

Konfigurieren von zwei ISPs auf FTD mithilfe von FDM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Dual Internet Service Provider (ISP)-Failover mithilfe des Firewall Device Manager (FDM) für die Secure Firewall Series konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegendes Routing
- Kenntnisse über das Firewall Device Manager-Dashboard
- Mindestens zwei Internet Service Provider, die mit der sicheren Firewall verbunden sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

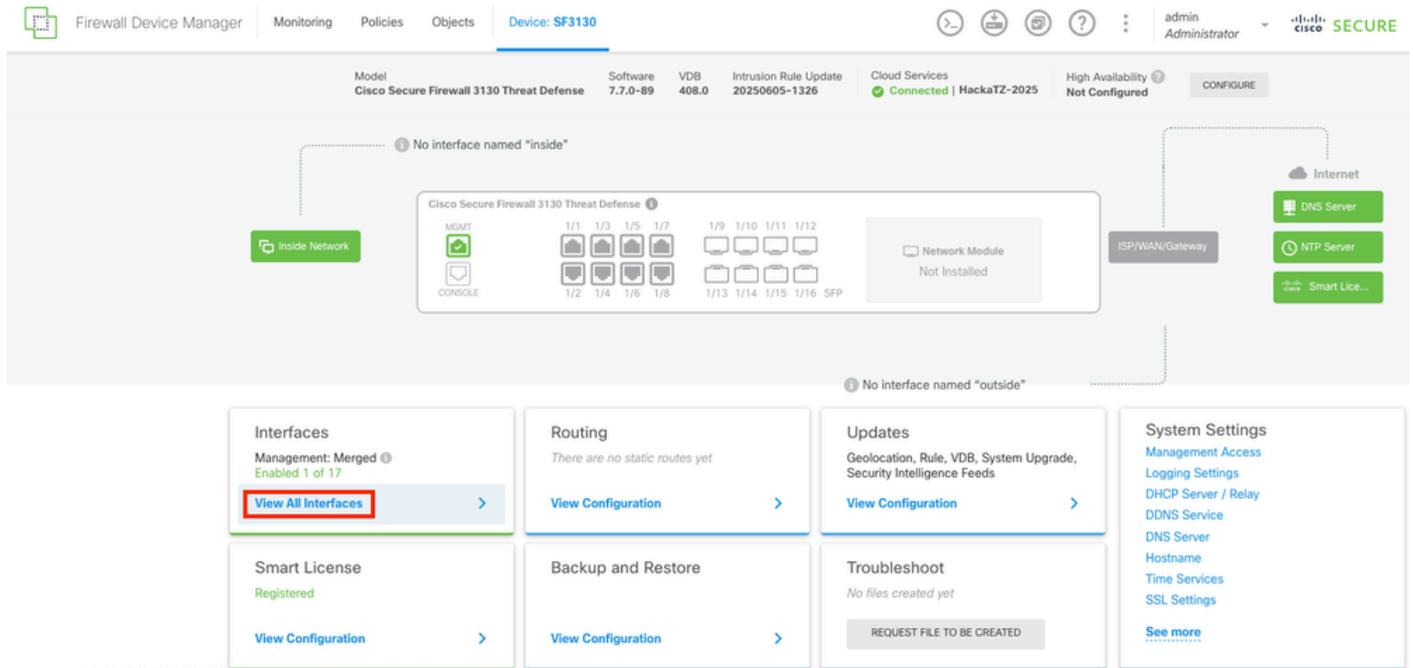
- Cisco Secure Firewall mit Version 7.7.x oder höher
- Secure Firewall 3130 mit Version 7.7.0.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Schritt 1:

