

Configurazione di Secure Access con Secure Firewall Threat Defense per l'accesso privato con routing basato su criteri

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione accesso sicuro](#)

[Configurazione gruppo tunnel di rete](#)

[Secure Access Routing](#)

[Policy Based Routing](#)

[Salva configurazione gruppo tunnel di rete](#)

[Crea una risorsa privata](#)

[Creare una regola dei criteri di accesso](#)

[Configurazione Secure Firewall Threat Defense \(FTD\)](#)

[Configurazione interfacce tunnel virtuale](#)

[Configurazione tunnel IPsec](#)

[Configurazione routing FTD](#)

[Policy-Based Routing](#)

[Configurazione criteri di accesso](#)

[Verifica](#)

[Verifica in FTD](#)

[Stato tunnel in FTD](#)

[Verifica in accesso sicuro](#)

[Stato tunnel in accesso sicuro](#)

[Eventi in accesso sicuro](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Secure Access con FTD tramite IPsec per l'accesso privato sicuro con routing basato su criteri.

Prerequisiti

Requisiti

- Conoscenze Cisco Secure Access
- Dashboard/tenant Cisco Secure Access
- Protezione sicura delle minacce firewall e conoscenza di Centro gestione firewall
- Conoscenza IPSec
- Conoscenze di Routing basate su policy

Componenti usati

- Secure Firewall con codice 7.7.10
- Centro gestione firewall distribuito tramite cloud. La configurazione è valida anche per un tipico FMC virtuale
- Dashboard Cisco Secure Access

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

I tunnel di rete in Secure Access possono essere utilizzati per due scopi principali: Accesso sicuro a Internet e accesso sicuro privato.

Per garantire la protezione dell'accesso privato, le organizzazioni possono utilizzare Zero Trust Access (ZTA) e/o VPN as a Service (VPNaaS) per connettere gli utenti a risorse private quali applicazioni interne o centri dati. I tunnel IPsec svolgono un ruolo chiave in questa architettura grazie alla crittografia protetta del traffico di rete tra gli utenti e le risorse private, che assicura la protezione dei dati sensibili durante l'attraversamento di reti non attendibili. Integrando i tunnel IPsec con ZTA o VPNaaS, le organizzazioni possono fornire un accesso semplice e sicuro alle risorse interne, mantenendo al contempo controlli di sicurezza e visibilità affidabili.

In questo documento viene descritto come configurare Secure Access con Secure Firewall Threat Defense (FTD) tramite IPsec per Secure Private Access.

In questa guida viene inoltre descritto come configurare il routing basato su criteri.

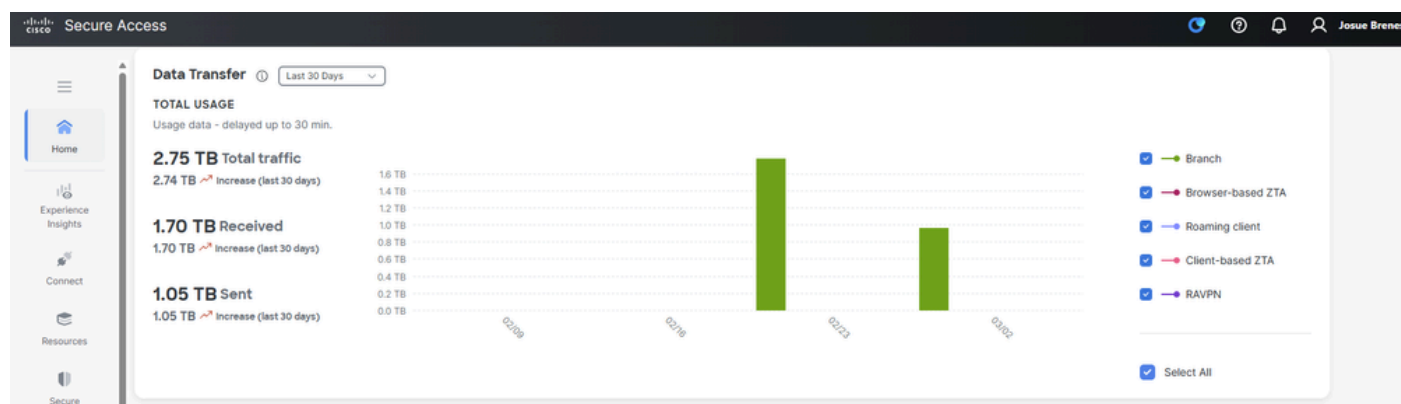
Anche se questo documento descrive la configurazione dei tunnel IPsec per l'accesso privato sicuro, la configurazione di Zero Trust Access (ZTA) o VPN as a Service (VPNaaS) per l'accesso alle applicazioni private esula dalle finalità di questa guida.

