

使用具有高可用性的安全防火墙配置安全访问

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[在安全访问中配置VPN](#)

[用于隧道设置的数据](#)

[在安全防火墙上配置隧道](#)

[配置隧道接口](#)

[配置辅助接口的静态路由](#)

[在VTI模式下将VPN配置为安全访问](#)

[端点配置](#)

[IKE 配置](#)

[IPSec 配置](#)

[高级配置](#)

[访问策略配置场景](#)

[Internet访问场景](#)

[RA-VPN环境](#)

[CLAP-BAP ZTNA Escenario](#)

[配置策略基础路由](#)

[在安全访问中配置互联网访问策略](#)

[配置ZTNA和RA-VPN的私有资源访问](#)

[故障排除](#)

[检验第1阶段\(IKEv2\)](#)

[检验第2阶段\(IPSEC\)](#)

[高可用性功能](#)

[检验流量路由以实现安全访问](#)

[相关信息](#)

简介

本文档介绍如何通过高可用性安全防火墙配置安全访问。

先决条件

- [配置用户调配](#)
- [ZTNA SSO身份验证配置](#)

- [配置远程访问VPN安全访问](#)

要求

Cisco 建议您了解以下主题：

- Firepower管理中心7.2
- Firepower威胁防御7.2
- 安全访问
- 思科安全客户端 — VPN
- 思科安全客户端 — ZTNA
- 无客户端ZTNA

使用的组件

本文档中的信息基于：

- Firepower管理中心7.2
- Firepower威胁防御7.2
- 安全访问
- 思科安全客户端 — VPN
- 思科安全客户端 — ZTNA

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

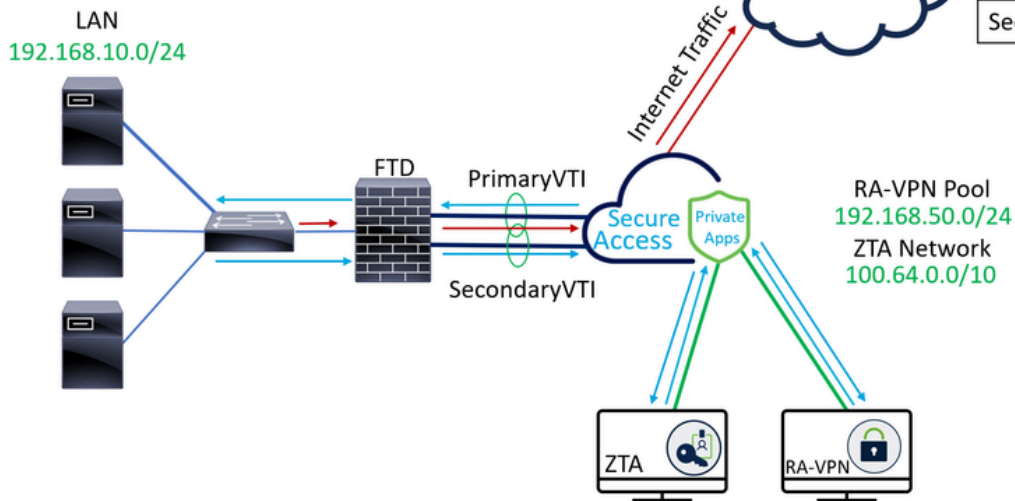


思科设计了安全访问(Secure Access)，用于保护和提供对内部和基于云的私有应用的访问。它还可以保护从网络到Internet的连接。这是通过实施多种安全方法和层来实现的，所有这些方法均旨在保护通过云访问信息时的安全。

网络图

Internet Access Traffic — (red line)
Private Apps Traffic — (blue line)

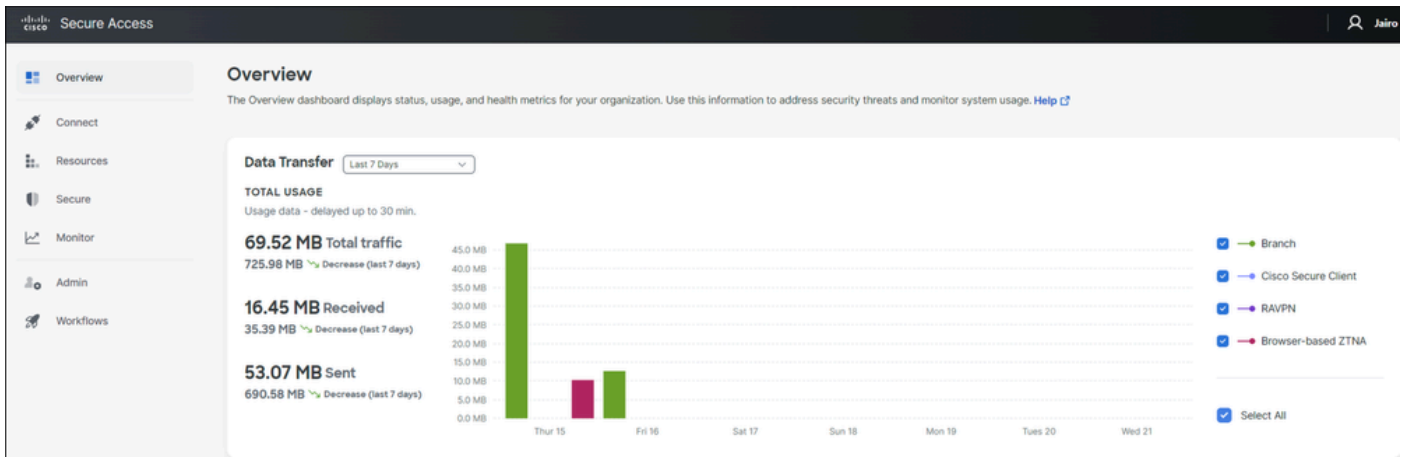
INTERFACE	IP
PrimaryWAN	192.168.30.5
PrimaryVTI	169.254.2.1
SecondaryWAN	192.168.0.202
SecondaryVTI	169.254.3.1



