

Beveiligde toegang configureren met Sonicwall Firewall

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[Network Tunnel Group \(VPN\) configureren voor beveiligde toegang](#)

[Configureer de tunnel op Sonicwall](#)

[De tunnel configureren - Regels en instellingen](#)

[VPN-tunnelinterface toevoegen](#)

[Netwerkobject en groepen toevoegen](#)

[Route toevoegen](#)

[Toegangsregels toevoegen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gebruiker-pc](#)

[beveiligde toegang](#)

[Sonicwall](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u een IPsec VTI-tunnel configureert tussen Secure Access to Sonicwall firewall met statische routing.

Voorwaarden

- [Provisioning van gebruiker configureren](#)
- [ZTNA SSO-verificatieconfiguratie](#)
- [Remote Access VPN Secure Access configureren](#)

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SonicWall-firewall (NSv270 - SonicOSX 7.0.1)

- beveiligde toegang
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless ZTNA

Gebruikte componenten

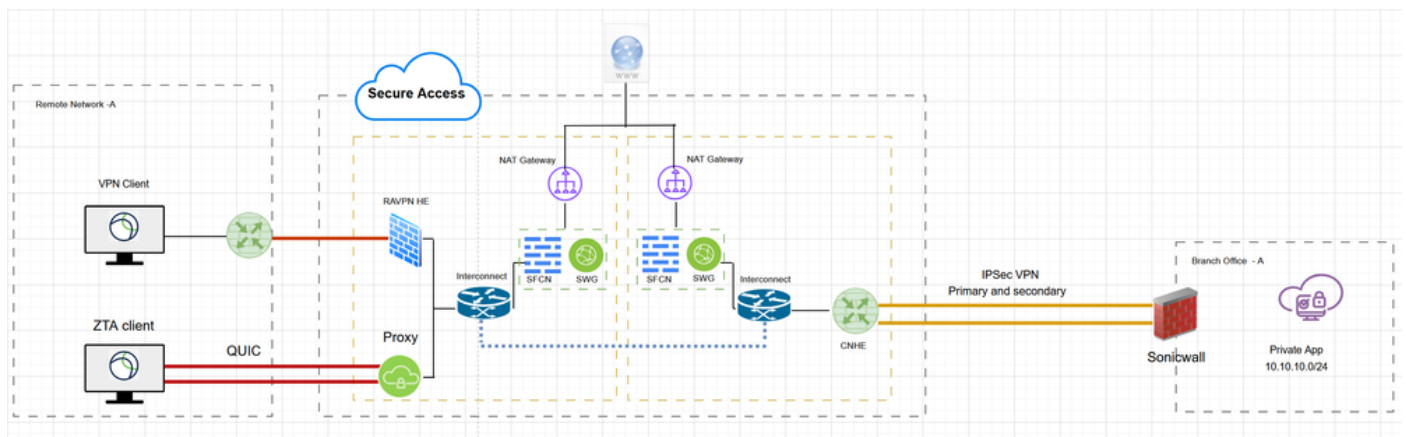
De informatie in dit document is gebaseerd op:

- SonicWall-firewall (NSv270 - SonicOSX 7.0.1)
- beveiligde toegang
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Netwerkdigram



