

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

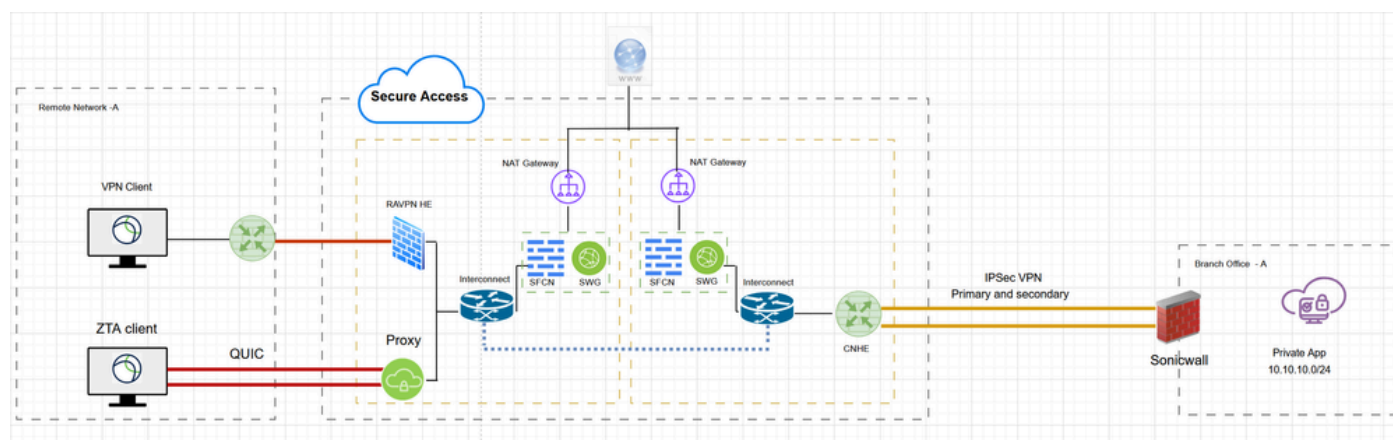
Le informazioni fornite in questo documento si basano su:

