

使用FDM在FTD上配置雙ISP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[驗證](#)

簡介

本文檔介紹如何使用安全防火牆系列的防火牆裝置管理器(FDM)配置雙網際網路服務提供商(ISP)故障切換。

必要條件

需求

思科建議您瞭解以下主題：

- 基本路由
- 防火牆裝置管理器控制面板知識
- 至少有2個網際網路服務提供商連線到安全防火牆。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

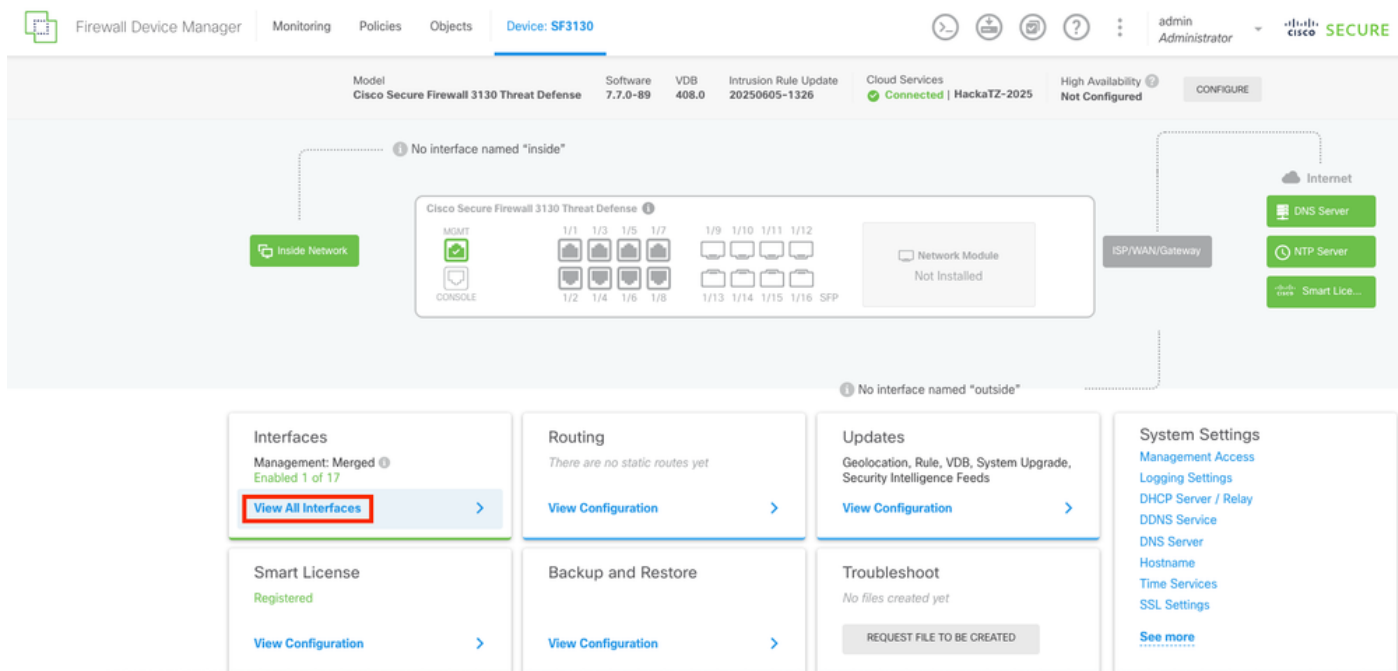
- 運行7.7.X或更高版本的思科安全防火牆。
- 7.7.0版本的安全防火牆3130。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

步驟 1.