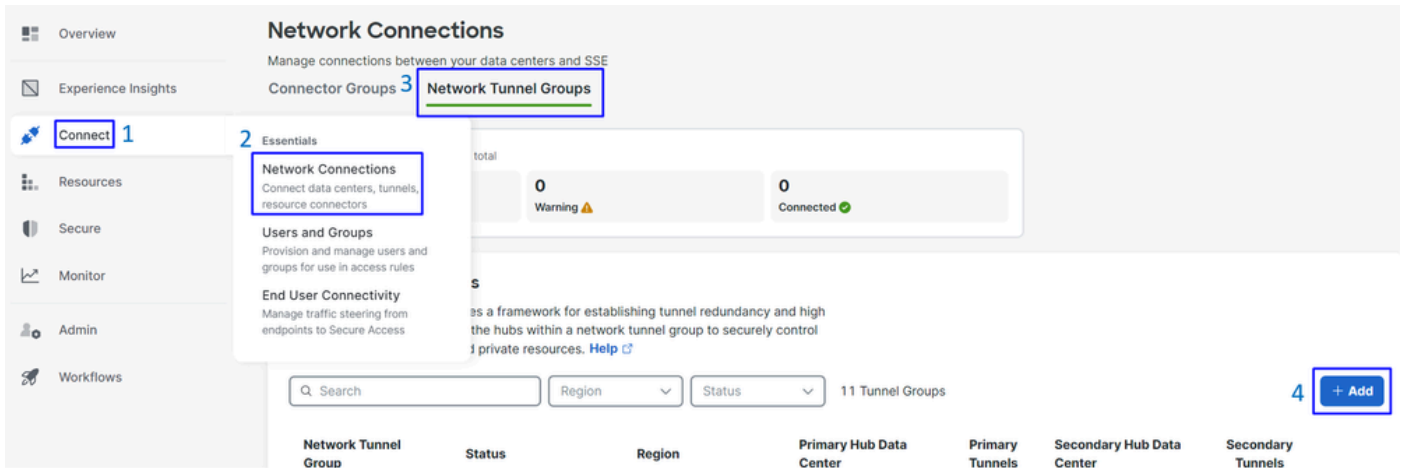
配置

在安全访问中配置VPN

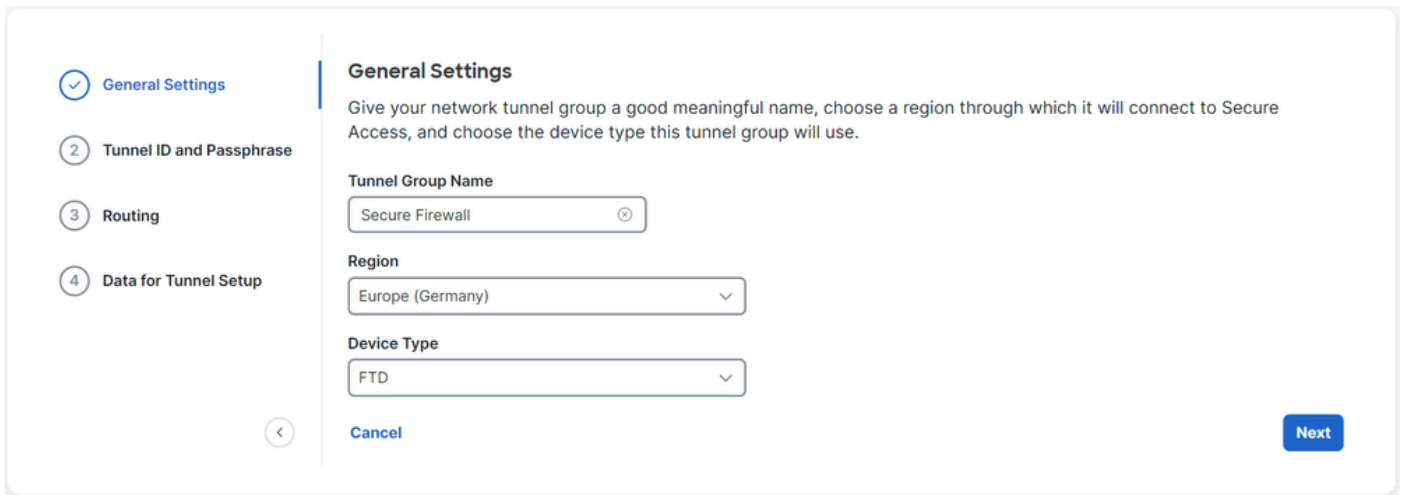
导航至的管理面板 [安全访问](#).



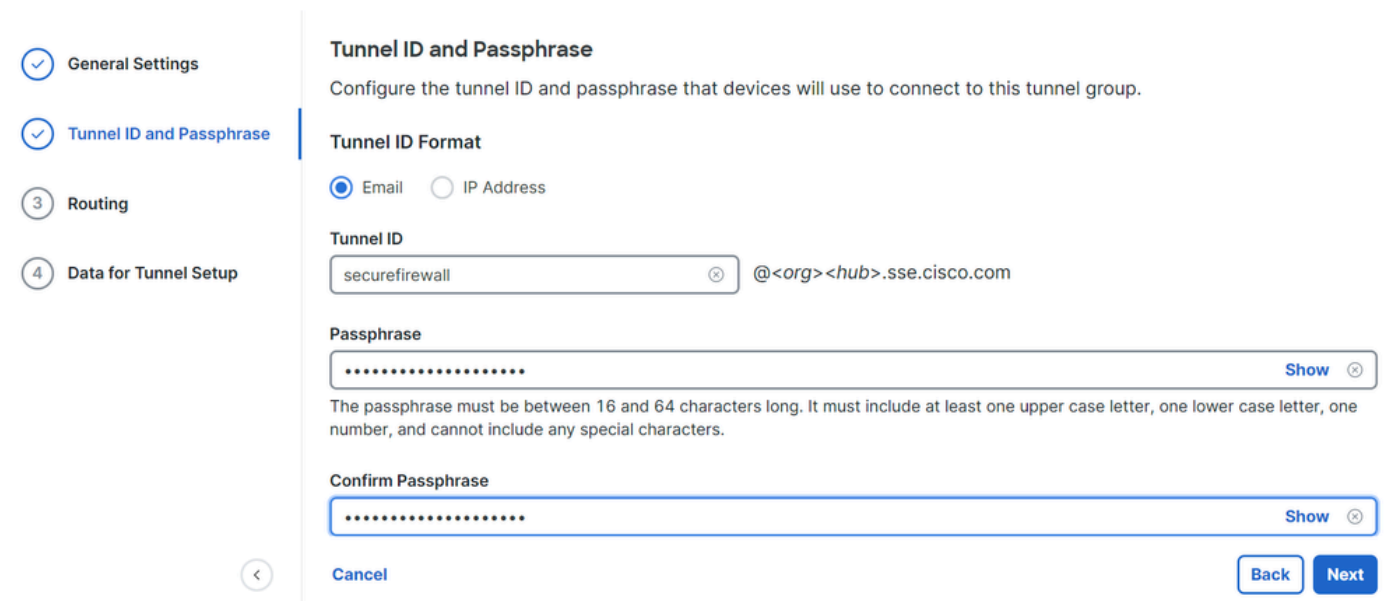
- 点击 Connect > Network Connections
- 在Network Tunnel Groups 下，单击 + Add



