

Dual ISP op FTD configureren met FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u de failover van de Dual Internet Service Provider (ISP) kunt configureren met Firewall Device Manager (FDM) voor de Secure Firewall-reeks.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- basisrouting
- Firewall Device Manager-dashboardkennis
- Minstens twee internetserviceproviders zijn verbonden met de beveiligde firewall.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

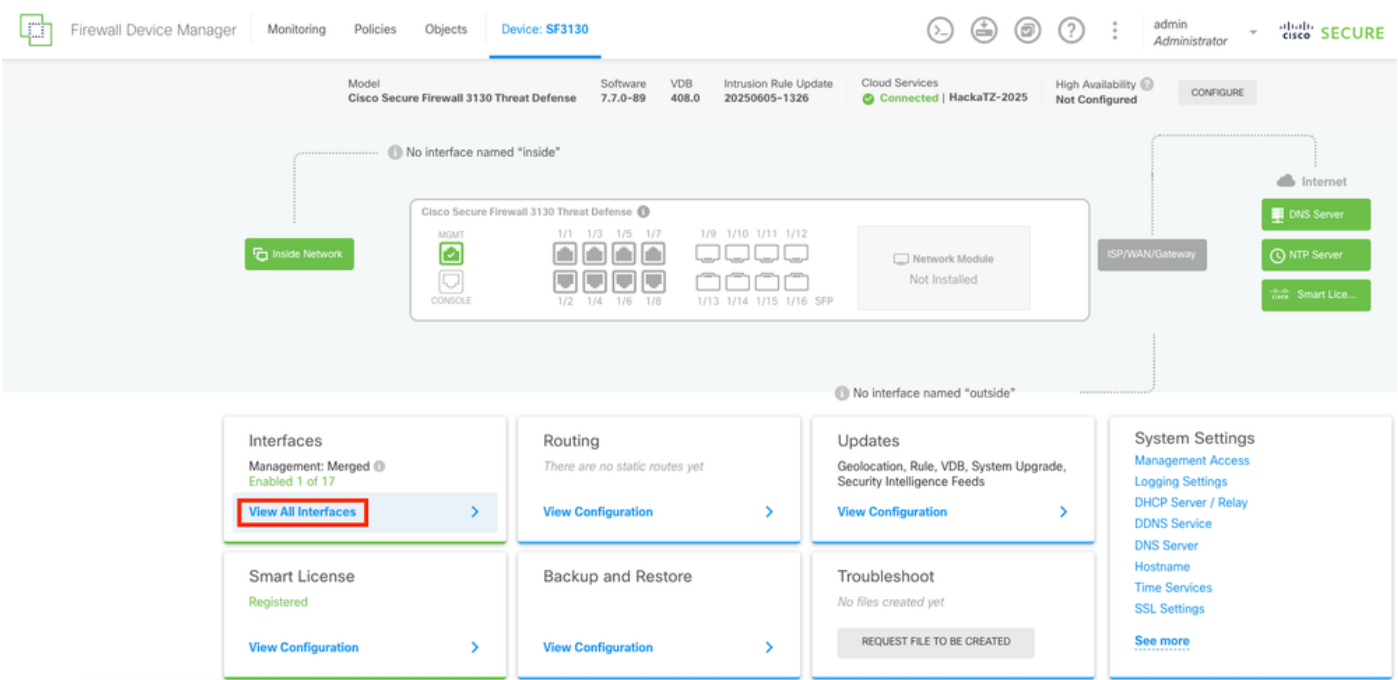
- Cisco Secure Firewall met versie 7.7.X of hogere versies.
- Beveiligde firewall 3130 met versie 7.7.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Stap 1.

