

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

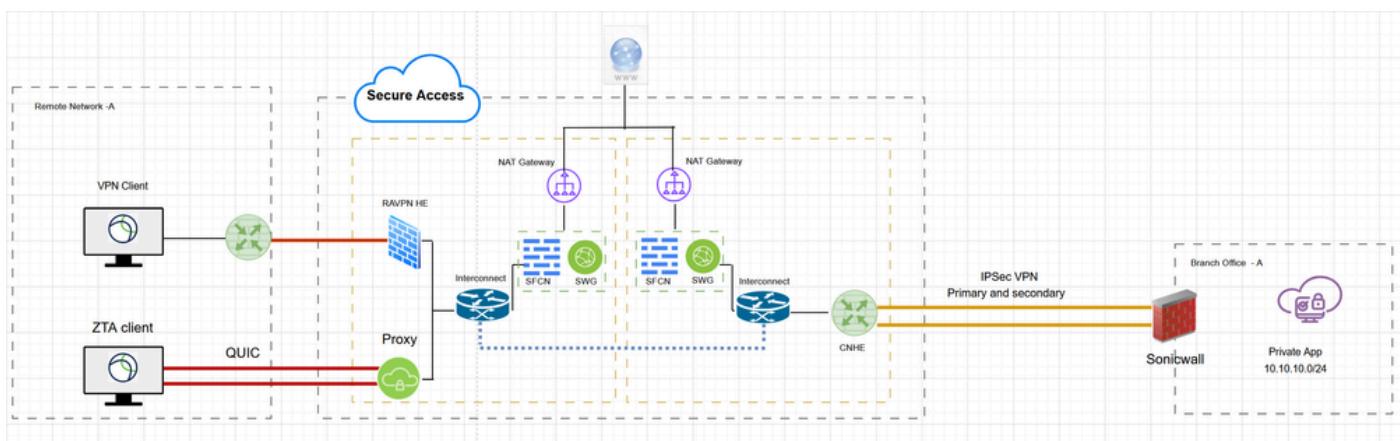
Die Informationen in diesem Dokument basieren auf:

