

Configurar ISP Duplo no FTD Usando o FDM

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Verificar](#)

Introdução

Este documento descreve como configurar o failover do Provedor de Serviços de Internet Duplo (ISP) usando o Gerenciador de Dispositivos de Firewall (FDM) para o Secure Firewall Series.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Roteamento básico
- Conhecimento do painel do Gerenciador de dispositivos de firewall
- Pelo menos dois provedores de serviço de Internet conectados ao firewall seguro.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

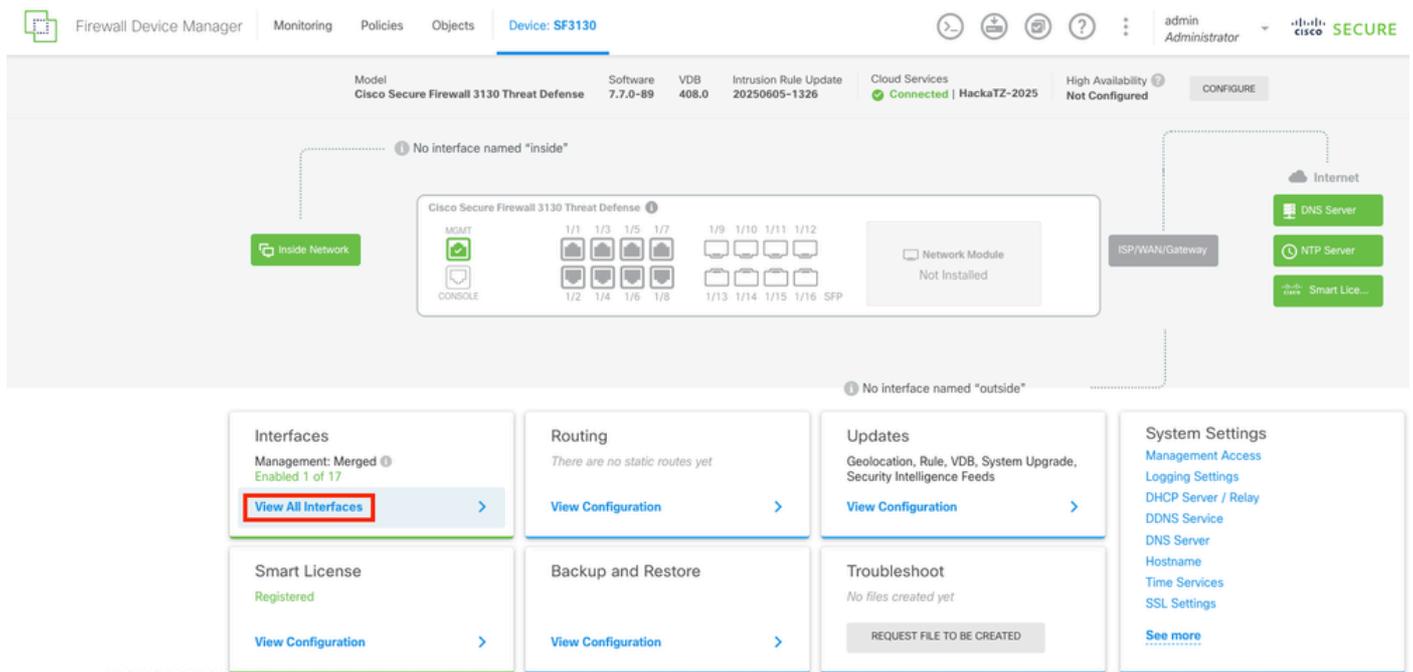
- Cisco Secure Firewall executando a versão 7.7.X ou versões superiores.
- Secure Firewall 3130 com versão 7.7.0.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar

Etapa 1.