Configurazione

Configurazione accesso sicuro

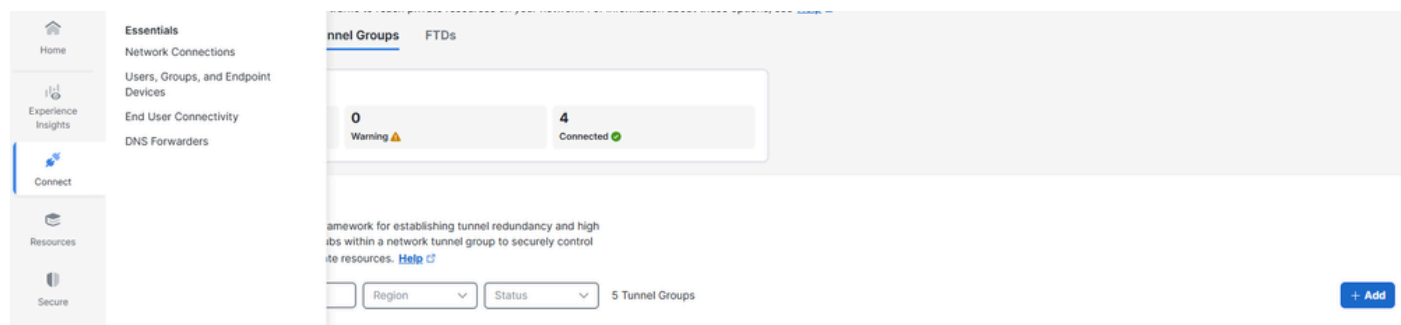
Configurazione gruppo tunnel di rete

1. Passare al pannello di amministrazione di [Accesso sicuro](#).



2. Aggiungere un gruppo di tunnel di rete.

- Fai clic su **Connect** > Network Connections
 - In **Network Tunnel Groups** clic su **> Add**



3. General Settings Configurazione.

- Configurare Tunnel Group Name, **Region** e Device Type
 - Fare clic su **Next**

1 General Settings

2 Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

General Settings

Give your network tunnel group a good meaningful name, choose type this tunnel group will use.

Tunnel Group Name

FTD

Region

Canada (Central)

Device Type

FTD

Impostazioni generali

4. Configurare Tunnel ID e Passphrase.

- Configurare l'**Tunnel ID** e **Passphrase**. Questo ID è importante, in quanto è necessario per la configurazione FTD
- Fare clic su **Next**

✓ General Settings

✓ Tunnel ID and Passphrase

3 Routing

4 Data for Tunnel Setup

Tunnel ID and Passphrase

Configure the tunnel ID and pa

Tunnel ID Format

☒ Email ☐ IP Address

Tunnel ID

ftd1-ipsec

Passphrase

.....

The passphrase must be between special characters.

Confirm Passphrase

.....

ID e PSK

5. Configurare il routing statico.

Secure Access Routing

Policy Based Routing

Aggiungere le reti protette dall'FTD a cui si desidera che gli utenti remoti accedano tramite ZTA e/o VPNaaS e fare clic su **Salva**.

- Fai clic su **Routing** > **Static routing**
 - Aggiungere gli intervalli di indirizzi IP o gli host configurati nella rete e passare il traffico attraverso l'accesso sicuro, quindi fare clic su **Add**
 - Fare clic su **Save**

CSA Static Routing

Salva configurazione gruppo tunnel di rete

Scaricare e salvare i dati di configurazione del tunnel come richiesto per la configurazione FTD.

- Fare clic su **Download CSV**
- Fare clic su **Done**

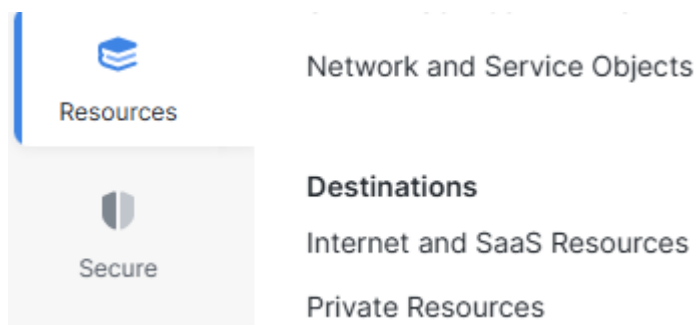
Dati NTG

Crea una risorsa privata

Le risorse private sono applicazioni interne, reti o subnet ospitate nel centro dati o in un ambiente cloud privato. Queste risorse non sono accessibili pubblicamente e sono protette dietro l'infrastruttura dell'organizzazione.

Definendole come risorse private in Secure Access, è possibile abilitare l'accesso controllato tramite soluzioni quali Zero Trust Access (ZTA) o VPN as a Service (VPNaaS). In questo modo gli utenti possono connettersi in modo sicuro ai sistemi interni in base all'identità, alla postura del dispositivo e alle policy di accesso, senza esporre le risorse direttamente a Internet.

Passare a **Resources > Private Resources** > fare clic su **Add**.



PR

- Specificare il **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Specificare porte e protocolli e aggiungere ulteriori risorse private in base alle esigenze
- Selezionare il tipo di connessione desiderato *Connection Method* in base alle proprie esigenze, ad esempio connessioni Zero Trust e/o VPN, in base alle proprie esigenze
- Fare clic su *Save*

Private Resource Name

Description (optional)

Private resource address
Define how the private resource will connect to applications through Secure Access.

Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H... ▼	8080

Risorsa privata

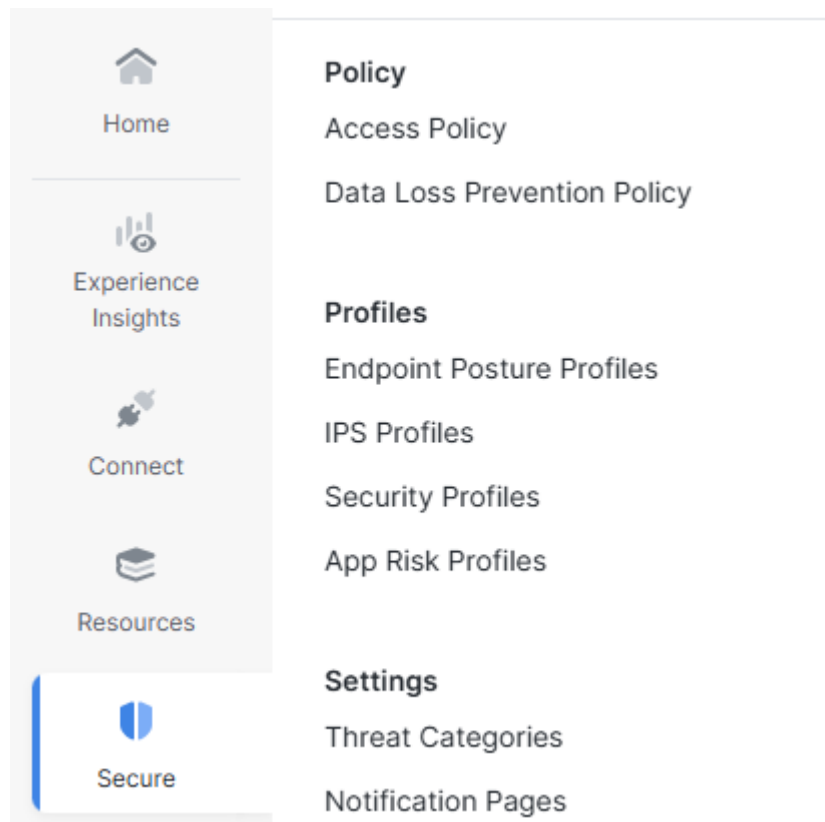
Creare una regola dei criteri di accesso

Le regole di accesso privato definiscono il modo in cui gli utenti possono connettersi in modo sicuro alle risorse e alle applicazioni interne non accessibili pubblicamente.

Queste regole applicano la sicurezza controllando gli utenti che possono accedere a risorse private specifiche in base a fattori quali l'identità degli utenti, l'appartenenza ai gruppi, la postura dei dispositivi, la posizione o altre condizioni dei criteri. Ciò garantisce che i sistemi interni sensibili rimangano protetti dall'accesso del pubblico generale, pur rimanendo al contempo disponibili in

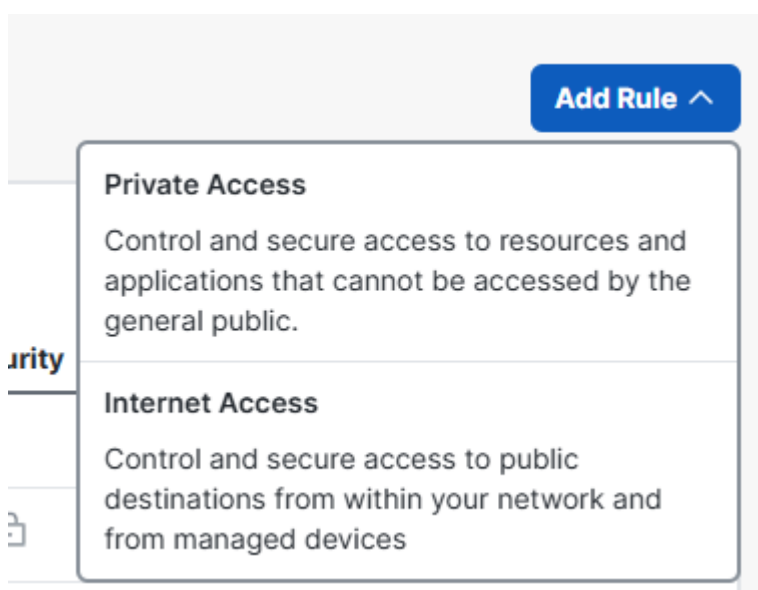
modo sicuro per gli utenti autorizzati tramite ZTA o VPNaaS.

Passa a Secure>Access Policy



ACP

- Fare clic su **Add Rule**
 - Fare clic su **Private Access**



Aggiungi ACP

- Fai clic su **Rule Name** e assegna un nome

- Fare clic su **Action**, selezionare **Allow** per autorizzare il traffico
- Fare clic su **From** uno e specificare gli utenti a cui vengono concesse le autorizzazioni
- Fare clic su **To** e specificare l'accesso di tali utenti in base a questa regola
- Fare clic su **Next**, quindi **Save** nella pagina successiva

Rule name ⓘ

FTD IPsec Rule

Rule order

1

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#) ⓘ

Action

✓ Allow

Allow specified traffic if security requirements are met.

✗ Block

Block specified traffic.

From

Specify one or more sources

AD Users • Josue

To

Specify one or more destinations

Private Resources • FTD Internal Server

+ AND

Endpoint Requirements

For VPN connections:

End-user endpoint devices that are connected to the network using VPN may be able to access destinations specified in this rule. ⓘ

Endpoint requirements are configured in the VPN posture profile. Requirements are evaluated at the time the endpoint device connects to the network. [VPN Posture Profiles](#) ⓘ

For Branch connections:

Endpoint device posture is not evaluated for endpoints connecting to these resources from a branch network.