- 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



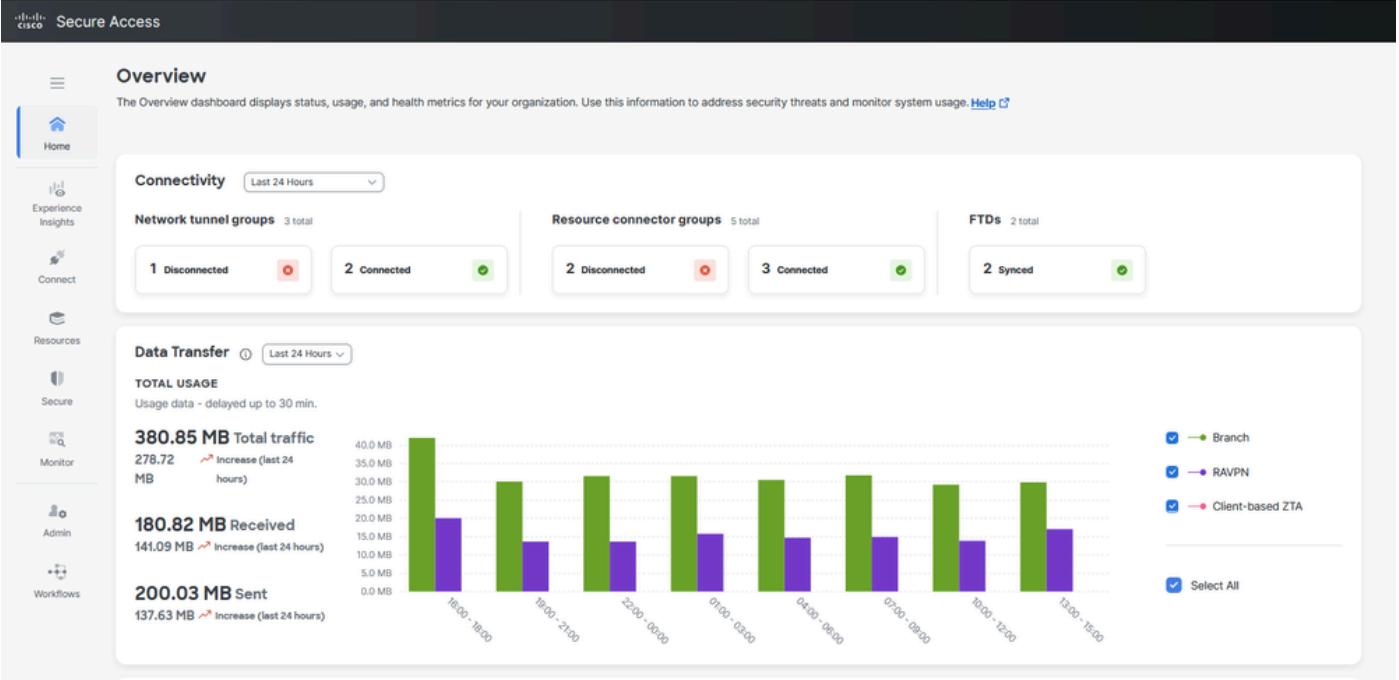
Netzwerkdiagramm

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.

Secure Access

Connect

Essentials

Network Connections (Selected)

Users, Groups, and Endpoint Devices

End User Connectivity

DNS Forwarders

Connect (Selected)

Resources

Secure

Monitor

Sicherer Zugriff - Netzwerkverbindungen

- Klicken Sie unter Netzwerk-Tunnelgruppen auf + Hinzufügen

Network Connections

Manage the connections that allow user traffic to reach private resources on your network. For information about these options, see [Help](#).

Connector Groups **Network Tunnel Groups** FTDs

Network Tunnel Groups 2 total

0 Disconnected 0 Warning 2 Connected

Network Tunnel Groups

A network tunnel group provides a framework for establishing tunnel redundancy and high availability. Connect tunnels to the hubs within a network tunnel group to securely control user access to the Internet and private resources. [Help](#)

Q. Search Region Status 2 Tunnel Groups + Add

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

Rows per page 10 < 1 >

- 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:

Device Type:

[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](#)

Sicherer Zugriff - Tunnel-ID und Passphrase

- 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).

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**

Sicherer Zugriff - Tunnelgruppen - Routing-Optionen

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

← 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@[sse.cisco.com](#)

Primary Data Center IP Address: 44.228.138.150

Secondary Tunnel ID: SonicWall-VPN@[sse.cisco.com](#)

Secondary Data Center IP Address: 52.35.201.56

Passphrase:

Save

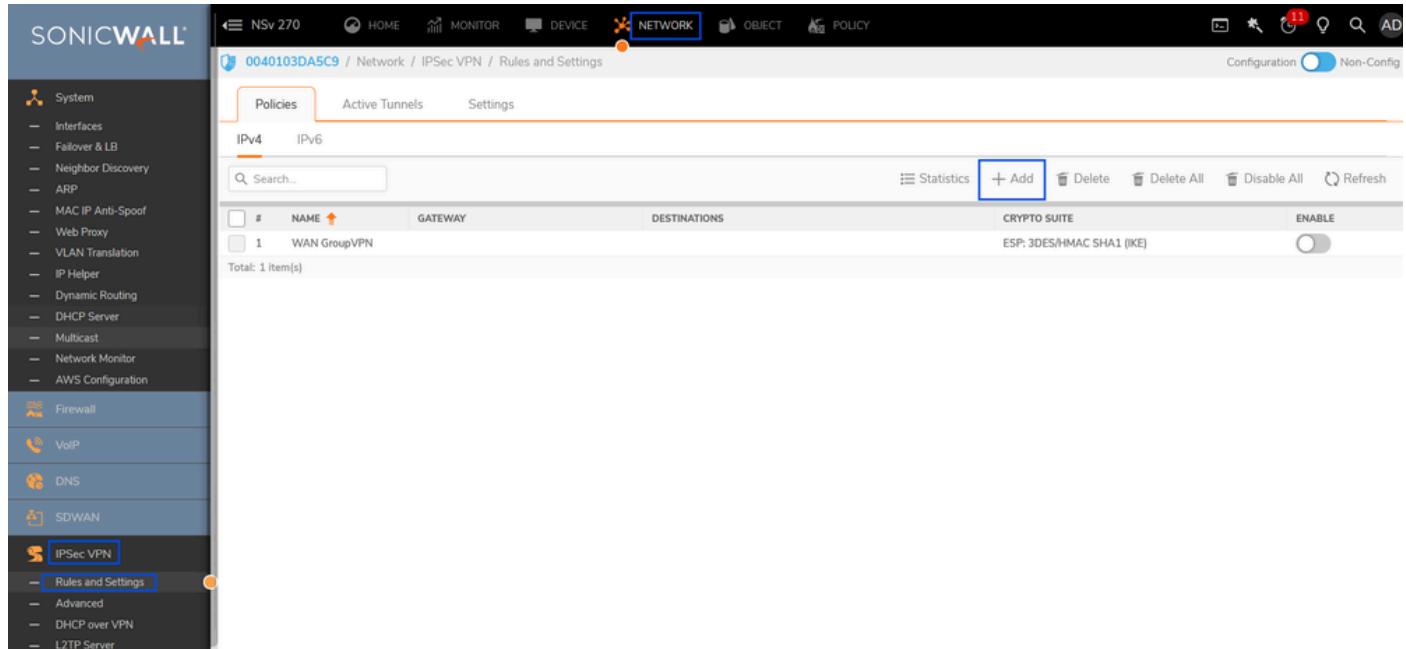
Sicherer Zugriff - Daten für Tunnel-Setup

