

Configurazione di Secure Access con Sonicwall Firewall

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Esempio di rete](#)

[Configurazione](#)

[Configura Network Tunnel Group \(VPN\) su Secure Access](#)

[Configurazione del tunnel su Sonicwall](#)

[Configurazione del tunnel - Regole e impostazioni](#)

[Aggiungi interfaccia tunnel VPN](#)

[Aggiungi oggetto e gruppi di rete](#)

[Aggiungi route](#)

[Aggiungi regole di accesso](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[PC utente](#)

[Accesso sicuro](#)

[Sonicwall](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare un tunnel VTI IPsec tra un firewall Secure Access to Sonicwall e l'altro utilizzando il routing statico.

Prerequisiti

- [Configura assegnazione ruoli utente](#)
- [Configurazione autenticazione SSO ZTNA](#)
- [Configura accesso sicuro VPN di accesso remoto](#)

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firewall di Sonicwall (NSv270 - SonicOSX 7.0.1)

- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- ZTNA senza client

Componenti usati

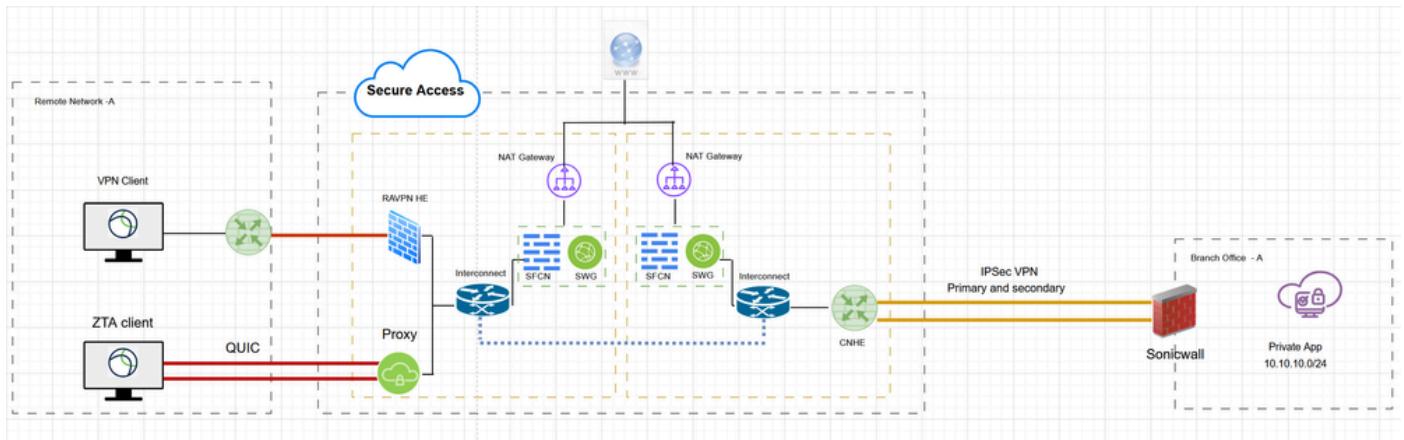
Le informazioni fornite in questo documento si basano su:

- Firewall di Sonicwall (NSv270 - SonicOSX 7.0.1)
- Accesso sicuro
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Esempio di rete