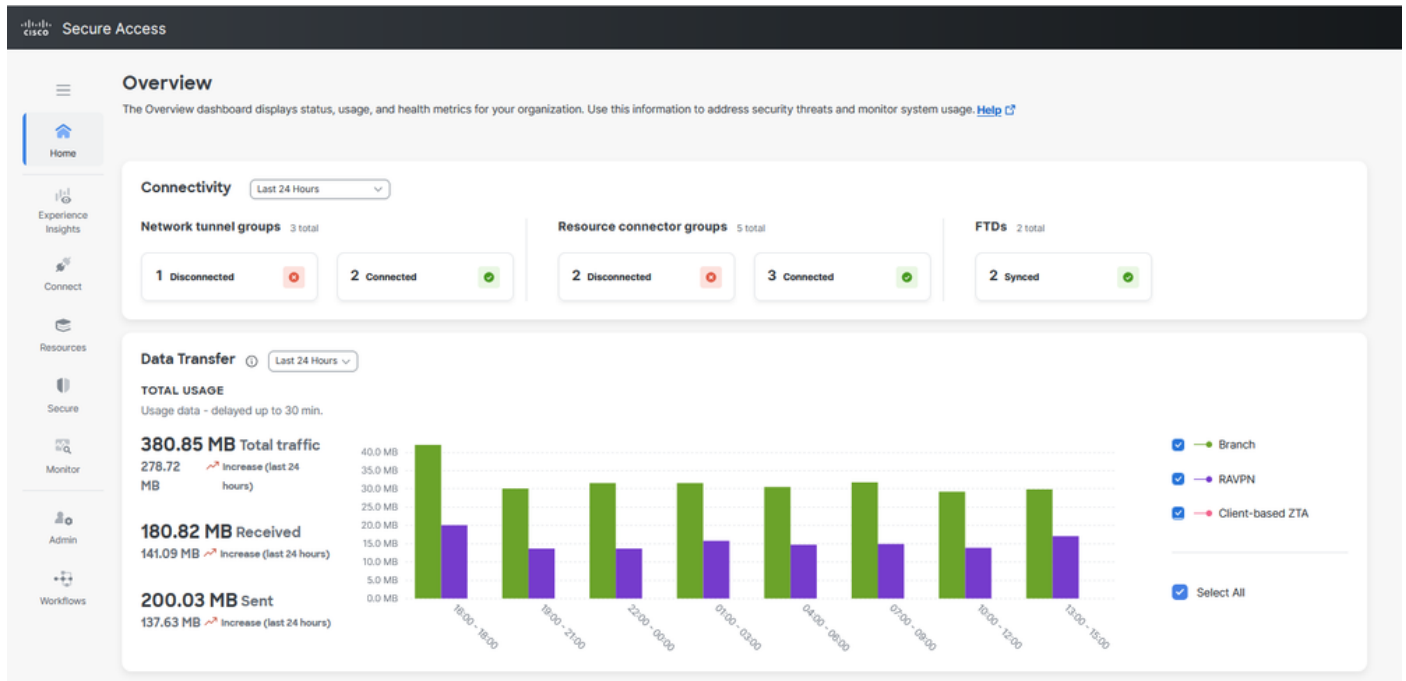
Netwerkdigram

Configureren

Network Tunnel Group (VPN) configureren voor beveiligde toegang

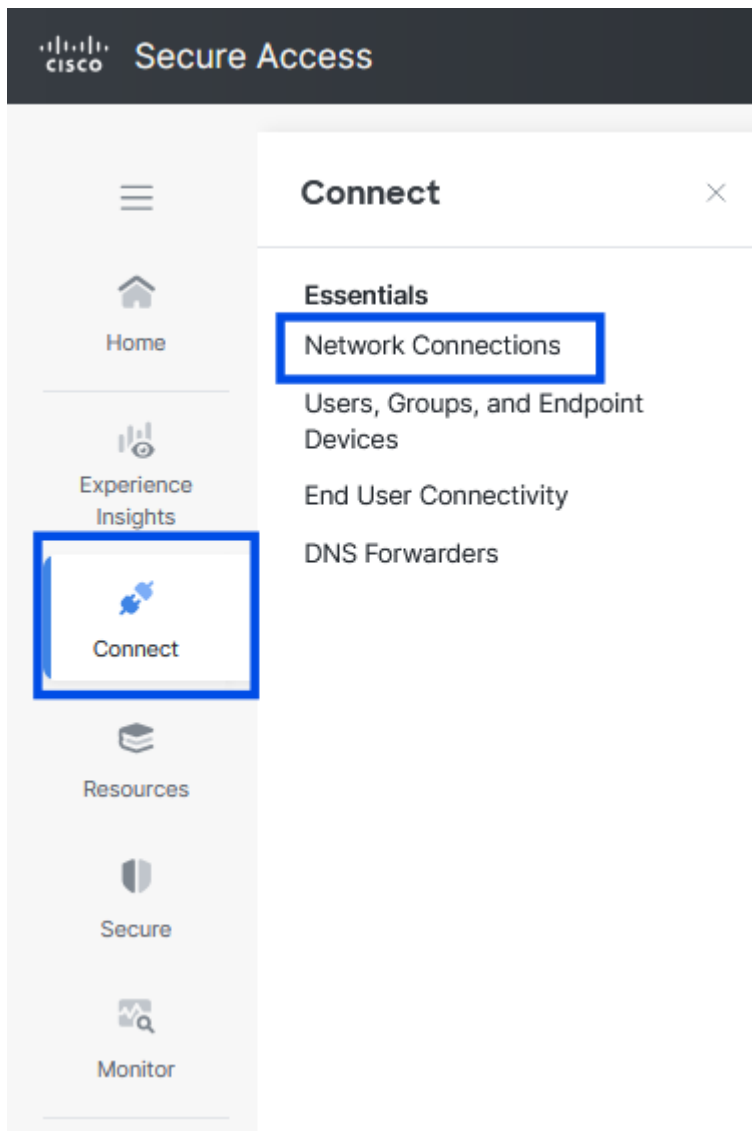
Om VPN-tunnel tussen Secure Access en Sonicwall te configureren