- 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



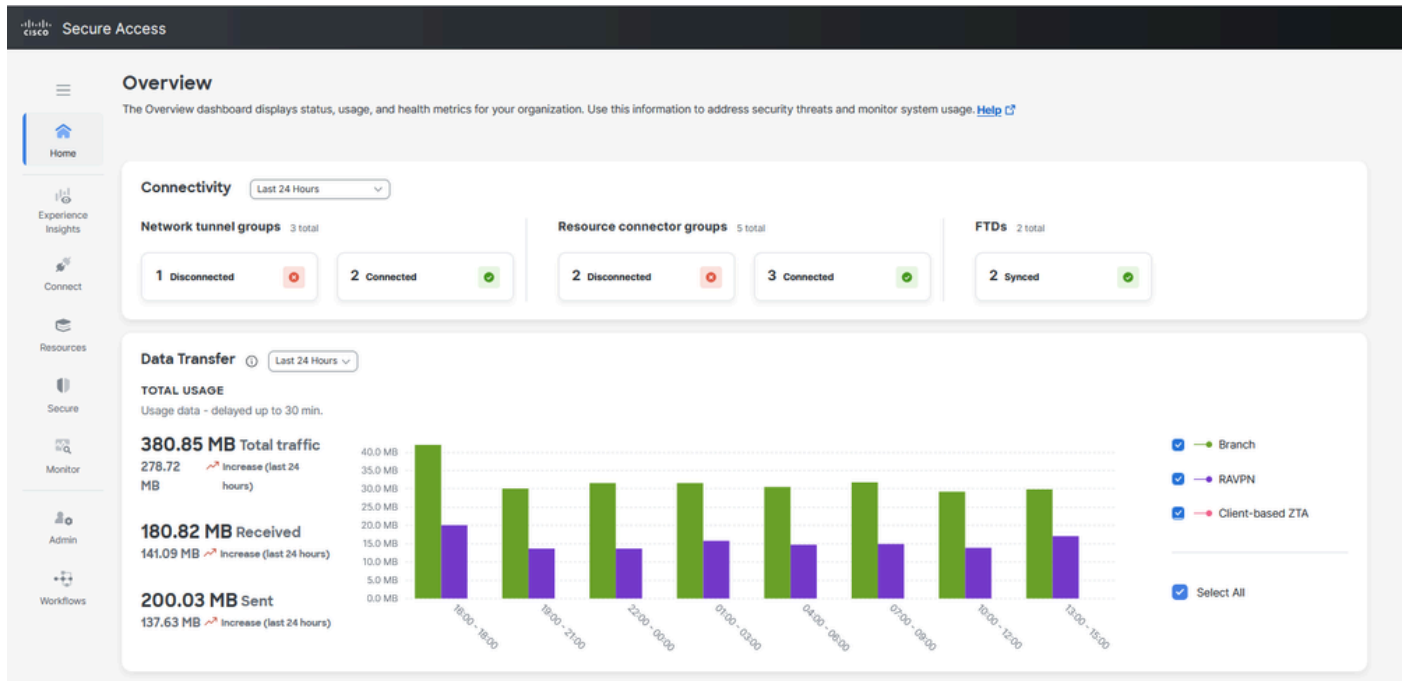
Esempio di rete

Configurazione

Configura Network Tunnel Group (VPN) su Secure Access

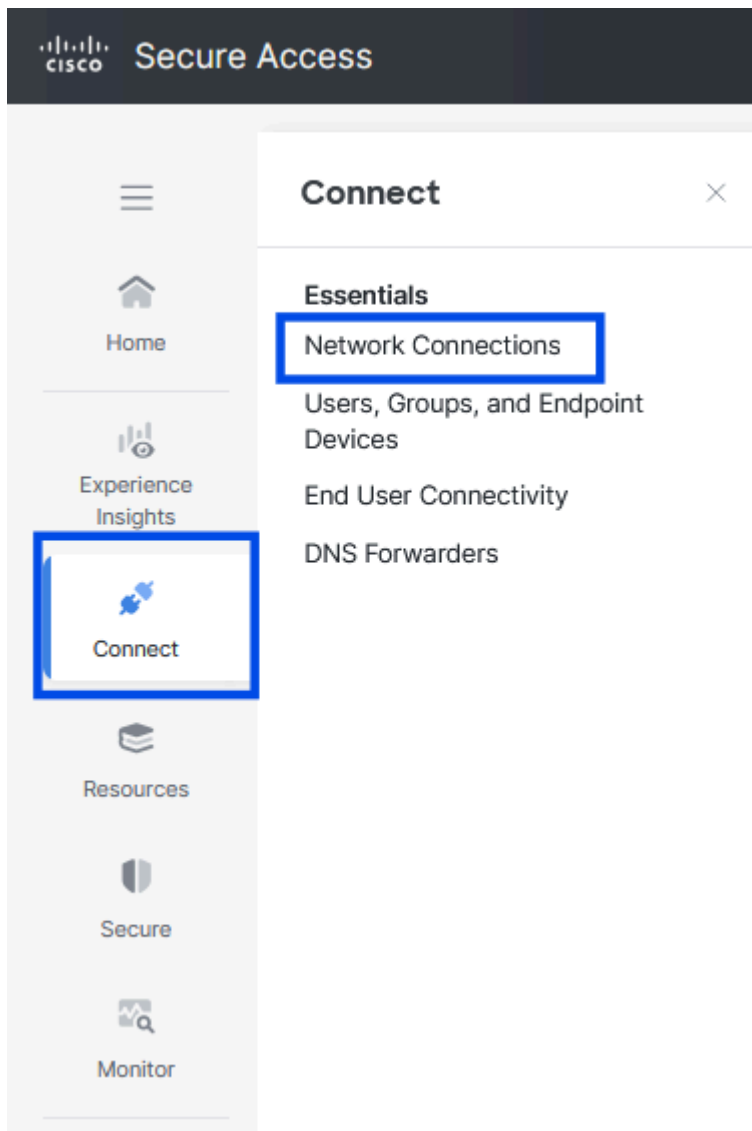
Per configurare il tunnel VPN tra Secure Access e Sonicwall

