

FDMを使用したFTDでのデュアルISPの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[確認](#)

はじめに

このドキュメントでは、Secure Firewallシリーズのファイアウォールデバイスマネージャ (FDM)を使用して、デュアルインターネットサービスプロバイダー (ISP) フェールオーバーを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 基本的なルーティング
- ファイアウォールデバイスマネージャダッシュボードの知識
- 少なくとも2つのインターネットサービスプロバイダーがセキュアファイアウォールに接続している。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

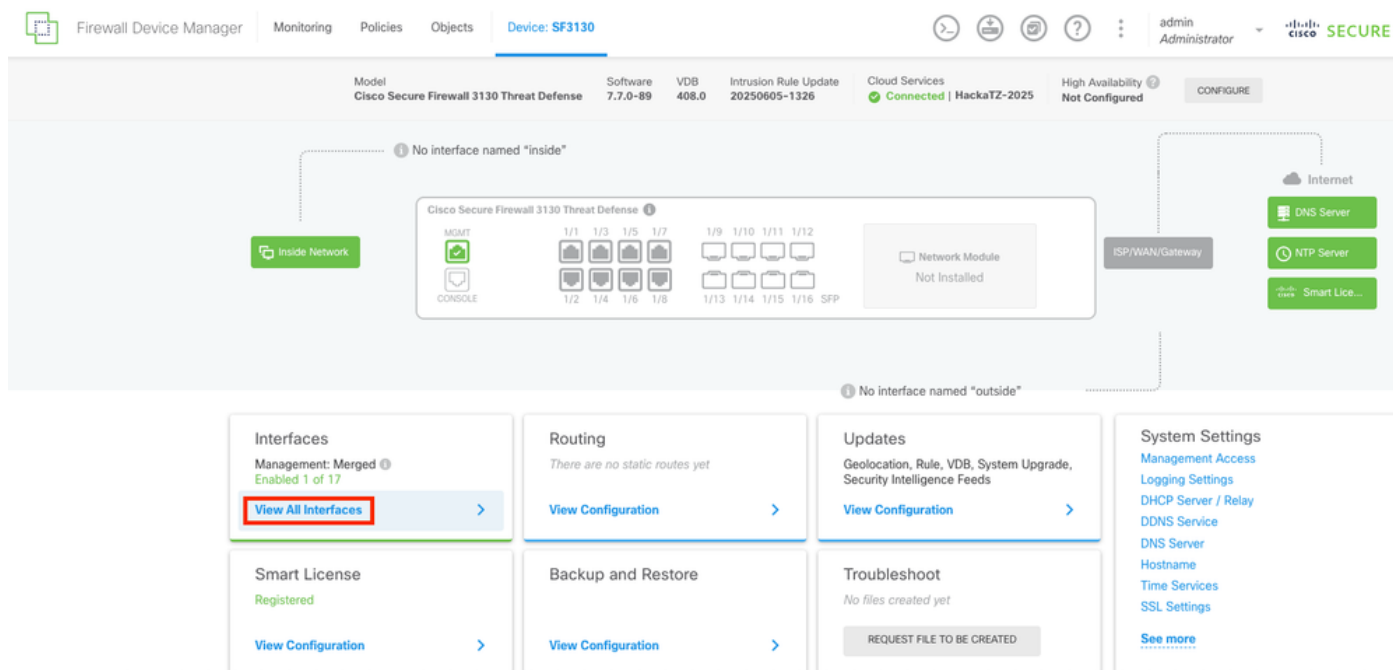
- 7.7.X以降のバージョンが稼働するCisco Secure Firewall
- 7.7.0バージョンがインストールされたファイアウォール3130を保護します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ステップ 1 :

