

Configuración de ISP dual en FTD mediante FDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar la conmutación por fallo del proveedor de servicios de Internet (ISP) dual mediante el Administrador de dispositivos de firewall (FDM) para la serie de firewall seguro.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Routing básico
- Conocimiento del panel del administrador de dispositivos de firewall
- Al menos 2 proveedores de servicios de Internet conectados al firewall seguro.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

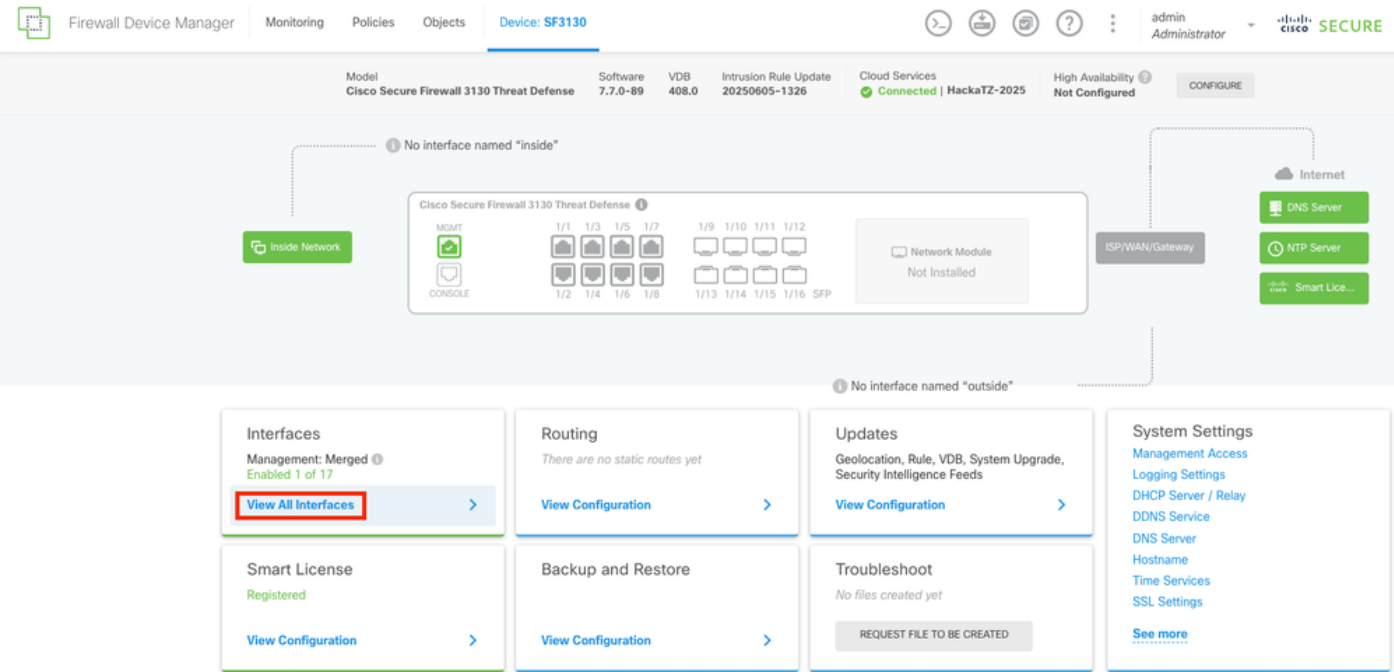
- Cisco Secure Firewall con la versión 7.7.X o versiones posteriores.
- Secure Firewall 3130 con versión 7.7.0.

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.

Configurar

Paso 1.

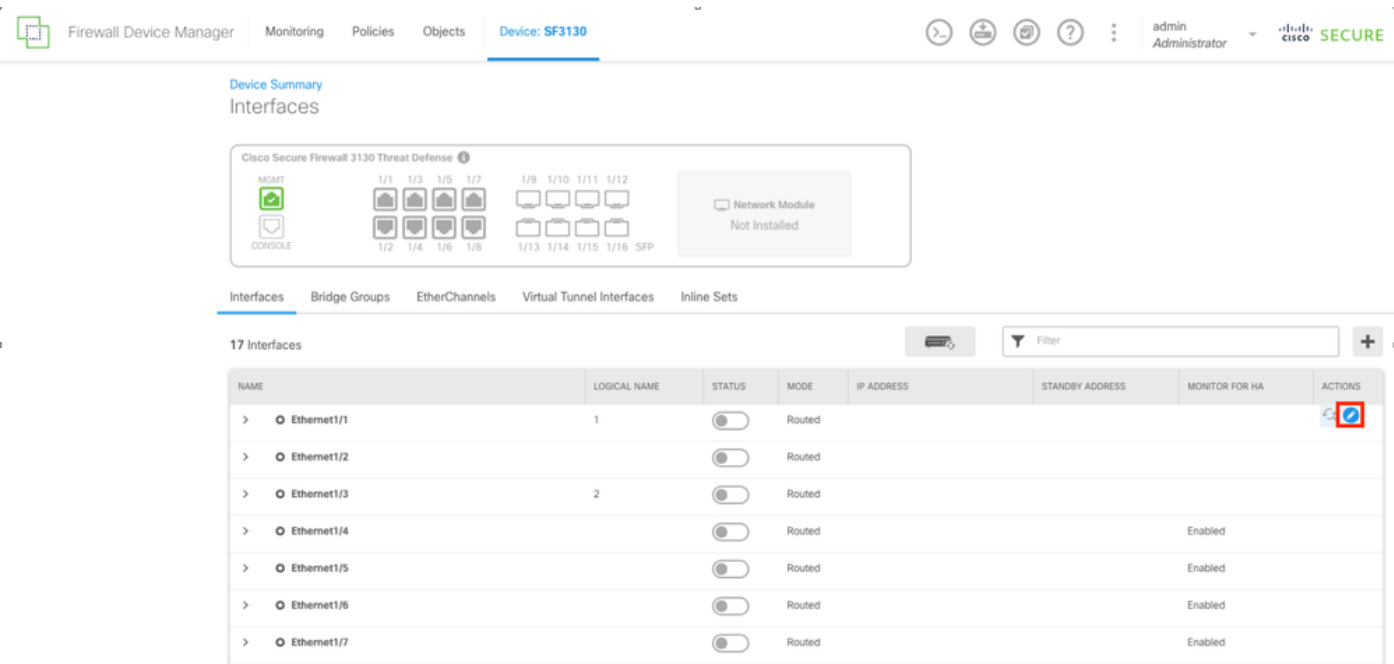
Inicie sesión en FDM en Secure Firewall y navegue hasta la sección de interfaces seleccionando el botón View All Interfaces.