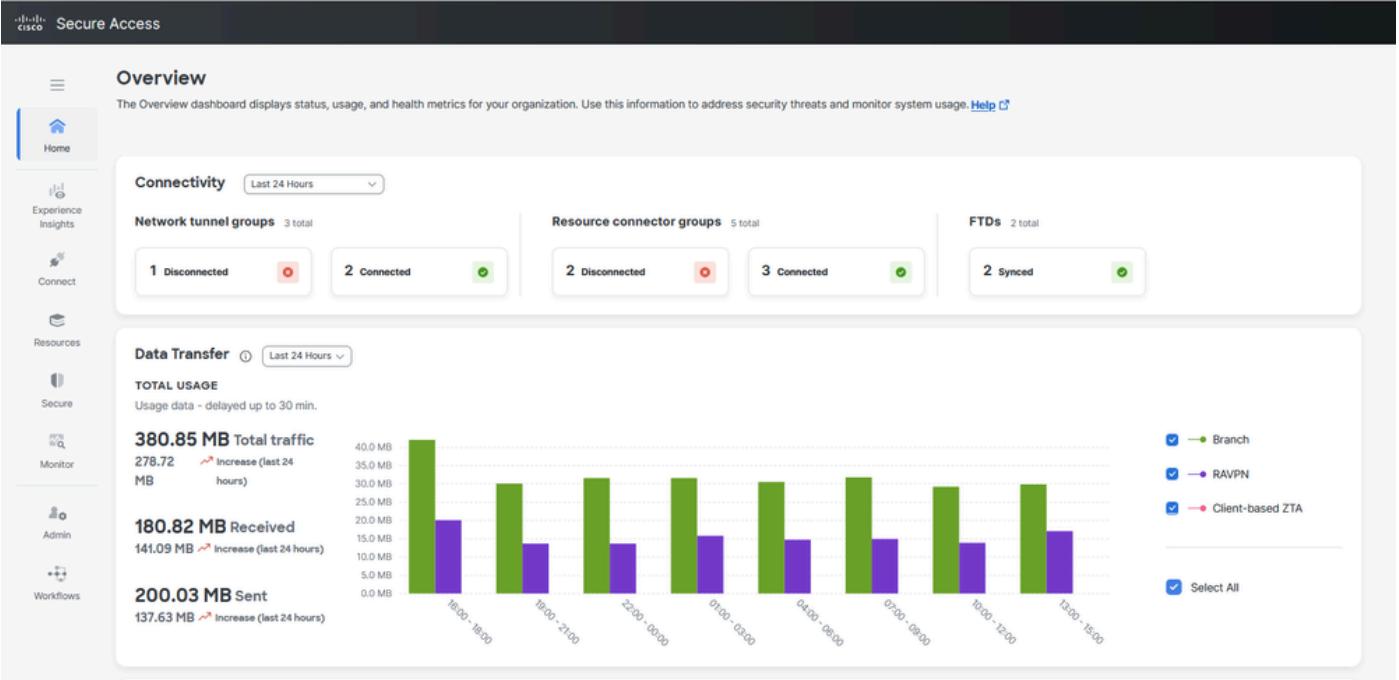
Esempio di rete

Configurazione

Configura Network Tunnel Group (VPN) su Secure Access

Per configurare il tunnel VPN tra Secure Access e Sonicwall

- Passare al [portale di amministrazione](#) di Secure Access



Secure Access - Pagina principale

- Fare clic su Connect > Network Connections

The screenshot shows the Cisco Secure Access web interface. On the left, there's a vertical navigation bar 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'.

Accesso sicuro - Connessioni di rete

- In Gruppi di tunnel di rete fare clic su + Aggiungi

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), 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' with columns for Name, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. Two entries are shown: 'AZURE' (Connected, US (Pacific Northwest), sse-usw-2-1-1, 1, sse-usw-2-1-0, 1) and 'LAB-BGP' (Connected, US (Pacific Northwest), sse-usw-2-1-1, 1, sse-usw-2-1-0, 1). A blue '+' button is located at the top right of the table header.

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

- Configurare il nome del gruppo di tunnel, l'area e il tipo di dispositivo
- Fare clic su Avanti.

← 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](#)



Nota: Scegliere l'area più vicina alla posizione del firewall.

- Configurazione del formato dell'ID del tunnel e della passphrase
- Fare clic su Avanti.

← 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](#)

Accesso sicuro - ID tunnel e passphrase

- Configurare gli intervalli di indirizzi IP, gli host o le subnet configurati nella rete e che si desidera passare il traffico attraverso l'accesso protetto
- Fare clic su Aggiungi
- Fare clic su Salva.