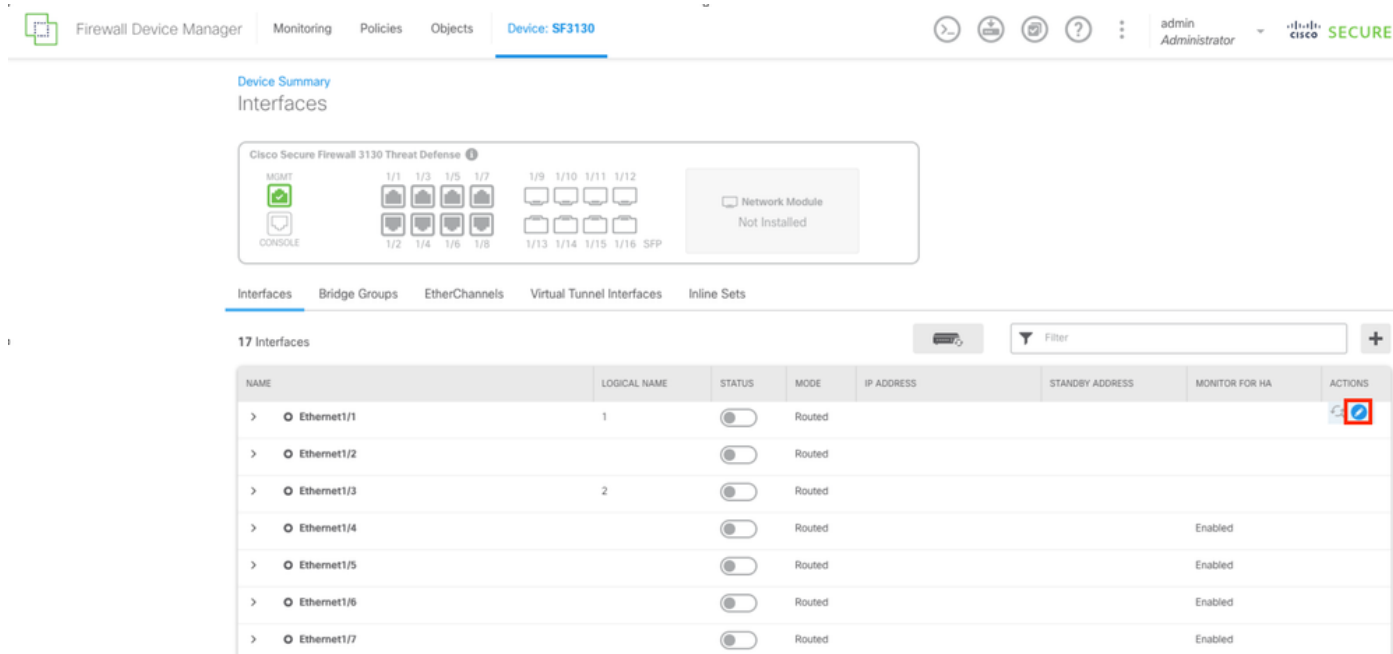
セキュアファイアウォールのFDMにログインし、View All Interfacesボタンを選択してinterfacesセクションに移動します。



FDMメイン・ダッシュボード

ステップ 2 :

プライマリISP接続のインターフェイスを設定するには、まず目的のインターフェイスを選択します。続行するには、対応するインターフェイスボタンを選択します。この例で使用するインターフェイスはEthernet1/1です。



Interfacesタブ

ステップ 3 :

プライマリISP接続の正しいパラメータを使用してインターフェイスを設定します。この例では、インターフェイスはoutside_primaryです。

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

プライマリISPインターフェイスの設定

ステップ 4 :

セカンダリISPインターフェイスに対して同じプロセスを繰り返します。この例では、インターフェイスEthernet1/2が使用されています。

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

セカンダリISPインターフェイスの設定

ステップ 5 :

ISPの2つのインターフェイスを設定した後、次の手順では、プライマリインターフェイスのSLAモニタを設定します。

メニューの上部にあるObjectsボタンを選択して、Objectsセクションに移動します。

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	

設定されたインターフェイス

手順 6 :

左側の列でSLA Monitorsボタンを選択します。

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

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

Filter

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

#	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

Objects画面

手順 7 :

Create SLA Monitorボタンを選択して、新しいSLAモニタを作成します。

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				

SLA Monitorセクション

ステップ 8 :