Panel principal de FDM

Paso 2.

Para configurar la interfaz para la conexión del ISP primario, comience seleccionando la interfaz que desee. Seleccionar el botón de interfaz correspondiente para continuar. En este ejemplo, la interfaz utilizada es Ethernet1/1.



Paso 3.

Configure la interfaz con los parámetros correctos para su conexión ISP principal. En este ejemplo, la interfaz es `outside_primary`.

Ethernet1/1
Edit Physical Interface

Interface Name

outside_primary

Mode

Routed

Status

☐

Description

ISP Primary

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

172.16.1.1 / 255.255.255.0

Standby IP Address and Subnet Mask

CANCEL

OK

Configuración de la interfaz ISP principal

Paso 4.

Repita el mismo proceso para la interfaz ISP secundaria. En este ejemplo, se utiliza la interfaz Ethernet1/2.

Ethernet1/2

Edit Physical Interface



Interface Name

outside_backup

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

ISP Backup



IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

172.16.2.1

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

Configuración de la interfaz ISP secundaria

Paso 5.

Después de configurar las dos interfaces para los ISP, el siguiente paso es configurar el Monitor de SLA para la interfaz principal.

Vaya a la sección Objetos seleccionando el botón Objetos situado en la parte superior del menú.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Device Summary
Interfaces

Cisco Secure Firewall 3130 Threat Defense

MGMT
CONSOLE

1/1 1/3 1/5 1/7
1/2 1/4 1/6 1/8

1/9 1/10 1/11 1/12
1/13 1/14 1/15 1/16 SFP

Network Module
Not Installed

Interfaces | Bridge Groups | EtherChannels | Virtual Tunnel Interfaces | Inline Sets

17 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> Ethernet1/1	outside_primary		Routed	172.16.1.1			
> Ethernet1/2	outside_backup		Routed	172.16.2.1			
> Ethernet1/3	inside		Routed	192.168.1.1			
> Ethernet1/4			Routed			Enabled	
> Ethernet1/5			Routed			Enabled	
> Ethernet1/6			Routed			Enabled	
> Ethernet1/7			Routed			Enabled	
> Ethernet1/8			Routed			Enabled	

Interfaces configuradas

Paso 6.

Seleccione en la columna de la izquierda el botón Monitores de SLA.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Network Objects and Groups

8 objects

#	NAME	TYPE	VALUE
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16
2	Gateway-Outside-1	HOST	172.16.1.254
3	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8
4	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12
5	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16
6	Inside	NETWORK	192.168.1.0/24
7	any-ipv4	NETWORK	0.0.0.0/0
8	any-ipv6	NETWORK	::/0

Filter

Preset filters: [System defined](#) [User defined](#)

Ports

- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups
- Event List Filters
- SLA Monitors**
- SGT Groups

Pantalla Objetos

Paso 7.

Cree un nuevo monitor de SLA seleccionando el botón Create SLA Monitor.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

admin Administrator | Cisco SECURE

SLA Monitors

Filter

#	NAME	MONITORED ADDRESS	TARGET INTERFACE	ACTIONS
There are no SLA Monitors yet. Start by creating the first SLA Monitor.				
CREATE SLA MONITOR				

Sección Supervisión de SLA

Paso 8.

Configure los parámetros para la conexión del ISP primario.