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



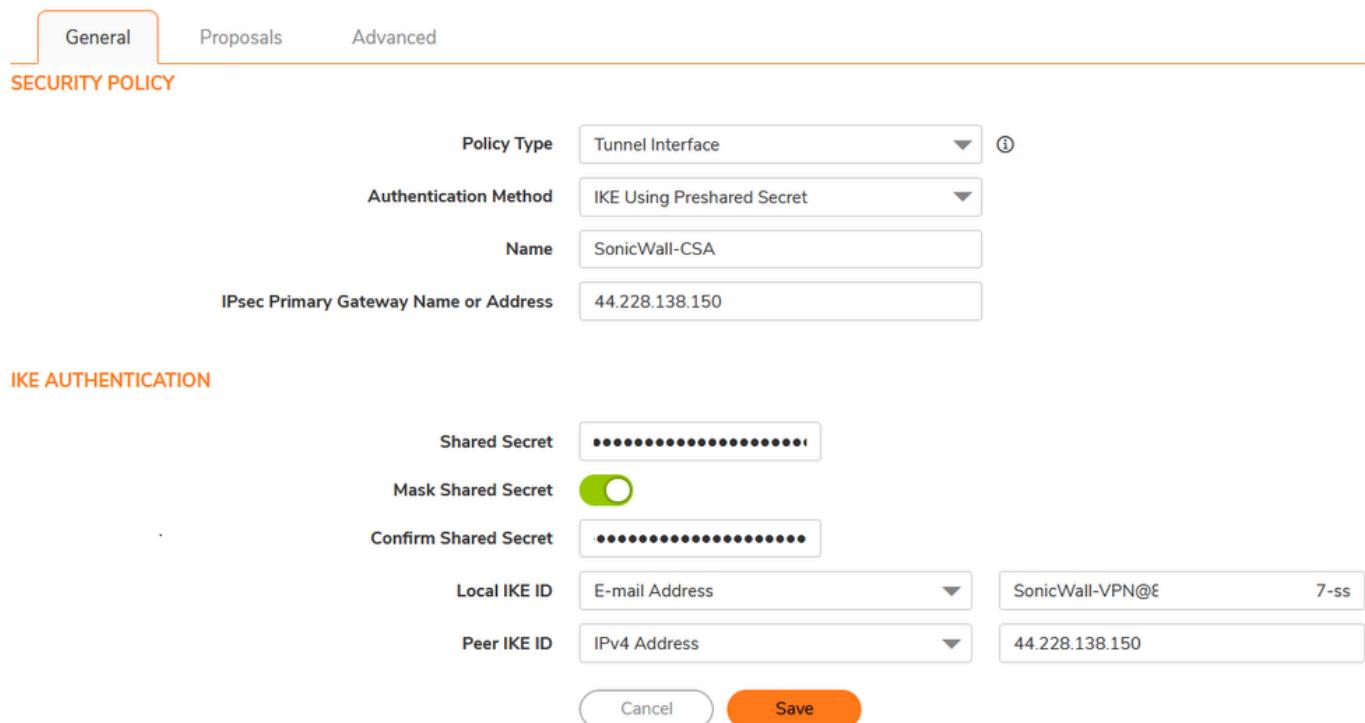
The screenshot shows the Sonicwall NSv 270 interface. The left sidebar is the navigation menu. The main area is titled '0040103DA5C9 / Network / IPsec VPN / Rules and Settings'. It shows a table with one item: 'WAN GroupVPN'. The 'Add' button in the top right is highlighted with a blue box. The table includes columns for NAME, GATEWAY, DESTINATIONS, CRYPTO SUITE, and ENABLE.