プライマリISP接続のパラメータを設定します。

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オブジェクトの作成

ステップ 9 :

オブジェクトが作成されたら、インターフェイスのステイックルルートでオブジェクトを作成する必要があります。Deviceボタンを選択して、メインダッシュボードに移動します。

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

SLA Monitors

1 object

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

SLAモニタが作成されました

ステップ 10 :

Routing PanelでView Configurationを選択して、Routing Sectionに移動します。

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

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

Smart License: Registered | View Configuration

Routing: There are no static routes yet | **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

メインダッシュボード

ステップ 11

Static Routingタブで、両方のISPの2つのデフォルトスタティックルートを作成します。新しいスタティックルートを作成するには、CREATE STATIC ROUTEボタンを選択します。

The screenshot shows the Cisco Firewall Device Manager interface for device SF3130. The 'Static Routing' tab is active, displaying a table with columns: #, NAME, INTERFACE, IP TYPE, NETWORKS, GATEWAY IP, SLA MONITOR, METRIC, and ACTIONS. The table is 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.

Static Routingセクション

ステップ 12

最初に、プライマリISPのスタティックルートを作成します。最後に、最後の手順で作成したSLAモニタオブジェクトを追加します。

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

プライマリISPのスタティックルート

ステップ 13

最後の手順を繰り返し、適切なゲートウェイと異なるメトリックを使用するISPセカンダリのデフォルトルートを作成します。この例では、200に増やされています。

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

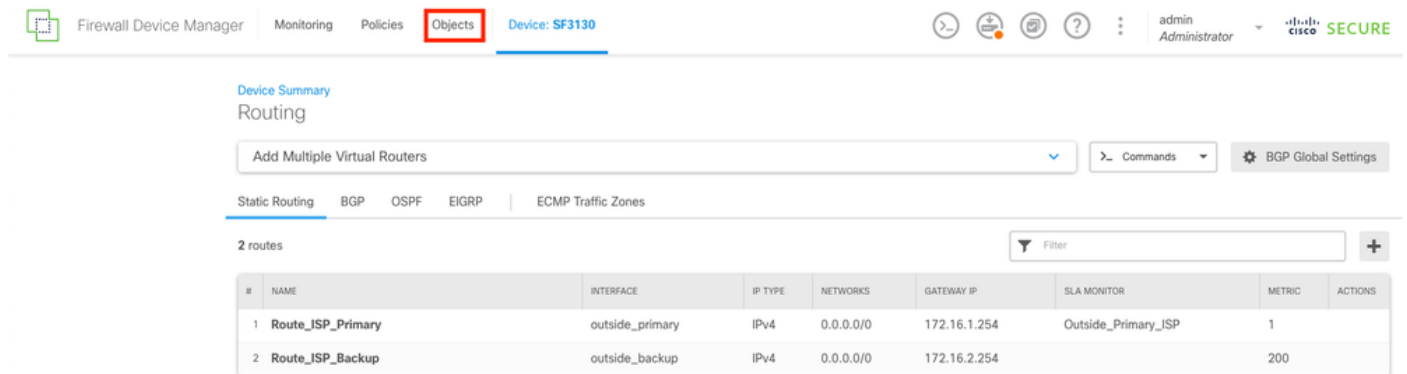
Please select an SLA Monitor

CANCEL

OK

ステップ 14 :

両方のスタティックルートが作成されたら、セキュリティゾーンを作成する必要があります。上部にあるObjectsボタンを選択して、Objectsセクションに移動します。



