

Configuración del acceso seguro con Secure Firewall Threat Defence para el acceso privado con enrutamiento dinámico

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuración de Secure Access](#)

[Configuración del Grupo de Túnel de Red](#)

[Routing de acceso seguro](#)

[Routing dinámico \(BGP\)](#)

[Guardar configuración de grupo de túnel de red](#)

[Crear un recurso privado](#)

[Crear una regla de directiva de acceso](#)

[Configuración de Secure Firewall Threat Defence \(FTD\)](#)

[Configuración de Interfaces de Túnel Virtual](#)

[Configuración del túnel IPsec](#)

[Configuración de enrutamiento de FTD](#)

[Routing dinámico \(BGP\)](#)

[Configuración de política de acceso](#)

[Verificación](#)

[Verificar en FTD](#)

[Estado del túnel en FTD](#)

[Estado del túnel en Secure Access](#)

[Eventos en Secure Access](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar Secure Access con FTD a través de IPsec para Secure Private Access con Dynamic Routing.

Prerequisites

Requirements

- Conocimientos sobre Cisco Secure Access
- Panel/arrendatario de Cisco Secure Access
- Conocimiento de Secure Firewall Threat Defence y Firewall Management Center
- conocimiento de IPsec
- Conocimiento del routing dinámico

Componentes Utilizados

- Secure Firewall con código 7.7.10
- Centro de gestión de firewalls en la nube. La configuración también se aplica al FMC virtual típico
- Panel de Cisco Secure Access

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los túneles de red de Secure Access se pueden utilizar para dos fines principales: Acceso seguro a Internet y acceso privado seguro.

En el caso del acceso privado seguro, las organizaciones pueden aprovechar el acceso de confianza cero (ZTA) o VPN como servicio (VPNaaS) para conectar a los usuarios con recursos privados, como aplicaciones internas o Data Centers. Los túneles IPsec desempeñan un papel clave en esta arquitectura, ya que cifran de forma segura el tráfico de red entre los usuarios y los recursos privados, lo que garantiza que los datos confidenciales permanezcan protegidos mientras atraviesan redes no fiables. Al integrar túneles IPsec con ZTA o VPNaaS, las organizaciones pueden proporcionar un acceso seguro y sin problemas a los recursos internos, a la vez que mantienen unos sólidos controles de seguridad y visibilidad.

Este documento describe cómo configurar Secure Access con Secure Firewall Threat Defence (FTD) a través de IPsec para Secure Private Access.

Además, esta guía proporciona los pasos para configurar el ruteo dinámico con BGP.

Aunque este documento trata sobre la configuración de túneles IPsec para el acceso privado seguro, la configuración de Zero Trust Access (ZTA) o VPN as a Service (VPNaaS) para acceder a aplicaciones privadas está fuera del alcance de esta guía.

Configurar

Configuración de Secure Access

Configuración del Grupo de Túnel de Red

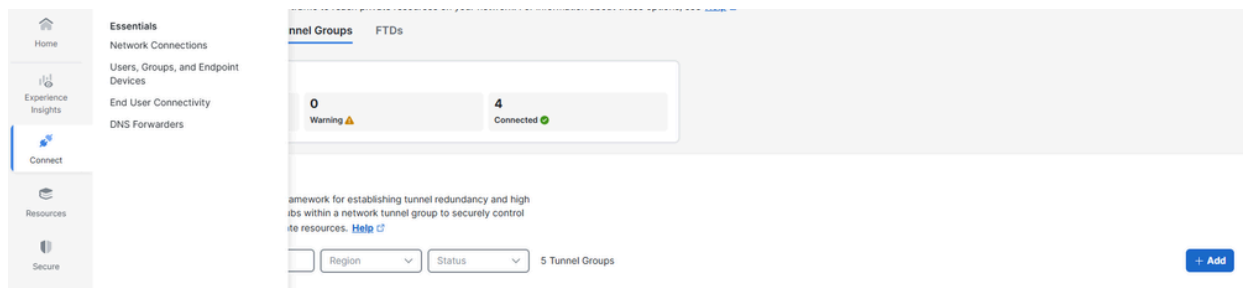
1. Acceda al panel de administración de [Acceso seguro](#).



Panel de CSA

2. Agregue un grupo de túnel de red.

- Haga clic en **Connect** > **Network Connections**
 - En **Network Tunnel Groups** haga clic en > **Add**



Comprobar NTG

3. General Settings Configuración.

- Configure el Tunnel Group Name, **Region** y Device Type
 - Haga clic en Next

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

Configuración general

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. Configure el Tunnel ID y Passphrase. Este ID es importante, ya que es necesario para la configuración de FTD

- Haga clic en Next

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

ID y 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. Configure el enrutamiento dinámico.