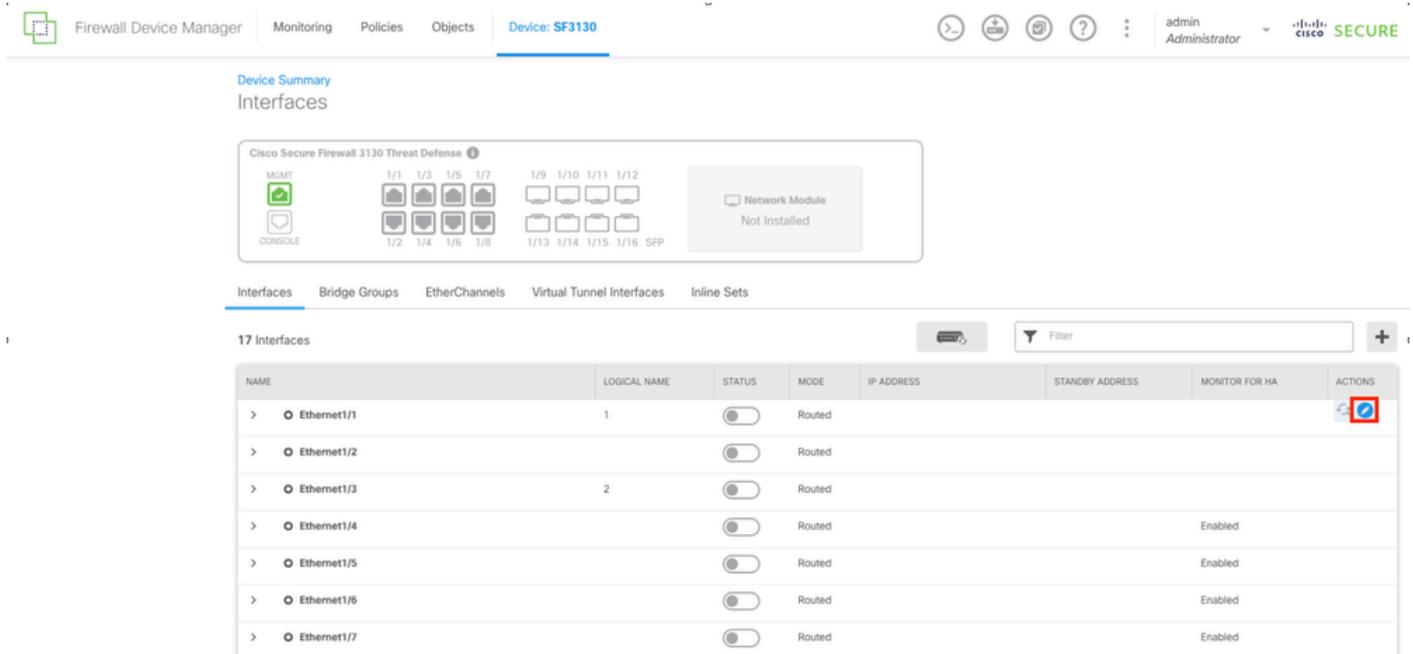
Efetue login no FDM no Firewall Seguro e navegue até a seção interfaces selecionando o botão Exibir Todas as Interfaces.



Painel Principal do FDM

Etapa 2.

Para configurar a interface para a conexão principal do ISP, comece selecionando a interface desejada. Selecionando o botão de interface correspondente para continuar. Neste exemplo, a interface usada é Ethernet1/1.



Guia Interfaces

Etapa 3.

Configure a interface com os parâmetros corretos para sua conexão principal do ISP. Neste exemplo, a interface é outside_primary.

Ethernet1/1

Edit Physical Interface

Interface Name: Mode: Status:

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

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /
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

Configuração da interface primária do ISP

Etapa 4.

Repita o mesmo processo para a interface ISP secundária. Neste exemplo, a interface Ethernet1/2 é usada.

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

Configuração da interface secundária do ISP

Etapa 5.

Depois de configurar as duas interfaces para os ISPs, a próxima etapa é configurar o Monitor SLA para a interface primária.

Navegue até a seção Objetos selecionando o botão Objetos localizado na parte superior do menu.