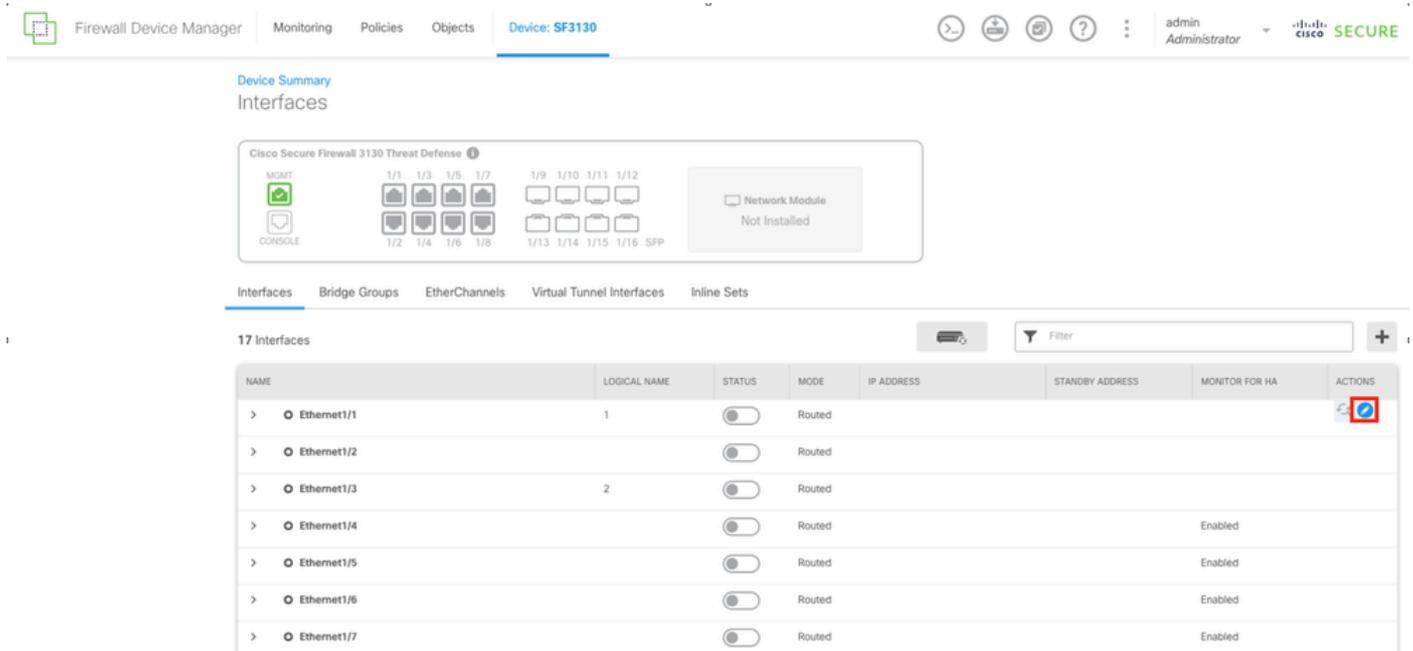
Melden Sie sich beim FDM an der sicheren Firewall an, und navigieren Sie zum Schnittstellenabschnitt, indem Sie auf die Schaltfläche Alle Schnittstellen anzeigen klicken.



FDM-Haupt-Dashboard

Schritt 2:

Um die Schnittstelle für die primäre ISP-Verbindung zu konfigurieren, wählen Sie zunächst die gewünschte Schnittstelle aus. Auswählen der entsprechenden Schnittstellentaste, um fortzufahren. In diesem Beispiel wird als Schnittstelle Ethernet1/1 verwendet.



Schritt 3:

Konfigurieren Sie die Schnittstelle mit den richtigen Parametern für Ihre primäre ISP-Verbindung. In diesem Beispiel ist die Schnittstelle `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

Konfiguration der primären ISP-Schnittstelle

Schritt 4:

Wiederholen Sie den gleichen Vorgang für die sekundäre ISP-Schnittstelle. In diesem Beispiel wird die Schnittstelle `Ethernet1/2` verwendet.

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

Konfiguration der sekundären ISP-Schnittstelle

Schritt 5:

Nach der Konfiguration der beiden Schnittstellen für die ISPs besteht der nächste Schritt darin, den SLA-Monitor für die primäre Schnittstelle einzurichten.

Navigieren Sie zum Abschnitt Objekte, indem Sie die Schaltfläche Objekte oben im Menü auswählen.

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

admin Administrator | cisco SECURE

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
> <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	

Konfigurierte Schnittstellen

Schritt 6:

Wählen Sie in der linken Spalte die Schaltfläche SLA Monitors aus.

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

admin Administrator | cisco SECURE

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

Bildschirm "Objekte"

Schritt 7.

Erstellen Sie einen neuen SLA-Monitor, indem Sie auf die Schaltfläche SLA-Monitor erstellen klicken.

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				

Abschnitt SLA-Monitor

Schritt 8:

Konfigurieren Sie die Parameter für die primäre ISP-Verbindung.

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

Erstellung von SLA-Objekten

Schritt 9.

Nachdem das Objekt erstellt wurde, muss es von der statischen Route für die Schnittstellen erstellt werden. Navigieren Sie zum Haupt-Dashboard, indem Sie auf die Schaltfläche Device (Gerät) klicken.

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	

SLA-Monitor erstellt

Schritt 10.