Add SLA Monitor Object



Name

Outside_Primary_ISP

Description

Monitor for ISP Primary

Monitor Address

Gateway-Outside-1

Target Interface

outside_primary (Ethernet1/1)

IP ICMP ECHO OPTIONS



Following properties have following correlation: $\text{Threshold} \leq \text{Timeout} \leq \text{Frequency}$

Threshold

5000

milliseconds

0 - 2147483647

Timeout

5000

milliseconds

0 - 604800000

Frequency

60000

milliseconds

1000 - 604800000, multiple of 1000

Type of Service

0

0 - 255

Number of Packets

1

0 - 100

Data Size

28

0 - 16384

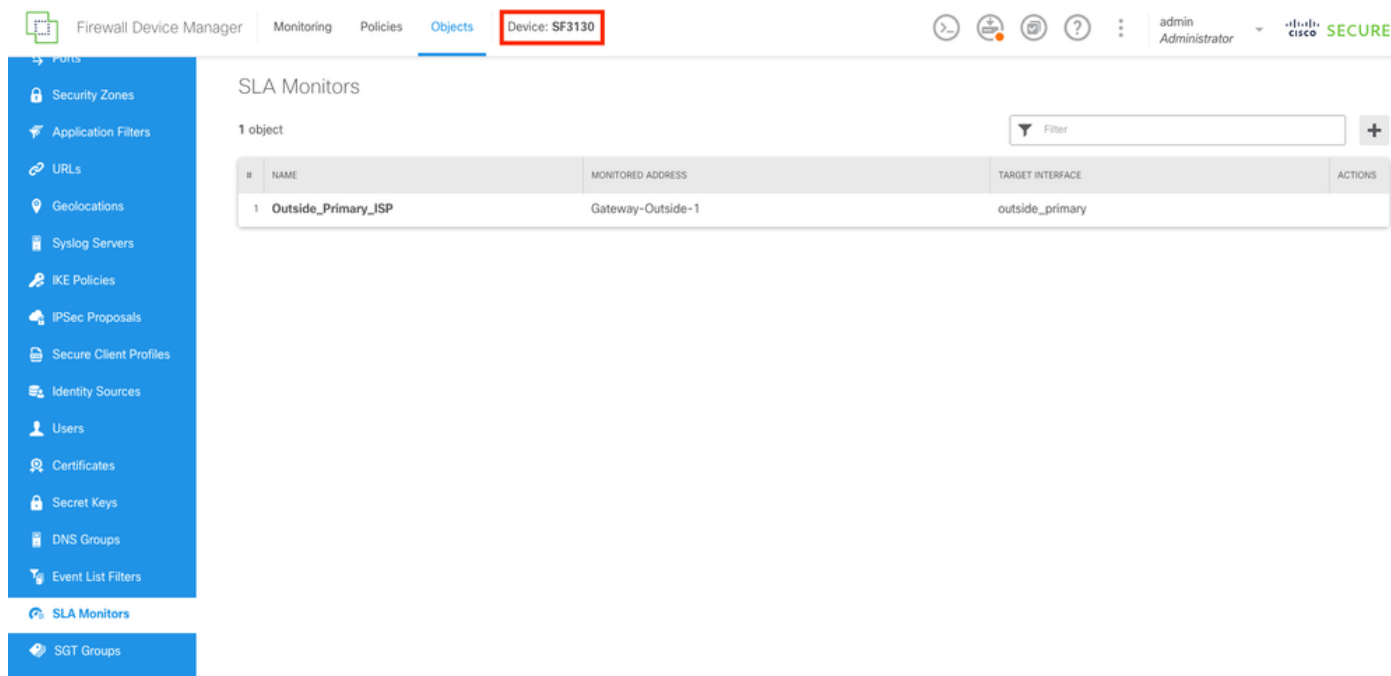
bytes

CANCEL

OK

Paso 9.

Una vez creado el objeto, la ruta estática de las interfaces debe crearlo. Vaya al panel principal seleccionando el botón Device.