Routing de acceso seguro

Routing dinámico (BGP)

- Especifique el número de sistema autónomo (AS) BGP del FTD al configurar el par BGP en Secure Access.
- Haga clic en [Routing](#) > [Dynamic routing](#)
 - Haga clic en [Device AS Number](#) y agregue los FTDs BGP ASN
 - Marque la [Block default route advertisement](#) casilla de verificación
 - Haga clic en [Save](#)

☒ **Dynamic routing**
Use this option when you have a BGP peer for your on-premise router.

Device AS Number

64513

Advanced Settings

☐ **Multihop BGP**
Select this option to enable the ability for BGP peers to establish a connection (hop) when not directly connected.

☐ **Multi-region backhaul**
Use Secure Access as the network backbone and prioritize regions based on origin.

☒ **Block default route advertisement**
Select to block the advertisement of the default route.

Configuración de CSA BGP



Nota: Las rutas anunciadas por Secure Access anteponen la ruta AS original para incluir: 1 para túneles primarios y 2 para túneles secundarios. Se admiten escenarios de red de retorno multiregión. Para obtener más información, haga clic en [link](#).

Guardar configuración de grupo de túnel de red

Descargue y guarde los datos de configuración del túnel, ya que son necesarios para la configuración del FTD.

- Haga clic en [Download CSV](#)
- Haga clic en [Done](#)

✓ 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:

ftd1-ipsec@

Primary Data Center IP Address:

ftd1-ipsec@

Secondary Tunnel ID:

ftd1-ipsec@

Secondary Data Center IP Address:

Passphrase:

Download CSV

Done

Datos NTG

Summary

✖ Disconnected

Region	Canada (Central)	Routing Type	Dynamic Routing (BGP)
Device Type	FTD	Device BGP AS	64513
Last Status Update	Feb 18, 2026 3:58 PM	Peer (Secure Access) BGP AS	64512
		BGP Peer (Secure Access) IP Addresses	169.254.0.9, 169.254.0.5, 2a04:e4c4:b:c723::b67:0000/120
		Multihop BGP Addresses	—
		Multihop TTL	—

Configuración de BGP



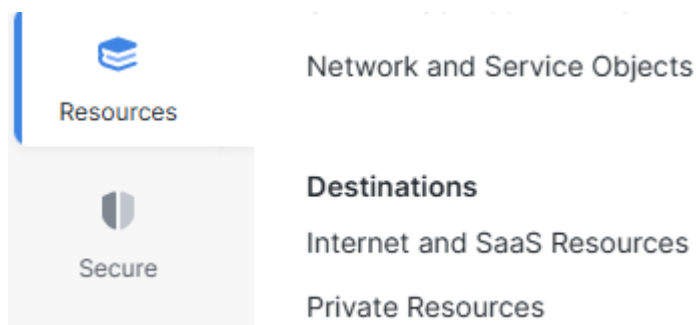
Nota: Haga clic en Network Tunnel Group para ver el número AS de BGP y las direcciones IP de peer BGP, que se configuran más adelante en el lado FTD.

Crear un recurso privado

Los recursos privados son aplicaciones internas, redes o subredes alojadas en su Data Center o entorno de nube privada. Estos recursos no son de acceso público y están protegidos detrás de la infraestructura de su organización.

Al definirlos como recursos privados en Secure Access, puede habilitar el acceso controlado a través de soluciones como Zero Trust Access (ZTA) o VPN as a Service (VPNaaS). Esto garantiza que los usuarios puedan conectarse de forma segura a los sistemas internos en función de la identidad, el estado del dispositivo y las políticas de acceso, sin exponer los recursos directamente a Internet.

Vaya a **Resources > Private Resources** haga clic en **Add**.



PR

- Especifique el **Private Resource Name**, Internally reachable address, Protocol, Port/Ranges. Especifique puertos y protocolos y agregue recursos privados adicionales según sea necesario
- Seleccione la opción deseada **Connection Method** en función de sus necesidades, por ejemplo, conexiones de confianza cero o conexiones VPN, según sus requisitos
- Haga clic en **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