- 配置 Tunnel Group Name, Region 和 Device Type
- 点击 Next



- 配置 Tunnel ID Format 和 Passphrase
- 点击 Next



- 配置网络上已配置且希望通过安全访问传递流量的IP地址范围或主机

- 点击Save

Routing option

Static routing

Use this option to manually add IP address ranges for this tunnel group.

IP Address Ranges

Add all public and private address ranges used internally by your organization. For example, 128.66.0.0/16, 192.0.2.0/24.

Add

192.168.0.0/24 X192.168.10.0/24 X

Dynamic routing

Use this option when you have a BGP peer for your on-premise router.

[Cancel](#)

[Back](#) [Save](#)

单击显示的Save“通道信息”后，请保存下一步的信息。 **Configure the tunnel on Secure Firewall.**

用于隧道设置的数据

- General Settings
- Tunnel ID and Passphrase
- Routing
- Data for Tunnel Setup

Data for Tunnel Setup

Review and save the following information for use when setting up your network tunnel devices. This is the only time that your passphrase is displayed.

Primary Tunnel ID:	securefirewall@[redacted]-sse.cisco.com <input type="checkbox"/>
Primary Data Center IP Address:	18.156.145.74 <input type="checkbox"/>
Secondary Tunnel ID:	securefirewall@[redacted]-sse.cisco.com <input type="checkbox"/>
Secondary Data Center IP Address:	3.120.45.23 <input type="checkbox"/>
Passphrase:	[redacted] <input type="checkbox"/>

[Download CSV](#)

[Done](#)