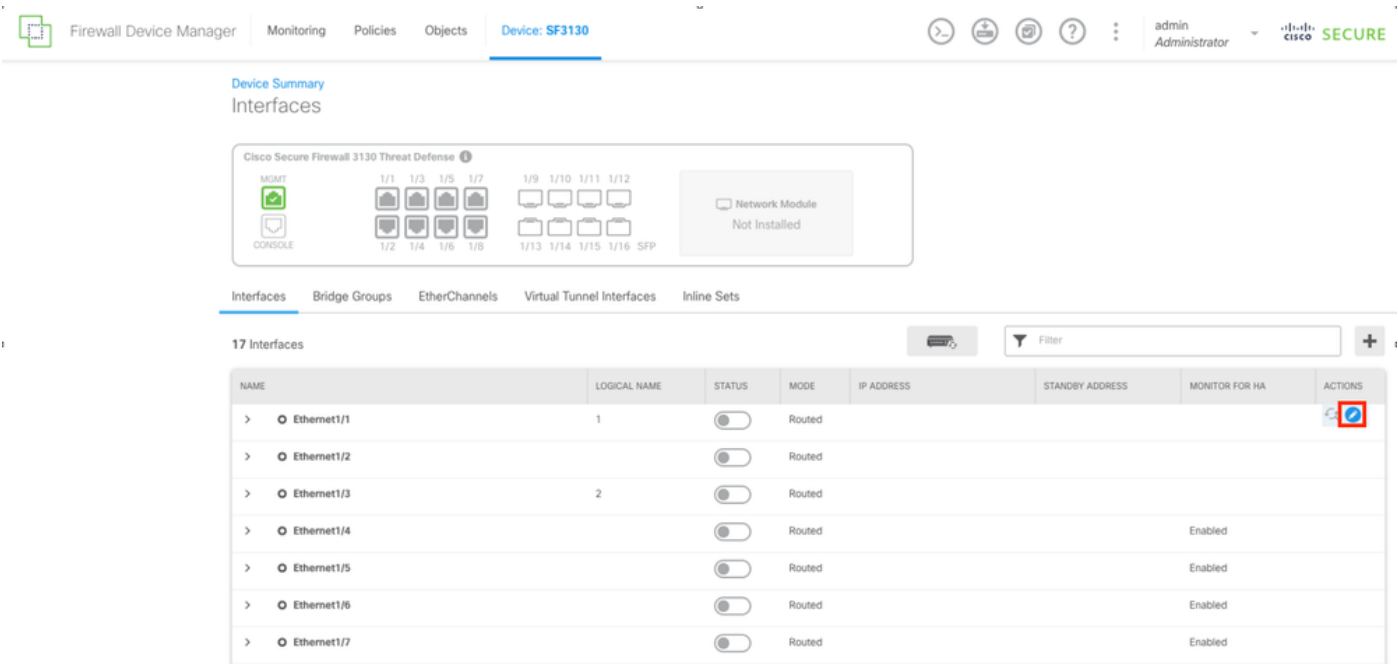
Meld u aan bij de FDM op de beveiligde firewall en navigeer naar de sectie interfaces door de knop Alle interfaces weergeven te selecteren.



Hoofddashboard van FDM

Step 2.

Om de interface voor de primaire ISP-verbinding te configureren, begint u met het selecteren van de gewenste interface. Selecteer de corresponderende knop voor de interface om door te gaan. In dit voorbeeld is de gebruikte interface Ethernet1/1.



Tabblad Interfaces

Step 3.

Configureer de interface met de juiste parameters voor uw primaire ISP-verbinding. In dit voorbeeld is de interface `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

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

Configuratie van primaire ISP-interface

Stap 4.

Herhaal hetzelfde proces voor de secundaire ISP-interface. In dit voorbeeld wordt de interface Ethernet1/2 gebruikt.

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

Configuratie van secundaire ISP-interface

Stap 5.

Nadat u de twee interfaces voor de ISP's hebt geconfigureerd, is de volgende stap het instellen van de SLA-monitor voor de primaire interface.

Navigeer naar de sectie Objecten door de knop Objecten boven in het menu te selecteren.

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	

Geconfigureerde interfaces

Stap 6.

Selecteer in de linkerkolom de knop SLA-monitoren.

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

Objectenscherm

Stap 7.

Maak een nieuwe SLA-monitor door de knop SLA-monitor maken te selecteren.

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				

Sectie SLA-monitor

Stap 8.

De parameters voor de primaire ISP-verbinding configureren.

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

SLA-object maken

Stap 9.

Nadat het object is gemaakt, moet de statische route voor de interfaces het maken. Navigeer naar het hoofddashboard door de knop Apparaat te selecteren.