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

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



The screenshot shows the 'General' tab of the VPN Policy configuration. The 'SECURITY POLICY' section contains fields for Policy Type (Tunnel Interface), Authentication Method (IKE Using Preshared Secret), Name (SonicWall-CSA), and IPsec Primary Gateway Name or Address (44.228.138.150). The 'IKE AUTHENTICATION' section contains fields for Shared Secret (masked), Mask Shared Secret (on), Confirm Shared Secret (masked), Local IKE ID (E-mail Address: SonicWall-VPN@E), and Peer IKE ID (IPv4 Address: 44.228.138.150). The 'Save' button is highlighted with an orange box.

Policy Type	Tunnel Interface
Authentication Method	IKE Using Preshared Secret
Name	SonicWall-CSA
IPsec Primary Gateway Name or Address	44.228.138.150

Shared Secret
Mask Shared Secret	<input checked="" type="checkbox"/>
Confirm Shared Secret
Local IKE ID	E-mail Address: SonicWall-VPN@E
Peer IKE ID	IPv4 Address: 44.228.138.150

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"/>	<small>i</small>	Display Suite B Compliant Algorithms Only	<input type="checkbox"/>
Disable IPsec Anti-Replay	<input type="checkbox"/>	<small>i</small>	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		Interface X1	

IKEV2 SETTINGS

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

- Klicken Sie auf Speichern

VPN-Tunnelschnittstelle hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

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

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

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

HTTPS	<input type="checkbox"/>
Port	<input type="checkbox"/>

USER LOGIN

HTTP	<input type="checkbox"/>
HTTPS	<input type="checkbox"/>

Buttons: Cancel (gray) OK (orange)

- Klicken Sie auf OK.

SONICWALL

0040103DASC9 / Network / System / Interfaces

Interface Settings Traffic Statistics

IPv4 IPv6

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 - Schnittstellen - VPN-Tunnelschnittstelle

Netzwerkobjekt und Gruppen hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

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

#	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 ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

Cancel Save

- Klicken Sie auf Save (Speichern).

Address Object Settings

Name ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

Cancel 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.

#	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 - 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

RAV

No Data

In Group 2 items

CgNAT[NW]

RAVPNUser-Pool[NW]

- Klicken Sie auf Save (Speichern).

Route hinzufügen

Navigieren Sie zum Sonicwall Dashboard.

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

	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	rd
			Route Policy_7	Any	X1 Default Gateway	Any	Any	X1	0.0.0.0	20	Standar	rd
			Route Policy_26	Any	CSA_Tunnel1 Subnet	Any	Any	CSA_Tunnel1	0.0.0.0	20	Standar	rd
			Route Policy_4	X0 Subnet	Any	Any	Any	X0	0.0.0.0	20	Standar	rd
			Route Policy_6	X1 Subnet	Any	Any	Any	X1	0.0.0.0	20	Standar	rd
			Route Policy_8	X1 IP	Any	Any	Any	X1	X1 Default Gateway	20	Standar	rd
			Route Policy_9	0.0.0.0/0	Any	Any	Any	X1	192.168.1.1	20	Standar	rd

