

Konfigurieren von sicherem Zugriff mit sicherem Firewall-Schutz für privaten Zugriff mit richtlinienbasiertem Routing

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfiguration des sicheren Zugriffs](#)

[Konfiguration der Netzwerk-Tunnelgruppe](#)

[Sicheres Access Routing](#)

[Richtlinienbasiertes Routing](#)

[Netzwerk-Tunnelgruppenkonfiguration speichern](#)

[Erstellen einer privaten Ressource](#)

[Erstellen einer Zugriffsrichtlinienregel](#)

[Konfiguration der sicheren Firewall-Bedrohungsabwehr \(FTD\)](#)

[Konfiguration der virtuellen Tunnelschnittstellen](#)

[IPsec-Tunnelkonfiguration](#)

[FTD-Routing-Konfiguration](#)

[Richtlinienbasiertes Routing](#)

[Konfiguration der Zugriffsrichtlinie](#)

[Überprüfung](#)

[In FTD überprüfen](#)

[Tunnelstatus in FTD](#)

[Überprüfung in sicherem Zugriff](#)

[Tunnelstatus bei sicherem Zugriff](#)

[Ereignisse in sicherem Zugriff](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit FTD über IPsec für sicheren privaten Zugriff mit richtlinienbasiertem Routing konfigurieren.

Voraussetzungen

Anforderungen

- Kenntnisse zu Cisco Secure Access
- Cisco Secure Access Dashboard/Tenant
- Sichere Firewall Threat Defense- und Firewall Management Center-Kenntnisse
- IPsec-Kenntnisse
- Richtlinienbasiertes Routing

Verwendete Komponenten

- Sichere Firewall mit Code 7.7.10
- Cloud-fähiges Firewall-Management-Center. Konfiguration gilt auch für typisches virtuelles FMC
- Cisco Secure Access Dashboard

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

Netzwerkunnel in Secure Access können für zwei primäre Zwecke verwendet werden: Sicherer Internetzugriff und sicherer privater Zugriff

Für einen sicheren privaten Zugriff können Unternehmen ZTA (Zero Trust Access) und/oder VPN-as-a-Service (VPNaaS) nutzen, um Benutzer mit privaten Ressourcen wie internen Anwendungen oder Rechenzentren zu verbinden. IPsec-Tunnel spielen eine Schlüsselrolle in dieser Architektur, indem sie den Netzwerkverkehr zwischen Benutzern und privaten Ressourcen sicher verschlüsseln und sicherstellen, dass vertrauliche Daten geschützt bleiben, während sie nicht vertrauenswürdige Netzwerke passieren. Durch die Integration von IPsec-Tunneln mit ZTA oder VPNaaS können Organisationen einen nahtlosen und sicheren Zugriff auf interne Ressourcen bereitstellen und gleichzeitig robuste Sicherheitskontrollen und Transparenz aufrechterhalten.

In diesem Dokument wird beschrieben, wie Sie sicheren Zugriff mit sicherem Firewall-Bedrohungsschutz (FTD) über IPsec für sicheren privaten Zugriff konfigurieren.

Darüber hinaus enthält dieses Handbuch die Schritte zum Konfigurieren von richtlinienbasiertem Routing.

Während in diesem Dokument die Konfiguration von IPsec-Tunneln für sicheren privaten Zugriff behandelt wird, wird die Einrichtung von ZTA (Zero Trust Access) oder VPN-as-a-Service (VPNaaS) für den Zugriff auf private Anwendungen in diesem Leitfaden nicht behandelt.

Konfigurieren

Konfiguration des sicheren Zugriffs

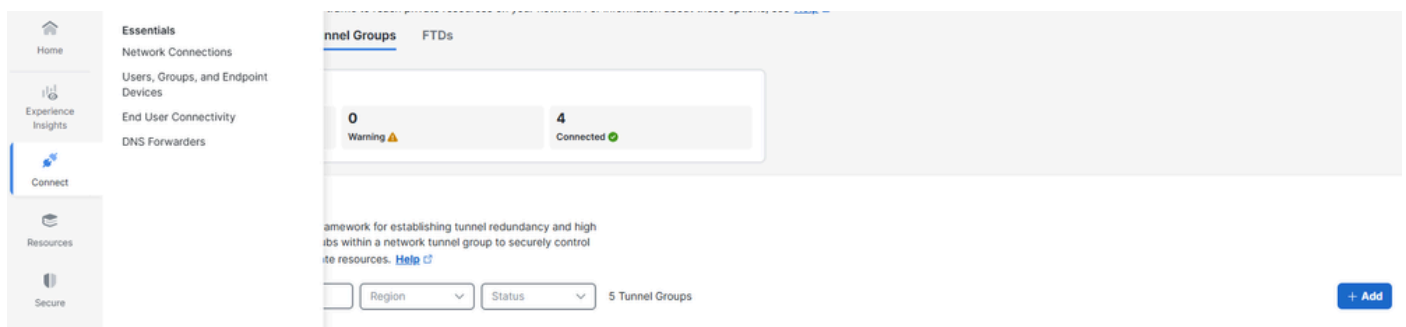
Konfiguration der Netzwerk-Tunnelgruppe

1. Navigieren Sie zum Admin-Bereich von [Sicherer Zugriff](#).



2. Hinzufügen einer Netzwerk-Tunnelgruppe

- Auf **Connect** > Network Connections
 - Klicken Sie unter Network Tunnel Groups > Add