Firewall Device Manager | Monitoring | Policies | Objects | **Device: SF3130**

SLA Monitors

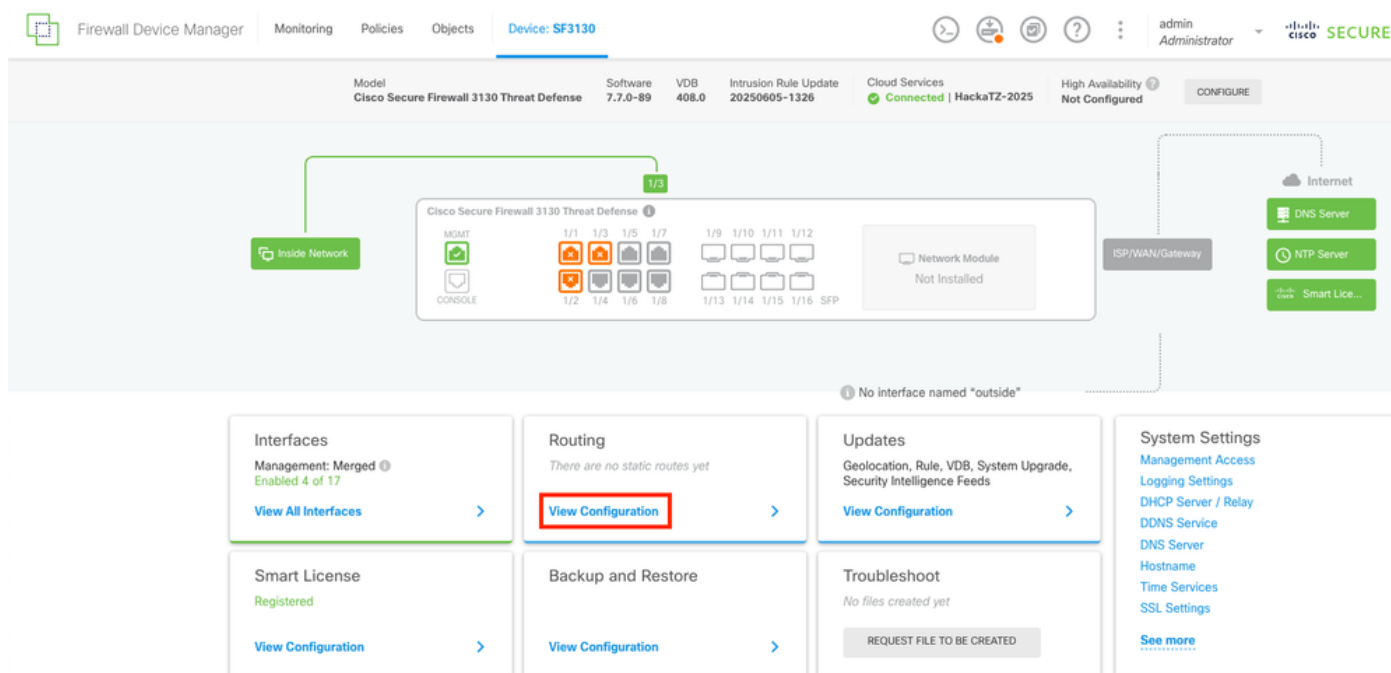
1 object

#	NAME	MONITORED ADDRESS	TARGET INTERFACE	ACTIONS
1	Outside_Primary_ISP	Gateway-Outside-1	outside_primary	

Monitor de SLA creado

Paso 10.

Navegue hasta la Sección de ruteo seleccionando Ver configuración en el Panel de ruteo.



Firewall Device Manager | Monitoring | Policies | Objects | **Device: SF3130**

Model: Cisco Secure Firewall 3130 Threat Defense | Software: 7.7.0-89 | VDB: 408.0 | Intrusion Rule Update: 20250605-1326 | Cloud Services: Connected | HackaTZ-2025 | High Availability: Not Configured

Inside Network | Cisco Secure Firewall 3130 Threat Defense | Internet

Routing: There are no static routes yet. **View Configuration**

Interfaces: Management: Merged. Enabled 4 of 17. View All Interfaces

Smart License: Registered. View Configuration

Backup and Restore: View Configuration

Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. View Configuration

Troubleshoot: No files created yet. REQUEST FILE TO BE CREATED

System Settings: Management Access, Logging Settings, DHCP Server / Relay, DDNS Service, DNS Server, Hostname, Time Services, SSL Settings. See more

Panel principal

Paso 11.

En la ficha Static Routing (Enrutamiento estático), cree las dos rutas estáticas predeterminadas para ambos ISP. Para crear una nueva ruta estática, seleccione el botón CREATE STATIC ROUTE.

Firewall Device Manager | Monitoring | Policies | Objects | **Device: SF3130**

admin Administrator | Cisco SECURE

Device Summary
Routing

Add Multiple Virtual Routers | Commands | BGP Global Settings

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

Filter

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
There are no static routes yet. Start by creating the first static route.								

CREATE STATIC ROUTE

Sección de Ruteo Estático

Paso 12.

Primero, cree la ruta estática para el ISP primario. Al final, agregue el objeto de monitoreo SLA que se creó en el último paso.

Add Static Route



Name

Route_ISP_Primary

Description

Static Route for ISP Primary

Interface

outside_primary (Ethernet1/1)

Protocol



IPv4



IPv6

Networks



any-ipv4

Gateway

Gateway-Outside-1

Metric

1

SLA Monitor Applicable only for IPv4 Protocol type

Outside_Primary_ISP

CANCEL

OK

Ruta estática para ISP principal

Paso 13.

Repita el último paso y cree una ruta predeterminada, para el ISP secundario con el gateway adecuado y una métrica diferente. En este ejemplo, se aumentó a 200.

Add Static Route

?

×

Name

Route_ISP_Backup

Description

Static Route for ISP Backup

Interface

outside_backup (Ethernet1/2)