The screenshot shows the Cisco Secure Firewall Device Manager interface. The top navigation bar includes 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: SF3130'. The left sidebar lists various configuration options, with 'SLA Monitors' highlighted. The main content area is titled 'SLA Monitors' and shows '1 object'. A table lists the object details:

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

SLA-monitor gemaakt

Stap 10.

Navigeer naar de routeringssectie door de weergaveconfiguratie te selecteren in het deelvenster Routing.

The screenshot shows the Cisco Secure Firewall 3130 Threat Defense configuration page. The top navigation bar includes 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: SF3130'. The main content area displays the firewall configuration, including 'Inside Network', 'Cisco Secure Firewall 3130 Threat Defense', and 'ISP/WAN/Gateway'. Below the main configuration, there are several tiles for different sections:

- Interfaces**: Management: Merged, Enabled 4 of 17. View All Interfaces.
- Routing**: There are no static routes yet. View Configuration (highlighted).
- 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.

Hoofddashboard

Stap 11.

Maak op het tabblad Statische routing de 2 standaard statische routes voor beide ISP's. Als u een nieuwe statische route wilt maken, selecteert u de knop STATISCHE ROUTE MAKEN.

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

statische routeringssectie

Stap 12.

Maak eerst de statische route voor de primaire ISP. Voeg aan het einde het SLA-monitorobject toe dat bij de laatste stap is gemaakt.

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

Statische route voor primaire ISP

Stap 13.

Herhaal de laatste stap en maak een standaardroute, voor de secundaire ISP met de juiste gateway en verschillende Metric. In dit voorbeeld is dit verhoogd naar 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

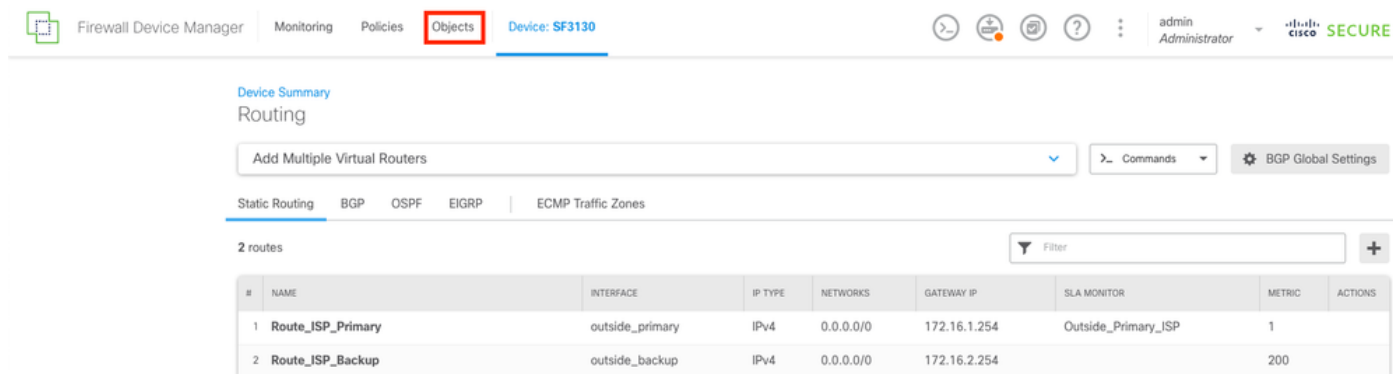
Please select an SLA Monitor

CANCEL

OK

Stap 14.

Zodra beide statische routes zijn gemaakt, moet een beveiligingszone worden gemaakt. Navigeer naar de sectie Objecten door de knop Objecten bovenaan te selecteren.