3. General Settings Konfiguration

- Konfigurieren Sie Tunnel Group Name und **Region** und Device Type
 - Klicken Sie auf Next

- ✓ General Settings
- 2 Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

Allgemeine Einstellungen

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

4. Konfigurieren Tunnel ID und Passphrase.

- Konfigurieren Sie das **Tunnel ID** und **Passphrase**. Diese ID ist wichtig, da sie für die FTD-Konfiguration erforderlich ist.
- Klicken Sie **Next**

- ✓ General Settings
- ✓ Tunnel ID and Passphrase
- 3 Routing
- 4 Data for Tunnel Setup

ID und PSK

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

.....

5. Konfigurieren Sie statisches Routing.

Sicheres Access Routing

Richtlinienbasiertes Routing

Fügen Sie die durch die FTD geschützten Netzwerke hinzu, auf die Remote-Benutzer über ZTA und/oder VPNaaS zugreifen sollen, und klicken Sie auf Save (Speichern).

- Auf **Routing** > **Static routing**
 - Fügen Sie die IP-Adressbereiche oder Hosts hinzu, die Sie in Ihrem Netzwerk konfiguriert haben und den Datenverkehr über Secure Access weiterleiten möchten, und klicken Sie auf **Add**
 - Klicken Sie **Save**

Statisches CSA-Routing

Netzwerk-Tunnelgruppenkonfiguration speichern

Laden Sie die Tunnel-Einrichtungsdaten herunter, und speichern Sie sie, wie es für die FTD-Konfiguration erforderlich ist.

- Klicken Sie **Download CSV**
- Klicken Sie **Done**

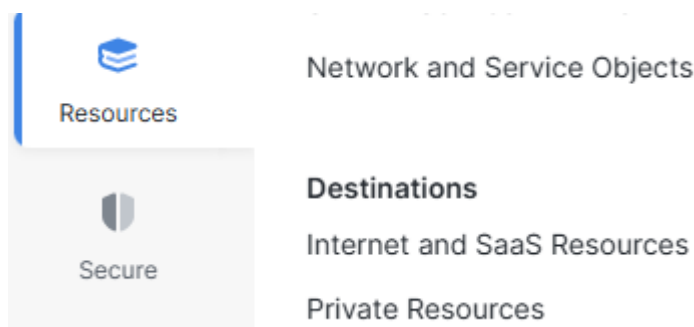
NTG-Daten

Erstellen einer privaten Ressource

Private Ressourcen sind interne Anwendungen, Netzwerke oder Subnetze, die in Ihrem Rechenzentrum oder Ihrer Private Cloud-Umgebung gehostet werden. Diese Ressourcen sind nicht öffentlich zugänglich und werden durch die Infrastruktur Ihres Unternehmens geschützt.

Durch die Definition als private Ressourcen im sicheren Zugriff können Sie einen kontrollierten Zugriff mithilfe von Lösungen wie ZTA (Zero Trust Access) oder VPN-as-a-Service (VPNaaS) ermöglichen. So wird sichergestellt, dass Benutzer basierend auf Identität, Gerätestatus und Zugriffsrichtlinien sicher auf interne Systeme zugreifen können, ohne die Ressourcen direkt dem Internet auszusetzen.

Navigieren Sie zu **Resources > Private Resources** und klicken Sie auf **Add**.



PR

- Geben Sie die **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Geben Sie Ports und Protokolle an, und fügen Sie bei Bedarf zusätzliche private Ressourcen hinzu.
- Wählen Sie je nach Bedarf die gewünschten **Connection Method** Verbindungen aus, z. B. Zero-Trust-Verbindungen und/oder VPN-Verbindungen.
- Klicken Sie **Save**

Private Resource Name

Description (optional)

Private resource address

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

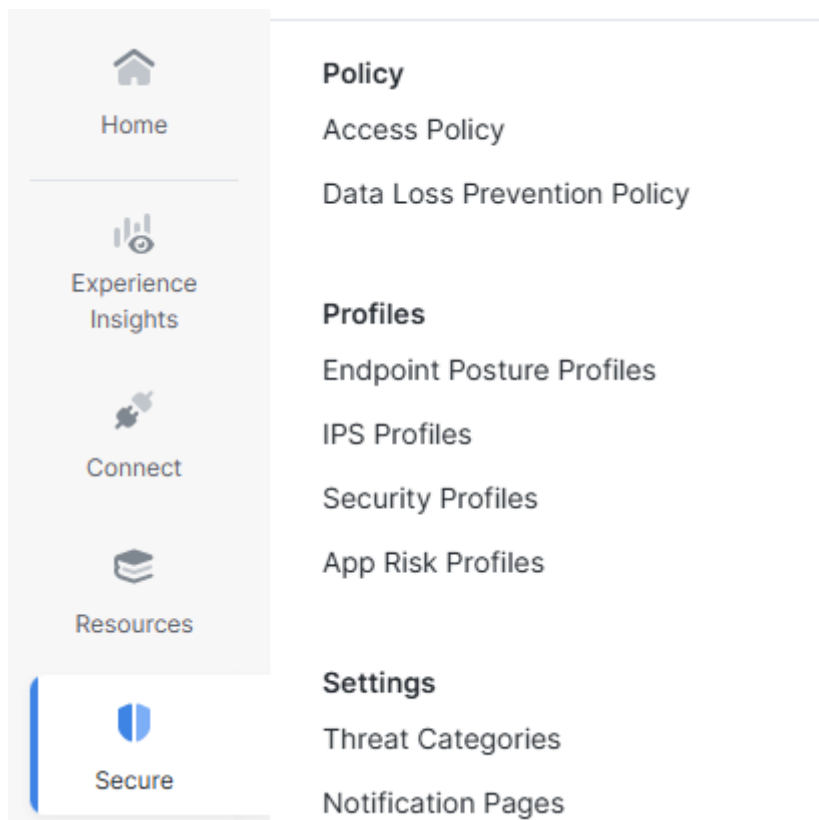
Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR) ⓘ	Protocol	Port / Ranges
172.16.15.55	TCP - (HTTP/H...	8080