Protocol

☒ IPv4

☐ IPv6

Networks

+

any-ipv4

Gateway

Gateway-Outside-2

Metric

200

SLA Monitor

Applicable only for IPv4 Protocol type

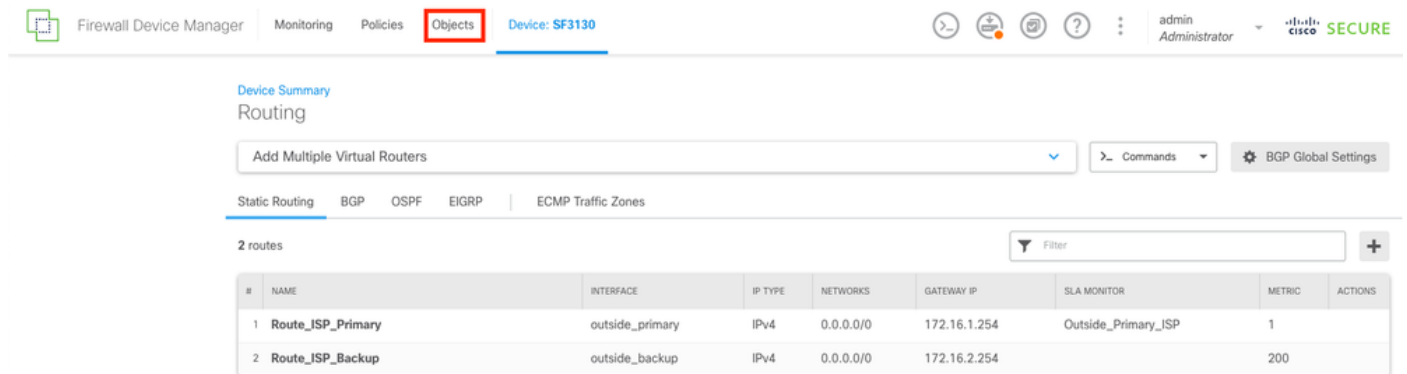
Please select an SLA Monitor

CANCEL

OK

Paso 14.

Una vez creadas ambas rutas estáticas, debe crearse una zona de seguridad. Navegue hasta la sección Objetos seleccionando el botón Objetos en la parte superior.



Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Device Summary
Routing

Add Multiple Virtual Routers [v] [Commands] [BGP Global Settings]

Static Routing | BGP | OSPF | EIGRP | ECMP Traffic Zones

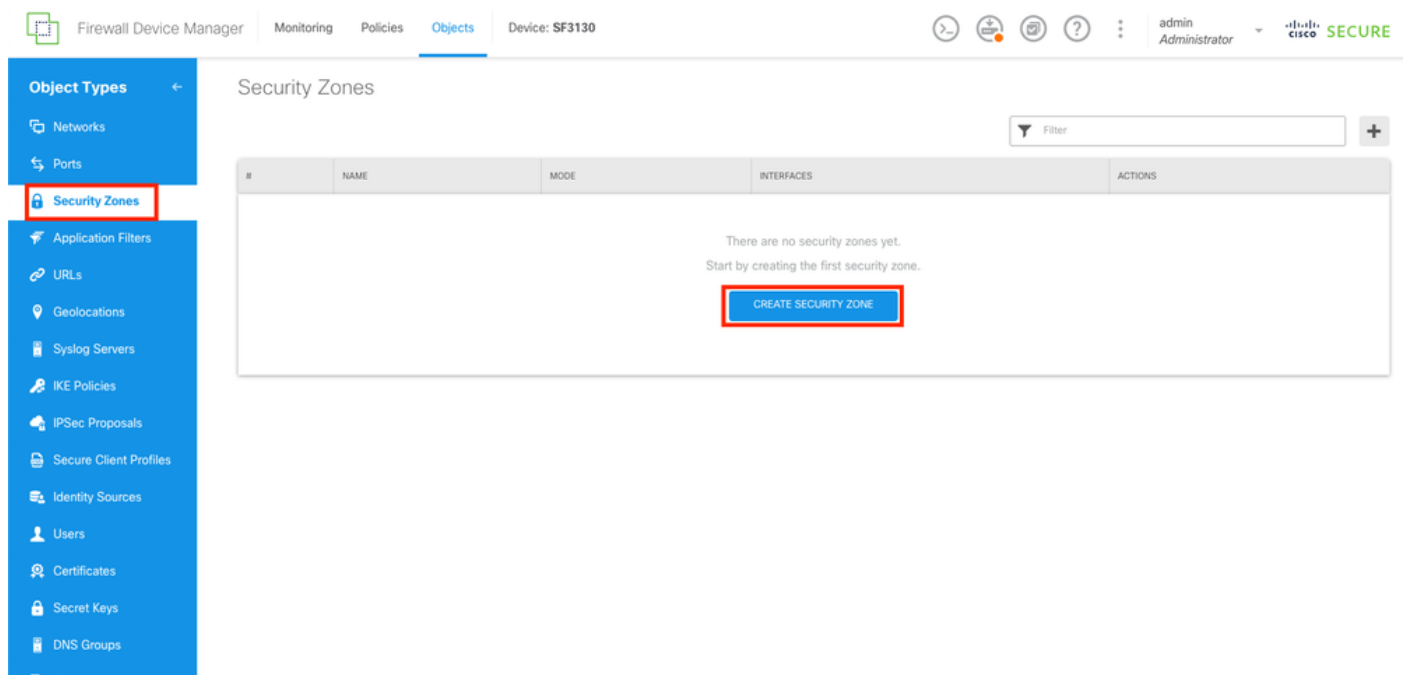
2 routes [Filter] +

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	Route_ISP_Primary	outside_primary	IPv4	0.0.0.0/0	172.16.1.254	Outside_Primary_ISP	1	
2	Route_ISP_Backup	outside_backup	IPv4	0.0.0.0/0	172.16.2.254		200	

Rutas estáticas creadas

Paso 15.

Navegue hasta la sección Zonas de seguridad seleccionando en la columna izquierda el botón Zonas de seguridad, y luego cree una nueva zona seleccionando el botón CREATE SECURITY ZONE.



