	DMZ	Any	Any	Any	All	None	Always
			Default Access Rule_23	Allow	DMZ	VPN	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

Type: IPv4

Priority: Manual 1

Schedule: Always

Enable: On

Source / Destination

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

Access Rules												
	PI	HITS	NAME	ACTION	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION P...	USER INCL.	USER EXCL.	SCHEDULE
			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

The screenshot shows the 'Network Tunnel Groups' page for 'SonicWall-NTG'. It includes sections for 'Summary', 'Primary Hub' (with 1 active tunnel, status 'Hub Up'), and 'Secondary Hub' (0 active tunnels, status 'Hub Down'). The 'Network Tunnels' section lists one tunnel: Primary 1 (Peer ID 131073, Peer Device IP Address 76.39.159.129, Data Center sse-usw-2-1-1, Data Center IP Address 44.228.138.150, Status Connected). A blue box highlights the 'Connected' status.

Accès sécurisé - Groupe de tunnels réseau - État VPN

- État du tunnel sur le pare-feu Sonicwall

The screenshot shows the 'IPSec VPN / Rules and Settings' page on the Sonicwall NSv 270. The 'Active Tunnels' tab is selected. It displays one tunnel entry: SonicWall-CSA (Created 07/06/2025 08:42:48, Local 0.0.0.0 - 255.255.255.255, Remote 0.0.0.0 - 255.255.255.255, Gateway 44.228.138.150). A blue box highlights the 'Active Tunnels' tab.

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.