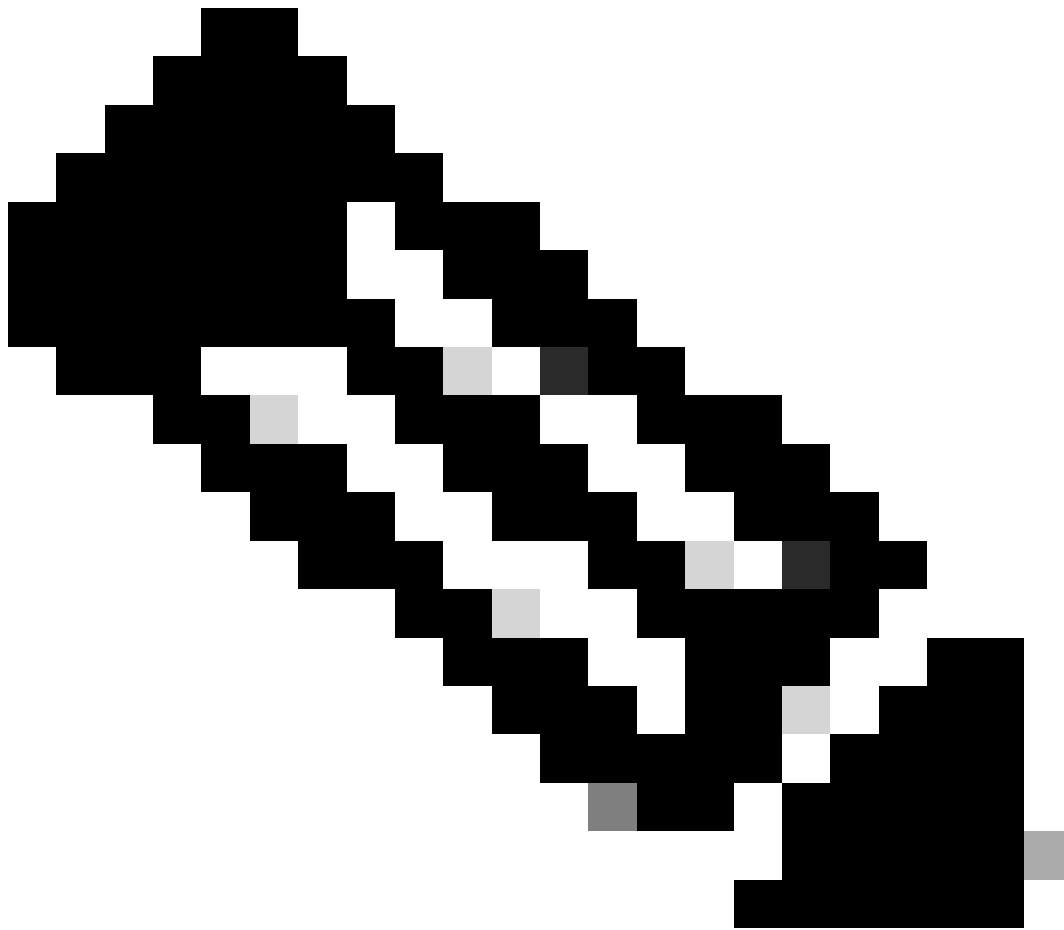
在安全防火墙上配置隧道

配置隧道接口

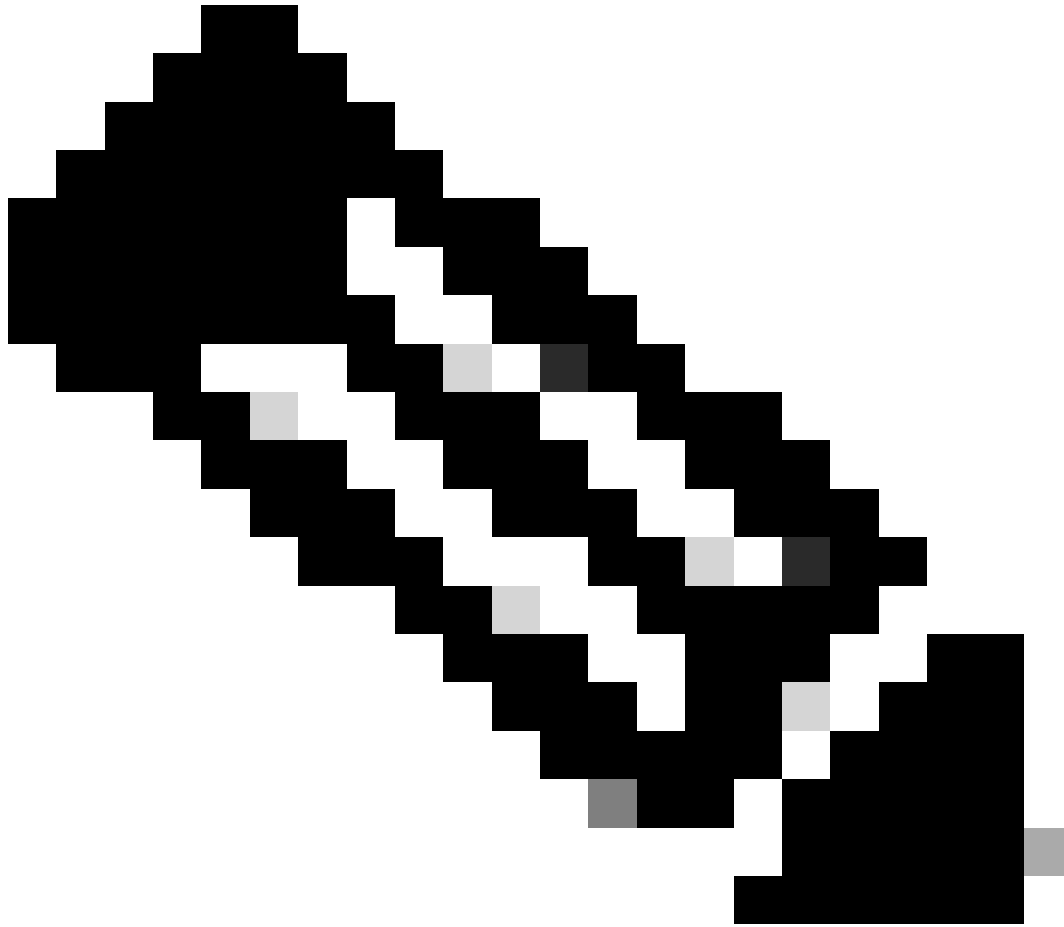
对于此场景，您使用安全防火墙上的虚拟隧道接口(VTI)配置来实现此目标；请记住，在本例中，您有两个ISP，如果其中一个ISP发生故障，我们希望有HA。

接口	角色
----	----

主WAN	主要互联网WAN
辅助WAN	辅助互联网WAN
主VTI	链接以将流量通过发送到Principal Internet WAN安全访问
辅助VTI	链接以将流量通过发送到Secondary Internet WAN安全访问



注意：1.需要向添加或分配静态路由 Primary or Secondary Datacenter IP ，才能启用两个隧道。



注意：2.如果在接口之间配置了ECMP，则无需创建到的任何静态路由即可启用两个隧道
Primary or Secondary Datacenter IP。

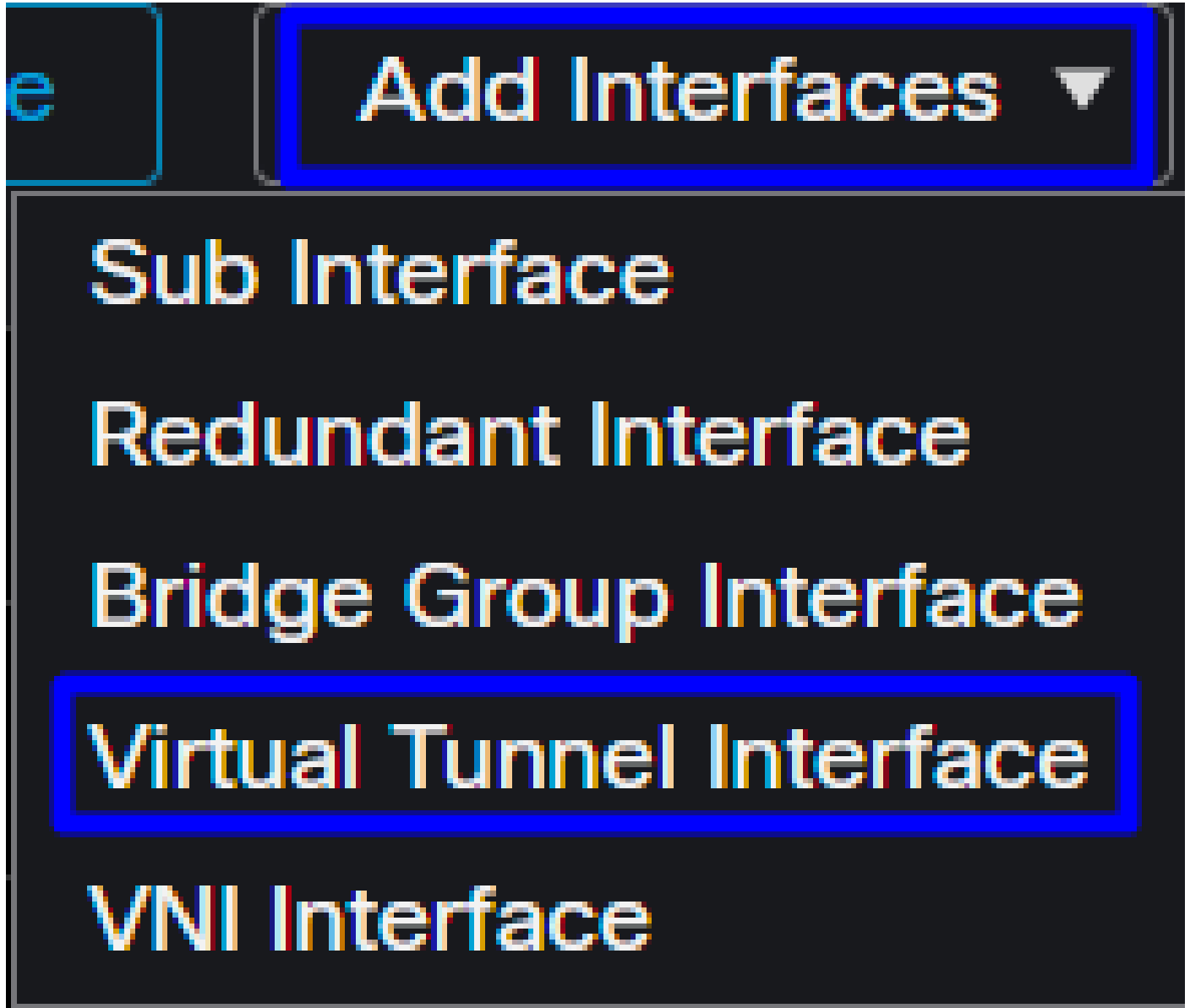
根据场景，我们有PrimaryWAN和，SecondaryWAN必须使用这些来创建VTI接口。