Navigieren Sie zum Abschnitt Routing, indem Sie im Routing-Bereich die Option View Configuration (Konfiguration anzeigen) auswählen.

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 | Network Module: Not Installed | ISP/WAN/Gateway | Internet | DNS Server | NTP Server | Smart Lic...

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

Schritt 11.

Erstellen Sie auf der Registerkarte Static Routing (Statisches Routing) die beiden statischen Standardrouten für beide ISPs. Um eine neue statische Route zu erstellen, wählen Sie die Schaltfläche STATISCHE Route ERSTELLEN.

The screenshot shows the 'Static Routing' configuration page for device SF3130. The page includes a navigation bar with 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: SF3130'. Below the navigation bar, there are tabs for 'Static Routing', 'BGP', 'OSPF', 'EIGRP', and 'ECMP Traffic Zones'. The 'Static Routing' tab is selected. The main content area displays a table with 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 blue button labeled 'CREATE STATIC ROUTE' is highlighted with a red rectangle.

Abschnitt für statisches Routing

Schritt 12:

Erstellen Sie zunächst die statische Route für den primären ISP. Fügen Sie am Ende das SLA-Überwachungsobjekt hinzu, das im letzten Schritt erstellt wurde.

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 für primären ISP

Schritt 13:

Wiederholen Sie den letzten Schritt, und erstellen Sie eine Standardroute für den sekundären ISP mit dem richtigen Gateway und einer anderen Metrik. In diesem Beispiel wurde sie auf 200 erhöht.

Add Static Route ? ×

Name

Description

Interface

Protocol

IPv4 IPv6

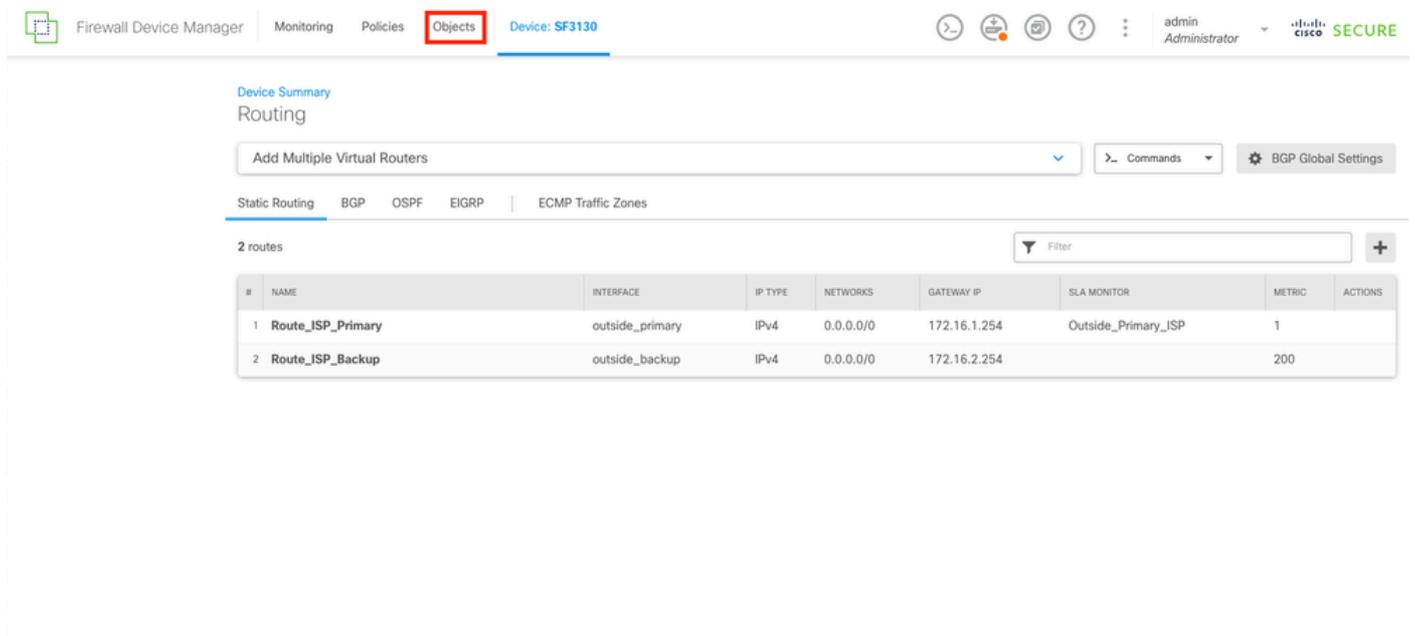
Networks

Gateway	Metric
<input type="text" value="Gateway-Outside-2"/>	<input type="text" value="200"/>