Erstellen einer Zugriffsrichtlinienregel

Private Zugriffsregeln definieren, wie Benutzer eine sichere Verbindung zu internen Ressourcen und Anwendungen herstellen können, auf die nicht öffentlich zugegriffen werden kann.

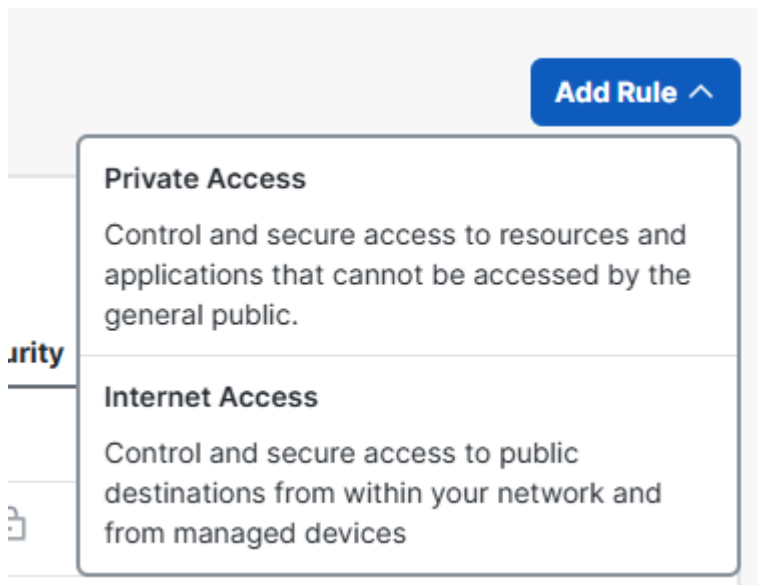
Mit diesen Regeln wird die Sicherheit durchgesetzt, indem gesteuert wird, wer auf bestimmte private Ressourcen zugreifen kann, und zwar basierend auf Faktoren wie der Benutzeridentität, der Gruppenmitgliedschaft, dem Gerätestatus, dem Standort oder anderen Richtlinienbedingungen. So wird sichergestellt, dass sensible interne Systeme vor dem allgemeinen öffentlichen Zugriff geschützt bleiben und gleichzeitig für autorisierte Benutzer über ZTA oder VPNaaS sicher verfügbar sind.

Navigieren Sie zu [Secure>Access Policy](#)



AKP

- Klicken Sie [Add Rule](#)
 - Klicken Sie [Private Access](#)



ACP hinzufügen

- Klicken Sie auf **Rule Name** , und geben Sie ihm einen Namen.
- Klicken Sie auf **Action**, und wählen Sie **Allow** aus, um diesen Datenverkehr zuzulassen.
- Klicken Sie auf **From** auf, und geben Sie die Benutzer an, denen die Berechtigung erteilt wurde.
- Klicken Sie auf **To** und geben Sie den Zugriff an, den diese Benutzer basierend auf dieser Regel haben.
- Klicken Sie auf **Next**, und dann **Save** in der nächsten Seite