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



Secure Access - Pagina principale

- Fare clic su **Connect > Network Connections**



Accesso sicuro - Connessioni di rete

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

The image shows the 'Network Connections' page in the Cisco Secure Access interface. The left navigation menu is the same as in the first image. The main content area has a title 'Network Connections' and a description. Below the title are tabs for 'Connector Groups', 'Network Tunnel Groups' (highlighted with a blue box), and 'FTDs'. A summary box for 'Network Tunnel Groups' shows 2 total, with 0 Disconnected, 0 Warning, and 2 Connected. Below this is a table of 'Network Tunnel Groups' with columns: Network Tunnel Group, Status, Region, Primary Hub Data Center, Primary Tunnels, Secondary Hub Data Center, and Secondary Tunnels. The table lists two groups: 'AZURE' and 'LAB-BGP', both with a 'Connected' status. An '+ Add' button (highlighted with a blue box) is 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' in a blue box.

- 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.

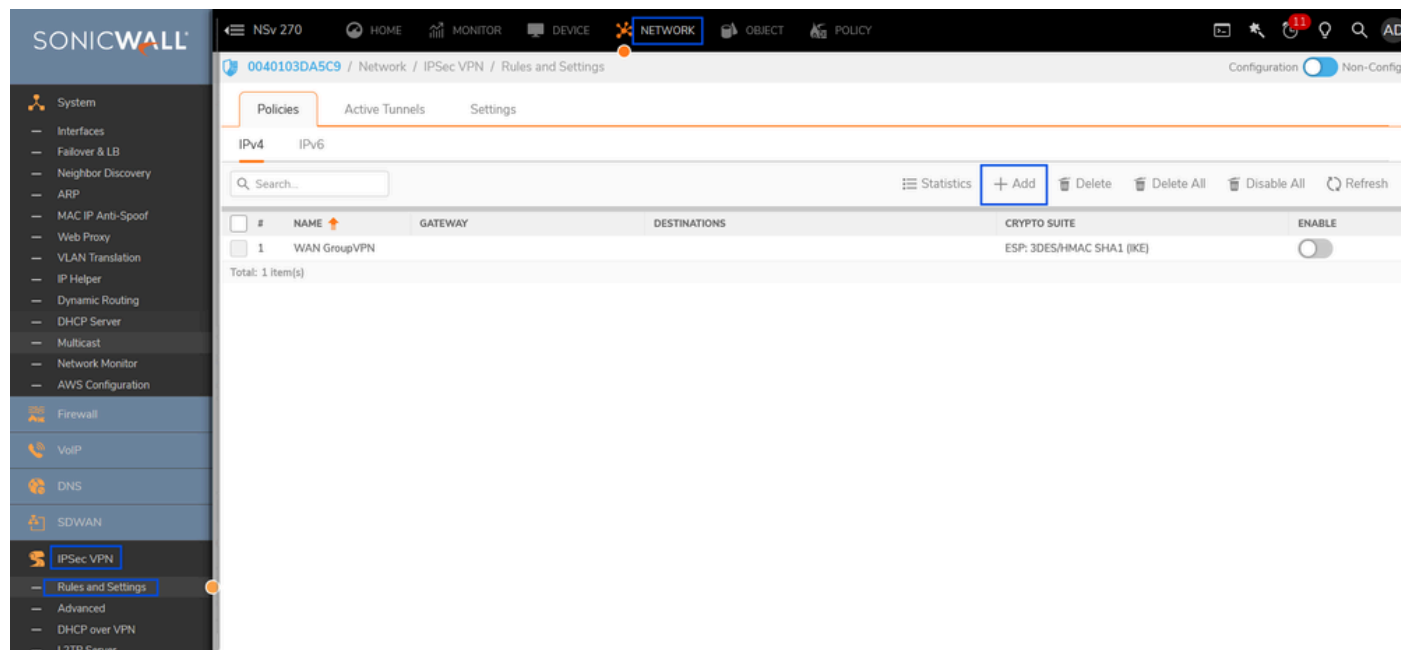
Dopo aver fatto clic su Save (Salva), vengono visualizzate le informazioni sul tunnel. Salvare le informazioni per il passaggio di configurazione successivo

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



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

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

- 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

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 - 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

USER LOGIN

HTTPS



Pina



HTTP



HTTPS



Cancel

OK

- Fare clic su OK.