- Navigeer naar het [beheerdersportaal](#) van de beveiligde toegang



Veilig toegang - Hoofdpagina

- Klik op Verbinden > Netwerkverbindingen



Veilige toegang - netwerkverbindingen

- Klik onder Netwerktunnelgroepen op + Toevoegen

The screenshot displays 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' and a sub-header 'Network Tunnel Groups' (highlighted with a blue box). Below this, there are three status boxes: '0 Disconnected', '0 Warning', and '2 Connected'. A table titled 'Network Tunnel Groups' lists two groups: 'AZURE' and 'LAB-BGP'. Both are in a 'Connected' status, located in the 'US (Pacific Northwest)' region. The table columns are: Network Tunnel Group, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. An '+ Add' button (highlighted with a blue box) is located in the top right corner of the table area. At the bottom right, there is a 'Rows per page' dropdown set to '10' and a page number '1'.

- Configureer de IP-adresbereiken, hosts of subnetten die u in uw netwerk hebt geconfigureerd en die het verkeer via Secure Access willen doorgeven
- Klik op Toevoegen
- Klik op Opslaan

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**

Nadat u op Opslaan hebt geklikt, wordt de informatie over de tunnel weergegeven. Bewaar deze informatie voor de volgende configuratiestap

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.

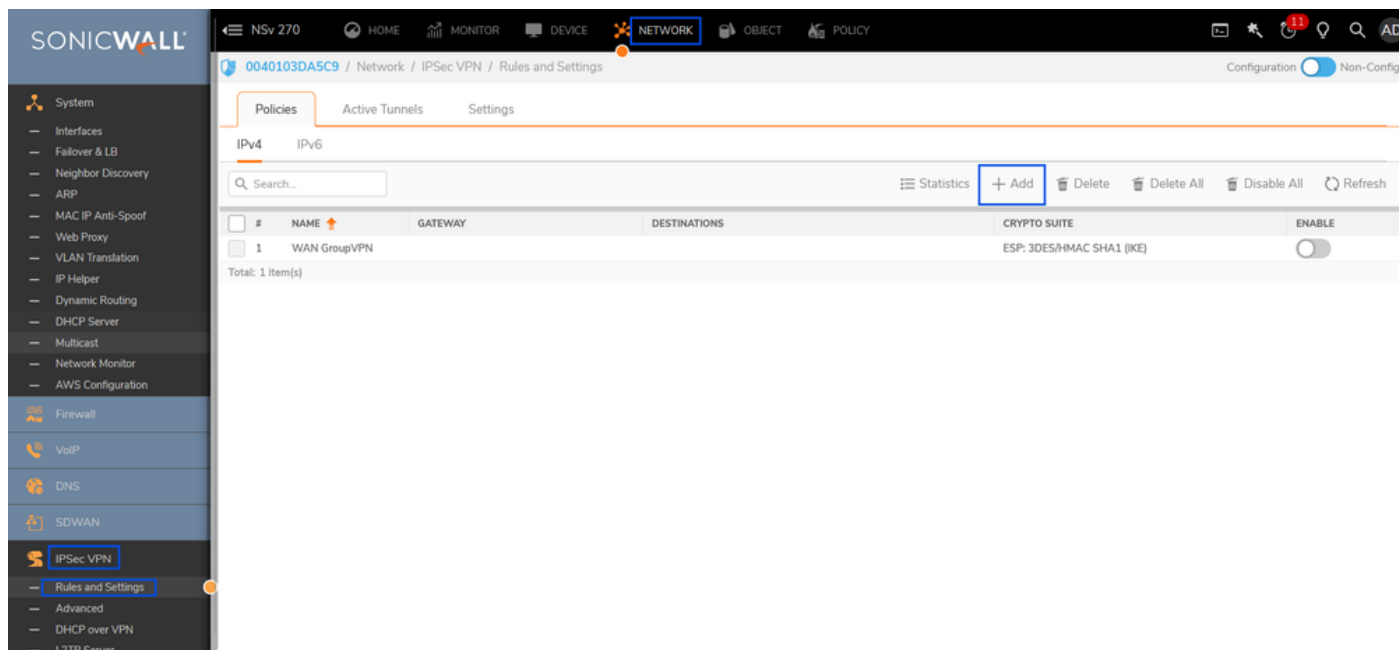
Primary Tunnel ID:	SonicWall-VPN@i	sse.cisco.com
Primary Data Center IP Address:	44.228.138.150	
Secondary Tunnel ID:	SonicWall-VPN@i	sse.cisco.com
Secondary Data Center IP Address:	52.35.201.56	
Passphrase:		