General Settings
Tunnel ID and Passphrase
Routing
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**

Accesso sicuro - Gruppi di tunnel - Opzioni di routing

Dopo aver fatto clic su Save (Salva), vengono visualizzate le informazioni sul tunnel. Salvare le informazioni per il passaggio di configurazione successivo

← 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	<input type="checkbox"/>
Primary Data Center IP Address:	44.228.138.150	<input type="checkbox"/>	
Secondary Tunnel ID:	SonicWall-VPN@1	sse.cisco.com	<input type="checkbox"/>
Secondary Data Center IP Address:	52.35.201.56	<input type="checkbox"/>	
Passphrase:	<input type="password"/>		

Accesso sicuro - Configurazione dati per tunnel

Configurazione del tunnel su Sonicwall

Configurazione del tunnel - Regole e impostazioni

Passare al dashboard di Sonicwall.

- Rete > VPN IPSec > Regole e impostazioni
- Fare clic su + Aggiungi

The screenshot shows the Sonicwall NSv 270 interface. The left sidebar has a tree view with 'System' expanded, showing various network components like Interfaces, Failover & LB, Neighbor Discovery, ARP, MAC IP Anti-Spoof, Web Proxy, VLAN Translation, IP Helper, Dynamic Routing, DHCP Server, Multicast, Network Monitor, and AWS Configuration. Below that is 'Firewall', 'VoIP', 'DNS', and 'SDWAN'. Under 'IPSec VPN', 'Rules and Settings' is selected. The main panel title is '0040103DA5C9 / Network / IPsec VPN / Rules and Settings'. It has tabs for 'Policies' (selected), 'Active Tunnels', and 'Settings'. Under 'Policies', there are tabs for 'IPv4' (selected) and 'IPv6'. A search bar says 'Search...'. Below is a table with one item: 'NAME' (WAN GroupVPN), 'GATEWAY' (empty), 'DESTINATIONS' (empty), 'CRYPTO SUITE' (ESP: 3DES/HMAC SHA1 (IKE)), and 'ENABLE' (switch off). Buttons at the top right include 'Statistics', '+ Add' (highlighted in blue), 'Delete', 'Delete All', 'Disable All', and 'Refresh'.

Sonicwall - IPsec VPN - Regole e impostazioni

- In Criteri VPN, compilare la configurazione della VPN in base ai dati del tunnel di Accesso sicuro e ai [parametri IPsec supportati](#)

VPN Policy

The screenshot shows the 'VPN Policy' configuration screen. At the top are tabs: 'General' (selected), 'Proposals', and 'Advanced'. Below is a section titled 'SECURITY POLICY' with the following fields:

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

Below this is the 'IKE AUTHENTICATION' section with the following fields:

- Shared Secret: masked value
- Mask Shared Secret: switch on
- Confirm Shared Secret: masked value
- Local IKE ID: E-mail Address (SonicWall-VPN@E)
- Peer IKE ID: IPv4 Address (44.228.138.150)

At the bottom are 'Cancel' and 'Save' buttons.

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"/>	

- Fare clic su Salva

Aggiungi interfaccia tunnel VPN

Passare al dashboard di Sonicwall.

- Rete > Sistema > Interfaccia
- Fare clic su + Aggiungi interfaccia
- Seleziona interfaccia 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 interfaces. A blue box highlights the 'Add Interface' button at the bottom right of the table area. The table columns are: NAME, ZONE, GROUP, IP ADDRESS, SUBNET MASK, IP ASSIGNMENT, and STATUS. The rows show two existing interfaces: X0 (LAN, N/A, 10.10.20.1, 255.255.255.0, Static IP, 10 Gbps Full Duplex) and X1 (WAN, Default LB Group, 192.168.1.70, 255.255.255.0, Static IP, 10 Gbps Full Duplex).

Sonicwall - Interfacce

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

- Fare clic su OK.

SONICWALL

0040103DASC9 / 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	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 - Interfacce - VPN Tunnel Interface

Aggiungi oggetto e gruppi di rete

Passare al dashboard di Sonicwall.

- Oggetto > Corrispondenza oggetti >Indirizzi
- Oggetti Address
- Fare clic su +Aggiungi

#	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 - Oggetto - Oggetti Address

Address Object Settings

Name

i

Zone Assignment

LAN

Type

Network

Network

Netmask / Prefix Length

Cancel
Save

- Fare clic su Salva.

Address Object Settings

Name ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

- Fare clic su Salva.