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

Sonicwall - Routingregeln

- Routingregel hinzufügen

Adding Rule

Name

Tags

Description

Type IPv4 IPv6

- Lookup
Next Hop
Advanced
Probe

Source

Destination

Service

App

Service

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

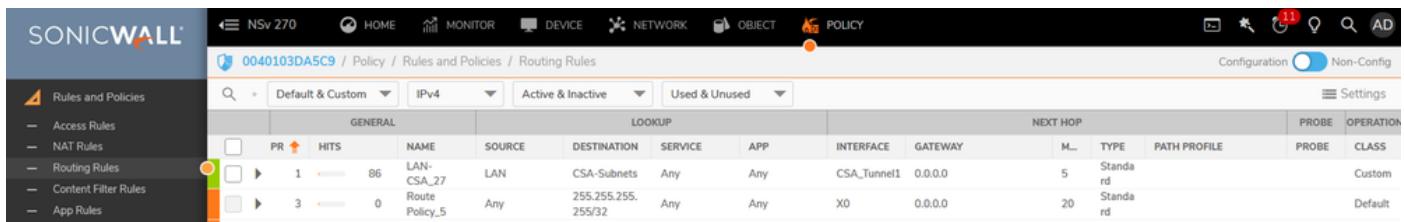
Interface: CSA_Tunnel1

Gateway: 0.0.0.0/0

Metric: 5

Show Diagram Cancel Add

- Klicken Sie auf + Hinzufügen



The screenshot shows the SonicWall NSv 270 Policy interface. The top navigation bar includes links for HOME, MONITOR, DEVICE, NETWORK, OBJECT, and POLICY. The POLICY section is active. Below the navigation is a search bar and a configuration toggle. The main content area is titled '0040103DA5C9 / Policy / Rules and Policies / Routing Rules'. The table has columns for PR, HITS, NAME, SOURCE, DESTINATION, SERVICE, APP, INTERFACE, GATEWAY, Metric, TYPE, PATH PROFILE, PROBE, and OPERATION. Two rows are visible: one for 'LAN-CSA_27' and another for 'Route Policy_5'.

	PR	HITS	NAME	SOURCE	DESTINATION	SERVICE	APP	INTERFACE	GATEWAY	Metric	TYPE	PATH PROFILE	PROBE	OPERATION
<input type="checkbox"/>	PR	1	86	LAN-CSA_27	LAN	CSA-Subnets	Any	Any	CSA_Tunnel1	0.0.0.0	5	Standard		Custom
<input type="checkbox"/>	PR	3	0	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 - Zugriffsregeln

