

# Sicheren Zugriff mit Sonicwall Firewall konfigurieren

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

#### [Anforderungen](#)

#### [Verwendete Komponenten](#)

#### [Hintergrundinformationen](#)

#### [Netzwerkdigramm](#)

### [Konfigurieren](#)

#### [Konfigurieren der Netzwerk-Tunnelgruppe \(VPN\) für sicheren Zugriff](#)

#### [Konfigurieren des Tunnels auf der Sonicwall](#)

#### [Konfigurieren des Tunnels - Regeln und Einstellungen](#)

#### [VPN-Tunnelschnittstelle hinzufügen](#)

#### [Netzwerkobjekt und Gruppen hinzufügen](#)

#### [Route hinzufügen](#)

#### [Zugriffsregeln hinzufügen](#)

### [Überprüfung](#)

### [Fehlerbehebung](#)

#### [Benutzer-PC](#)

#### [Sicherer Zugriff](#)

#### [Schallwand](#)

### [Zugehörige Informationen](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration eines IPsec-VTI-Tunnels zwischen dem sicheren Zugriff auf die Sonicwall-Firewall mithilfe von statischem Routing beschrieben.

## Voraussetzungen

- [Konfiguration der Benutzerbereitstellung](#)
- [Konfiguration der ZTNA SSO-Authentifizierung](#)
- [Konfigurieren des sicheren Remotezugriff-VPN](#)

## Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Sonicwall-Firewall (NSv270 - SonicOSX 7.0.1)

- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- Clientless-ZTNA

## Verwendete Komponenten

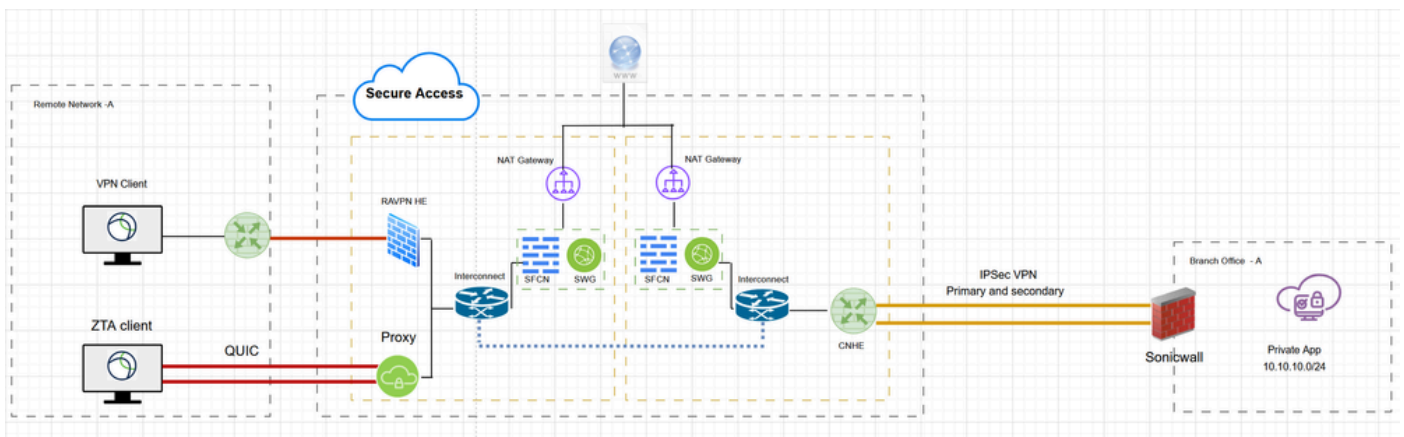
Die Informationen in diesem Dokument basieren auf:

- Sonicwall-Firewall (NSv270 - SonicOSX 7.0.1)
- Sicherer Zugriff
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