Address Object Settings

Name ⓘ

Zone Assignment ⏺

Type ⏺

Network

Netmask / Prefix Length

- Fare clic su Salva.
- Crea gruppi di indirizzi
- Fare clic su +Aggiungi
- Selezionare l'oggetto indirizzo e aggiungerlo ai gruppi di indirizzi

Sonicwall - Oggetto - Gruppi di indirizzi

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
<input type="checkbox"/> RAV	
No Data	

In Group	2 items
<input type="checkbox"/> CgNAT[NW]	
<input type="checkbox"/> RAVPNUser-Pool[NW]	

- Fare clic su Salva.

Aggiungi route

Passare al dashboard di Sonicwall.

- Criterio > Regole e criteri > Regole di routing
- Fare clic su + Aggiungi

	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 - Regole Di Routing

- Aggiungi regola di routing

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

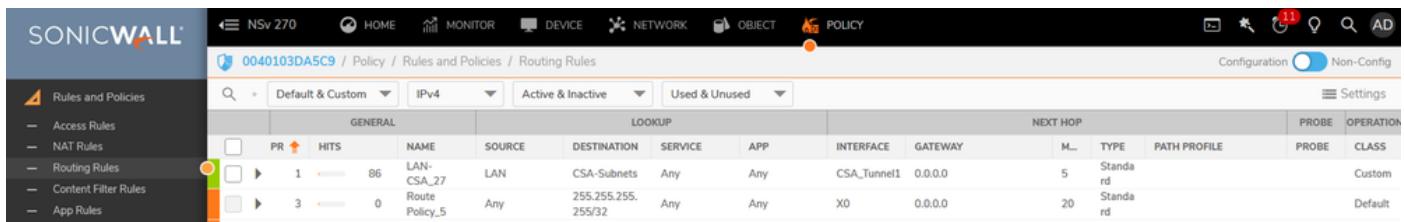
Interface: CSA_Tunnel1

Gateway: 0.0.0.0/0

Metric: 5

Show Diagram Cancel Add

- Fare clic su + Aggiungi



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 - Regole Di Routing

Aggiungi regole di accesso

Passare al dashboard di Sonicwall.

- Criterio > Regole e criteri > Regole di accesso
- Fare clic su + Aggiungi

Sonicwall - Rules and Policies / 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

+ Add Edit Delete + Move Enable Disable Live Counters Reset Counters Displaying 42 of 69 rules

Sonicwall - Regole di accesso

Adding Rule

Name	CSA-Inbound-Allow	Action	<input checked="" type="button"/> Allow <input type="button"/> Deny <input type="button"/> Discard			
Description	Access rule to allow CSA subnets (RAVPN and CgNAT) to access the internal network/s	Type	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6			
		Priority	Manual 1			
		Schedule	Always			
		Enable	<input checked="" type="checkbox"/>			
Source / Destination		User & TCP/UDP	Security Profiles	Traffic Shaping	Logging	Optional Settings
<div style="display: flex; justify-content: space-between;"> <div style="flex: 1;"> SOURCE <div style="display: flex; justify-content: space-between;"> <div>Zone/Interface: <input type="text" value="VPN"/></div> <div>Address: <input type="text" value="CSA-Subnets"/></div> <div>Port/Services: <input type="text" value="Any"/></div> </div> </div> <div style="flex: 1;"> DESTINATION <div style="display: flex; justify-content: space-between;"> <div>Zone/Interface: <input type="text" value="LAN"/></div> <div>Address: <input type="text" value="LAN"/></div> <div>Port/Services: <input type="text" value="Any"/></div> </div> </div> </div>						
<div style="display: flex; justify-content: space-between; align-items: center;"> Show Diagram <input type="checkbox"/> <input type="button"/> Cancel <input checked="" type="button"/> Add </div>						

- Fare clic su +Aggiungi

Sonicwall - Rules and Policies / 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 - Regole di accesso