SLA Monitor Applicable only for IPv4 Protocol type

Schritt 14:

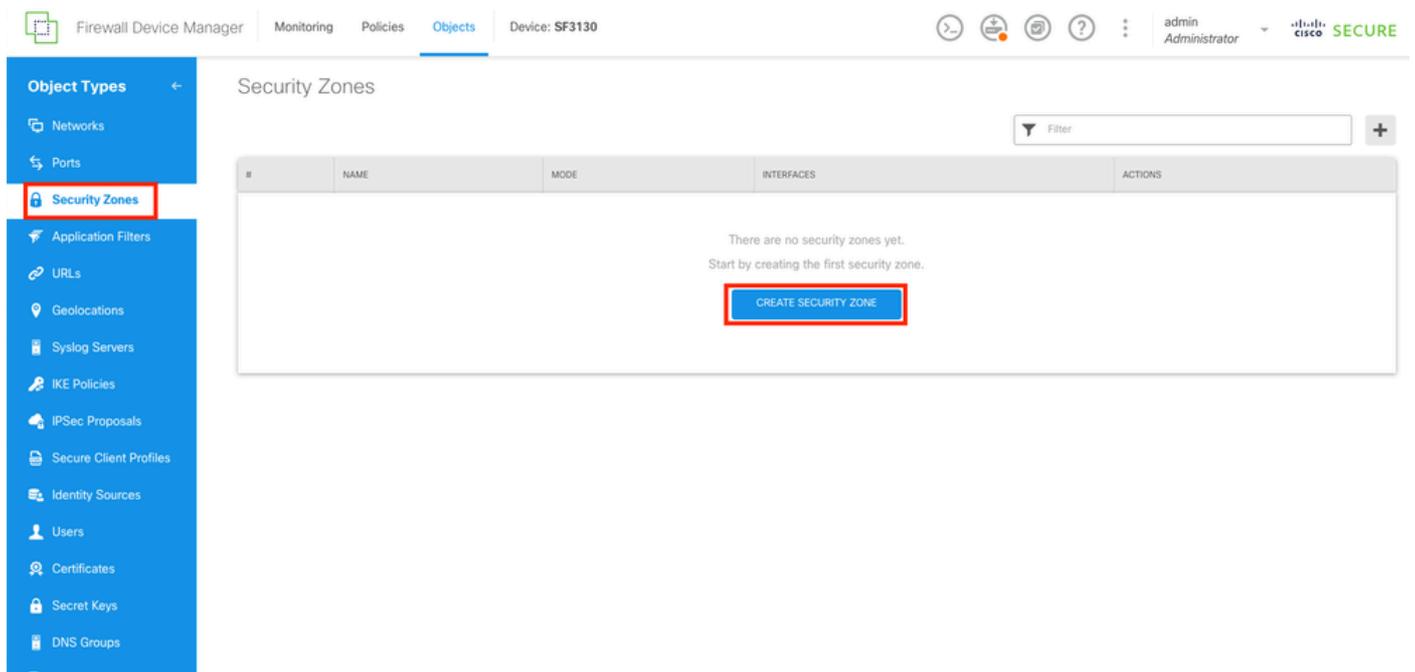
Nachdem beide statischen Routen erstellt wurden, muss eine Sicherheitszone erstellt werden. Navigieren Sie zum Abschnitt Objekte, indem Sie oben auf die Schaltfläche Objekte klicken.



Statische Routen erstellt

Schritt 15:

Navigieren Sie zum Abschnitt Sicherheitszonen, indem Sie in der linken Spalte die Schaltfläche Sicherheitszonen auswählen. Erstellen Sie dann eine neue Zone, indem Sie die Schaltfläche SICHERHEITSSZONE ERSTELLEN auswählen.



Schritt 16:

Erstellen Sie die externe Sicherheitszone mit den beiden externen Schnittstellen für die ISP-Verbindungen.

Add Security Zone

Name
outside_zone

Description
Outside Zone

Mode
 Routed Passive Inline

Interfaces
+
outside_backup (Ethernet1/2)
outside_primary (Ethernet1/1)

CANCEL OK

Sicherheitszone außerhalb

Schritt 17:

Nachdem die Sicherheitszone erstellt wurde, muss eine NAT erstellt werden. Navigieren Sie zum Abschnitt Policies (Richtlinien), indem Sie oben auf die Schaltfläche Policies (Richtlinien) klicken.