Firewall Device Manager | Monitoring | Policies | **Objects** | Device: SF3130

Object Types [←]
 Networks
 Ports
Security Zones
 Application Filters
 URLs
 Geolocations
 Syslog Servers
 IKE Policies
 IPSec Proposals
 Secure Client Profiles
 Identity Sources
 Users
 Certificates
 Secret Keys
 DNS Groups
 Event List Filters

Security Zones [Filter] +

#	NAME	MODE	INTERFACES	ACTIONS
There are no security zones yet. Start by creating the first security zone. CREATE SECURITY ZONE				

Paso 16.

Cree la Zona de seguridad externa con las dos interfaces externas para las conexiones de los ISP.

Add Security Zone

Name

outside_zone

Description

Outside Zone

Mode

☒ Routed ☐ Passive ☐ Inline

Interfaces

+

 outside_backup (Ethernet1/2)

 outside_primary (Ethernet1/1)

CANCEL

OK

Zona de seguridad externa

Paso 17.

Una vez creada la zona de seguridad, debe crearse una NAT. Vaya a la sección Políticas seleccionando el botón Políticas en la parte superior.

Firewall Device Manager | Monitoring | **Policies** | Objects | Device: SF3130

Object Types

- Networks
- Ports
- Security Zones**
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys
- DNS Groups

Security Zones

2 objects

#	NAME	MODE	INTERFACES	ACTIONS
1	outside_zone	Routed	outside_backup, outside_primary	
2	inside_zone	Routed	inside	

Zonas de seguridad creadas

Paso 18.

Navegue hasta la sección NAT seleccionando el botón NAT, y luego cree una nueva regla seleccionando el botón CREATE NAT RULE.

Firewall Device Manager | Monitoring | **Policies** | Objects | Device: SF3130

Security Policies

→ **NAT** → Access Control → Intrusion

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
There are no NAT Rules yet. Start by creating the first NAT rule. CREATE NAT RULE												

Sección NAT

Paso 19.

Para la conmutación por fallas del ISP, la configuración debe tener 2 rutas a través de interfaces externas. En primer lugar, para la conexión de la interfaz externa principal al ISP principal.

Add NAT Rule

Title

Create Rule for

Status

To_Internet

Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Type

Automatically placed in Auto NAT rules

Dynamic

Packet Translation

Advanced Options

ORIGINAL PACKET

Source Interface

inside

Original Address

Inside

Original Port

Any

TRANSLATED PACKET

Destination Interface

outside_primary

Translated Address

Interface

Translated Port

Any

Show Diagram

CANCEL

OK

NAT para ISP principal

Paso 20.

Ahora, una segunda NAT para la conexión del ISP secundario.

Nota: No se puede utilizar la misma red para la dirección original. En este ejemplo, para el ISP secundario, la dirección original es el objeto any-ipv4.

Edit NAT Rule

×

Title

Create Rule for

Status

To_Internet_Backup

Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement

Type

Automatically placed in Auto NAT rules

Dynamic

Packet Translation

Advanced Options

ORIGINAL PACKET

Source Interface

inside

Original Address

any-ipv4

Original Port

Any

TRANSLATED PACKET

Destination Interface

outside_backup

Translated Address

Interface

Translated Port

Any

Show Diagram

CANCEL

OK

NAT para ISP secundario

Paso 21.

Después de crear ambas reglas NAT, se debe establecer una regla de control de acceso para permitir el tráfico saliente. Seleccione el botón Control de acceso.

Security Policies

→
→
→
→
→
→
→
→
→

SSL Decryption
Identity
Security Intelligence
NAT
Access Control
Intrusion

2 rules

Filter

+

#	NAME	TYPE	INTERFACES	ORIGINAL PACKET				TRANSLATED PACKET				ACTIONS
				SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	
Auto NAT Rules												
>	# To_Internet	DYNAMIC	↓ Inside outside_pr...	Inside	ANY	ANY	ANY	Interface	ANY	ANY	ANY	
>	# To_Internet_Ba...	DYNAMIC	↓ Inside outside_b...	any-ipv4	ANY	ANY	ANY	Interface	ANY	ANY	ANY	

Reglas NAT creadas

Paso 22.

Para crear la regla de control de acceso, seleccione el botón CREATE ACCESS RULE.

Security Policies

→
→
→
→
→
→
→
→
→

SSL Decryption
Identity
Security Intelligence
NAT
Access Control
Intrusion

Filter



#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
There are no access rules yet. Start by creating the first access rule. CREATE ACCESS RULE												

Default Action

Access Control Block

Sección de control de acceso

Paso 23.

Seleccione las zonas y redes deseadas.

Add Access Rule

Order
1

Title
To_Internet

Action
Allow

Source/Destination
Applications
URLs
Users
Intrusion Policy
File policy
Logging

SOURCE

Zones
+

Networks
+

Ports
+

SGT Groups
+

inside_zone

Inside

ANY

ANY

DESTINATION

Zones
+

Networks
+

Ports
+

SGT Groups
+

outside_zone

ANY

ANY

ANY



Paso 25.

Verifique los cambios y, a continuación, seleccione el botón Deploy Now.