2 Configure Security

Configure security requirements that must be met before traffic is allowed. [Help](#) ⓘ

Cancel

Back Next

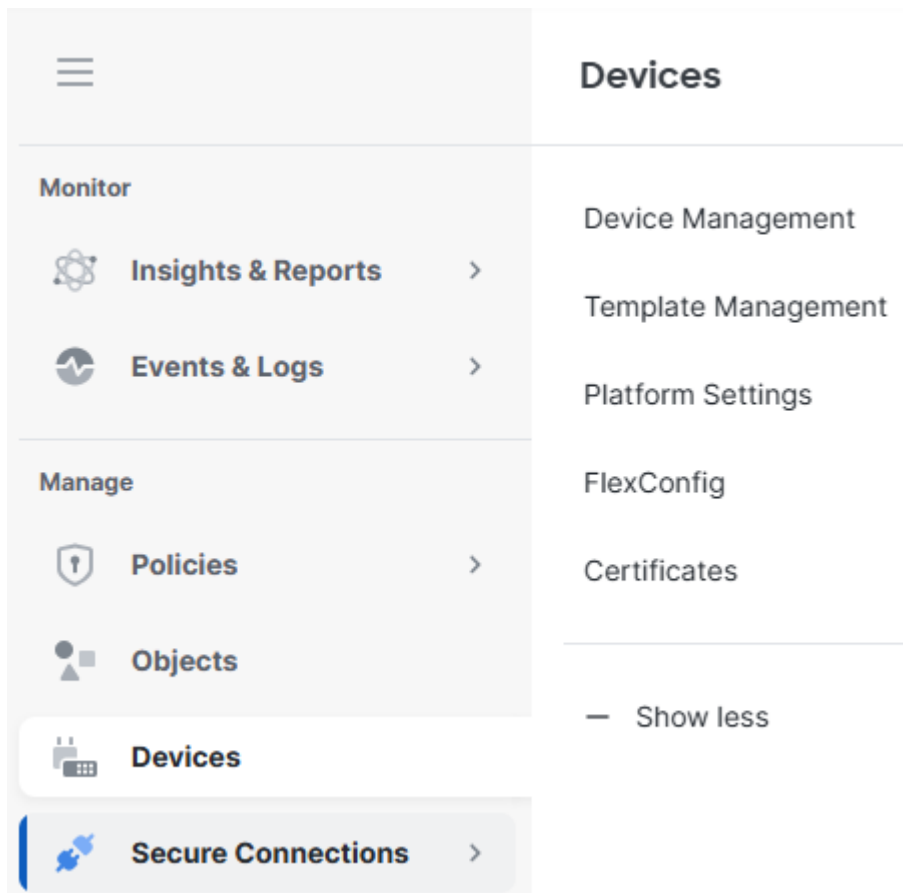
Configurazione ACP

Configurazione Secure Firewall Threat Defense (FTD)

Configurazione interfacce tunnel virtuale

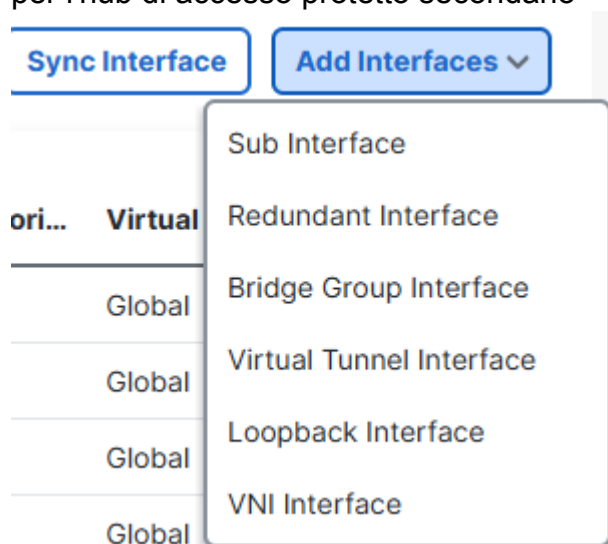
Una VTI (Virtual Tunnel Interface) su FTD è un'interfaccia logica di layer 3 utilizzata per configurare i tunnel VPN IPsec basati su route.

1. Passare a **Devices** > **Device Management**.



Dispositivi FTD

- Fare clic sul dispositivo FTD, **Interfaces**
 - Fare clic su **Add Interfaces**
 - Fare clic su **Virtual Tunnel Interface**
 - Creare due interfacce tunnel virtuali, una per l'hub di accesso protetto primario e l'altra per l'hub di accesso protetto secondario



Aggiungi VTI

Virtual Tunnel Interface 1:

- Dai un nome, fai clic su **Enable**

- Selezionare o creare un Security Zone
- Fare clic su Tunnel ID e assegnare un valore.
- Fare clic su Tunnel Source e specificare l'interfaccia WAN da cui verrà stabilito il tunnel
- Fare clic su IPsec Tunnel Mode, selezionare IPv4
- Fare clic su IP Address e configurare l'indirizzo IP per la VTI
- Fare clic su OK

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-1

☒ Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

1

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

VTI 1.1

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

☒ Configure IP

169.254.0.1/30



Virtual Tunnel Interface 2:

- Dai un nome, fai clic su **Enable**
- Selezionare o creare un **Security Zone**
- Fare clic su **Tunnel ID** e assegnare un valore
- Fare clic su **Tunnel Source** e specificare l'interfaccia WAN da cui verrà stabilito il tunnel
- Fare clic su **IPsec Tunnel Mode**, selezionare IPv4
- Fare clic su **IP Address** e configurare l'indirizzo IP per la VTI
- Fare clic su **OK**

Tunnel Type

☒ Static ☐ Dynamic

Name:*

VTI-2

☒ Enabled

Description:

Security Zone:

zone_vti

Priority:

0

(0 - 65535)

Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:*

2

(0 - 10413)

Tunnel Source:*

GigabitEthernet0/0 (outside)

192.168.0.20

IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:*

☒ IPv4 ☐ IPv6

IP Address:*

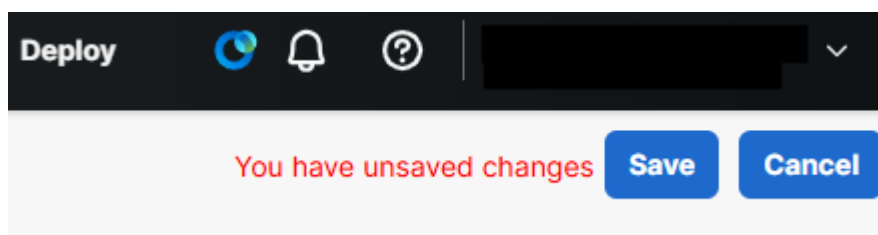
☒ Configure IP

169.254.0.5/30



VTI 2.2

- Fare clic su Save.

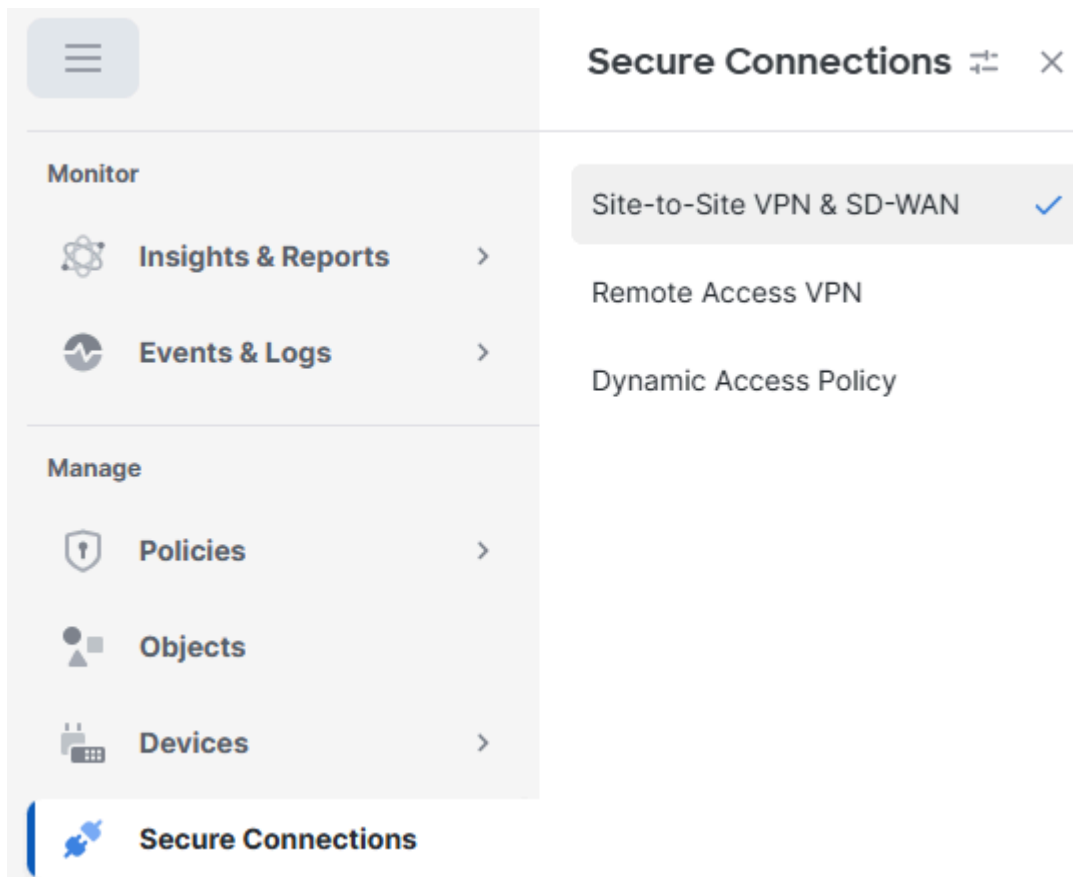


Salva modifiche VTI

Configurazione tunnel IPsec

Passare al dashboard di cdFMC.

- Fai clic su [Secure Connection](#) > [Site-to-Site VPN & SD-WAN](#)



S2S

- Fare clic su **Add**
 - Fare clic su **Route-Based VPN**
 - Fare clic su **Peer to Peer**

Last Updated: 12:56 PM [Refresh](#) [NAT Exemptions](#) [Add](#)

Create VPN Topology

Topology name *

CSA

VPN Type

☐ **SD-WAN Topology**
Simplifies and automates the VPN and routing configuration in a hub and spoke topology, enabling SD-WAN capabilities.

Select VPN Topology

☐ ☒ Hub and Spoke

[Prerequisites](#)

☒ **Route-Based VPN**
Secures traffic dynamically between peers based on routing over Virtual Tunnel Interfaces.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ **Policy-Based VPN**
Secures traffic between peers based on a static policy using protected networks.

Select VPN Topology

☐ ☒ Hub and Spoke

☐ ☒ Peer to Peer

☐ ☒ Full Mesh

☐ **SASE Topology**

⚠ SASE Topology cannot be selected because Cisco Umbrella Connection is not configured.