Configureer de tunnel op Sonicwall

De tunnel configureren - Regels en instellingen

Navigeer naar het Sonicwall Dashboard.

- Netwerk > IPsec VPN > Regels en instellingen
- Klik op + Toevoegen



Sonicwall - IPsec VPN - Regels en instellingen

- Onder VPN-beleid vult u de VPN-configuratie in op basis van de tunnelgegevens van Secure Access en [ondersteunde ipsec-parameters](#)

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	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	☒
DH Group	Group 14
Life Time (seconds)	28800

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

- Klik op Opslaan

VPN-tunnelinterface toevoegen

Navigeer naar het Sonicwall Dashboard.

- Netwerk > Systeem > Interface
- Klik op + Add Interface
- Selecteer VPN-tunnelinterface

The screenshot shows the SonicWall dashboard with the 'Network' tab selected. The breadcrumb trail is '0040103DA5C9 / Network / System / Interfaces'. The 'Interface Settings' tab is active. A table lists interfaces X0 and X1. The 'Add Interface' button is highlighted, and a dropdown menu is open, showing 'Virtual Interface', 'VPN Tunnel Interface', and '4to6 Tunnel Interface'. The 'VPN Tunnel Interface' is selected.

NAME	ZONE	GROUP	IP ADDRESS	SUBNET MASK	IP ASSIGNMENT	STATUS
X0	LAN	N/A	10.10.20.1	255.255.255.0	Static IP	10 Gbps Full Duplex
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex

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

- Klik op OK

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 - VPN Tunnel Interface

Netwerkoject en groepen toevoegen

Navigeer naar het Sonicwall Dashboard.

- Object > Overeenkomende objecten >Adressen
- Adresobjecten
- Klik op +Add

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 - Object- Adresobjecten

Address Object Settings

Name ⓘ

Zone Assignment ▼

Type ▼

Network

Netmask / Prefix Length

- Klik op Opslaan

Address Object Settings

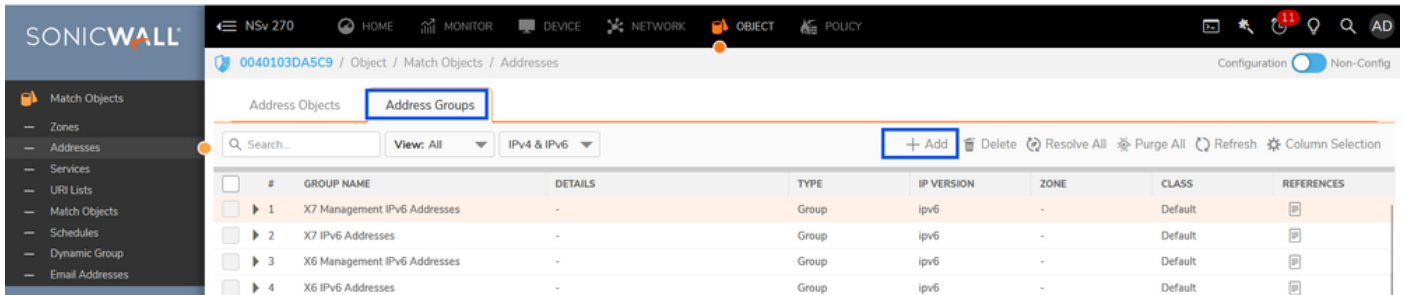
Name	CgNAT	
Zone Assignment	VPN	▼
Type	Network	▼
Network	100.64.0.0	
Netmask / Prefix Length	255.192.0.0	
Cancel		Save