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

admin Administrator | CISCO SECURE

Device Summary

Interfaces

Cisco Secure Firewall 3130 Threat Defense

MSMT | CONSOLE | 1/1, 1/3, 1/5, 1/7 | 1/9, 1/10, 1/11, 1/12 | 1/2, 1/4, 1/6, 1/8 | 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
> <input checked="" type="checkbox"/> Ethernet1/1	outside_primary	<input checked="" type="checkbox"/>	Routed	172.16.1.1			
> <input checked="" type="checkbox"/> Ethernet1/2	outside_backup	<input checked="" type="checkbox"/>	Routed	172.16.2.1			
> <input checked="" type="checkbox"/> Ethernet1/3	inside	<input checked="" type="checkbox"/>	Routed	192.168.1.1			
> <input type="checkbox"/> Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	
> <input type="checkbox"/> Ethernet1/5		<input type="checkbox"/>	Routed			Enabled	
> <input type="checkbox"/> Ethernet1/6		<input type="checkbox"/>	Routed			Enabled	
> <input type="checkbox"/> Ethernet1/7		<input type="checkbox"/>	Routed			Enabled	
> <input type="checkbox"/> Ethernet1/8		<input type="checkbox"/>	Routed			Enabled	

Interfaces configuradas

Etapa 6.

Selecione na coluna esquerda o botão Monitores de SLA.

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

admin Administrator | CISCO

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

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

Tela de Objetos

Passo 7.

Crie um novo Monitor de SLA selecionando o botão Criar Monitor de SLA.

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				

Seção Monitor do SLA

Etapa 8.

Configure os parâmetros para a conexão do ISP Principal.

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

Criação de objeto de SLA

Etapa 9.

Depois que o objeto for criado, a rota estática para as interfaces deverá criá-lo. Navegue até o painel principal selecionando o botão 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 do SLA criado

Etapa 10.

Navegue até a Seção de roteamento selecionando a Configuração de exibição no Painel de roteamento.

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 | ISP/WAN/Gateway | Internet | DNS Server | NTP Server | Smart License

No interface named "outside"

Interfaces: Management: Merged, Enabled 4 of 17 | **View All Interfaces**

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

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

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

Smart License: Registered | **View Configuration**

Backup and Restore: **View Configuration**

Troubleshoot: No files created yet | **REQUEST FILE TO BE CREATED**

Painel principal

Etapa 11.

Na guia Static Routing (Roteamento estático), crie as 2 rotas estáticas padrão para ambos os ISPs. Para criar uma nova rota estática, selecione o botão CREATE STATIC ROUTE.

The screenshot shows the 'Static Routing' configuration page in the Cisco Firewall Device Manager. The page is for device 'SF3130'. At the top, there are navigation tabs: 'Monitoring', 'Policies', 'Objects', and 'Device: SF3130'. Below the navigation, there are several buttons: 'Add Multiple Virtual Routers', 'Commands', and 'BGP Global Settings'. The main content area has tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. A filter box is present above the table. The table has the following columns: #, NAME, INTERFACE, IP TYPE, NETWORKS, GATEWAY IP, SLA MONITOR, METRIC, and ACTIONS. The table is currently empty, and a message states 'There are no static routes yet. Start by creating the first static route.' A red box highlights the 'CREATE STATIC ROUTE' button.

Seção de roteamento estático

Etapa 12.

Primeiro, crie a rota estática para o ISP primário. No final, adicione o objeto de monitor de SLA que foi criado na última etapa.

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

Rota estática para ISP primário

Etapa 13.

Repita a última etapa e crie uma rota padrão, para o ISP secundário com o gateway apropriado e uma Métrica diferente. Neste exemplo, ele foi aumentado para 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