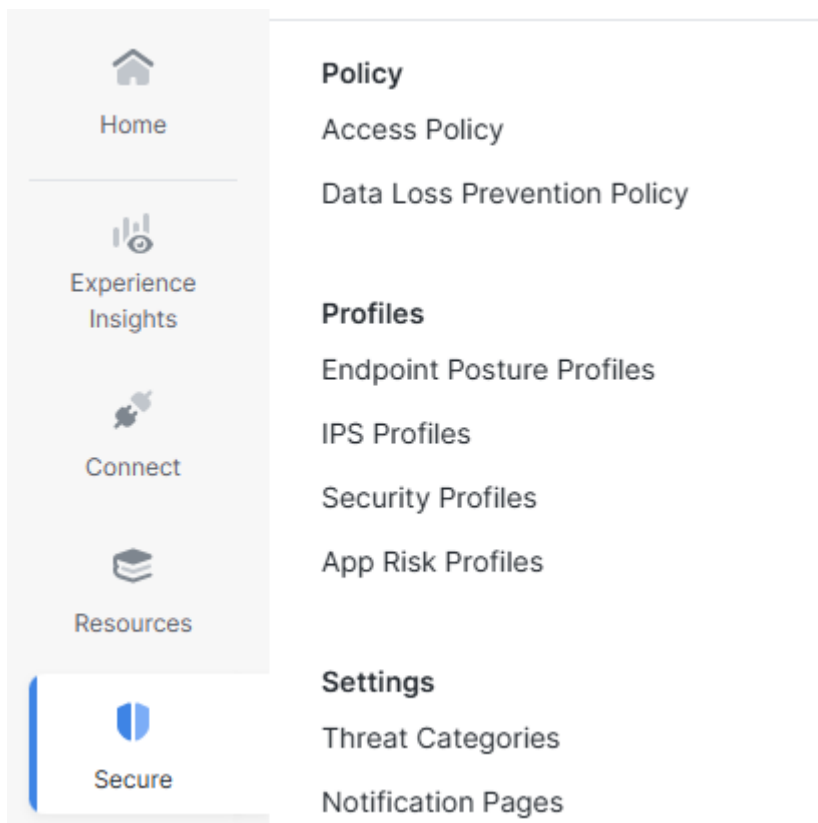
Recurso privado

Crear una regla de directiva de acceso

Las reglas de acceso privado definen cómo los usuarios pueden conectarse de forma segura a recursos internos y aplicaciones que no son de acceso público.

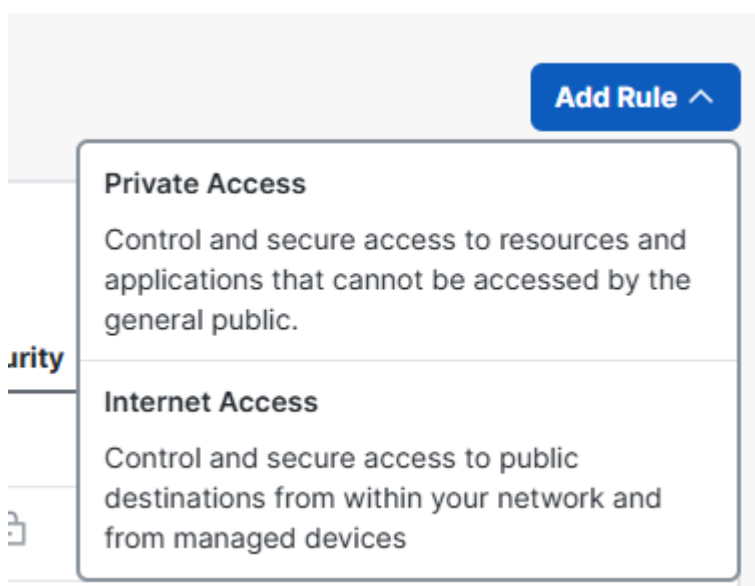
Estas reglas aplican la seguridad al controlar quién puede acceder a recursos privados específicos en función de factores como la identidad del usuario, la pertenencia a un grupo, el estado del dispositivo, la ubicación u otras condiciones de la directiva. Esto garantiza que los sistemas internos confidenciales permanezcan protegidos frente al acceso público general, al tiempo que se encuentran disponibles de forma segura para los usuarios autorizados a través de ZTA o VPNaaS.

Vaya a [Secure](#)>[Access Policy](#)



ACP

- Haga clic en [Add Rule](#)
 - Haga clic en [Private Access](#)



Agregar ACP

- Haga clic en [Rule Name](#) y asigne un nombre
- Haga clic en [Action](#), seleccione [Allow](#) para permitir este tráfico
- Haga clic en [From](#) y especifique los usuarios a los que se concede permiso

- Haga clic en **To** y especifique el acceso que tienen esos usuarios según esta regla
- Haga clic en **Next** y **Save** en la página siguiente