- Klik op Opslaan

Address Object Settings

Name	RAVPNUser-Pool	
Zone Assignment	VPN	▼
Type	Network	▼
Network	10.10.50.0	
Netmask / Prefix Length	255.255.255.0	
Cancel		Save

- Klik op Opslaan
- Adresgroepen maken
- Klik op +Toevoegen
- Selecteer het Adresobject en voeg ze toe aan Adresgroepen



SonicWall - Object- Adresgroepen

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

- Klik op Opslaan

Route toevoegen

Navigeer naar het Sonicwall Dashboard.

- Beleid > Regels en beleid > Routeringsregels
- Klik op + Toevoegen

SONICWALL

NSv 270HOMEMONITORDEVICENETWORKOBJECTPOLICY

0040103DA5C9 / Policy / Rules and Policies / Routing Rules

Rules and PoliciesRouting RulesAccess RulesNAT RulesContent Filter RulesApp RulesEndpoint RulesDPI-SSLDPI-SSHSecurity ServicesCapture ATPEndpoint Security

Default & CustomIPv4Active & InactiveUsed & Unused

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

+ AddDeleteDelete AllEditLive CountersReset Counters

Sonicwall - Routeringsregels

- Routeringsregel toevoegen

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 0.0.0.0/1

Metric 5

Show Diagram ☐

Cancel

Add

- Klik op + Toevoegen

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

Sonicwall - Routeringsregels

Toegangsregels toevoegen

Navigeer naar het Sonicwall Dashboard.

- Beleid > Regels en beleid > Toegangsregels
- Klik op + Toevoegen

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

Default & Custom

IPv4

All Zones -> All Zones

Active & Inactive

Used & Unused

Max Count

Reset Rules

Settings

	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	➕	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
☐	2 (M)	0	Default Access Rule_3	➕	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
☐	3 (M)	0	Default Access Rule_4	➕	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
☐	4 (M)	0	Default Access Rule_5	➕	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
☐	5 (M)	0	Default Access Rule_6	➕	LAN	LAN	Any	Any	Any	All	None	Always
☐	6 (M)	0	Default Access Rule_9	➕	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
☐	7 (M)	0	Default Access Rule_124	➕	LAN	VPN	obj_10.10.20.0.24	CSA-Subnets	Any	All	None	Always
☐	8 (M)	0	Default Access Rule_12	➕	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
☐	9 (M)	0	Default Access Rule_13	➕	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
☐	10 (M)	11.4k	Default Access Rule_14	➕	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
☐	11 (M)	0	Default Access Rule_15	➕	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
☐	12 (M)	2	Default Access Rule_123	➕	WAN	WAN	X1 IP	Any	IKE	All	None	Always
☐	13 (A)	0	Default Access Rule_122	➕	WAN	WAN	Any	X1 IP	IKE	All	None	Always
☐	14 (M)	0	Default Access Rule_22	➕	DMZ	DMZ	Any	Any	Any	All	None	Always
☐	15 (M)	0	Default Access Rule_23	➕	DMZ	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always