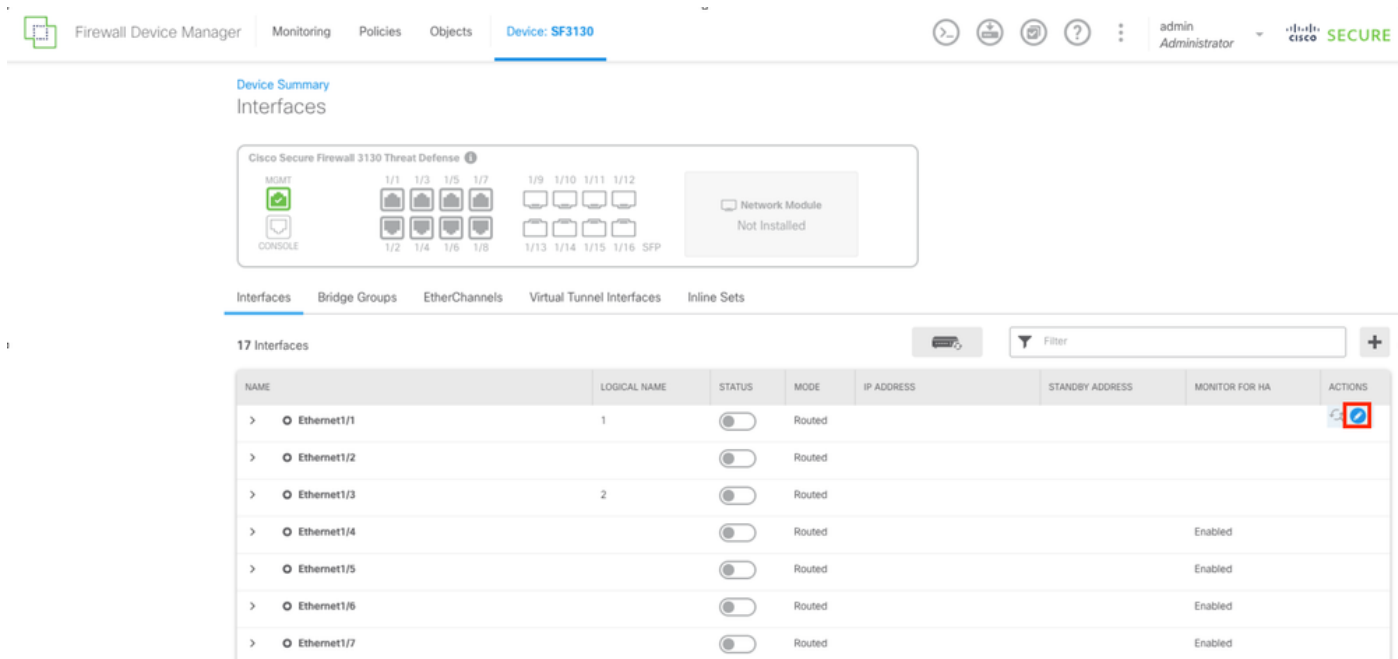
登入到Secure Firewall上的FDM，然後選擇View All Interfaces按鈕導航到Interfaces部分。



FDM主儀表板

步驟 2.

要配置主ISP連線的介面，首先選擇所需的介面。選擇相應的interface按鈕以繼續。在本範例中，使用的介面是Ethernet1/1。



Interfaces頁籤

步驟 3.

使用適合您的主ISP連線的正確引數配置介面。在本示例中，介面為outside_primary。

Ethernet1/1

Edit Physical Interface



Interface Name

outside_primary

Mode

Routed

Status



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

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

主ISP介面的配置

步驟 4.

對輔助ISP介面重複相同的過程。在本範例中，使用介面Ethernet1/2。

Ethernet1/2

Edit Physical Interface



Interface Name

outside_backup

Mode

Routed

Status



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

Description

ISP Backup



IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

172.16.2.1

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

/

e.g. 192.168.5.16

CANCEL

OK

輔助ISP介面的配置

步驟 5.

為ISP配置兩個介面後，下一步是為主介面設定SLA監控器。

通過選擇位於選單頂部的對象按鈕導航到對象部分。

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	

已配置的介面

步驟 6.

在左側的列中選擇SLA Monitor按鈕。

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

對象螢幕

步驟 7.

通過選擇Create SLA Monitor按鈕建立新的SLA Monitor。

Firewall Device Manager

MonitoringPoliciesObjects

Device: SF3130

>

adminAdministrator

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

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部分

步驟 8.

配置主ISP連線的引數。

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對象建立

步驟 9.

建立對象後，介面的靜態路由必須建立該對象。選擇Device(設備)按鈕，導航到主控制面板。

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	

已建立SLA監控器

步驟 10.