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

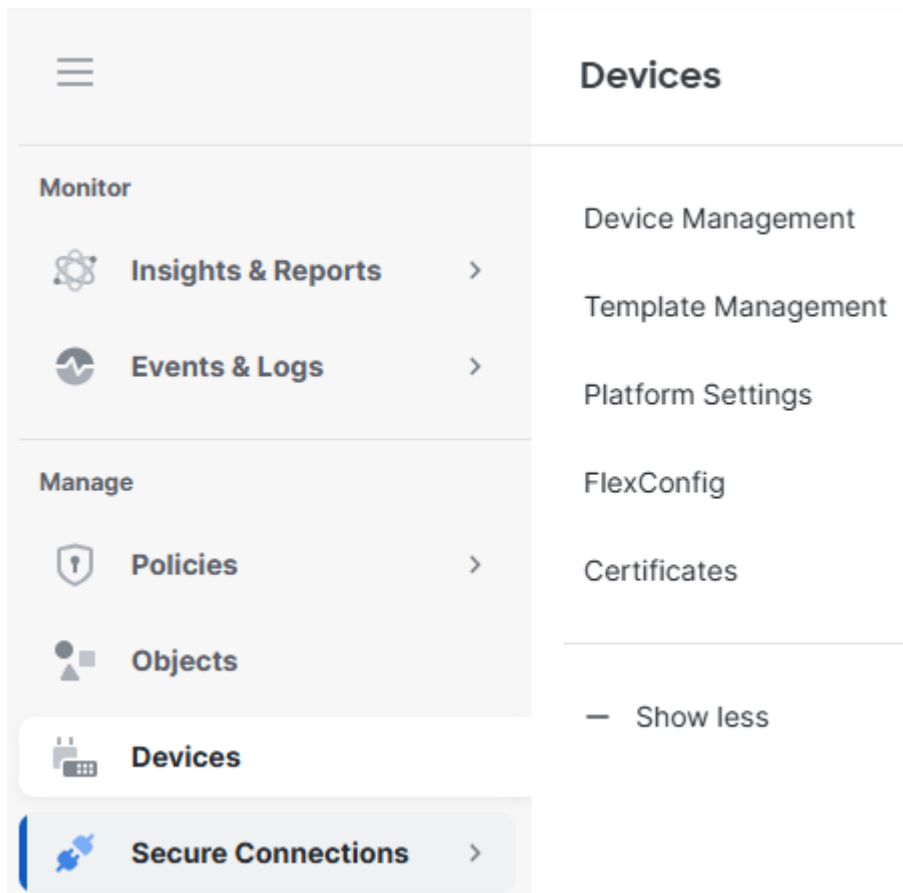
configuración de ACP

Configuración de Secure Firewall Threat Defence (FTD)

Configuración de Interfaces de Túnel Virtual

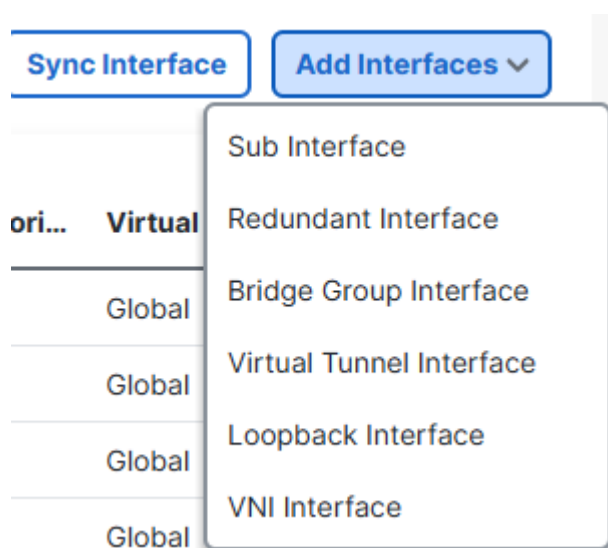
Una interfaz de túnel virtual (VTI) en FTD es una interfaz de capa 3 lógica que se utiliza para configurar túneles VPN IPsec basados en ruta.

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



Dispositivos FTD

- Haga clic en el dispositivo FTD, Interfaces
 - Haga clic en Add Interfaces
 - Haga clic en Virtual Tunnel Interface
 - Cree dos interfaces de túnel virtuales, una para el Secure Access Hub principal y otra para el Secure Access Hub secundario



Agregar VTI

Interfaz de túnel virtual 1:

- Dé un nombre, haga clic en **Enable**
- Seleccione o cree un **Security Zone**
- Haga clic en **Tunnel ID** y asigne un valor.
- Haga clic en **Tunnel Source** y especifique la interfaz WAN desde la que se establecerá el túnel
- Haga clic en **IPsec Tunnel Mode**, **seleccione IPv4**
- Haga clic en **IP Address** y configure la dirección IP para el VTI

Haga clic en **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

VTI1.1

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



VTI1.2

Interfaz de túnel virtual 2:

- Dé un nombre, haga clic en **Enable**
- Seleccione o cree un **Security Zone**
- Haga clic en **Tunnel ID** y asígnele un valor
- Haga clic en **Tunnel Source** y especifique la interfaz WAN desde la que se establecerá el túnel
- Haga clic en **IPsec Tunnel Mode**, seleccione **IPv4**
- Haga clic en **IP Address** y configure la dirección IP para el VTI
- Haga clic en **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