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

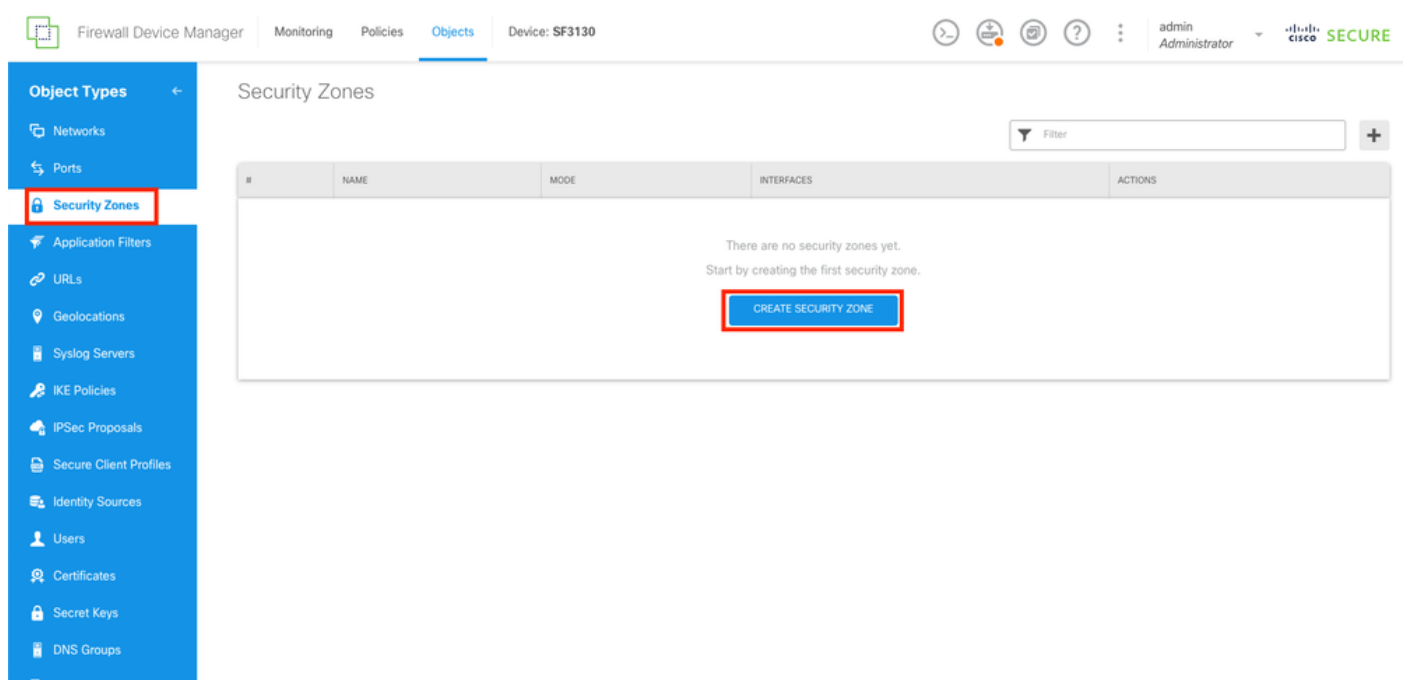
2 routes [Filter] +

#	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	

作成されたスタティックルート

ステップ 15 :

Security Zonesセクションの左側の列でSecurity Zonesボタンを選択してSecurity Zonesセクションに移動し、CREATE SECURITY ZONEボタンを選択して新しいゾーンを作成します。



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
 Guest List Filter

Security Zones [Filter] +

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

Security Zonesセクション

ステップ 16 :

ISP接続の両方の外部インターフェイスを使用して外部セキュリティゾーンを作成します。

Add Security Zone

Name

outside_zone

Description

Outside Zone

Mode

☒ Routed ☐ Passive ☐ Inline

Interfaces

+

 outside_backup (Ethernet1/2)

 outside_primary (Ethernet1/1)

CANCEL

OK

外部のセキュリティゾーン

ステップ 17 :

セキュリティゾーンが作成された後、NATを作成する必要があります。上部にあるPoliciesボタンを選択して、Policiesセクションに移動します。

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	

作成されたセキュリティゾーン

ステップ 18 :

NATボタンを選択してNATセクションに移動してから、CREATE NAT RULEボタンを選択して新しいルールを作成します。

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セクション

ステップ 19 :

ISPフェールオーバーの場合、設定には外部インターフェイスを経由する2つのルートが必要です。まず、プライマリISPへのプライマリ外部インターフェイス接続が必要です。