在「路由選擇面板」中選擇View Configuration，即可導航到Routing部分。

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 | Internet | DNS Server | NTP Server | Smart License

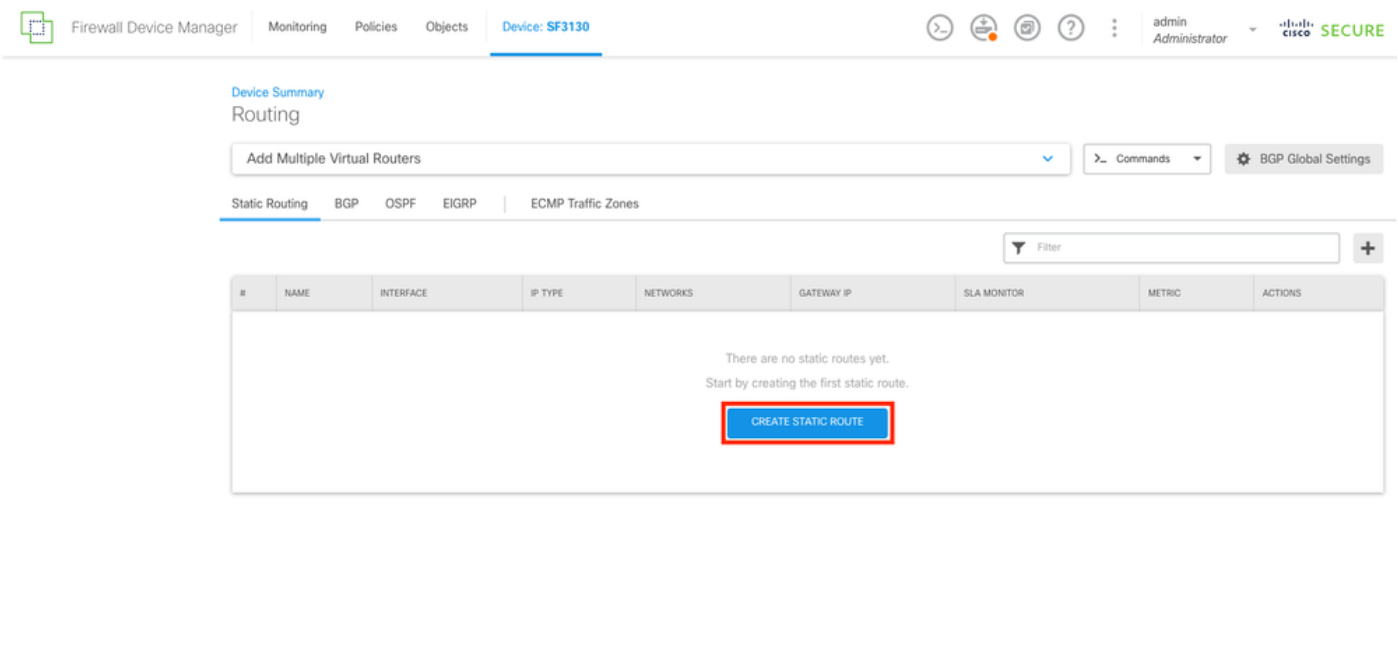
Interfaces: Management: Merged (Enabled 4 of 17) | View All Interfaces | Routing: There are no static routes yet | **View Configuration** | Updates: Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds | View Configuration | System Settings: Management Access, Logging Settings, DHCP Server / 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

主控制面板

步驟 11.

在Static Routing頁籤上，為兩個ISP建立2個預設靜態路由。要建立新的靜態路由，請選擇CREATE STATIC ROUTE按鈕。



靜態路由部分

步驟 12.

首先，為主要ISP建立Static Route。最後，新增在上一步中建立的SLA監控對象。

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

主ISP的靜態路由

步驟 13.

重複最後一步，為ISP輔助建立預設路由，該路由具有正確的網關和不同的度量。在本例中，它增加到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