Rule name ⓘ Rule order

FTD IPsec Rule 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 x

To
Specify one or more destinations

Private Resources • FTD Internal Server x

+ 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

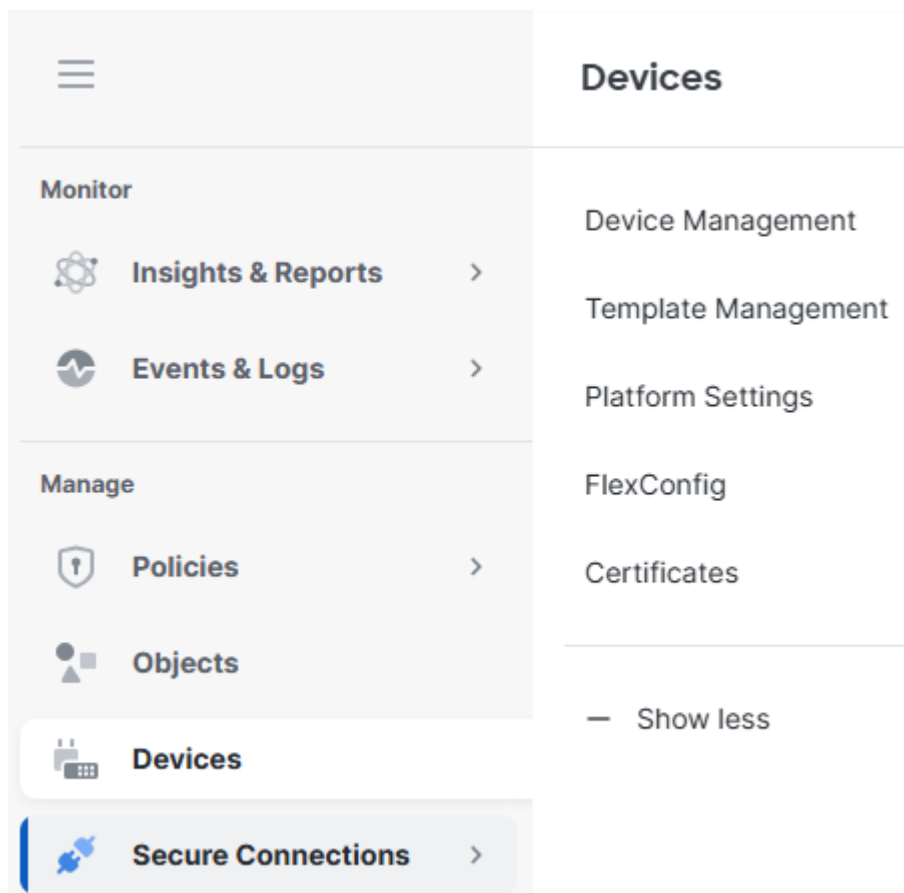
AKP-Konfiguration

Konfiguration der sicheren Firewall-Bedrohungsabwehr (FTD)

Konfiguration der virtuellen Tunnelschnittstellen

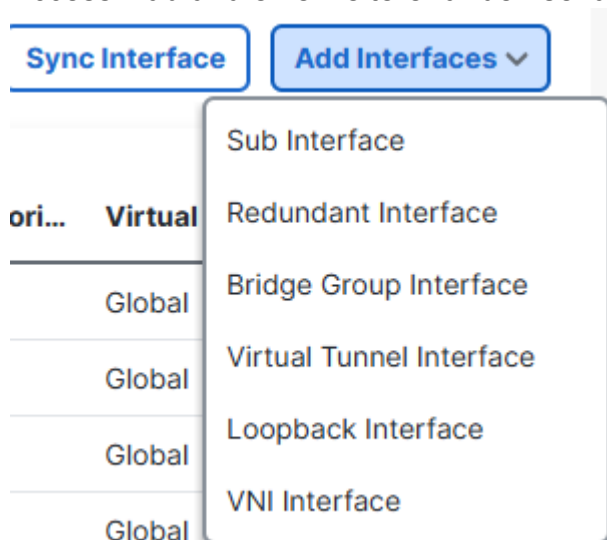
Eine Virtual Tunnel Interface (VTI) auf FTD ist eine logische Layer 3-Schnittstelle, die zum Konfigurieren von routenbasierten IPsec-VPN-Tunneln verwendet wird.

1. Navigieren Sie zu **Devices** > **Device Management**.



FTD-Geräte

- Klicken Sie auf das FTD-Gerät, **Interfaces**
 - Klicken Sie **Add Interfaces**
 - Klicken Sie **Virtual Tunnel Interface**
 - Erstellung von zwei virtuellen Tunnelschnittstellen, eine für den primären sicheren Access Hub und eine weitere für den sekundären sicheren Access Hub



Virtuelle Tunnelschnittstelle 1:

- Gib ihm einen Namen, klicke auf **Enable**
- Wählen oder erstellen Sie eine **Security Zone**
- Klicken Sie auf **Tunnel ID** und geben Sie ihm einen Wert.
- Klicken Sie auf **Tunnel Source** , und geben Sie die WAN-Schnittstelle an, von der der Tunnel erstellt werden soll.
- Klicken Sie auf **IPsec Tunnel Mode**, wählen Sie **IPv4**
- Klicken Sie auf **IP Address** , und konfigurieren Sie die IP-Adresse für den VTI.
- Klicken Sie **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

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



VTI1,2

Virtuelle Tunnelschnittstelle 2:

- Gib ihm einen Namen, klicke auf **Enable**
- Wählen oder erstellen Sie eine **Security Zone**
- Klicken Sie auf **Tunnel ID** , und geben Sie ihm einen Wert
- Klicken Sie auf **Tunnel Source** , und geben Sie die WAN-Schnittstelle an, von der der Tunnel erstellt werden soll.
- Klicken Sie auf **IPsec Tunnel Mode**, wählen Sie **IPv4**
- Klicken Sie auf **IP Address** , und konfigurieren Sie die IP-Adresse für den VTI.
- Klicken Sie **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

VTI 2.1

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:*

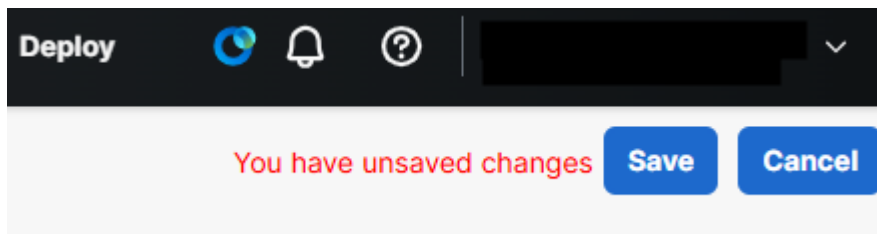
☒ Configure IP

169.254.0.5/30



VTI 2.2

- Klicken Sie auf Speichern.