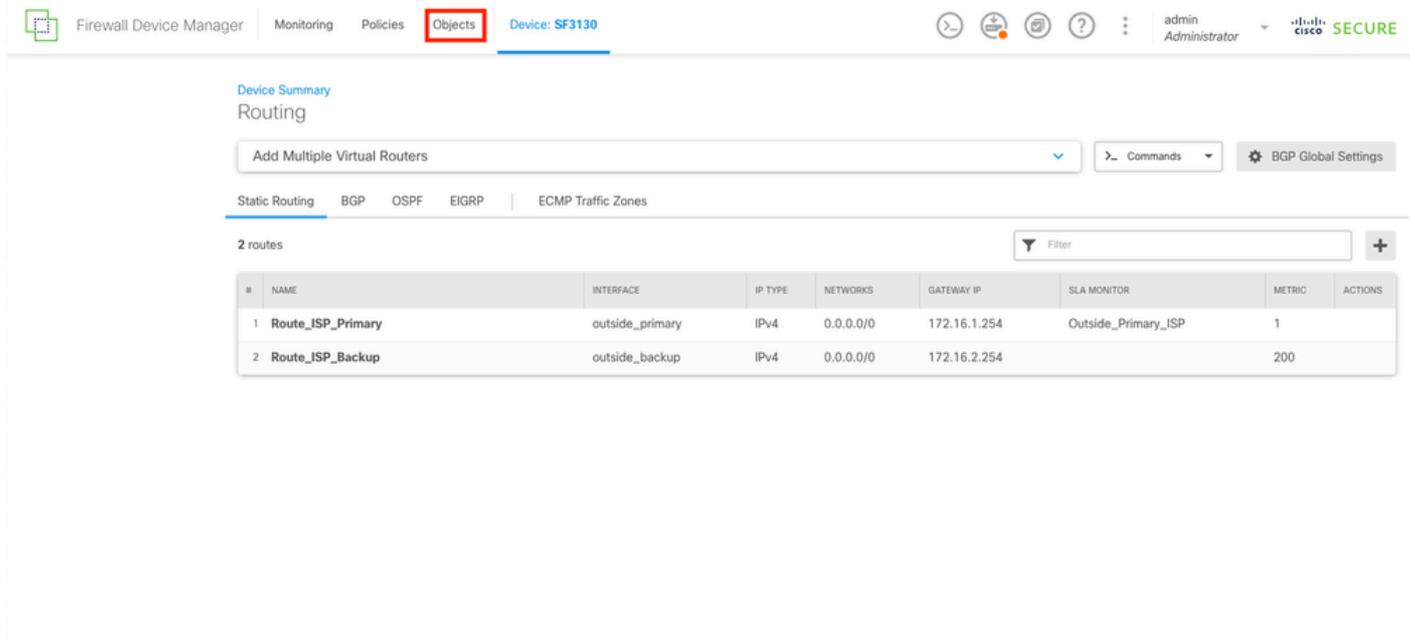
Gateway	Metric
Gateway-Outside-2	200

SLA Monitor Applicable only for IPv4 Protocol type
Please select an SLA Monitor

CANCEL OK

Etapa 14.