[Prerequisites](#)

[Refresh](#)

[Cancel](#) [Create](#)

Aggiungi VPN

- Dal passaggio 5 della configurazione Secure Access, ottenere gli ID e gli indirizzi IP del

tunnel per i data center primario e secondario

- Fare clic su Endpoints
 - In Node A, fare clic su Device uno e selezionare Extranet
 - Fai clic Device Name e assegna un nome
 - Fare clic su Endpoint IP Addresses e immettere gli indirizzi IP primario e secondario di Secure Access separati da una virgola (da "Save Network Tunnel Group Configuration") in Secure Access Configurazione)
 - In Node B, fare clic su Device e selezionare il dispositivo FTD
 - Fare clic su Virtual Tunnel Interface e selezionare la prima interfaccia VTI creata nel passaggio precedente
 - Fare clic sull'opzione Send Local Identity to Peers e selezionare Email ID, immettere l'ID del tunnel primario (da "Save Network Tunnel Group Configuration" in Secure Access Configurazione)
 - Fare clic su Add Backup VTI
 - Fare clic su Virtual Tunnel Interface e selezionare la seconda interfaccia VTI creata nel passaggio precedente
 - Fare clic su Send Local Identity to Peers un'opzione e selezionare Email ID, immettere l'ID del tunnel secondario (da "Save Network Tunnel Group Configuration" in Secure Access Configurazione)
 - Fare clic su Salva

Network Topology:

IKE Version:* ☐ IKEv1 ☒ IKEv2

[Endpoints](#)
[IKE](#)
[IPsec](#)
[Advanced](#)

Node A

Device:*

Extranet
▼

Device Name*:

CSA

Endpoint IP Address*:

Primary-IP,Secondary-IP

Node B

Device:*

cdFTD-1
▼

Virtual Tunnel Interface:*

VTI-1 (IP: 169.254.0.1)
▼
+

Tunnel Source: outside (IP: 192.168.0.20)[Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

Backup VTI: Remove

Virtual Tunnel Interface:*

VTI-2 (IP: 169.254.0.5)
▼
+

Tunnel Source: outside (IP: 192.168.0.20)[Edit VTI](#)

☐ Tunnel Source IP is Private

☒ Send Local Identity to Peers

Local Identity Configuration*

Email ID
▼

ftd1-ipsec@

[Cancel](#)
[Save](#)

Configurazione VTI FTD

- Fare clic su **IKE**
 - Fare clic su **IKEv2 Settings** > Policies
 - Selezionare l'**Umbrella-AES-GCM-256** opzione
 - Fare clic su **OK**

IKEv2 Policy



Available IKEv2 Policy  +

AES-GCM-NUL-SHA

AES-GCM-NUL-SHA-LA...

AES-SHA-SHA

AES-SHA-SHA-LATEST

DES-SHA-SHA

DES-SHA-SHA-LATEST

Umbrella-AES-GCM-256

Add

Selected IKEv2 Policy

Umbrella-AES-GCM-256 

Cancel

OK

Criterio IKEv2

- Fare clic su Authentication Type e selezionare Pre Shared Manual Key, immettere il PSK configurato in Secure Access (passphrase)

Endpoints

IKE

IPsec

Advanced

Pre-shared Key Length:*

24

Characters (Range 1-127)

IKEv2 Settings

Policies:*

Umbrella-AES-GCM-256 

Authentication Type:

Pre-shared Manual Key

▼

Key:*

.....

Confirm Key:*

.....

☐

 Enforce hex-based pre-shared key only

IKE

- Fare clic su IPSEC
 - Fare clic su IKEv2 Proposals
 - Seleziona Umbrella-AES-GCM-256
 - Fare clic su OK

EndpointsIKEIPsecAdvanced

Crypto Map Type:

☒ Static☐ Dynamic

IKEv2 Mode:

Tunnel

Transform Sets:

IKEv1 IPsec ProposalsIKEv2 IPsec Proposals*

tunnel_aes256_sha

Umbrella-AES-GCM-...

IPSec

Cancel

OK

Salva proposte IKEv2

Configurazione routing FTD

Policy-Based Routing (PBR) consente di controllare l'inoltro del traffico in base a criteri diversi dall'indirizzo IP di destinazione. Anziché basarsi esclusivamente sulla tabella di routing, PBR può indirizzare il traffico in base all'origine, all'applicazione, al protocollo, alle porte o ad altri criteri definiti.

Ciò consente alle organizzazioni di indirizzare il traffico specifico o ad alta priorità sui collegamenti preferiti (ad esempio, un collegamento Internet diretto o ad ampia larghezza di banda), ottimizzare le prestazioni e suddividere in modo sicuro le applicazioni selezionate senza inviare tutto il traffico attraverso un tunnel VPN.

Policy-Based Routing

- Passa a Objects
 - Fare clic su Access List
 - Fare clic su Extended
 - Fare clic su Add Extended Access List

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

AAA Server

Access List

Extended

Service Access

Standard

Address Pools

Application Filters

AS Path

BFD Template

Cipher Suite List

Extended

An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-identifies traffic based on destination on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route map

Add Extended Access List

Name

Value

Aggiungi ACL

Creare un elenco di controllo di accesso esteso (ACL) che corrisponda alla rete di origine protetta dall'FTD (ad esempio, 172.16.15.0/24) da inviare tramite il tunnel. Per la destinazione, aggiungere le reti utilizzate da ZTA (intervallo CGNAT) e la rete utilizzata dalla VPNaaS (selezionare Pool IP rete privata virtuale).