### Netzwerkdiagramm



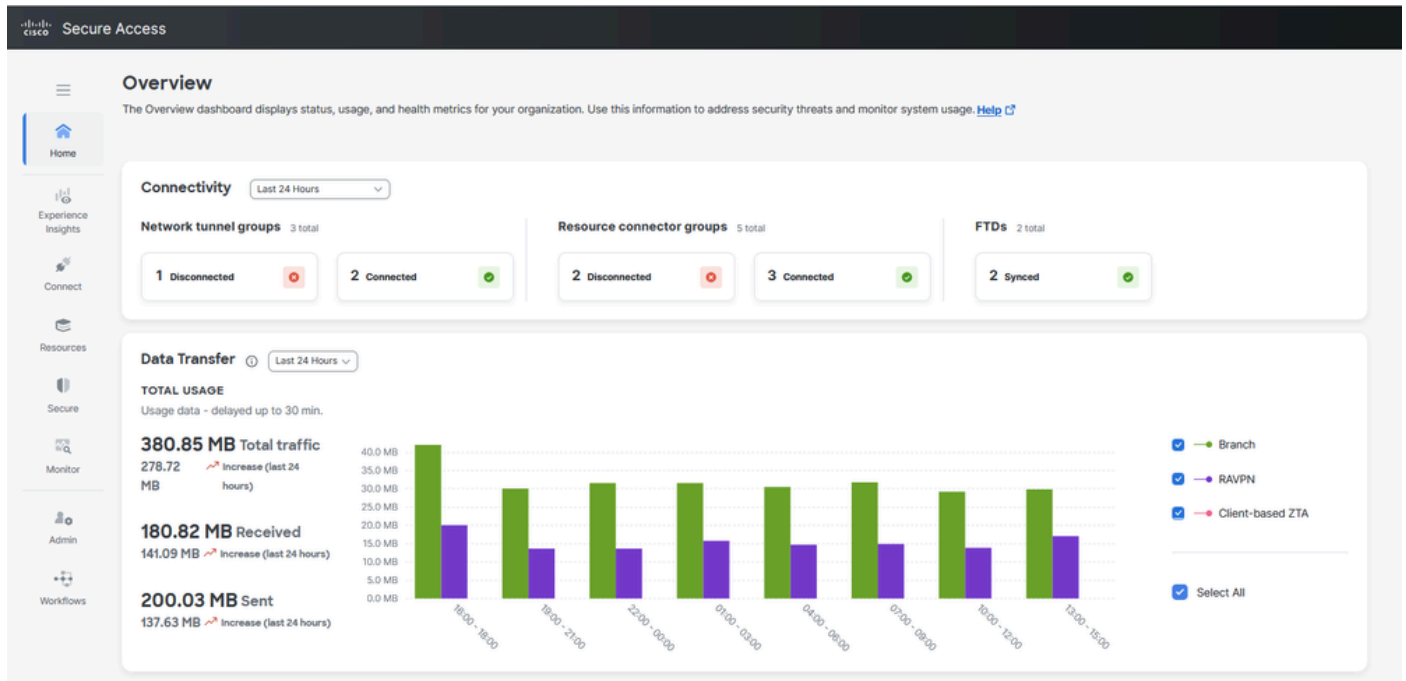
Netzwerkdiagramm

## Konfigurieren

### Konfigurieren der Netzwerk-Tunnelgruppe (VPN) für sicheren Zugriff

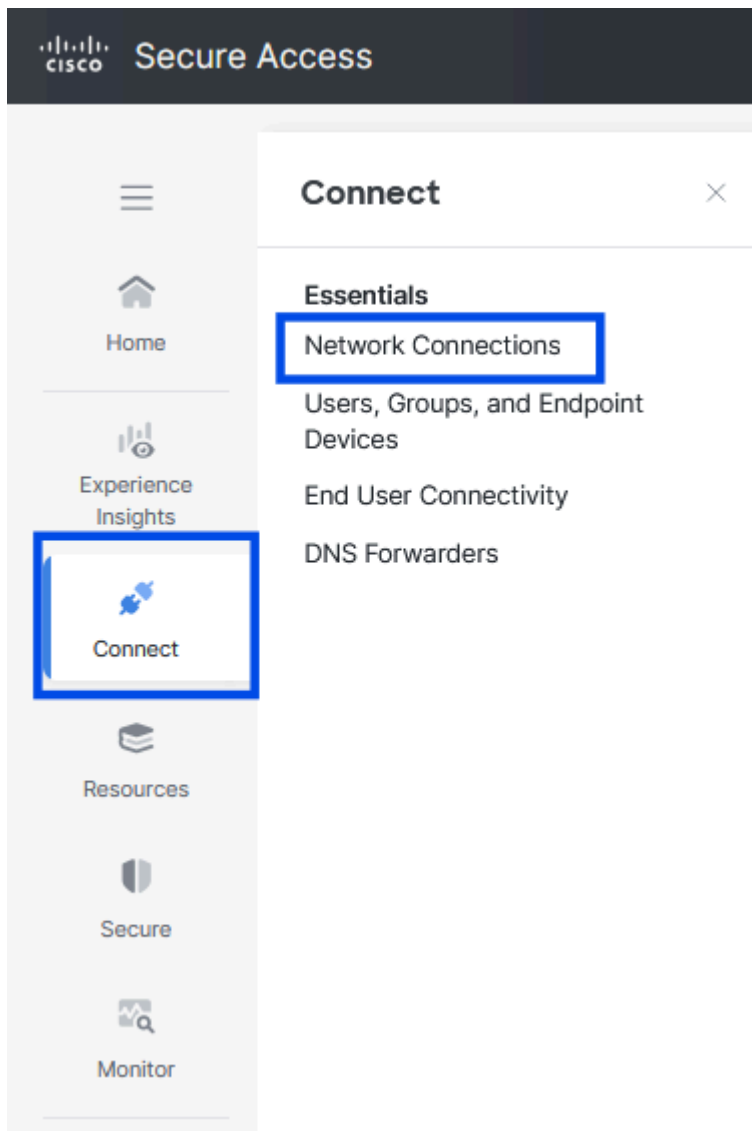
#### Konfiguration eines VPN-Tunnels zwischen sicherem Zugriff und Sonicwall