VTI2.1

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:*

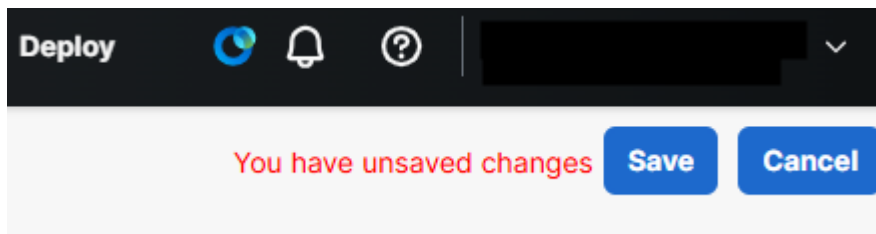
☒ Configure IP

169.254.0.5/30



VTI2.2

Haga clic en Guardar.

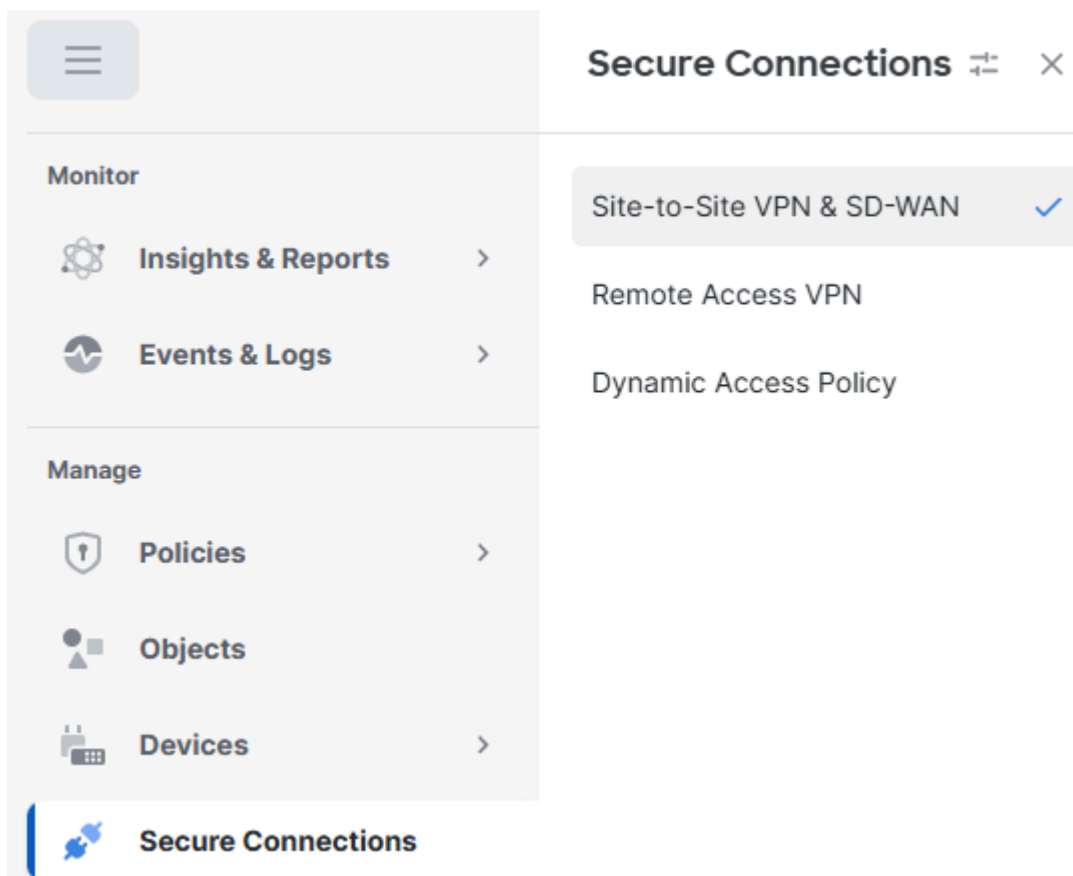


Guardar cambios VTI

Configuración del túnel IPsec

Vaya al panel de cdFMC.

- Haga clic en **Secure Connection** > **Site-to-Site VPN & SD-WAN**



S2S

- Haga clic en **Add**
 - Haga clic en **Route-Based VPN**
 - Haga clic en **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](#)

☒ **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](#)