Name

CSA_ACL

Entries (1)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	 Allow	Subnet-172.16.15.0	Any	CSA-Management CSA-VPNaaS CSA-ZTA	Any

ACL

- Fai clic su **Devices** > **Device Management**

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Devices

Device Management

Template Management

Platform Settings

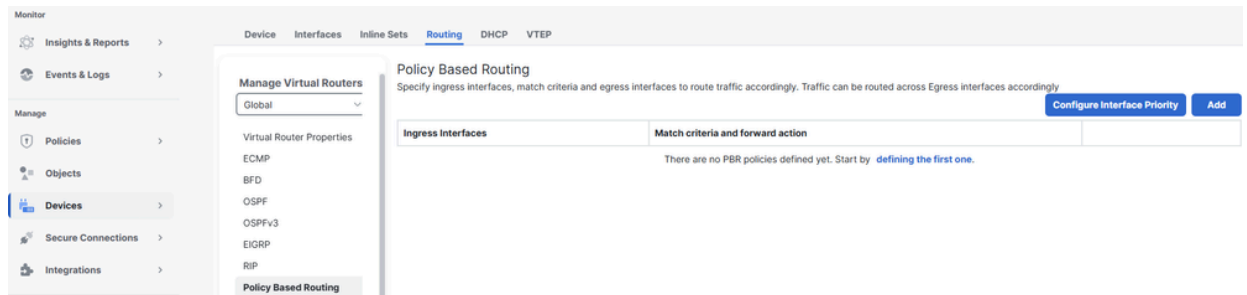
FlexConfig

Certificates

Show less

Sul dispositivo bootflash o slot0:

- Fare clic sull'FTD
 - Fare clic su Routing
 - Fare clic su Policy Based Routing
 - Fare clic su Add



Aggiungi PBR

- Fare clic su Ingress Interface e selezionare l'interfaccia in entrata da cui entra il traffico delle reti interne
- In Criteri di corrispondenza e interfaccia in uscita fare clic su Add

Add Policy Based Route



A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface *

Match Criteria and Egress Interface

Specify forward action for chosen match criteria.

Add

Interfaccia in ingresso

- Fare clic su Match ACL e selezionare l'ACL esteso creato in precedenza
- Fare clic su Send To and select IP Address
- Fare clic su IPv4 Addresses e impostare come hop successivo gli indirizzi IP nelle subnet dell'interfaccia VTI configurate in precedenza nell'FTD (169.254.0.2 e 169.254.0.6)
- Fare clic su Save

Match ACL: *



Send To: *

IPv4 Addresses:

[Cancel](#)[Save](#)

Salva PBR

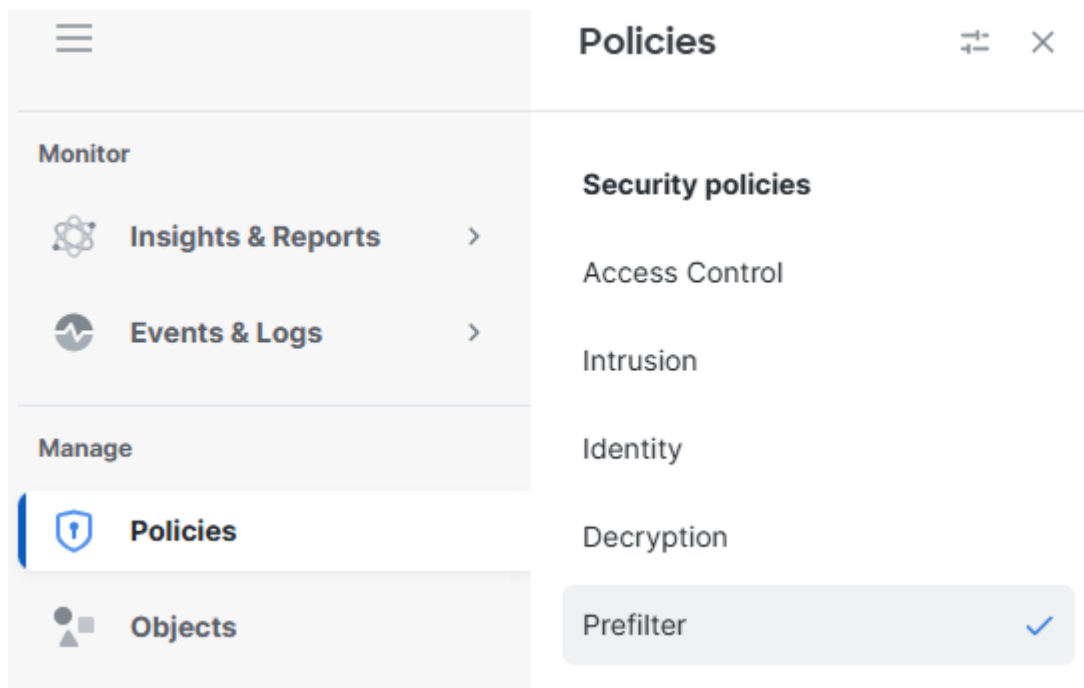
Assicuratevi di selezionare l'opzione **Send To > IP Address** e non l'Egress Interface opzione.

Configurazione criteri di accesso

Per consentire il traffico su un Cisco Firepower Threat Defense (FTD) e l'accesso a risorse private, il traffico deve prima passare attraverso la fase iniziale di controllo dell'accesso nota come prefiltro.