Pending Changes?×

✔ Last Deployment Completed Successfully

10 Jun 2025 12:35 PM. [See Deployment History](#)

Deployed Version (10 Jun 2025 12:35 PM)	Pending Version « LEGEND																				
+ Access Rule Added: <i>To_Internet</i> <table><tbody><tr><td>-</td><td>logFiles: false</td></tr><tr><td>-</td><td>eventLogAction: LOG_NONE</td></tr><tr><td>-</td><td>ruleId: 268435458</td></tr><tr><td>-</td><td>name: To_Internet</td></tr><tr><td>sourceZones:</td><td></td></tr><tr><td>-</td><td>inside_zone</td></tr><tr><td>destinationZones:</td><td></td></tr><tr><td>-</td><td>outside_zone</td></tr><tr><td>sourceNetworks:</td><td></td></tr><tr><td>-</td><td>Inside</td></tr></tbody></table>		-	logFiles: false	-	eventLogAction: LOG_NONE	-	ruleId: 268435458	-	name: To_Internet	sourceZones:		-	inside_zone	destinationZones:		-	outside_zone	sourceNetworks:		-	Inside
-	logFiles: false																				
-	eventLogAction: LOG_NONE																				
-	ruleId: 268435458																				
-	name: To_Internet																				
sourceZones:																					
-	inside_zone																				
destinationZones:																					
-	outside_zone																				
sourceNetworks:																					
-	Inside																				
+ Security Zone Added: <i>inside_zone</i> <table><tbody><tr><td>-</td><td>mode: ROUTED</td></tr><tr><td>-</td><td>description: Inside Zone</td></tr><tr><td>-</td><td>name: inside_zone</td></tr><tr><td>interfaces:</td><td></td></tr><tr><td>-</td><td>inside</td></tr></tbody></table>		-	mode: ROUTED	-	description: Inside Zone	-	name: inside_zone	interfaces:		-	inside										
-	mode: ROUTED																				
-	description: Inside Zone																				
-	name: inside_zone																				
interfaces:																					
-	inside																				
+ SLA Monitor Added: <i>Outside_Primary_ISP</i> <table><tbody><tr><td>-</td><td>slaOperation.frequency: 60000</td></tr><tr><td>-</td><td>slaOperation.threshold: 5000</td></tr><tr><td>-</td><td>slaOperation.dataSize: 28</td></tr><tr><td>-</td><td>slaOperation.numOfPackets: 1</td></tr><tr><td>-</td><td>slaOperation.typeOfService: 0</td></tr><tr><td>-</td><td>slaOperation.timeout: 5000</td></tr><tr><td>-</td><td>description: Monitor for ISP Primary</td></tr><tr><td>-</td><td>name: Outside_Primary_ISP</td></tr></tbody></table>		-	slaOperation.frequency: 60000	-	slaOperation.threshold: 5000	-	slaOperation.dataSize: 28	-	slaOperation.numOfPackets: 1	-	slaOperation.typeOfService: 0	-	slaOperation.timeout: 5000	-	description: Monitor for ISP Primary	-	name: Outside_Primary_ISP				
-	slaOperation.frequency: 60000																				
-	slaOperation.threshold: 5000																				
-	slaOperation.dataSize: 28																				
-	slaOperation.numOfPackets: 1																				
-	slaOperation.typeOfService: 0																				
-	slaOperation.timeout: 5000																				
-	description: Monitor for ISP Primary																				
-	name: Outside_Primary_ISP																				

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

Verificación de implementación

Diagrama de la red

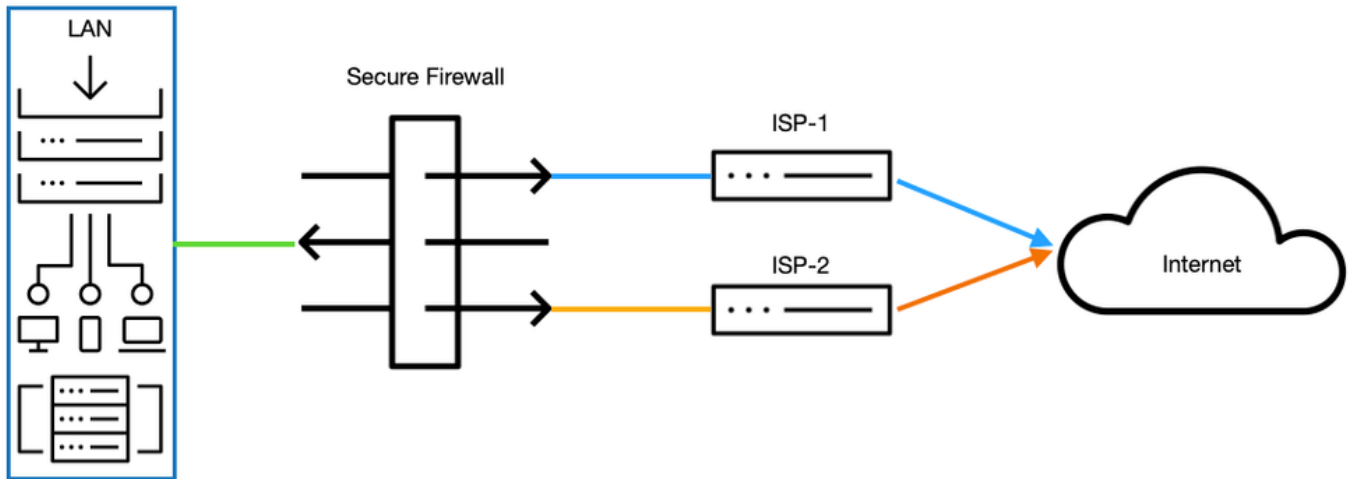


Diagrama de la red

Verificación

<#root>

>

system support diagnostic-cli

Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

SF3130#

show ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
Ethernet1/1	outside_primary	172.16.1.1	255.255.255.0	manual