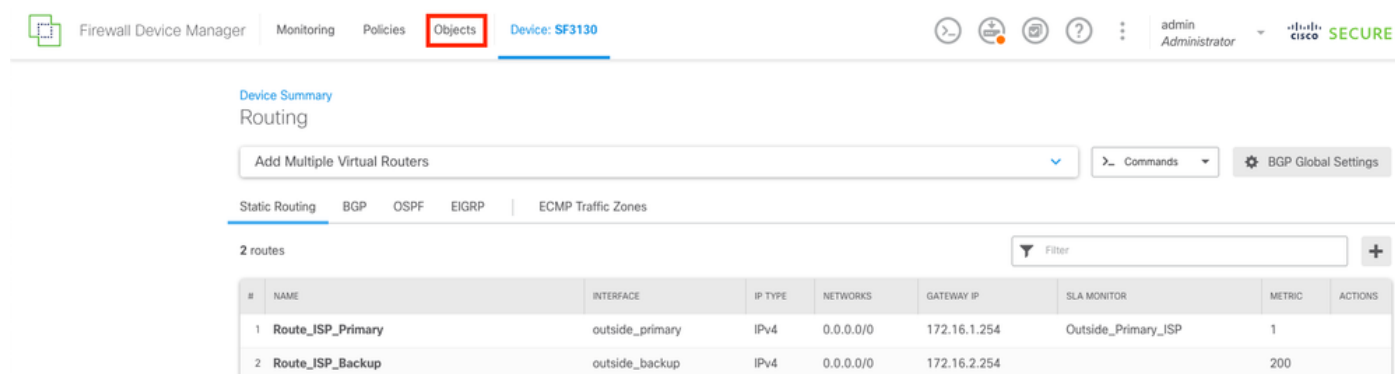
CANCEL

OK

輔助ISP的靜態路由

步驟 14.

建立兩個靜態路由後，必須建立安全區域。通過選擇頂部的對象按鈕導航到對象部分。



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

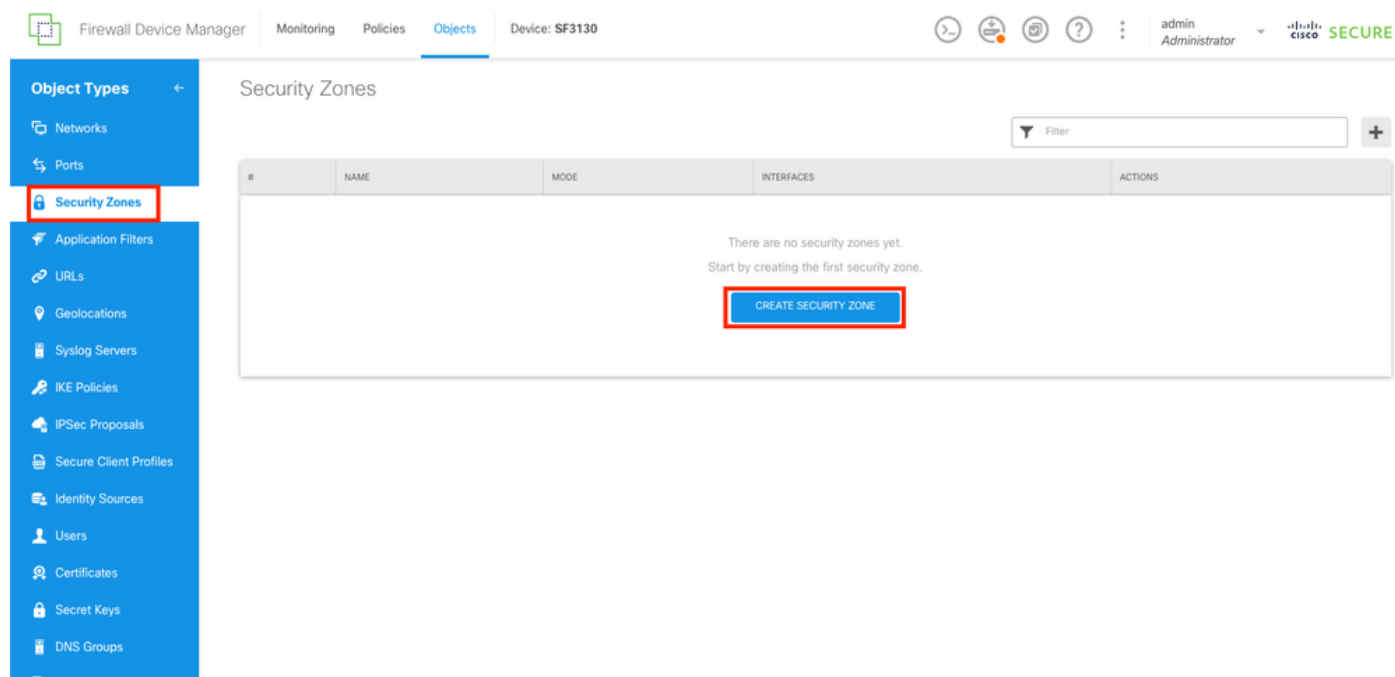
2 routes [Filter] +

#	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	

已建立靜態路由

步驟 15.

在左側列中選擇Security Zones按鈕，導航到Security Zones部分，然後通過選擇CREATE SECURITY ZONE按鈕建立一個新區域。



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
Custom 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				

安全區域部分

步驟 16.

為ISP連線建立兩個外部介面的外部安全區域。

Add Security Zone

Name

outside_zone

Description

Outside Zone

Mode

☒ Routed ☐ Passive ☐ Inline

Interfaces

+

 outside_backup (Ethernet1/2)

 outside_primary (Ethernet1/1)

CANCEL

OK

外部安全區域

步驟 17.