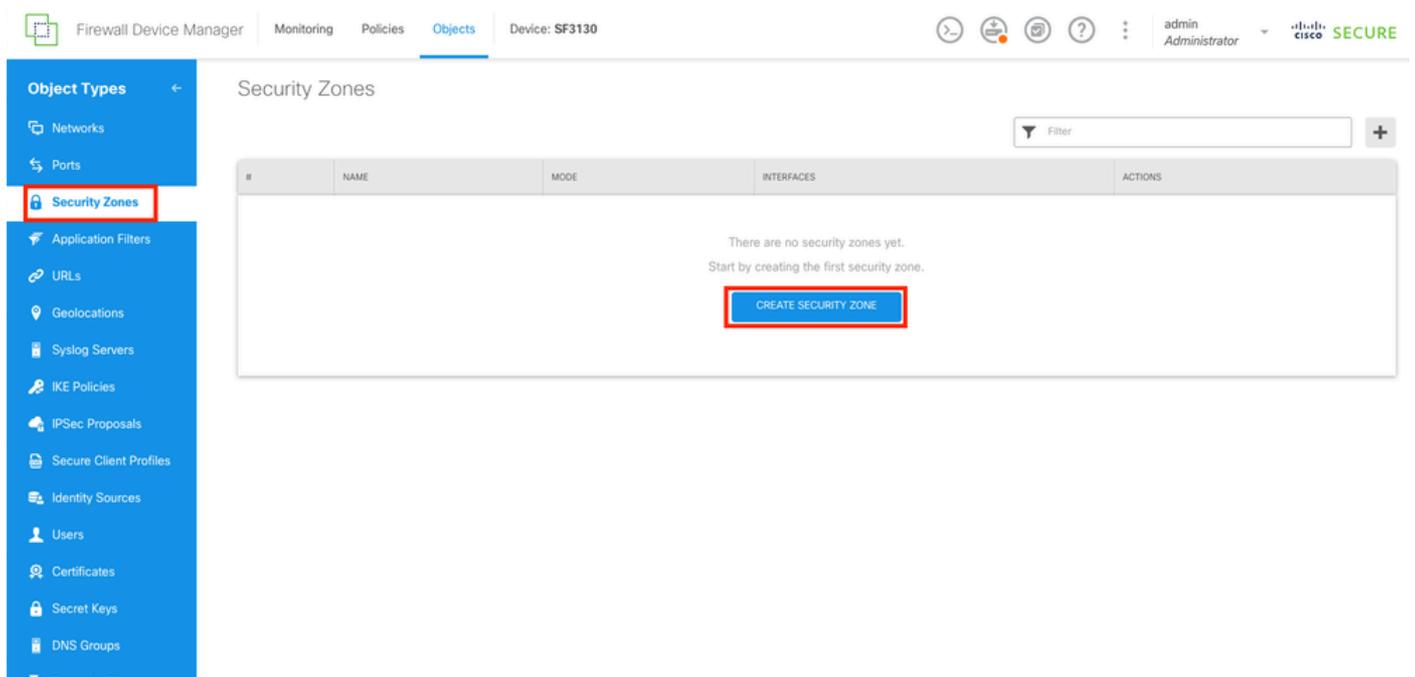
Depois que as duas rotas estáticas forem criadas, uma zona de segurança deverá ser criada. Navegue até a seção Objetos selecionando o botão Objetos na parte superior.



Rotas estáticas criadas

Etapa 15.

Navegue até a seção Zonas de segurança selecionando na coluna esquerda o botão Zonas de segurança e crie uma nova zona selecionando o botão CRIAR ZONA DE SEGURANÇA.



Seção Zonas de Segurança

Etapa 16.

Crie a Outside Security Zone com as duas interfaces externas para as conexões dos ISPs.

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 Segurança Externa

Etapa 17.

Depois que a zona de segurança for criada, um NAT deverá ser criado. Navegue até a seção Policies selecionando o botão Policies na parte superior.

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

admin Administrator | CISCO SECURE

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 segurança criadas

Etapa 18.

Navegue até a seção NAT selecionando o botão NAT e crie uma nova regra selecionando o botão CREATE NAT RULE.

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

admin Administrator | CISCO SECURE

Security Policies

SSL Decryption → Identity → Security Intelligence → **NAT** → Access Control → Intrusion

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

Seção NAT

Etapa 19.

Para o failover do ISP, a configuração deve ter 2 rotas através de interfaces externas. Primeiro, para a conexão da interface externa primária com o ISP primário.

Add NAT Rule

Title: Create Rule for: Status:

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:

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	<input type="text" value="inside"/>	Destination Interface	<input type="text" value="outside_primary"/>
Original Address	<input type="text" value="Inside"/>	Translated Address	<input type="text" value="Interface"/>
Original Port	<input type="text" value="Any"/>	Translated Port	<input type="text" value="Any"/>

Show Diagram

NAT para ISP primário

Etapa 20.

Agora, um segundo NAT para a conexão do ISP secundário.

 Note: Para o endereço original, a mesma rede não pode ser usada. Neste exemplo, para o ISP secundário, o Endereço original é o objeto any-ipv4.

Edit NAT Rule

Title **Create Rule for** **Status**

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**

Packet Translation **Advanced Options**

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	<input type="text" value="inside"/>	Destination Interface	<input type="text" value="outside_backup"/>
Original Address	<input type="text" value="any-ipv4"/>	Translated Address	<input type="text" value="Interface"/>
Original Port	<input type="text" value="Any"/>	Translated Port	<input type="text" value="Any"/>

Show Diagram

NAT para ISP secundário

Etapa 21.

Depois de criar as duas regras de NAT, uma Regra de controle de acesso deve ser estabelecida para permitir o tráfego de saída. Selecione o botão Controle de acesso.