Agregar VPN

- En el paso 5 de la configuración de Secure Access, obtenga los ID de túnel y las direcciones IP de los Data Centers principales y secundarios
- Haga clic en Endpoints
 - En Node A, haga clic en Device y seleccione Extranet
 - Haga clic en Device Name y asigne un nombre
 - Haga clic en Endpoint IP Addresses e introduzca las direcciones IP primaria y secundaria de Secure Access separadas por una coma (en "Save Network Tunnel Group Configuration" [Guardar configuración de grupo de túnel de red] en Secure Access Configuración)
 - En Node B, haga clic en Device y seleccione el dispositivo FTD
 - Haga clic en Virtual Tunnel Interface y seleccione la primera interfaz VTI creada en el paso anterior
 - Haga clic en Send Local Identity to Peers option (opción) y seleccione Email ID, ingrese el ID de túnel principal (de "Save Network Tunnel Group Configuration" (Guardar configuración de grupo de túnel de red) bajo la configuración de acceso seguro)
 - Haga clic en Add Backup VTI
 - Haga clic en Virtual Tunnel Interface y seleccione la segunda interfaz VTI creada en el paso anterior
 - Haga clic en Send Local Identity to Peers option y seleccione Email ID, ingrese el ID del túnel secundario (de "Save Network Tunnel Group Configuration" en Secure Access Configuración)
 - Haga clic en Guardar

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](#)

Configuración de FTD VTI

- Haga clic en **IKE**
 - Haga clic en **IKEv2 Settings** > Policies
 - Seleccione la **Umbrella-AES-GCM-256** opción

Haga clic en **OK**

IKEv2 Policy



Available IKEv2 Policy  

Search

AES-GCM-NULL-SHA

AES-GCM-NULL-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

Política IKEv2

- Haga clic en Authentication Type y seleccione Pre Shared Manual Key e introduzca la PSK configurada en Secure Access (frase de paso)

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

- Haga clic en IPSEC

- Haga clic en IKEv2 Proposals
- Seleccionar Umbrella-AES-GCM-256
- Haga clic en 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

Guardar las propuestas de IKEv2

Configuración de enrutamiento de FTD

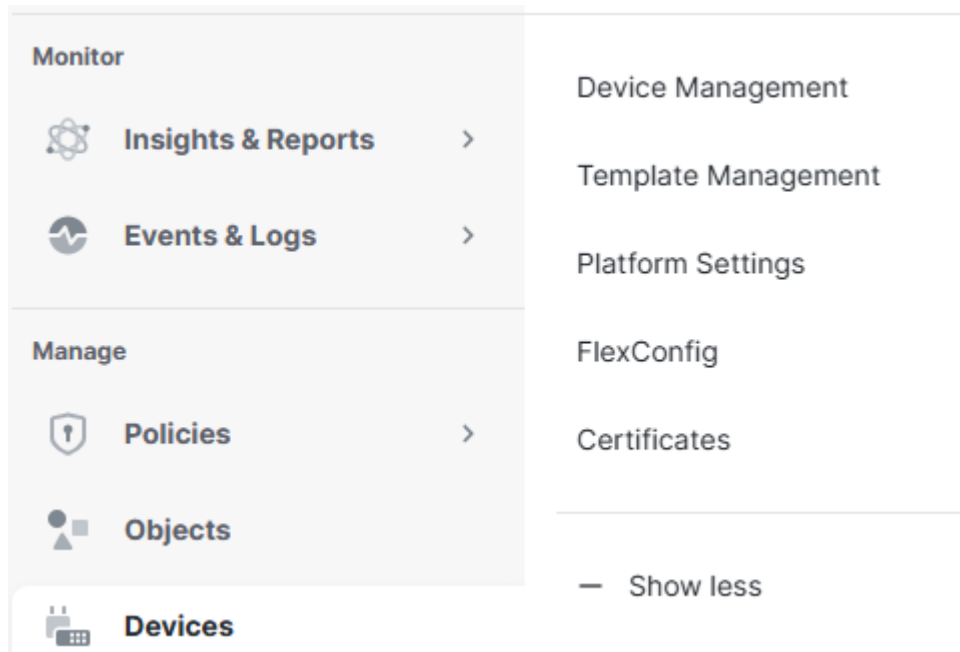
Routing dinámico (BGP)

El protocolo de gateway fronterizo (BGP) es un protocolo de routing dinámico que automatiza el intercambio de información de routing entre sistemas autónomos (AS). Determina la mejor ruta disponible para el tráfico de datos basándose en atributos y políticas, en lugar de depender de rutas estáticas.

Mediante el aprendizaje y la actualización dinámicos de las rutas, BGP mejora la escalabilidad, optimiza la selección de rutas y proporciona conmutación por fallo automática en caso de cambios en los enlaces o en la red.

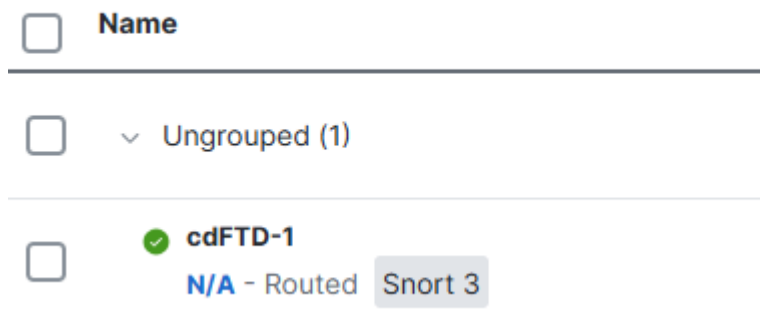
Vaya al panel de cdFMC.