The screenshot shows the SonicWall management interface. The left sidebar contains a menu with options like System, Interfaces, Firewall, and DNS. The main area displays the 'Interface Settings' for 'CSA_Tunnel1'. The table below lists the configured interfaces.

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 - 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

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 - Oggetto - Oggetti Address

Address Object Settings

Name ⓘ

Zone Assignment ▼

Type ▼

Network


Netmask / Prefix Length

Cancel

Save


- Fare clic su Salva.

Address Object Settings

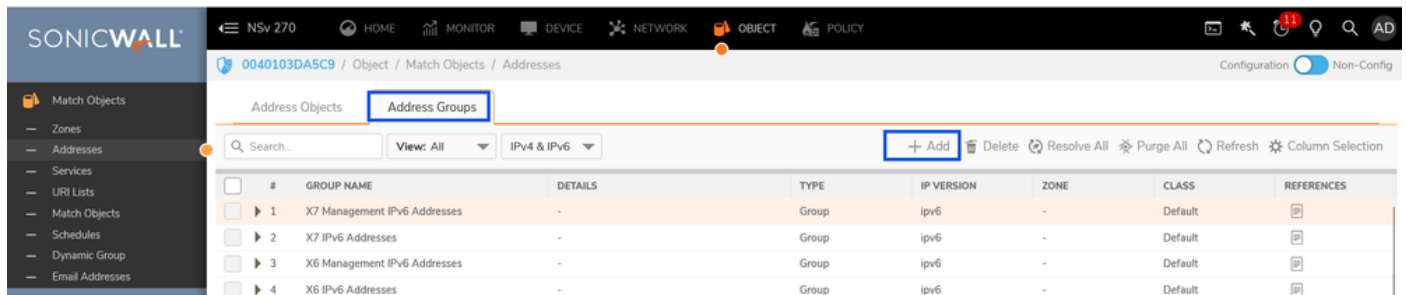
Name	<input type="text" value="CgNAT"/>	
Zone Assignment	<input type="text" value="VPN"/>	▼
Type	<input type="text" value="Network"/>	▼
Network	<input type="text" value="100.64.0.0"/>	
Netmask / Prefix Length	<input type="text" value="255.192.0.0"/>	
<input type="button" value="Cancel"/>		<input type="button"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

- Fare clic su Salva.

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"/>

- 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

Q RAV

No Data

In Group 2 items

Q

CgNAT[NW]

RAVPNUser-Pool[NW]

Cancel

Save

- Fare clic su Salva.

Aggiungi route

Passare al dashboard di Sonicwall.

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

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 - Regole Di Routing

- Aggiungi regola di routing

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

- Fare clic su + Aggiungi

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 - Regole Di Routing

Aggiungi regole di accesso

Passare al dashboard di Sonicwall.

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

SONICWALL												
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY												
0040103DA5C9 / Policy / Rules and Policies / Access Rules												
Configuration Non-Config												
Q * 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	Any	All	None	Always
	13 (A)	0	Default Access Rule_122	→	WAN	WAN	Any	X1 IP	Any	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

Sonicwall - Regole di accesso

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

Zone/Interface

VPN

Address

CSA-Subnets

Port/Services

Any

DESTINATION

Zone/Interface

LAN

Address

LAN

Port/Services

Any

Show Diagram

☐

Cancel

Add

- Fare clic su +Aggiungi

SONICWALL												
NSv 270 HOME MONITOR DEVICE NETWORK OBJECT POLICY												
0040103DA5C9 / Policy / Rules and Policies / Access Rules												
Configuration Non-Config												
Q CSA * 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	CSA-Inbound-Allow_127	→	VPN	LAN	CSA-Subnets	LAN	Any	All	None	Always

Sonicwall - Regole di accesso

Verifica

- Stato tunnel su accesso sicuro

← 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

Accesso sicuro - Gruppo tunnel di rete - Stato VPN

- Stato del tunnel su 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)

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'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).