- Navigieren Sie zum [Admin-Portal](#) des sicheren Zugriffs.



Sicherer Zugriff - Hauptseite

- Klicken Sie auf Verbinden > Netzwerkverbindungen.



Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Netzwerk-Tunnelgruppen auf + Hinzufügen

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's a summary section showing '0 Disconnected', '0 Warning', and '2 Connected' tunnel groups. A table titled 'Network Tunnel Groups' lists two groups: 'AZURE' and 'LAB-BGP', both with a 'Connected' status. The table columns are: Network Tunnel Group, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. At the bottom right, there is a '+ Add' button (highlighted with a blue box) and a pagination control showing 'Rows per page 10' and '1' of 1 page.

- Konfigurieren von Tunnelgruppenname, Region und Gerätetyp
- Klicken Sie auf Next (Weiter).

← 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](#)



Anmerkung: Wählen Sie die Region aus, die dem Standort Ihrer Firewall am nächsten liegt.

- Konfigurieren des Tunnel-ID-Formats und der Passphrase
- Klicken Sie auf Next (Weiter).

← 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](#)

- Konfigurieren Sie die IP-Adressbereiche, Hosts oder Subnetze, die Sie in Ihrem Netzwerk konfiguriert haben, und leiten Sie den Datenverkehr über den sicheren Zugriff weiter.
- Klicken Sie auf Hinzufügen
- Klicken Sie auf Save (Speichern).

**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**

Nachdem Sie auf Speichern geklickt haben, werden die Informationen zum Tunnel angezeigt. Speichern Sie diese Informationen für den nächsten Konfigurationsschritt.