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	

Sicherheitszonen erstellt

Schritt 18:

Navigieren Sie zum Abschnitt NAT, indem Sie die Schaltfläche NAT auswählen, und erstellen Sie dann eine neue Regel, indem Sie die Schaltfläche CREATE NAT RULE (NAT-REGEL ERSTELLEN) auswählen.

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>												

NAT-Abschnitt

Schritt 19:

Für den ISP-Failover muss die Konfiguration über zwei Routen über externe Schnittstellen verfügen. Zunächst für die primäre externe Schnittstellenverbindung zum primären ISP.

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 für primären ISP

Schritt 20:

Nun eine zweite NAT für die sekundäre ISP-Verbindung.

 Anmerkung: Für die ursprüngliche Adresse kann nicht dasselbe Netzwerk verwendet werden. In diesem Beispiel ist die ursprüngliche Adresse für den sekundären ISP das Objekt 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 für sekundären ISP

Schritt 21:

Nachdem beide NAT-Regeln erstellt wurden, muss eine Zugriffskontrollregel eingerichtet werden, die ausgehenden Verkehr zulässt. Wählen Sie die Schaltfläche Zugriffskontrolle aus.

Security Policies

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

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-Regeln erstellt

Schritt 22:

Wählen Sie zum Erstellen der Zugriffskontrollregel die Schaltfläche ZUGRIFFSREGEL ERSTELLEN.

Security Policies

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

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

Default Action: Access Control Block

Abschnitt "Zugriffskontrolle"

Schritt 23:

Wählen Sie die gewünschten Zonen und Netzwerke aus.

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



Zugriffskontrollregel

Schritt 24:

Nachdem die Zugriffskontrollregel erstellt wurde, können Sie mit der Bereitstellung aller Änderungen fortfahren, indem Sie oben auf die Schaltfläche Bereitstellen klicken.

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

Zugriffskontrollregel erstellt

Schritt 25:

Überprüfen Sie die Änderungen, und klicken Sie dann auf die Schaltfläche Jetzt bereitstellen.

Pending Changes ? ×

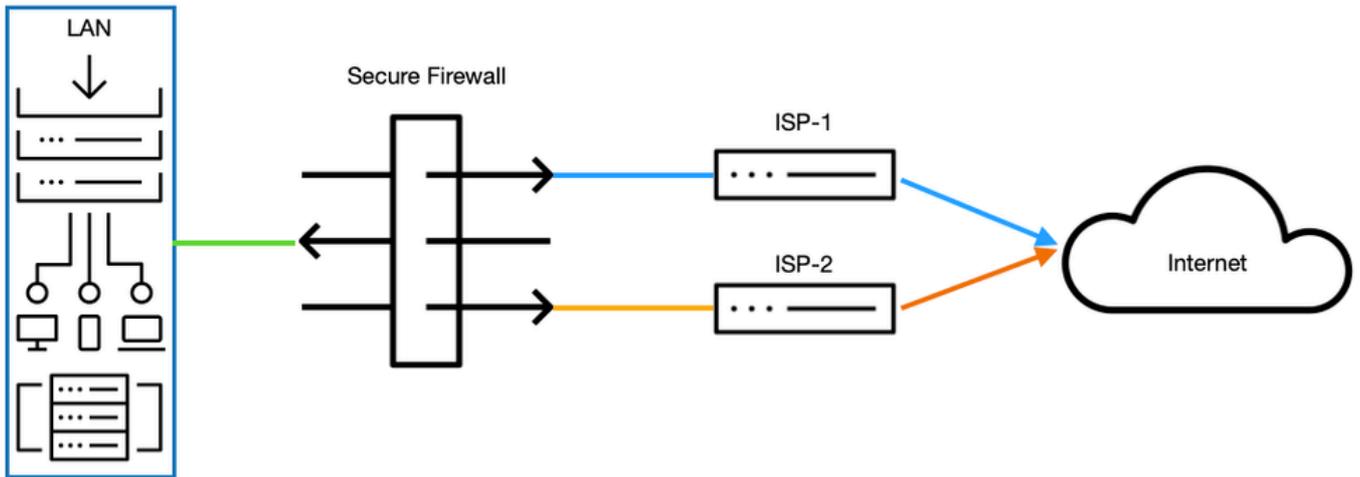
✔ **Last Deployment Completed Successfully**
10 Jun 2025 12:35 PM. [See Deployment History](#)

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 ▼

Bereitstellungsüberprüfung

Netzwerkdiagramm



Netzwerkdigramm

Überprüfung

```
<#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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.