Verifica

- Stato tunnel su accesso sicuro

The screenshot shows the 'Network Tunnel Groups' section for 'SonicWall-NTG'. It includes a summary table with region (US (Pacific Northwest)), routing type (Static Routing), and device type (Other). The 'Primary Hub' section shows 1 active tunnel (Hub Up) with details: Tunnel Group ID (SonicWall-VPN@), Data Center (sse-usw-2-1-1), and IP Address (44.228.138.150). The 'Secondary Hub' section shows 0 active tunnels (Hub Down) with details: Tunnel Group ID (SonicWall-VPN@f), Data Center (sse-usw-2-1-0), and IP Address (52.35.201.56). A table below lists network tunnels, showing one entry for 'Primary 1' with Peer ID 131073, Peer Device IP Address 76.39.159.129, Data Center Name sse-usw-2-1-1, Data Center IP Address 44.228.138.150, Status Connected, and Last Status Update Jul 06, 2025 4:11 PM.

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

Accesso sicuro - Gruppo tunnel di rete - Stato VPN

- Stato del tunnel su Sonicwall Firewall

The screenshot shows the 'IPSec VPN / Rules and Settings' page on the Sonicwall NSv 270. The left sidebar has categories like System, Firewall, VoIP, DNS, SDWAN, and IPSec VPN (selected). The main area shows an 'Active Tunnels' tab with an IPv4 filter selected. A table lists one tunnel: SonicWall-CSA, created on 07/06/2025 at 08:42:48, with local range 0.0.0.0 - 255.255.255.255 and remote range 0.0.0.0 - 255.255.255.255, gateway 44.228.138.150, and comment blank.

#	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 - Stato VPN IPSec

La stessa procedura può essere utilizzata per configurare il tunnel tra il data center secondario di Secure Access e Sonicwall

Ora che il tunnel è attivo su Secure Access e Sonicwall, è possibile continuare a configurare l'accesso alle risorse private tramite RA-VPN, Browser-Based ZTA o Client Based ZTA su Secure Access Dashboard

Risoluzione dei problemi

PC utente

- Verificare che l'utente sia in grado o meno di connettersi/registrarsi a RAVPN/ZTNA. In caso contrario, risolvere ulteriormente il problema relativo alla mancata connessione del control plane.
- Verificare che la rete a cui l'utente sta tentando di accedere debba passare attraverso il tunnel RAVPN o ZTNA. In caso contrario, verificare la configurazione sull'headend.

Accesso sicuro

- Verificare la configurazione della direzione del traffico nel profilo di connessione RAVPN per confermare che la rete di destinazione è configurata per l'invio tramite il tunnel a Secure Access.
- Verificare che la risorsa privata sia definita con porte/protocolli validi e che i meccanismi di connessione ZTNA/RAVPN siano selezionati.
- Verificare che i criteri di accesso siano configurati in modo da consentire agli utenti RAVPN/ZTNA di accedere alla rete di risorse private e che i criteri siano ordinati in modo che nessun'altra regola abbia la precedenza per bloccare il traffico.
- Verificare che il tunnel IPSec sia attivo e che Accesso sicuro visualizzi le route client valide tramite il routing statico che copre le risorse private a cui l'utente sta tentando di accedere.

Sonicwall

- Verificare che il tunnel IPSec sia attivo o meno (IKE & IPSec SA).
- Verificare che le route del client siano annunciate correttamente.
- Verificare che il traffico proveniente dall'utente RAVPN/ZTNA e destinato a una risorsa privata dietro Sonicwall stia raggiungendo il firewall di Sonicwall attraverso il tunnel acquisendo i pacchetti su Sonicwall.
- Verificare che il traffico abbia raggiunto la risorsa privata e rispondere al client RAVPN/ZTNA o meno. In caso affermativo, verificare che i pacchetti stiano raggiungendo l'interfaccia X0 (LAN) di Sonic.
- Verificare che Sonicwall stia inoltrando il traffico di ritorno attraverso il tunnel IPSec verso l'accesso sicuro.

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Cisco Secure Access Help Center](#)
- [Zero Trust Access Module](#)
- [Errore Di Risoluzione Dei Problemi Relativi All'Accesso Sicuro: Il Servizio Di Registrazione Non Risponde. Contatta il tuo help desk IT"](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuracy di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).