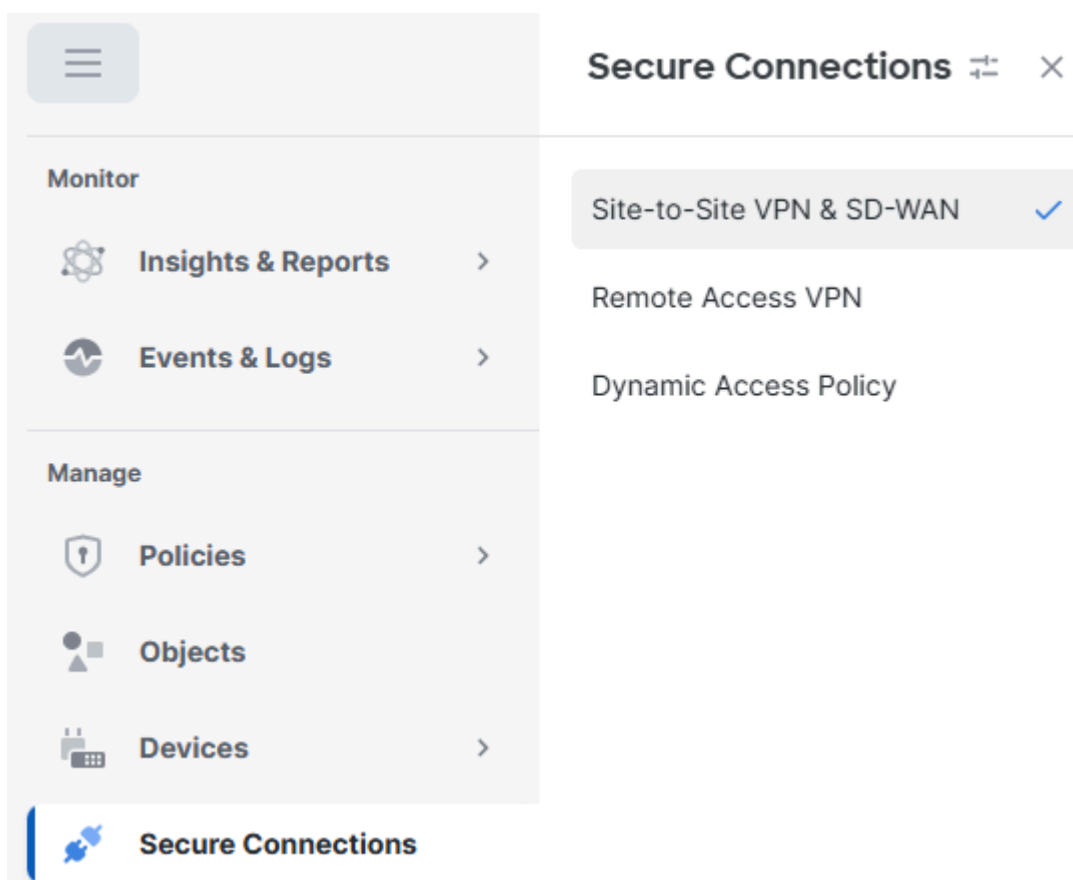


VTI-Änderungen speichern

IPsec-Tunnelkonfiguration

Navigieren Sie zu Ihrem cdFMC-Dashboard.

- Auf **Secure Connection** > **Site-to-Site VPN & SD-WAN**



S2S

- Klicken Sie **Add**
 - Klicken Sie **Route-Based VPN**
 - Klicken Sie **Peer to Peer**

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

Create VPN Topology

Topology name *

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](#)

New

☒ **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](#)

VPN hinzufügen

- Rufen Sie in Schritt 5 der Konfiguration für sicheren Zugriff die Tunnel-IDs und IP-Adressen für das primäre und sekundäre Rechenzentrum ab.
- Klicken Sie **Endpoints**
 - Klicken Sie unter **Node A** auf **Device** und wählen Sie **Extranet**.
 - Klicken Sie auf **Device Name** und geben Sie ihm einen Namen.
 - Klicken Sie auf **Endpoint IP Addresses**, und geben Sie die primäre und sekundäre IP-Adresse für sicheren Zugriff durch ein Komma getrennt ein (aus "Save Network Tunnel Group Configuration" unter **Sicherer Zugriff**).
- Konfiguration)**
- Klicken Sie unter **Node B** auf **Device** und wählen Sie Ihr FTD-Gerät aus.
- Klicken Sie auf **Virtual Tunnel Interface**, und wählen Sie die erste im vorherigen Schritt erstellte VTI-Schnittstelle aus.
- Klicken Sie auf **Send Local Identity to Peers** Option und wählen Sie **Email ID**, geben Sie die primäre Tunnel-ID (aus "Save Network Tunnel Group Configuration" unter **Secure Access Configuration**)
- Klicken Sie **Add Backup VTI**
- Klicken Sie auf **Virtual Tunnel Interface**, und wählen Sie die zweite im vorherigen Schritt erstellte VTI-Schnittstelle aus.
- Klicken Sie auf **Send Local Identity to Peers** eine Option, und wählen Sie **Email ID**, geben Sie die sekundäre Tunnel-ID ein (unter "Save Network Tunnel Group Configuration" unter **Secure Access Configuration**).
- Klicken Sie auf **Speichern**