导航到您的Firepower Management Center > Devices。

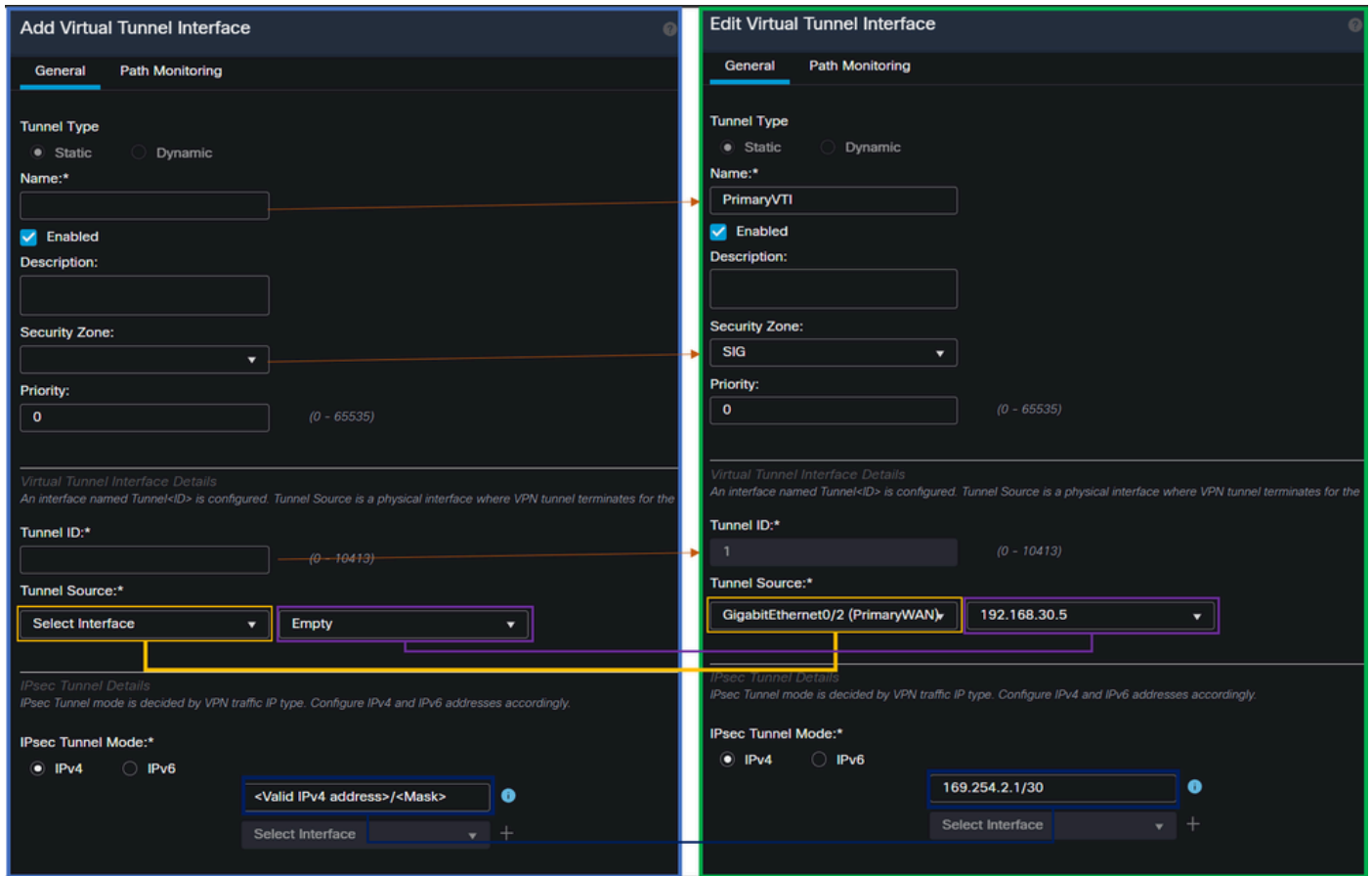
- 选择您的FTD
- 选择 Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)

- 点击 Add Interfaces > Virtual Tunnel Interface



- 根据下一信息配置接口



- Name :配置引用 PrimaryWAN interface
- Security Zone :您可以重复使用另一Security Zone个地址，但最好为安全访问流量创建一个新地址
- Tunnel ID :为隧道ID添加一个数字
- Tunnel Source :选择PrimaryWAN interface并选择接口的私有IP或公共IP
- IPsec Tunnel Mode :选择IPv4并配置网络中带有掩码30的不可路由IP

注意：对于VTI接口，必须使用不可路由的IP；例如，如果您有两个VTI接口，则可以将169.254.2.1/30用PrimaryVTI于，将169.254.3.1/30用SecondaryVTI于。