- Haga clic en **Devices** > Device Management



Dispositivo

- Haga clic en el FTD



Dispositivo FTD

- Haga clic en Routing > BGP > IPv4 > Enable IPv4
- Haga clic en Neighbory especifique el número de sistema autónomo (AS) BGP para Secure Access, junto con las direcciones IP vecinas
Consulte la Nota de la Configuración de Secure Access, donde se proporcionan todos los detalles de configuración relevantes para este proceso.
- Haga clic en Save

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General **Neighbor** Add Aggregate Address Filtering Networks Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

Address	Remote AS Number	Address Family	Remote Private AS Number	Description
169.254.0.2	64512	Enabled		
169.254.0.6	64512	Enabled		

+ Add

vecino BGP



Nota: a partir de noviembre de 2025, todas las organizaciones Secure Access recién creadas utilizan el ASN 32644 público de forma predeterminada para el peering BGP en los grupos de túnel de red. Las organizaciones existentes establecidas antes de noviembre de 2025 siguen utilizando el ASN 64512 privado que se reservaba anteriormente para los peers BGP de acceso seguro.

- Haga clic en **Networks** y agregue las redes sobre las que desea anunciar a Secure Access
- Haga clic en **Save**

cdFTD-1 You have unsaved changes [Save](#) [Cancel](#)

Cisco Secure Firewall Threat Defense for VMware

Device Interfaces Inline Sets **Routing** DHCP VTEP

Enable IPv4: ☒ AS Number 64513

General Neighbor Add Aggregate Address Filtering **Networks** Redistribution Route Injection

Manage Virtual Routers: Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

▼ BGP

IPv4

Network	RouteMap
Subnet-172.16.15.0	

+ Add

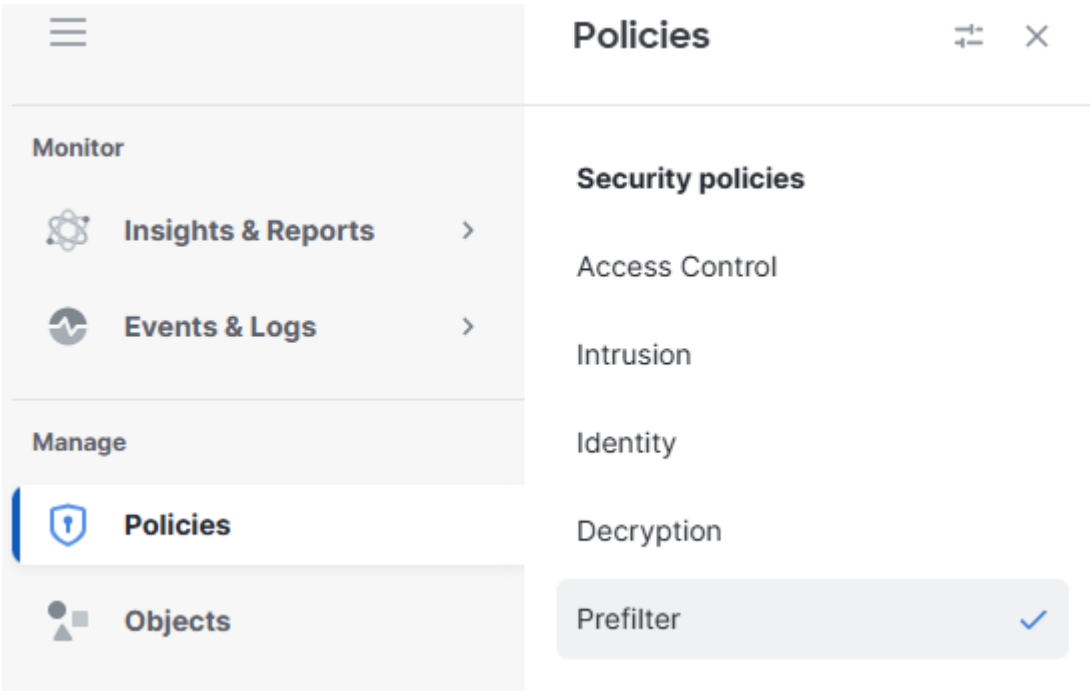
Agregar red

Configuración de política de acceso

Para permitir el tráfico en un Cisco Firepower Threat Defence (FTD) y permitir el acceso a recursos privados, el tráfico debe pasar primero por la fase inicial del control de acceso conocida como filtrado previo.