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

FTD VTI-Konfiguration

- Klicken Sie IKE
 - Auf IKEv2 Settings > klicken Policies
 - Wählen Sie die Umbrella-AES-GCM-256 Option
 - Klicken Sie 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

IKEv2-Richtlinie

- Klicken Sie auf **Authentication Type** , und wählen Sie **Pre Shared Manual Key**, geben Sie den PSK ein, der unter **Sicherer Zugriff (Passphrase)** konfiguriert wurde.

Endpoints **IKE** **IPsec** **Advanced**

Pre-shared Key Length:* 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

- Klicken Sie **IPSEC**
 - Klicken Sie **IKEv2 Proposals**
 - Auswählen **Umbrella-AES-GCM-256**
 - Klicken Sie **OK**

Endpoints
IKE
IPsec
Advanced

Crypto Map Type:
☒ Static
☐ Dynamic

IKEv2 Mode:
Tunnel

Transform Sets:
IKEv1 IPsec Proposals
IKEv2 IPsec Proposals*

tunnel_aes256_sha
Umbrella-AES-GCM-...

Cancel
OK

IPsec

IKEv2-Angebote speichern

FTD-Routing-Konfiguration

Mit richtlinienbasiertem Routing (Policy-Based Routing, PBR) können Sie die Weiterleitung von Datenverkehr anhand von Kriterien steuern, die über die Ziel-IP-Adresse hinausgehen. Der PBR verlässt sich nicht mehr ausschließlich auf die Routing-Tabelle, sondern kann den Datenverkehr basierend auf der Quelle, der Anwendung, dem Protokoll, den Ports oder anderen definierten Richtlinien routen.

Auf diese Weise können Unternehmen bestimmten oder vorrangigen Datenverkehr über bevorzugte Verbindungen (z. B. eine Verbindung mit hoher Bandbreite oder eine direkte Internetverbindung) steuern, die Leistung optimieren und bestimmte Anwendungen sicher ausbrechen, ohne den gesamten Datenverkehr über einen VPN-Tunnel zu senden.

Richtlinienbasiertes Routing

- Navigieren Sie zu Objects
 - Klicken Sie Access List
 - Klicken Sie Extended
 - Klicken Sie 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

ACL hinzufügen

Erstellen Sie eine erweiterte Zugriffskontrollliste (ACL), die mit dem durch den FTD geschützten Quellnetzwerk (z. B. 172.16.15.0/24) übereinstimmt, das durch den Tunnel gesendet werden soll. Fügen Sie als Ziel die von ZTA verwendeten Netzwerke (CGNAT-Bereich) und das von Ihrem VPNaaS verwendete Netzwerk hinzu (siehe IP-Pool des virtuellen privaten Netzwerks).

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

- Auf **Devices** > Device Management

Monitor

Insights & Reports

Events & Logs

Manage

Policies

Objects

Devices

Device Management

Template Management

Platform Settings

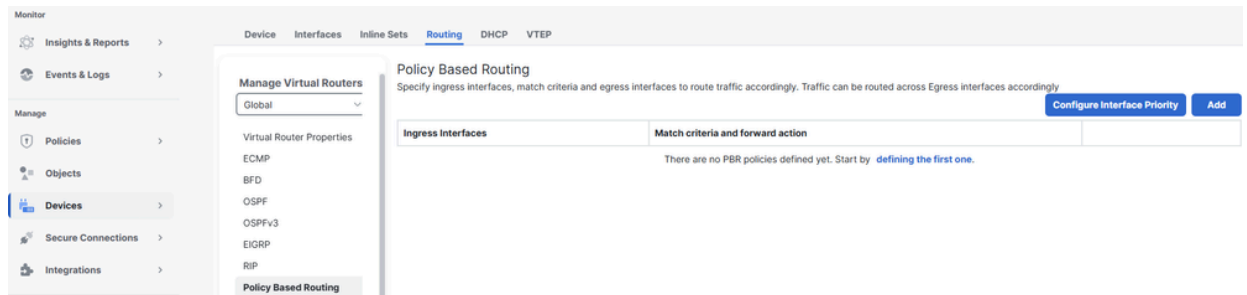
FlexConfig

Certificates

Show less

"Slot0:"

- Klicken Sie auf die FTD
 - Klicken Sie Routing
 - Klicken Sie Policy Based Routing
 - Klicken Sie Add



PBR hinzufügen

- Klicken Sie auf Ingress Interface , und wählen Sie die Eingangsschnittstelle aus, über die der Datenverkehr aus internen Netzwerken eingeht.
- Klicken Sie unter "Match Criteria" und "Egress Interface" auf 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