建立安全區域後，必須建立NAT。通過選擇頂部的Policies按鈕導航到Policies部分。

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	

已建立安全區域

步驟 18.

選擇NAT按鈕導航到NAT部分，然後選擇CREATE NAT RULE按鈕建立新規則。

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

Security Policies

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

Filter

#	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部分

步驟 19.

對於ISP故障切換，配置必須有2條通過外部介面的路由。首先，用於主外部介面與主ISP的連線。

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

主ISP的NAT

步驟 20.

現在，為輔助ISP連線配置第二個NAT。

 附註：對於原始地址，不能使用同一網路。在本例中，對於輔助ISP，Original Address是 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

輔助ISP的NAT

步驟 21.

建立兩個NAT規則後，必須建立訪問控制規則以允許出站流量。選擇Access Control按鈕。

 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	

已建立NAT規則

步驟 22.

要建立訪問控制規則，請選擇CREATE ACCESS RULE按鈕。

 Security Policies

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

Filter

⚙️ 1 🎯 +

#	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** ▼

訪問控制部分

步驟 23.

選擇所需的zones和network。

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



訪問控制規則

步驟 24.

建立訪問控制規則後，通過選擇頂部的Deploy按鈕繼續部署所有更改。

Firewall Device Manager
Monitoring
Policies
Objects
Device: SF3130

Security Policies

SSL Decryption
Identity
Security Intelligence
NAT
Access Control
Intrusion

1 rule

#
NAME
ACTION
SOURCE
ZONES
NETWORKS
PORTS
DESTINATION
ZONES
NETWORKS
PORTS
APPLICATIONS
URLS
USERS
ACTIONS

1
To_Internet
Allow
inside_zone
Inside
ANY
outside_zone
ANY
ANY
ANY
ANY
ANY

Default Action
Access Control
Block

已建立訪問控制規則

步驟 25.

驗證更改，然後選擇Deploy Now按鈕。

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
+ 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

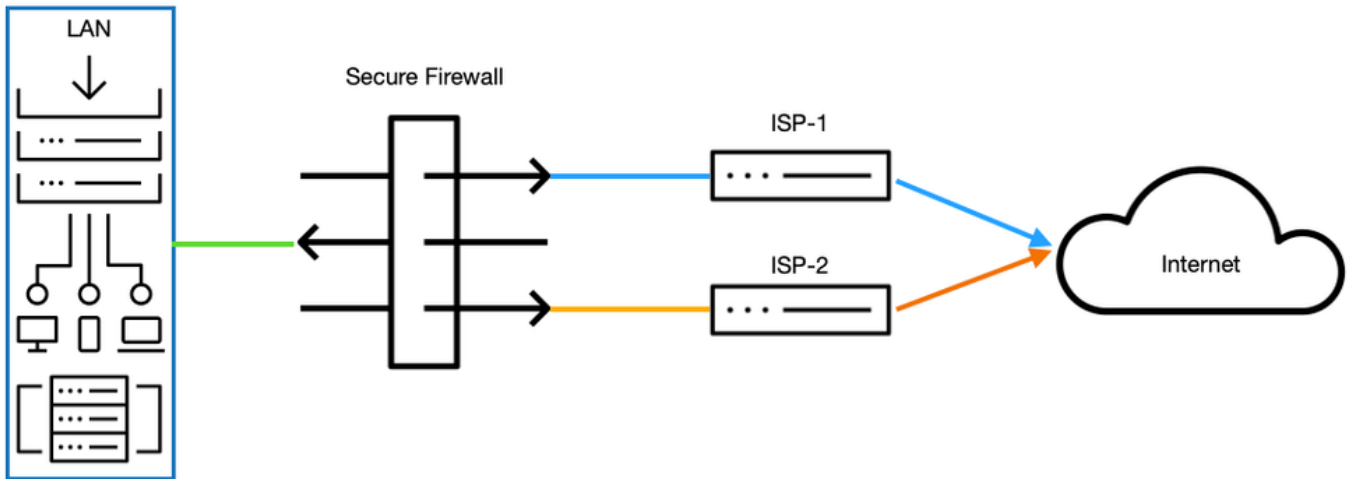
MORE ACTIONS

CANCEL

DEPLOY NOW

部署驗證

網路圖表



網路圖表

驗證

<#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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。