之后，您需要对执行相同的操作，并且已对VTI高可用性进行了所有设置，因此，您将得到下一个结果：

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

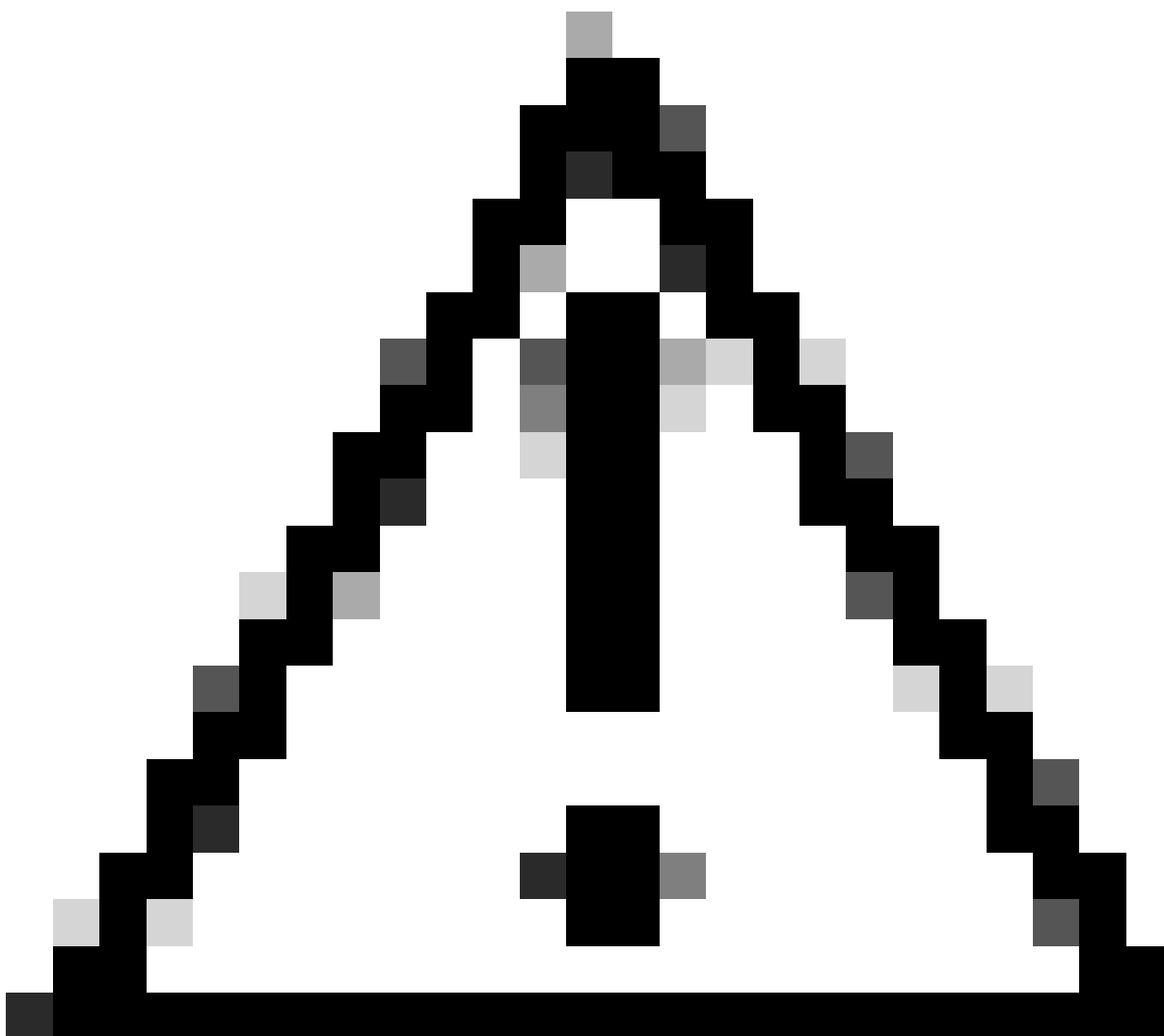
在本场景中，使用的IP是：

VTI IP配置

逻辑名称	IP	范围
主VTI	169.254.2.1/30	169.254.2.1-169.254.2.2
辅助VTI	169.254.3.1/30	169.254.3.1-169.254.3.2

配置辅助接口的静态路由

要允许的流量到达Secondary WAN interface 的流量Secondary Datacenter IP Address，您需要配置到数据中心IP的静态路由。可以使用度量一(1)配置它，使其位于路由表的顶部；此外，指定IP作为主机。



警告：仅在广域网信道之间没有ECMP设置时才需要此项；如果已配置ECMP，则可以跳至下一步。

- 点击FTD设备
- 点击 Routing
- 选择 Static Route > + Add Route

Edit Static Route Configuration

Type: IPv4 IPv6

Interface* SecondaryWAN → Choose the SecondaryWAN interface

(Interface starting with this icon signifies it is available for route leak)

Available Network ↻ +

192.168.0.150

192.168.10.153

any-ipv4

ASA_GW

CSA_Primary

GWWT1

Add

Selected Network

SecureAccessTunnel 🗑️

↓

Choose the Secondary Datacenter IP

Ensure that egress virtualrouter has route to that destination

Gateway Outside_GW → Choose the SecondaryWAN Gateway

Metric:
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking: +

Cancel
OK

- Interface:选择辅助WAN接口

- Gateway:选择辅助WAN网关
- Selected Network:添加辅助数据中心IP作为主机；您可以在安全访问步骤中配置隧道时找到相关信息，[Data for Tunnel Setup](#)
- Metric:使用-(1)
- OK点击Save并保存信息，然后部署。

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
SecureAccessTunnel	SecondaryWAN	Global	Outside_GW	false	1	
any-ipv4	PrimaryWAN	Global	ASA_GW	false	1	
▼ IPv6 Routes						

在VTI模式下将VPN配置为安全访问

要配置VPN，请导航到您的防火墙：

- 点击 **Devices > Site to Site**
- 点击 **+ Site to Site VPN**

端点配置

要配置Endpoints步骤，您需要使用步骤[Data for Tunnel Setup](#)下提供的信息。

Create New VPN Topology

Topology Name:*
SecureAccess

Policy Based (Crypto Map) Route Based (VTI)