Eingangsschnittstelle

- Klicken Sie auf Match ACL , und wählen Sie die zuvor erstellte erweiterte Zugriffskontrollliste aus.
- Klicken Sie Send To and select IP Address
- Klicken Sie auf IPv4 Addresses , und legen Sie die IP-Adressen in den zuvor im FTD konfigurierten VTI-Schnittstellen-Subnetzen als nächste Hops fest (169.254.0.2 und 169.254.0.6).
- Klicken Sie Save

Match ACL: * +

Send To: *

IPv4 Addresses:

Richtlinienbasierte Konfiguration

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

PBR speichern

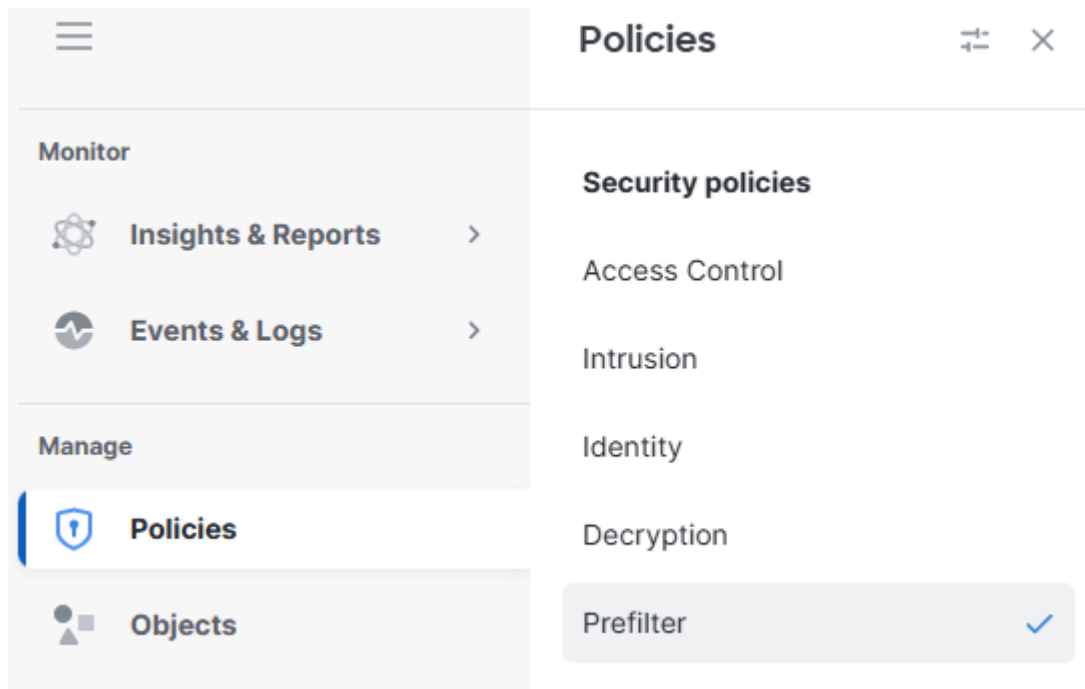
Stellen Sie sicher, dass Sie die Option **Send To > IP Address** und nicht die **Egress Interface** Option auswählen.

Konfiguration der Zugriffsrichtlinie

Um Datenverkehr über eine Cisco FirePOWER Threat Defense (FTD) zuzulassen und den Zugriff auf private Ressourcen zu ermöglichen, muss der Datenverkehr zunächst die erste Phase der Zugriffskontrolle passieren, die als Vorfilterung bezeichnet wird.

Die Vorfilterung wird vor der tiefer gehenden Prüfung verarbeitet und ist einfach und schnell konzipiert. Zur Bewertung des Datenverkehrs werden grundlegende Kriterien des äußeren Headers (wie Quell- und Ziel-IP-Adressen und -Ports) herangezogen, um Datenverkehr schnell zuzulassen, zu blockieren oder zu umgehen. Wenn der Datenverkehr in dieser Phase zugelassen wird, können ressourcenintensivere Prüfungen wie Deep Packet Inspection oder Intrusion Policies übersprungen werden, wodurch die Leistung verbessert und gleichzeitig die Sicherheitskontrolle aufrechterhalten wird.

- Navigieren Sie zu **Policies > Prefilter**



Vorfilter

- Klicken Sie auf die von Ihrer Zugriffsrichtlinie verwendete Vorfilterrichtlinie bearbeiten.

Prefilter Policy				New Policy
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		

Vorfilter anklicken

- Klicken Sie Add Tunnel Rule
 - Hinzufügen und Zulassen des Datenverkehrs aus dem VPNaaS-Netzwerk und/oder dem ZTA-Subnetz zu Ihren privaten Ressourcen
 - Klicken Sie Save

Prefilter - Josue											
Enter Description											
Rules											
Add Tunnel Rule Add Prefilter Rule Search Rules											
#	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	0

Regel speichern

Sobald die Konfiguration auf dem FTD abgeschlossen und verifiziert wurde, können Sie mit der

Bereitstellung fortfahren. Nach der Bereitstellung werden die IPsec-Tunnel erfolgreich hochgefahren und bestätigen, dass eine sichere Verbindung zu den privaten Ressourcen hergestellt ist.