El prefiltrado se procesa antes de que se produzca una inspección más profunda y está diseñado para ser sencillo y rápido. Evalúa el tráfico utilizando criterios básicos de encabezado externo (como direcciones IP y puertos de origen y destino) para permitir, bloquear o omitir el tráfico rápidamente. Cuando se permite el tráfico en esta etapa, puede omitir inspecciones que requieren más recursos, como la inspección profunda de paquetes o las políticas de intrusión, lo que mejora el rendimiento al tiempo que mantiene el control de seguridad.

Vaya a Policies> Prefilter



Prefiltrar

- Haga clic en Editar la política de filtro previo que utiliza su política de acceso

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

haga clic en prefiltrar

- Haga clic en Add Tunnel Rule
 - Agregue y permita el tráfico de la red VPNaaS y/o la subred ZTA a sus recursos privados
 - Haga clic en 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_vrt (Routed)	zone_in (Routed)	CSA-Manager CSA-VPNaaS CSA-ZTA	Internal-Subnet Subnet-172.16.15	any	any	any	Fastpath	na

Guardar regla

Llegados a este punto, una vez completada y verificada la configuración del FTD, podrá continuar con la implementación. Después de la implementación, tanto los túneles IPsec como las sesiones de vecino BGP se activan correctamente, lo que confirma que la conectividad y el routing

dinámico funcionan según lo esperado.

Verificación

Verificar en FTD

Estado del túnel en FTD

Puede ver el estado actual del túnel, incluso si está activo o inactivo. Esto ayuda a verificar que el túnel IPsec esté establecido correctamente.

- Haga clic en Conexiones seguras
- Haga clic en VPN de sitio a sitio y SD-WAN
- Haga clic en el nombre de topología

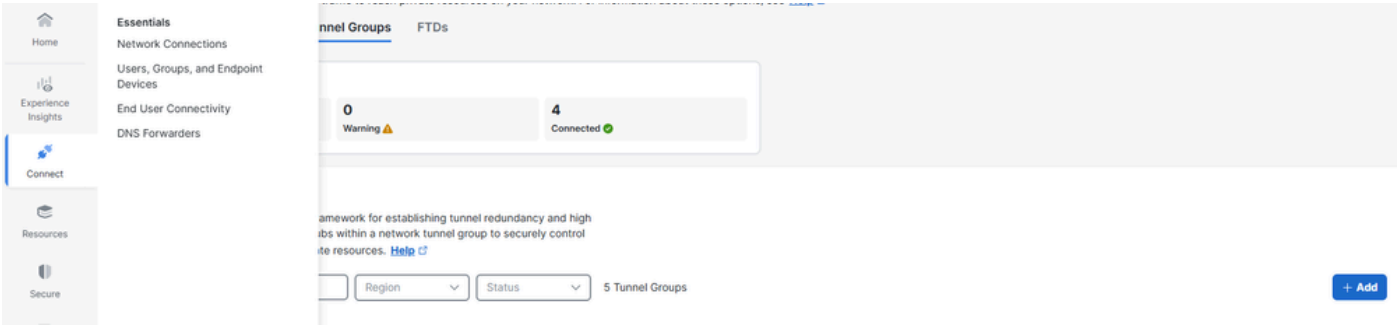
Topology name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
CSA	Route Based (VTI)	Point-to-Point	2 Tunnels		✓
Node A DeviceVPN InterfaceVTI Interface EXTRANETExtranet EXTRANETExtranet Node B DeviceVPN InterfaceVTI Interface FTDcdFTD-1outside (192.168.0.20)VTI-1 (169.254.0.1) FTDcdFTD-1outside (192.168.0.20)VTI-2 (169.254.0.5)					

Estado del túnel FTD

Estado del túnel en Secure Access

Puede ver el estado actual del túnel, incluido si está desconectado, con advertencia o conectado. Esto ayuda a verificar que el túnel IPsec esté establecido correctamente.

- Haga clic en Connect > Network Connections
- Haga clic en Network Tunnel Groups .



Comprobar NTG

- Haga clic en el grupo de túnel de red

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

Estado del túnel CSA

Eventos en Secure Access

Puede ver los eventos de túnel y BGP y confirmar si el estado de los túneles IPsec es activo y estable, y si las sesiones BGP están establecidas.

Haga clic en 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

Supervisar registros de conexión

FTD

All severity levels

All services

All regions

Last 24 hours

Refresh

120 results

Search Text: FTD X

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

Registros NTG

Vaya a Monitor > Activity Search.

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

Supervisar registros de conexión

En cualquiera de los eventos relacionados, haga clic en View Full Details.

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

Detalles completos

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

Búsqueda de actividad

Información Relacionada

- [Soporte técnico y descargas de Cisco](#)
- [Guía de configuración de dispositivos de Cisco Secure Firewall Management Center, 7.7](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).