**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.

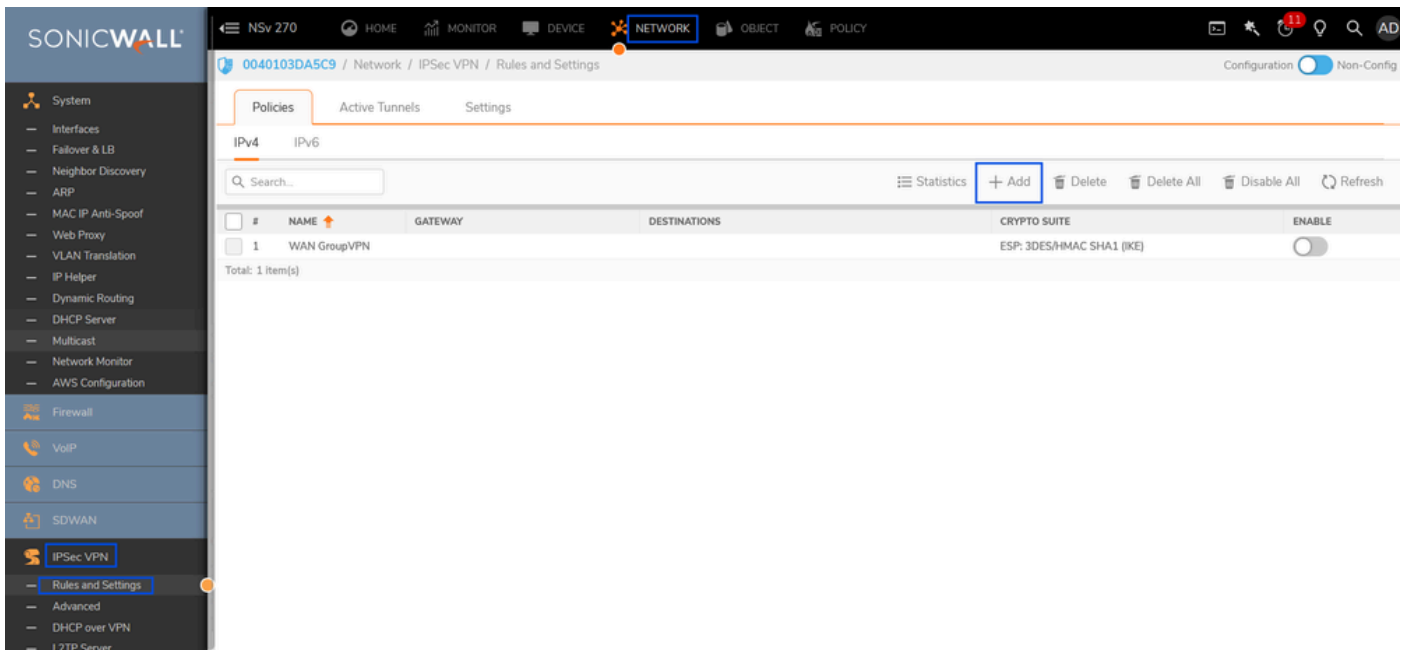
<b>Primary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Primary Data Center IP Address:</b>	44.228.138.150	
<b>Secondary Tunnel ID:</b>	SonicWall-VPN@i	sse.cisco.com
<b>Secondary Data Center IP Address:</b>	52.35.201.56	
<b>Passphrase:</b>		

### Konfigurieren des Tunnels auf der Sonicwall

### Konfigurieren des Tunnels - Regeln und Einstellungen

Navigieren Sie zum Sonicwall Dashboard.

- Netzwerk > IPsec VPN > Regeln und Einstellungen
- Klicken Sie auf + Hinzufügen



Sonicwall - IPsec VPN - Regeln und Einstellungen

- Füllen Sie unter VPN Policy (VPN-Richtlinie) die VPN-Konfiguration basierend auf den Tunneldaten von Secure Access und den [unterstützten ipsec-Parametern aus](#).

## 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: [Masked]

Mask Shared Secret: ☒

Confirm Shared Secret: [Masked]

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

- Klicken Sie auf Speichern

## VPN-Tunnelschnittstelle hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

- Netzwerk > System > Schnittstelle
- Klicken Sie auf + Schnittstelle hinzufügen.
- VPN-Tunnelschnittstelle auswählen

SONICWALL

NSv 270

HOME MONITOR DEVICE NETWORK OBJECT POLICY

0040103DA5C9 / Network / System / Interfaces

Configuration Non-Config

Interface Settings Traffic Statistics

IPv4 IPv6

+ Add Interface Refresh

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	Virtual Interface
X1	WAN	Default LB Group	192.168.1.70	255.255.255.0	Static IP	10 Gbps Full Duplex	VPN Tunnel Interface

Sonicwall - Schnittstellen

# 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

- Klicken Sie auf 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 - Schnittstellen - VPN-Tunnelschnittstelle

## Netzwerkobjekt und Gruppen hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

- Objekt > Objekte zuordnen > Adressen
- Adressobjekte
- Klicken Sie auf + Hinzufügen

0040103DA5C9 / Object / Match Objects / Addresses

Configuration ☒ Config ☐ 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 - Objekt - Adressobjekte

## Address Object Settings

**Name**  ⓘ

**Zone Assignment**  ▼


**Type**  ▼

**Network**

**Netmask / Prefix Length**


- Klicken Sie auf Save (Speichern).