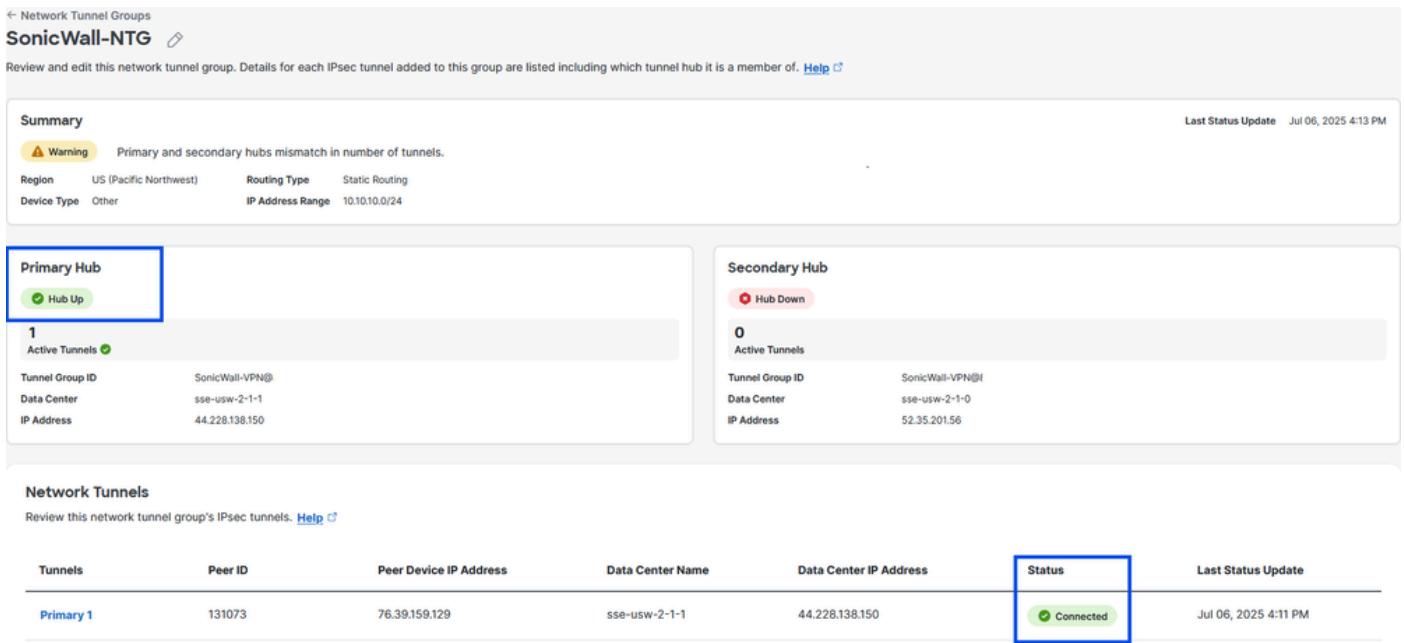
Adding Rule

- Klicken Sie auf +Hinzufügen

Sonicwall - Zugriffsregeln

Überprüfung

- Tunnelstatus bei sicherem Zugriff



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

Primary Hub

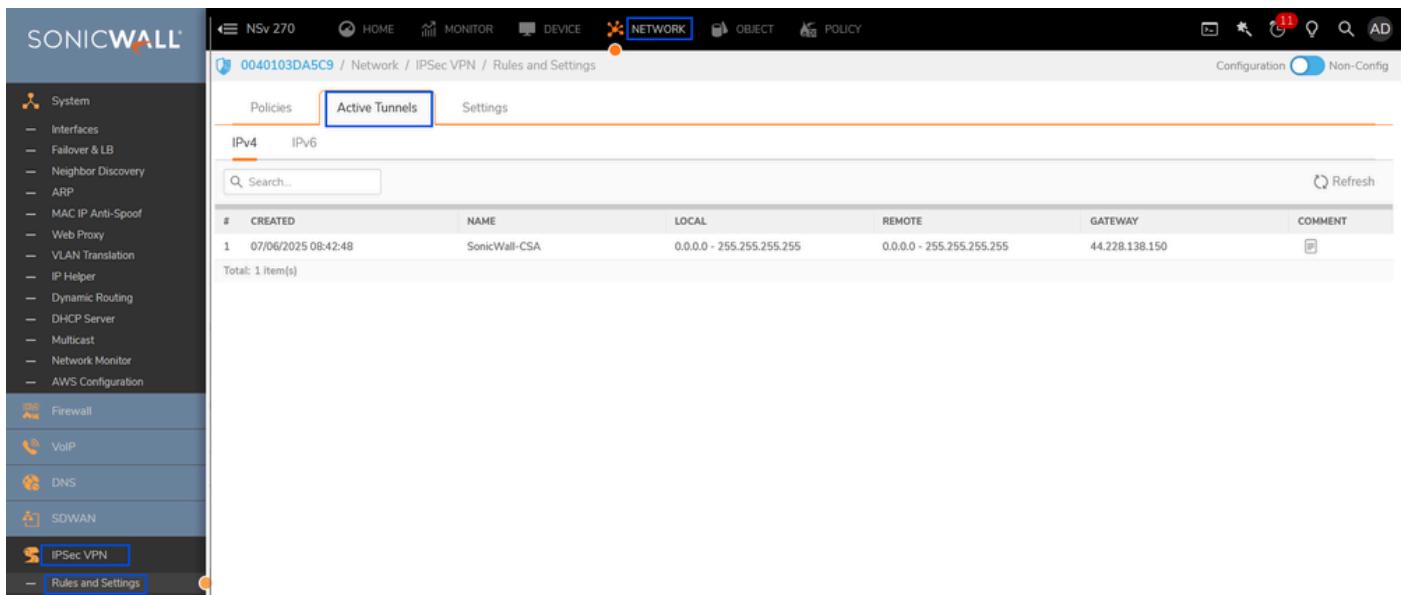
Secondary Hub

Network Tunnels

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



NSv 270

HOME MONITOR DEVICE NETWORK OBJECT POLICY

Configuration Non-Config

0040103DA5C9 / Network / IPsec VPN / Rules and Settings

Polices 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	

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.