Überprüfung

In FTD überprüfen

Tunnelstatus in FTD

Sie können den aktuellen Status des Tunnels anzeigen, einschließlich dessen, ob er aktiv oder inaktiv ist. Dadurch kann überprüft werden, ob der IPsec-Tunnel ordnungsgemäß eingerichtet ist.

- Klicken Sie auf Sichere Verbindungen.
- Klicken Sie auf Site-to-Site-VPN und SD-WAN.
- Klicken Sie auf den Topologienamen.

Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node ANode 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)

FTD-Tunnelstatus

Überprüfung in sicherem Zugriff

Tunnelstatus bei sicherem Zugriff

Sie können den aktuellen Status des Tunnels anzeigen, einschließlich ob er "Getrennt", "Warnung" oder "Verbunden" ist. Dadurch kann überprüft werden, ob der IPsec-Tunnel ordnungsgemäß eingerichtet ist.

- Klicken Sie auf Verbinden > Netzwerkverbindungen.
- Klicken Sie auf Network Tunnel Groups (Netzwerk-tunnelgruppen)

Home

Experience Insights

Connect

Resources

Secure

Essentials

Network Connections

Users, Groups, and Endpoint Devices

End User Connectivity

DNS Forwarders

nnel Groups

FTDs

0Warning

4Connected

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

Region

Status

5 Tunnel Groups

+ Add

NTG überprüfen

- Klicken Sie auf die Netzwerk-Tunnelgruppe.

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

CSA-Tunnelstatus

Ereignisse in sicherem Zugriff

Sie können Tunnel-Ereignisse anzeigen und überprüfen, ob der Status der IPsec-Tunnel aktiv und stabil ist.

Klicken Sie auf Monitor > Network Connectivity (Überwachen > Netzwerkverbindung).

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

Protokolle überwachen

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

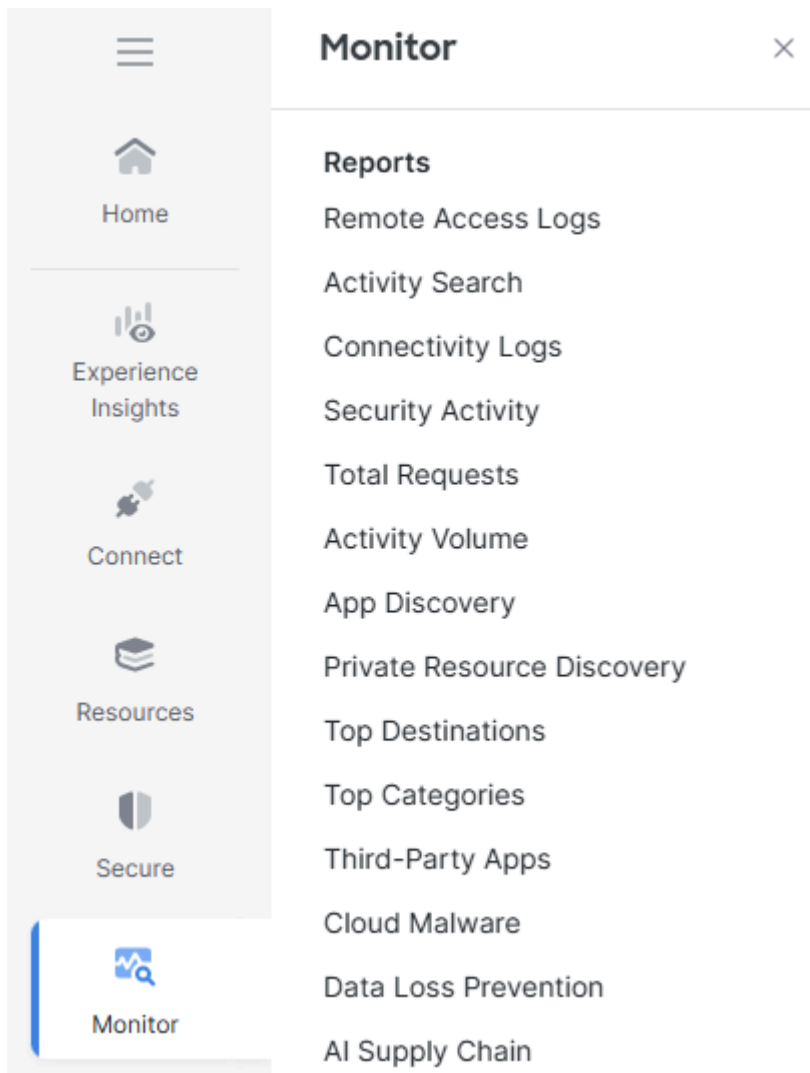
Search Text: FTD

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

Konn. Protokolle

Navigieren Sie zu auf Monitor > Activity Search.



Protokolle überwachen

Klicken Sie bei einem der verwandten Ereignisse auf Alle Details anzeigen.

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		

Vollständige Details

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

Aktivitätssuche

Zugehörige Informationen

- [Technischer Support und Downloads von Cisco](#)
- [Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 7.7](#)

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.