Security Policies

2 rules

#	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	

Regras NAT criadas

Etapa 22.

Para criar a Regra de Controle de Acesso, selecione o botão CRIAR REGRA DE ACESSO.

Security Policies

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

Default Action | Access Control | Block

Seção de Controle de Acesso

Etapa 23.

Selecione as zonas e redes desejadas.

Add Access Rule

Order: 1 | Title: To_Internet | Action: Allow

Source/Destination | Applications | URLs | Users | Intrusion Policy | File policy | Logging

SOURCE				DESTINATION			
Zones	Networks	Ports	SGT Groups	Zones	Networks	Ports	SGT Groups
inside_zone	Inside	ANY	ANY	outside_zone	ANY	ANY	ANY

Show Diagram



Regra de controle de acesso

Etapa 24.

Depois que a Regra de controle de acesso for criada, continue para implantar todas as alterações selecionando o botão Implantar na parte superior.

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

admin Administrator | CISCO SECURE

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
> 1	To_Internet	Allow	inside_zone	Inside	ANY	outside_zone	ANY	ANY	ANY	ANY		

Default Action: Access Control Block

Regra de Controle de Acesso Criada

Etapa 25.

Verifique as alterações e selecione o botão Implantar agora.

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: To_Internet	
-	logFiles: false
-	eventLogAction: LOG_NONE
-	ruleId: 268435458
-	name: To_Internet
sourceZones:	
-	inside_zone
destinationZones:	
-	outside_zone
sourceNetworks:	
-	Inside
+ Security Zone Added: inside_zone	
-	mode: ROUTED
-	description: Inside Zone
-	name: inside_zone
interfaces:	
-	inside
+ SLA Monitor Added: 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 ▾

Verificação de Implantação

Diagrama de Rede

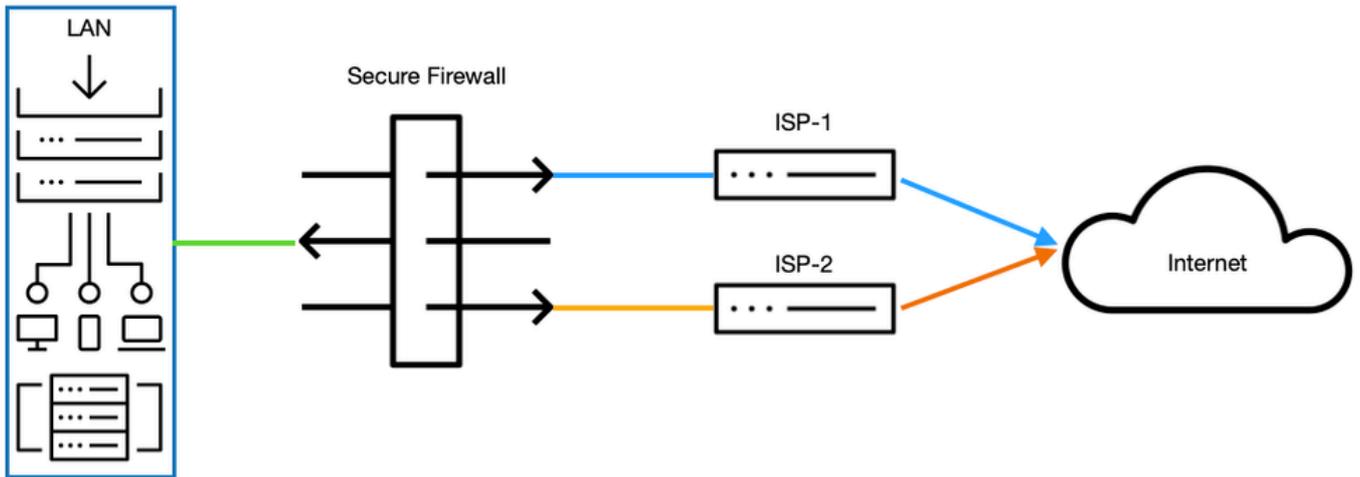


Diagrama de Rede

Verificar

```
<#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

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.