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

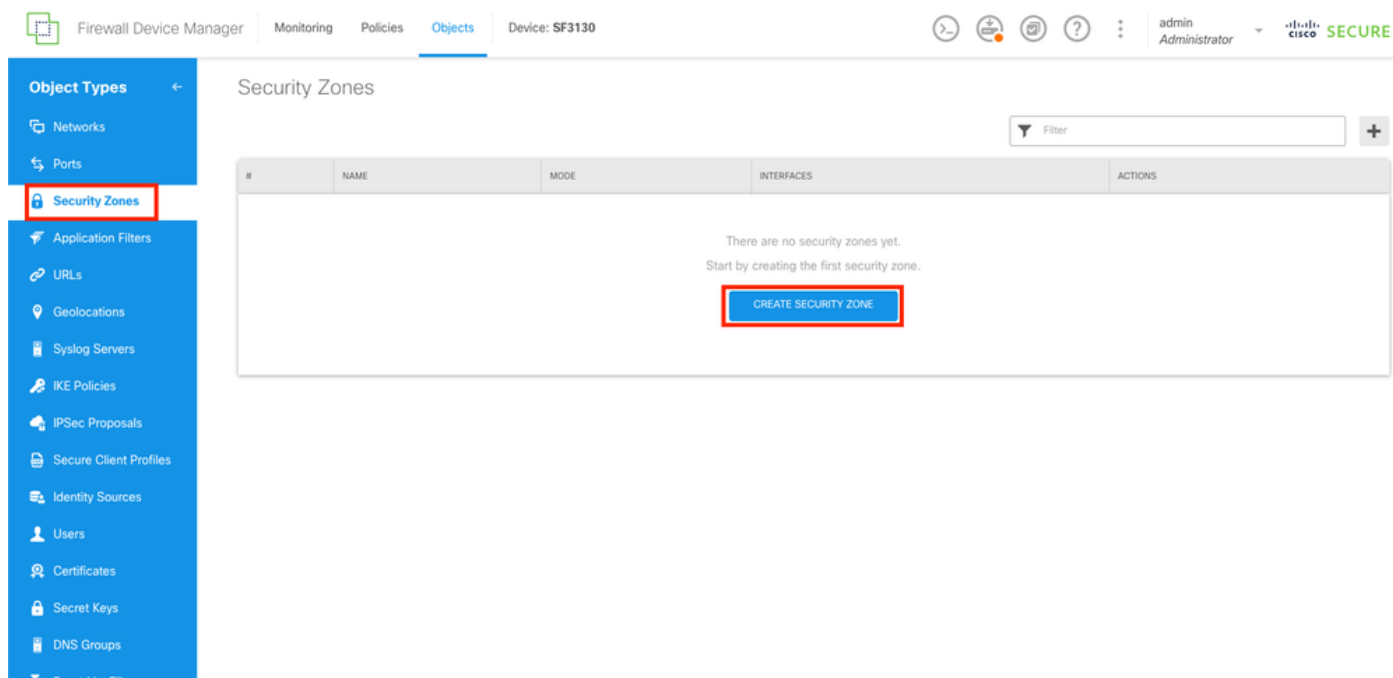
2 routes [Filter] +

#	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	

Statische routes aangemaakt

Stap 15.

Navigeer naar de sectie Beveiligingszones door in de linkerkolom de knop Beveiligingszones te selecteren en maak vervolgens een nieuwe zone door de knop BEVEILIGINGSZONE MAKEN te selecteren.



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				

Stap 16.

Maak de externe beveiligingszone met de beide externe interfaces voor de ISP-verbindingen.

Add Security Zone

Name

outside_zone

Description

Outside Zone

Mode

☒ Routed ☐ Passive ☐ Inline

Interfaces

+

 outside_backup (Ethernet1/2)

 outside_primary (Ethernet1/1)

CANCEL

OK

Veiligheidszone buiten

Stap 17.

Nadat de veiligheidszone is gecreëerd, moet een NAT worden gecreëerd. Navigeer naar het gedeelte Beleid door bovenaan de knop Beleid te selecteren.

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	

Beveiligingszones gemaakt

Stap 18.

Navigeer naar de NAT-sectie door de knop NAT te selecteren en maak vervolgens een nieuwe regel door de knop NAT-REGEL MAKEN te selecteren.

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												

NAT-sectie

Stap 19.

Voor de ISP-failover moet de configuratie twee routes hebben via externe interfaces. Ten eerste voor de verbinding van de primaire externe interface met de primaire ISP.

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 voor primaire ISP

Stap 20.

Nu een tweede NAT voor de Secundaire ISP-verbinding.