Network Topology:

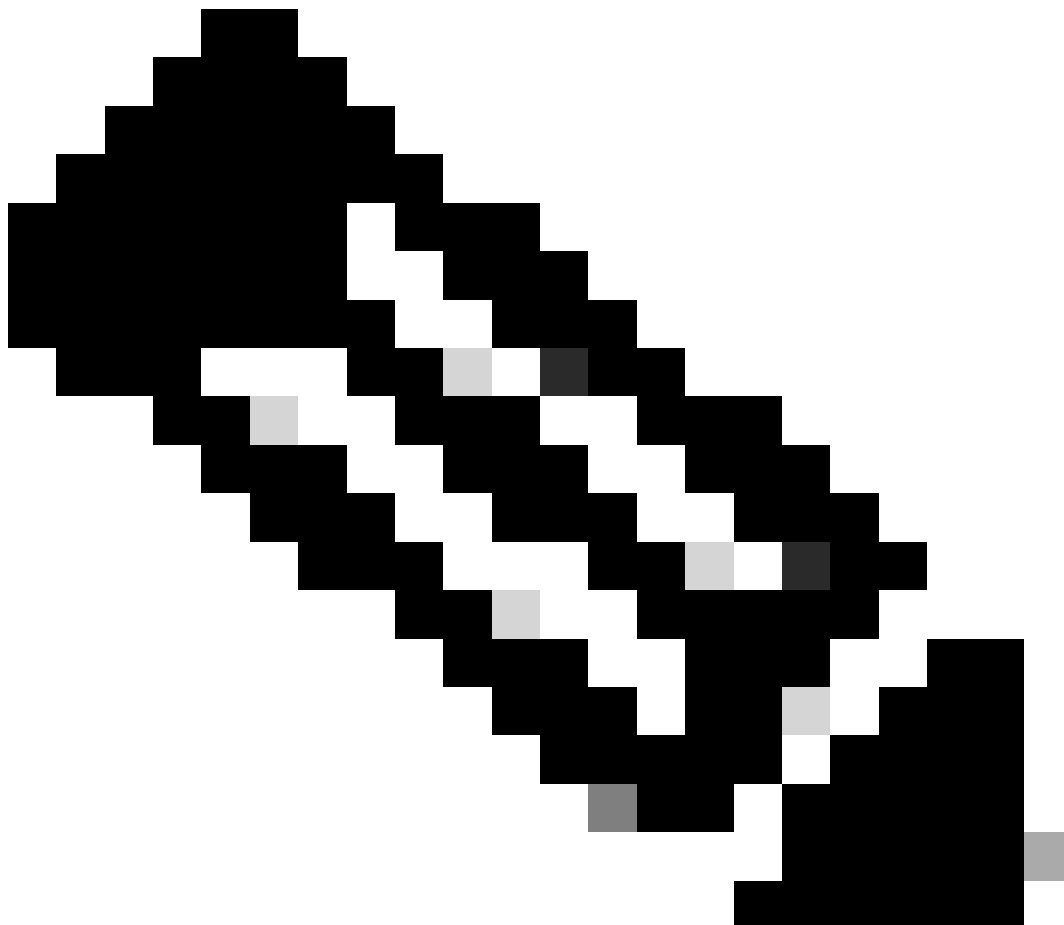
IKE Version:* IKEv1 IKEv2

Endpoints | IKE | IPsec | Advanced

Node A	Node B
Device:* FTD_HOME	Device:* Extranet
Virtual Tunnel Interface:* PrimaryVTI (IP: 169.254.2.1) +	Device Name*: SecureAccess
Tunnel Source: PrimaryWAN (IP: 192.168.30.5) Edit VTI <input type="checkbox"/> Tunnel Source IP is Private <input checked="" type="checkbox"/> Send Local Identity to Peers	Endpoint IP Address*: 18.156.145.74,3.120.45.23
Local Identity Configuration:* Email ID jairohome@8195126-615626006-	

Backup VTI: [Remove](#)

- 拓扑名称：创建与安全访问集成相关的名称
 - 选择 **Routed Based (VTI)**
 - 选择 **Point to Point**
 - IKE Version:选择IKEv2
-



注意：IKEv1不支持与安全访问集成。

在下Node A面，您需要配置以下参数：

Node A

Device:*

FTD_HOME

Virtual Tunnel Interface:*

PrimaryVTI (IP: 169.254.2.1)



Tunnel Source: PrimaryWAN (IP: 192.168.30.5) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID

jairohome@

[+ Add Backup VTI \(optional\)](#)

- Device:选择您的FTD设备
- Virtual Tunnel Interface:选择与相关的PrimaryWAN InterfaceVTI。
- 选中复选框 Send Local Identity to Peers
- Local Identity Configuration:选择Email ID (电子邮件ID) ，然后根据在步骤Primary Tunnel IDData for Tunnel Setup (隧道设置的数据) 中提供的[配置填写信息](#)

配置上的信息后，PrimaryVTI请点+ Add Backup VTI击：

Backup VTI: Remove

Virtual Tunnel Interface:*

SecondaryVTI (IP: 169.254.3.1) ▼ +

Tunnel Source: SecondaryWAN (IP: 192.168.0.202) [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

Local Identity Configuration:*

Email ID ▼

jairohome@ [redacted]

- Virtual Tunnel Interface:选择与相关的PrimaryWAN InterfaceVTI。
- 选中复选框 Send Local Identity to Peers
- Local Identity Configuration:选择Email ID (电子邮件ID) ，然后根据在步骤Secondary Tunnel IDData for Tunnel Setup (隧道设置的数据) 中提供的[配置填写信息](#)

在下Node B面，您需要配置以下参数：

Node B

Device:*

Extranet

Device Name*:

SecureAccess

Endpoint IP Address*:

18.156.145.74, 3.120.45.23

- Device:外联网
- Device Name:选择Name以将Secure Access识别为目标。
- Endpoint IP Address:主要和辅助的配置必须为主要，Datacenter IP,Secondary Datacenter IP您可以在步骤 [Data for Tunnel Setup](#)中找到该信息