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

プライマリISPのNAT

ステップ 20 :

次に、セカンダリISP接続用の2番目のNATです。

 注：元のアドレスに対して、同じネットワークを使用することはできません。この例では、セカンダリISPの場合、元のアドレスはオブジェクトany-ipv4です。

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

セカンダリISP用NAT

ステップ 21 :

両方のNATルールを作成した後、アウトバウンドトラフィックを許可するためにアクセスコントロールルールを確立する必要があります。Access Controlボタンを選択します。

Security Policies

→ → → → → **Access Control** → Intrusion

2 rules

			ORIGINAL PACKET				TRANSLATED PACKET					
#	NAME	TYPE	INTERFACES	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	SOURCE AD...	DESTINATIO...	SOURCE PORT	DESTINATIO...	ACTIONS
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	

作成されたNATルール

ステップ 22 :

アクセスコントロールルールを作成するには、CREATE ACCESS RULEボタンを選択します。

Security Policies

→ → → → → **Access Control** → Intrusion

#	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**

Access Controlセクション

ステップ 23 :

必要なゾーンとネットワークを選択します。

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 ☒



アクセスコントロールルール

ステップ 24 :

アクセスコントロールルールを作成したら、上部のDeployボタンを選択して、すべての変更の展開に進みます。

Firewall Device Manager Monitoring Policies Objects Device: SF3130

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	ANY	

Default Action: Access Control Block

アクセスコントロールルールが作成されました

ステップ 25 :

変更を確認し、「今すぐ配備」ボタンを選択します。

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>	
-	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>	
-	mode: ROUTED
-	description: Inside Zone
-	name: inside_zone
interfaces:	
-	inside
+ SLA Monitor Added: <i>Outside_Primary_ISP</i>	
-	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

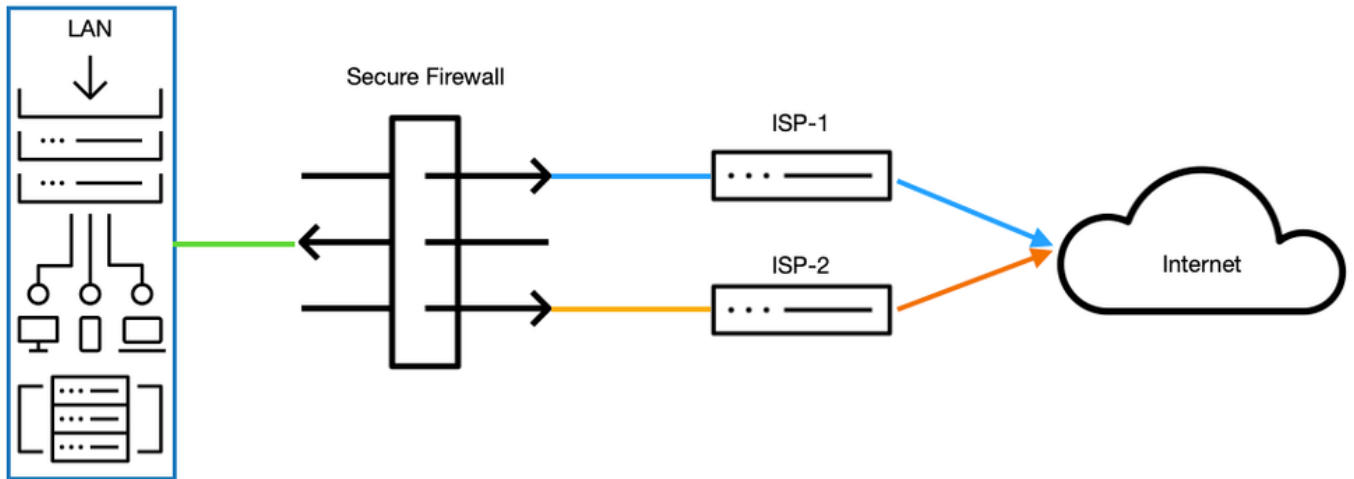
MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

導入の検証

ネットワーク図



ネットワーク図

確認

<#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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。