La prefiltrazione viene elaborata prima di un'ispezione più approfondita ed è progettata per essere semplice e veloce. Valuta il traffico utilizzando criteri di base dell'intestazione esterna (come le porte e gli indirizzi IP di origine e destinazione) per consentire, bloccare o ignorare rapidamente il traffico. Quando il traffico è autorizzato in questa fase, può ignorare ispezioni che richiedono un uso intensivo delle risorse, come ad esempio l'ispezione approfondita dei pacchetti o le policy di intrusione, migliorando le prestazioni e mantenendo il controllo della sicurezza.

- Passa a **Policies > Prefilter**



Filtro preliminare

- Fare clic per modificare il criterio di prefiltro utilizzato dal criterio di accesso



Prefilter Policy	Domain	Last Modified	
Default Prefilter Policy Default Prefilter Policy with default action to allow all tunnels	Global	2025-07-24 08:27:51 Modified by "admin"	 
Prefilter - Josue	Global	2026-02-18 15:26:37 Modified by	 

fare clic su prefiltro

- Fare clic su Add Tunnel Rule
 - Aggiungere e autorizzare il traffico dalla rete VPNaaS e/o dalla subnet ZTA alle risorse private
 - Fare clic su Save



#	Name	Rule Type	Source Interface Objects	Destination Interface Objects	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone	
1	CSA Rule	Prefilter	zone_vti (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na	 

Salva regola

A questo punto, una volta completata e verificata la configurazione sull'FTD, è possibile procedere con la distribuzione. Dopo la distribuzione, i tunnel IPSec vengono visualizzati correttamente, a conferma che è stata stabilita una connettività protetta alle risorse private.

Verifica

Verifica in FTD

Stato tunnel in FTD

È possibile visualizzare lo stato corrente del tunnel, specificando anche se è attivo o inattivo. Ciò consente di verificare che il tunnel IPsec sia stato stabilito correttamente.

- Fare clic su Secure Connections.
- Fai clic su VPN da sito a sito e SD-WAN.
- Fare clic sul nome della topologia.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-1 (169.254.0.1)
EXTRANET Extranet			FTD cdFTD-1	outside (192.168.0.20)	VTI-2 (169.254.0.5)

Stato tunnel FTD

Verifica in accesso sicuro

Stato tunnel in accesso sicuro

È possibile visualizzare lo stato corrente del tunnel, specificando tra l'altro se è disconnesso, in avviso o connesso. Ciò consente di verificare che il tunnel IPsec sia stato stabilito correttamente.

- Fare clic su Connect > Network Connections
- Fare clic su Network Tunnel Groups

Home

Experience Insights

Connect

Resources

Secure

Essentials

Network Connections

Users, Groups, and Endpoint Devices

End User Connectivity

DNS Forwarders

Network Tunnel Groups

FTDs

0 Warning

4 Connected

Framework for establishing tunnel redundancy and high availability within a network tunnel group to securely control network resources. [Help](#)

Region

Status

5 Tunnel Groups

+ Add

Controlla NTG

- Fare clic su Network Tunnel Group

Summary

Connected

Region

Canada (Central)

Routing Type

Static Routing

Device Type

FTD

IP Address Range

172.16.15.0/24

Last Status Update

Feb 18, 2026 3:34 PM

Primary Hub

See Logs

Hub Up

1 Active Tunnels

Tunnel Group ID

ftd1-ipsec@

Secondary Hub

Hub Up

1 Active Tunnels

Tunnel Group ID

Eventi in accesso sicuro

È possibile visualizzare gli eventi del tunnel e verificare che lo stato dei tunnel IPsec sia attivo e stabile.

Fare clic su Monitor > Network Connectivity.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Monitoraggio registri conn

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

Search Text: FTD

Reset All

Network tunnel group	Data center IP address	Hub type	Region	Alerts	Service	Device type	Details	Time (UTC)
FTD		Secondary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:07 PM
FTD		Secondary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:07 PM
FTD		Primary	ca-central-1	Info	BGP	FTD	BGP peer up	Feb 18, 2026 4:06 PM
FTD		Primary	ca-central-1	Info	IKE	FTD	Successful CHILD re...	Feb 18, 2026 4:06 PM

Passare a su Monitor > Ricerca attività.

Home

Experience Insights

Connect

Resources

Secure

Monitor

Monitor

×

Reports

Remote Access Logs

Activity Search

Connectivity Logs

Security Activity

Total Requests

Activity Volume

App Discovery

Private Resource Discovery

Top Destinations

Top Categories

Third-Party Apps

Cloud Malware

Data Loss Prevention

AI Supply Chain

Monitoraggio registri conn

Su uno qualsiasi degli eventi correlati, fare clic su View Full Details (Visualizza dettagli completi).

13,606 Total

Page: 1 Results per page: 50 1 - 50 < >

Source	Rule Identity ⓘ	Destination	
Josue	Josue		View Full Details
Josue	Josue		Filter by Josue
Josue	Josue		Filter by
Josue	Josue		Filter by
Josue	Josue		View Rule
Josue	Josue		Edit Rule
Josue	Josue		

Dettagli completi

Event Details

×

Action

Allowed

Time

Feb 18, 2026 3:30 PM

Rule Name

FTD IPsec Rule (2386307)

Enforced By

-

Source

 Josue

Source IP

-

Destination

http://172.16.15.55:8080/favicon.ico

Security Group Tag (SGT)

-

Destination IP

172.16.15.55

Ricerca attività

Informazioni correlate

- [Supporto tecnico Cisco e download](#)
- [Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center, 7.7](#)

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).