 **Opmerking:** voor het oorspronkelijke adres kan niet hetzelfde netwerk worden gebruikt. In dit voorbeeld, voor de secundaire ISP, is het oorspronkelijke adres het object 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 voor secundaire ISP

Stap 21.

Nadat beide NAT-regels zijn gemaakt, moet een toegangscontroleregels worden vastgesteld om uitgaand verkeer mogelijk te maken. Selecteer de knop Toegangscontrole.

Security Policies

→ → → → → **Access Control** → →

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	

NAT-regels gemaakt

Stap 22.

Als u de toegangsregel wilt maken, selecteert u de knop TOEGANGSREGEL MAKEN.

Security Policies

→ → → → → **Access Control** → →

#	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**

sectie Toegangscontrole

Stap 23.

Selecteer de gewenste zones en netwerken.

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
+

DESTINATION

Zones
+

Networks
+

Ports
+

SGT Groups
+

Inside_zone

Inside

ANY

ANY

outside_zone

ANY

ANY

ANY



toegangscontroleregels

Stap 24.

Zodra de toegangsregel is gemaakt, gaat u verder met het implementeren van alle wijzigingen door bovenaan de knop Implementeren te selecteren.

Firewall Device Manager
Monitoring
Policies
Objects
Device: SF3130

Security Policies

→

SSL Decryption

→

Identity

→

Security Intelligence

→

NAT

→

Access Control

→

Intrusion

1 rule

1

NAME
To_Internet

ACTION
Allow

SOURCE

ZONES
Inside_zone

NETWORKS
Inside

PORTS
ANY

DESTINATION

ZONES
outside_zone

NETWORKS
ANY

PORTS
ANY

APPLICATIONS
ANY

URLS
ANY

USERS
ANY

ACTIONS

Default Action
Access Control
Block

Toegangsregel gemaakt

Stap 25.

Controleer de wijzigingen en selecteer vervolgens de knop Nu implementeren.

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																				

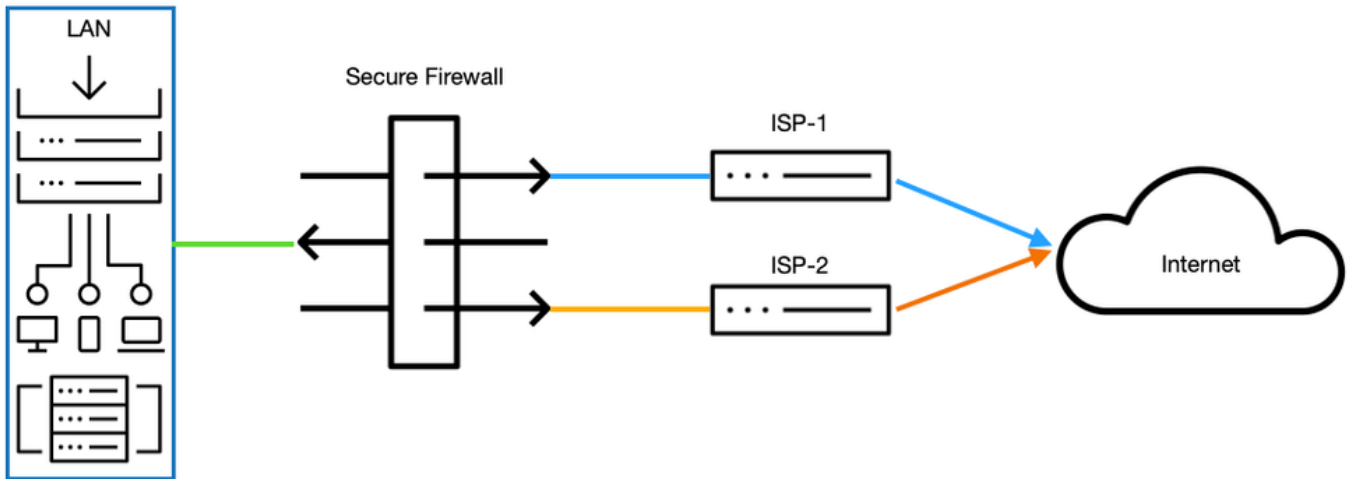
MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

Verificatie van implementatie

Netwerkdigram



Netzwerkdigram

Verifiieren

```
<#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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.