# Address Object Settings

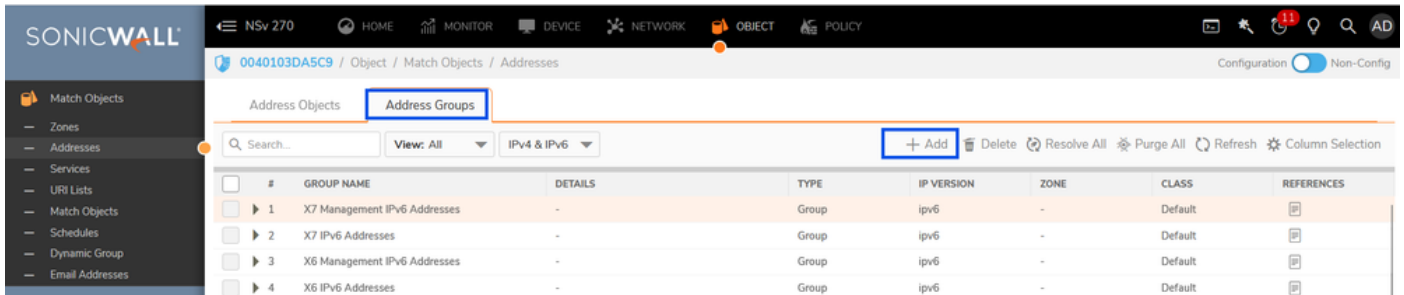
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button"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

- Klicken Sie auf Save (Speichern).

# 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"/>

- Klicken Sie auf Save (Speichern).
- Erstellen von Adressgruppen
- Klicken Sie auf +Hinzufügen
- Wählen Sie das Adressobjekt aus, und fügen Sie es zu Adressgruppen hinzu.



Sonicwall - Objekt - Adressgruppen

## 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

- Klicken Sie auf Save (Speichern).

## Route hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

- Richtlinie > Regeln und Richtlinien > Weiterleitungsregeln
- Klicken Sie auf + Hinzufügen

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 - Routingregeln

- Routingregel hinzufügen

## 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

- Klicken Sie auf + Hinzufügen

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 Any Route Policy_5 Any 255.255.255.255/32 Any Any X0 0.0.0.0 20 Standard Default														

Sonicwall - Routingregeln

## Zugriffsregeln hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

- Richtlinie > Regeln und Richtlinien > Zugriffsregeln
- Klicken Sie auf + Hinzufügen

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
<input type="checkbox"/>	1 (M)	0	Default Access Rule_2	➕	LAN	LAN	Any	All X0 Management IP	Ping	All	None	Always
<input type="checkbox"/>	2 (M)	0	Default Access Rule_3	➕	LAN	LAN	Any	All X0 Management IP	SSH Management	All	None	Always
<input type="checkbox"/>	3 (M)	0	Default Access Rule_4	➕	LAN	LAN	Any	All X0 Management IP	HTTPS Management	All	None	Always
<input type="checkbox"/>	4 (M)	0	Default Access Rule_5	➕	LAN	LAN	Any	All X0 Management IP	HTTP Management	All	None	Always
<input type="checkbox"/>	5 (M)	0	Default Access Rule_6	➕	LAN	LAN	Any	Any	Any	All	None	Always
<input type="checkbox"/>	6 (M)	0	Default Access Rule_9	➕	LAN	VPN	WAN RemoteAccess Networks	Any	Any	All	None	Always
<input type="checkbox"/>	7 (M)	0	Default Access Rule_124	➕	LAN	VPN	obj_10.10.20.0.24	CSA-Subnets	Any	All	None	Always
<input type="checkbox"/>	8 (M)	0	Default Access Rule_12	➕	WAN	WAN	Any	All X1 Management IP	Ping	All	None	Always
<input type="checkbox"/>	9 (M)	0	Default Access Rule_13	➕	WAN	WAN	Any	All X1 Management IP	SSH Management	All	None	Always
<input type="checkbox"/>	10 (M)	11.4k	Default Access Rule_14	➕	WAN	WAN	Any	All X1 Management IP	HTTPS Management	All	None	Always
<input type="checkbox"/>	11 (M)	0	Default Access Rule_15	➕	WAN	WAN	Any	All X1 Management IP	HTTP Management	All	None	Always
<input type="checkbox"/>	12 (M)	2	Default Access Rule_123	➕	WAN	WAN	X1 IP	Any	IKE	All	None	Always
<input type="checkbox"/>	13 (A)	0	Default Access Rule_122	➕	WAN	WAN	Any	X1 IP	IKE	All	None	Always
<input type="checkbox"/>	14 (M)	0	Default Access Rule_22	➕	DMZ	DMZ	Any	Any	Any	All	None	Always
<input type="checkbox"/>	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 - Zugriffsregeln