-----> **THE PRIMARY INTERFACE OF THE ISP IS SET**

Ethernet1/2	outside_backup	172.16.2.1	255.255.255.0	manual
-------------	----------------	------------	---------------	--------

-----> **THE SECONDARY INTERFACE OF THE ISP IS SET**

Ethernet1/3	inside	192.168.1.1	255.255.255.0	manual
-------------	--------	-------------	---------------	--------

SF3130#

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet1/1	172.16.1.1	YES	manual	up	up

-----> **THE INTERFACE IS UP AND RUNNING**

Ethernet1/2 172.16.2.1 YES manual up up

-----> THE INTERFACE IS UP AND RUNNING

Ethernet1/3 192.168.1.1 YES manual up up

SF3130#

show route

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary

----> THE DEFAULT ROUTE IS CONNECTED THROUGH THE PRIMARY ISP

C 172.16.1.0 255.255.255.0 is directly connected, outside_primary

L 172.16.1.1 255.255.255.255 is directly connected, outside_primary

C 172.16.2.0 255.255.255.0 is directly connected, outside_backup

L 172.16.2.1 255.255.255.255 is directly connected, outside_backup

C 192.168.1.0 255.255.255.0 is directly connected, inside

L 192.168.1.1 255.255.255.255 is directly connected, inside

SF3130#

show run route

route outside_primary 0.0.0.0 0.0.0.0 172.16.1.254 1 track 1

route outside_backup 0.0.0.0 0.0.0.0 172.16.2.254 200

SF3130#

show sla monitor configuration

---> CHECKING THE SLA MONITOR CONFIGURATION

SA Agent, Infrastructure Engine-II

Entry number: 539523651

Owner:

Tag:

Type of operation to perform: echo

Target address: 172.16.1.254

Interface: outside_primary

Number of packets: 1

Request size (ARR data portion): 28

Operation timeout (milliseconds): 3000

Type Of Service parameters: 0x0

Verify data: No

Operation frequency (seconds): 3

Next Scheduled Start Time: Start Time already passed

Group Scheduled : FALSE

Life (seconds): Forever

Entry Ageout (seconds): never

Recurring (Starting Everyday): FALSE

Status of entry (SNMP RowStatus): Active

Enhanced History:

SF3130#

show sla monitor operational-state

Entry number: 739848060
Modification time: 01:24:11.029 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE

-----> **THE ISP PRIMARY IS IN A HEALTHY STATE**

Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

AFTERARGBSETHBNDGFSHNDFGSDDBFB

SF3130#

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet1/1	172.16.1.1	YES	manual	down	down

-----> **THE PRIMARY ISP IS DOWN**

Ethernet1/2	172.16.2.1	YES	manual	up	up
Ethernet1/3	192.168.1.1	YES	manual	up	up

SF3130#

show route

Gateway of last resort is 172.16.2.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [200/0] via 172.16.2.254, outside_backup

-----> **AFTER THE ISP PRIMARY FAILS, INSTANTLY THE ISP BACKUP IS FAILOVER AND IS INSTALL IN THE ROUTE**

C	172.16.2.0	255.255.255.0	is directly connected, outside_backup
L	172.16.2.1	255.255.255.255	is directly connected, outside_backup
C	192.168.1.0	255.255.255.0	is directly connected, inside
L	192.168.1.1	255.255.255.255	is directly connected, inside

SF3130#

show sla monitor operational-state

Entry number: 739848060
Modification time: 01:24:11.140 UTC Thu Jun 12 2025
Number of Octets Used by this Entry: 1840
Number of operations attempted: 0
Number of operations skipped: 0
Current seconds left in Life: Forever

Operational state of entry: Pending
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE

-----> AFTER THE DOWNTIME OF THE PRIMARY ISP THE TIMEOUT IS FLAGGED

Over thresholds occurred: FALSE
Latest RTT (milliseconds) : Unknown
Latest operation return code: Unknown
Latest operation start time: Unknown

SF3130#

show route

Gateway of last resort is 172.16.1.254 to network 0.0.0.0

S* 0.0.0.0 0.0.0.0 [1/0] via 172.16.1.254, outside_primary

-----> AFTER A FEW SECONDS ONCE THE PRIMARY INTERFACE IS BACK THE DEFAULT ROUTE INSTALLS AGAIN IN

C 172.16.1.0 255.255.255.0 is directly connected, outside_primary
L 172.16.1.1 255.255.255.255 is directly connected, outside_primary
C 172.16.2.0 255.255.255.0 is directly connected, outside_backup
L 172.16.2.1 255.255.255.255 is directly connected, outside_backup
C 192.168.1.0 255.255.255.0 is directly connected, inside
L 192.168.1.1 255.255.255.255 is directly connected, inside

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).