+ Add

Edit

Delete

Move

Enable

Disable

Live Counters

Reset Counters

Displaying 42 of 69 rules

Sonicwall - Toegangsregels

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

DESTINATION

Zone/Interface

VPN

Address

CSA-Subnets

Port/Services

Any

Zone/Interface

LAN

Address

LAN

Port/Services

Any

Show Diagram

Cancel

Add

- Klik op +Toevoegen

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																																													
CSA Default & Custom IPv4 All Zones -> All Zones Active & Inactive Used & Unused Max Count Reset Rules Settings																																													
<table> <thead> <tr> <th></th><th>GENERAL</th><th>ZONE</th><th>ADDRESS</th><th>SERVICE</th><th>USER</th><th>SCHEDULE</th></tr> <tr> <th></th><th>PI</th><th>HITS</th><th>NAME</th><th>ACTION</th><th>SOURCE</th><th>DESTINATION</th><th>SOURCE</th><th>DESTINATION</th><th>DESTINATION P...</th><th>USER INCL.</th><th>USER EXCL.</th><th>SCHEDULE</th></tr> </thead> <tbody> <tr> <td>☐</td><td>1 (M)</td><td>0</td><td>CSA-Inbound-Allow_127</td><td>→</td><td>VPN</td><td>LAN</td><td>CSA-Subnets</td><td>LAN</td><td>Any</td><td>All</td><td>None</td><td>Always</td></tr> </tbody> </table>														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	→	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always
	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	→	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always																																	

Sonicwall - Toegangsregels

Verifiëren

- Tunnel status bij beveiligde toegang

← 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

Veilige toegang - Network Tunnel Group - VPN-status

- Tunnelstatus op SonicWall-firewall

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)

System

Interfaces

Fallover & LB

Neighbor Discovery

ARP

MAC IP Anti-Spoof

Web Proxy

VLAN Translation

IP Helper

Dynamic Routing

DHCP Server

Multicast

Network Monitor

AWS Configuration

Firewall

VoIP

DNS

SDWAN

IPSec VPN

Rules and Settings

Sonicwall - IPSec VPN-status

U kunt hetzelfde proces uitvoeren om de tunnel tussen het Secundaire datacenter met beveiligde toegang en de Sonicwall te configureren

Nu, de tunnel is UP op Secure Access en Sonicwall, kunt u doorgaan met het configureren van de toegang tot de particuliere bronnen via RA-VPN, browser-gebaseerde ZTA of client-gebaseerde ZTA op Secure Access Dashboard

Problemen oplossen

Gebruiker-pc

- Controleer of de gebruiker al dan niet succesvol verbinding kan maken met RAVPN/ZTNA. Als dat niet het geval is, kunt u het probleem verder oplossen waarom de verbinding van het besturingsvliegtuig niet werkt.
- Controleer of het netwerk waartoe de gebruiker toegang probeert te krijgen, via de RAVPN-tunnel of ZTNA moet gaan. Zo niet, controleer de configuratie op de kop.

beveiligde toegang

- Controleer de configuratie van de verkeersbesturing in het RAVPN-verbindingsprofiel om te bevestigen dat het bestemmingsnetwerk is geconfigureerd om via de tunnel naar Secure Access te verzenden.
- Controleer of Private Resource is gedefinieerd met geldige protocol/poorten en de verbindingsmechanismen van ZTNA/RAVPN zijn gecontroleerd.
- Verify Access-beleid is geconfigureerd om de RAVPN / ZTNA-gebruiker toegang te geven tot Private Resource Network en zijn geplaatst in een bestelling die geen andere regel heeft voorrang om het verkeer te blokkeren.
- Controleer of de IPSec-tunnel UP en Secure Access is en of geldige clientroutes worden weergegeven via statische routing die betrekking heeft op de privébronnen waartoe de gebruiker toegang probeert te krijgen.

Sonicwall

- Controleer of de IPSec-tunnel UP is of niet (IKE & IPSec SA).
- Controleer of de clientroute of -routes correct zijn geadverteerd.
- Controleer verkeersbronnen van RAVPN / ZTNA-gebruiker die bestemd is voor privébronnen achter Sonicwall bereikt de Sonicwall-firewall door de tunnel door pakketopnames op Sonicwall te maken.
- Controleer of het verkeer een privébron heeft bereikt en reageer op de RAVPN/ZTNA-client of niet. Zo ja, controleer of die pakketten de Sonicall X0 (LAN)-interface bereiken.
- Controleer of Sonicwall het retourverkeer via de IPSec-tunnel doorstuurt naar Secure Access.

Gerelateerde informatie

- [Cisco Technical Support en downloads](#)
- [Cisco Secure Access Help Center](#)
- [Zero Trust Access Module](#)
- [Problemen oplossen bij fout bij beveiligde toegang "Inschrijvingservice reageert niet. Neem contact op met uw IT-helpdesk"](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.