## 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

- Klicken Sie auf +Hinzufügen

SONICWALL																																													
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY																																													
0040103DA5C9 / Policy / Rules and Policies / Access Rules Configuration Non-Config																																													
<div>Rules and Policies</div> <div>Access Rules</div> <div>NAT Rules</div> <div>Routing Rules</div> <div>Content Filter Rules</div> <div>App Rules</div> <div>Endpoint Rules</div> <div>DPI-SSL</div> <div>DPI-SSH</div> <div>Security Services</div> <div>Capture ATP</div> <div>Endpoint Security</div>																																													
<div> <div>CSA</div> <div>Default &amp; Custom</div> <div>IPv4</div> <div>All Zones -&gt; All Zones</div> <div>Active &amp; Inactive</div> <div>Used &amp; Unused</div> <div>Max Count</div> <div>Reset Rules</div> <div>Settings</div> </div>																																													
<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><input type="checkbox"/></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	<input type="checkbox"/>	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																																	
<input type="checkbox"/>	1 (M)	0	CSA-Inbound-Allow_127	→	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always																																	

Sonicwall - Zugriffsregeln



# Überprüfung

- Tunnelstatus bei sicherem Zugriff

← 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

Sicherer Zugriff - Netzwerk-Tunnelgruppe - VPN-Status

- Tunnelstatus auf 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

Sie können den gleichen Prozess für die Konfiguration eines Tunnels zwischen dem sekundären Secure Access-Rechenzentrum und Sonicwall ausführen.

Jetzt ist der Tunnel für sicheren Zugriff und Sonicwall aktiviert. Sie können den Zugriff auf die privaten Ressourcen weiterhin über RA-VPN, browserbasiertes ZTA oder clientbasiertes ZTA auf Secure Access Dashboard konfigurieren.

# Fehlerbehebung

## Benutzer-PC

- Überprüfen Sie, ob der Benutzer erfolgreich eine Verbindung mit RAVPN/ZTNA herstellen/sich anmelden kann. Wenn nicht, suchen Sie weiter nach den Gründen, warum die Verbindung der Kontrollebene fehlschlägt.
- Überprüfen Sie, ob das Netzwerk, auf das der Benutzer zuzugreifen versucht, über einen RAVPN-Tunnel oder ZTNA geleitet werden soll. Wenn nicht, überprüfen Sie die Konfiguration am Headend .

## Sicherer Zugriff

- Überprüfen Sie die Konfiguration der Verkehrssteuerung im RAVPN-Verbindungsprofil, um zu bestätigen, dass das Zielnetzwerk für das Senden über den Tunnel an Secure Access konfiguriert ist.
- Überprüfen Sie, ob eine private Ressource mit einem gültigen Protokoll bzw. gültigen Ports definiert ist, und ob die ZTNA-/RAVPN-Verbindungsmechanismen überprüft wurden.
- Überprüfen Sie, ob die Zugriffsrichtlinie so konfiguriert ist, dass RAVPN-/ZTNA-Benutzer auf das private Ressourcennetzwerk zugreifen können, und platzieren Sie sie in einer Reihenfolge, in der keine andere Regel zur Blockierung des Datenverkehrs Vorrang hat.
- Vergewissern Sie sich, dass der IPSec-Tunnel aktiviert ist und für sicheren Zugriff gültige Client-Routen über statisches Routing angezeigt werden, das private Ressourcen abdeckt, auf die der Benutzer zugreifen möchte.

## Schallwand

- Überprüfen Sie, ob der IPSec-Tunnel aktiv ist oder nicht (IKE & IPSec SA).
- Überprüfen Sie, ob die Client-Route oder -Routen ordnungsgemäß angekündigt wurden.
- Überprüfen Sie, ob die Datenverkehrsquellen des RAVPN-/ZTNA-Benutzers, die an eine private Ressource hinter Sonicwall gerichtet sind, die Sonicwall-Firewall über einen Tunnel erreichen, indem Sie die Paketerfassung auf Sonicwall durchführen.
- Überprüfen Sie, ob der Datenverkehr die private Ressource erreicht hat und auf den RAVPN-/ZTNA-Client antwortet oder nicht. Wenn ja, stellen Sie sicher, dass diese Pakete die Sonic X0 (LAN)-Schnittstelle erreichen.
- Überprüfen Sie, ob Sonicwall den zurückfließenden Datenverkehr über den IPSec-Tunnel an Secure Access weiterleitet.

## Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Cisco Secure Access-Hilfecenter](#)
- [Zugriffsmodul ohne Vertrauen](#)
- [Fehler beim sicheren Zugriff: "Der Registrierungsdienst reagiert nicht. Kontaktieren Sie Ihren IT-Helpdesk"](#)

### Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.