之后，配置完Endpoints成，现在您可以转到步骤IKE Configuration。

IKE 配置

要配置IKE参数，请点击IKE。

Endpoints

IKE

IPsec

Advanced

在IKE, 下, 您需要配置以下参数:

Endpoints IKE IPsec Advanced

IKEv2 Settings

Policies:* Umbrella-AES-GCM-256

Authentication Type: Pre-shared Manual Key

Key:*

Confirm Key:*

Enforce hex-based pre-shared key only

- Policies: 您可以使用默认的Umbrella配置Umbrella-AES-GCM-256, 也可以根据 [Supported IKEv2 and IPSEC Parameters](#)
- Authentication Type: 预共享手动密钥
- Key和: Confirm Key 您可以在步骤Passphrase [Data for Tunnel Setup](#)中找到信息

之后, 配置完IKE成, 现在您可以转到步骤IPSEC配置。

IPSec 配置

要配置IPSEC参数, 请点击IPSEC。

Endpoints

IKE



IPsec

Advanced

在IPSEC, 下，您需要配置以下参数：

Crypto Map Type: Static Dynamic

IKEv2 Mode: Tunnel

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals* 

tunnel_aes256_sha	Umbrella-AES-GCM-256
-------------------	-----------------------------

Enable Security Association (SA) Strength Enforcement

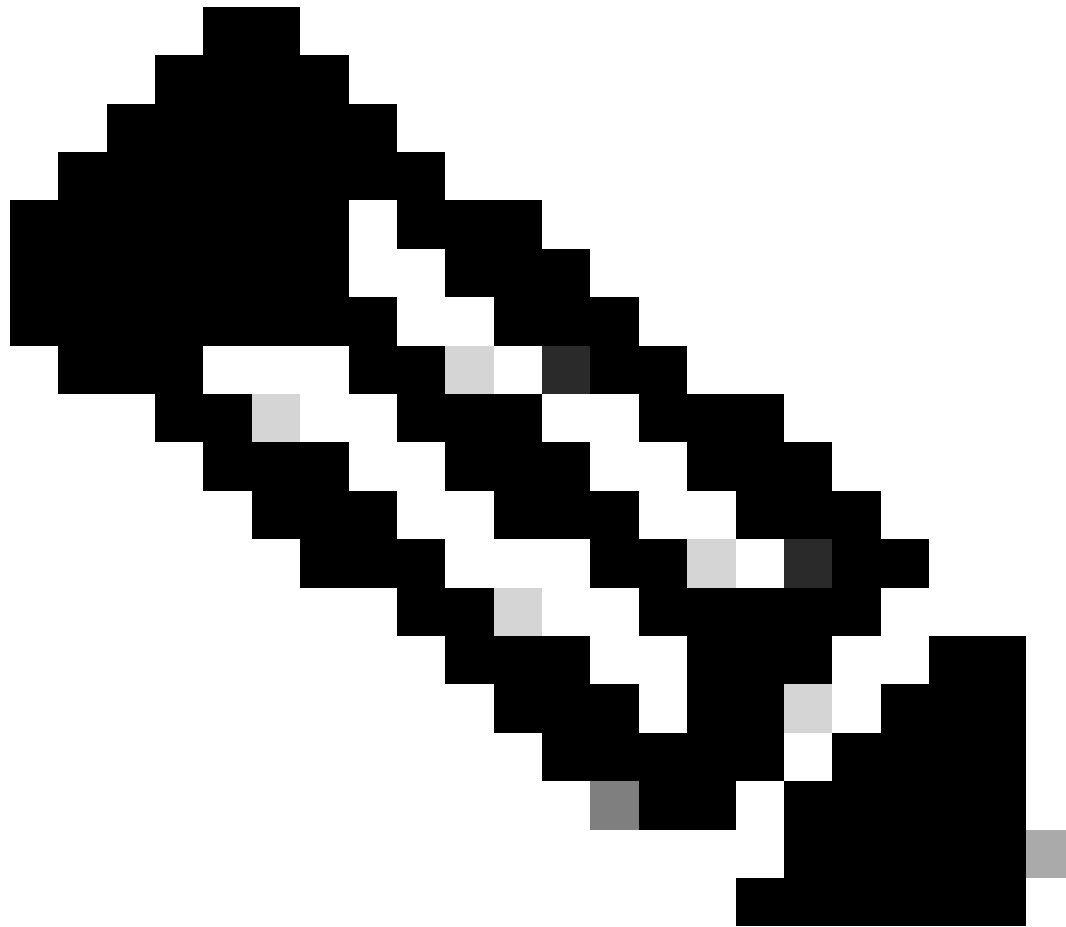
Enable Perfect Forward Secrecy

Modulus Group: 14

Lifetime Duration*: 28800 Seconds (Range 120-2147483647)

Lifetime Size: 4608000 Kbytes (Range 10-2147483647)

- Policies: 您可以使用默认的Umbrella配Umbrella-AES-GCM-256置，也可以根据 [Supported IKEv2 and IPSEC Parameters](#)

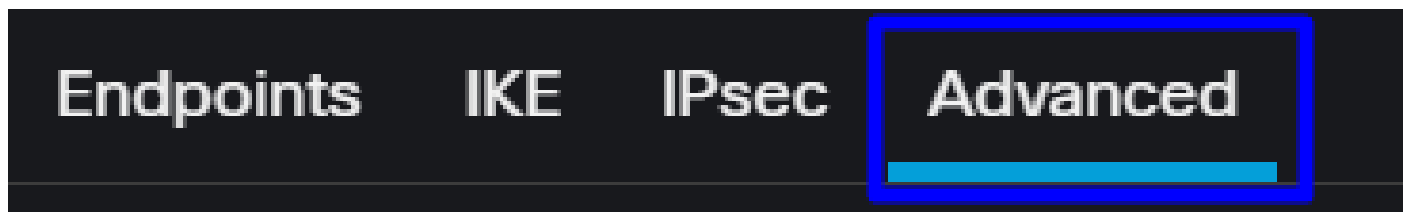


注意：IPSEC不需要其他任何内容。

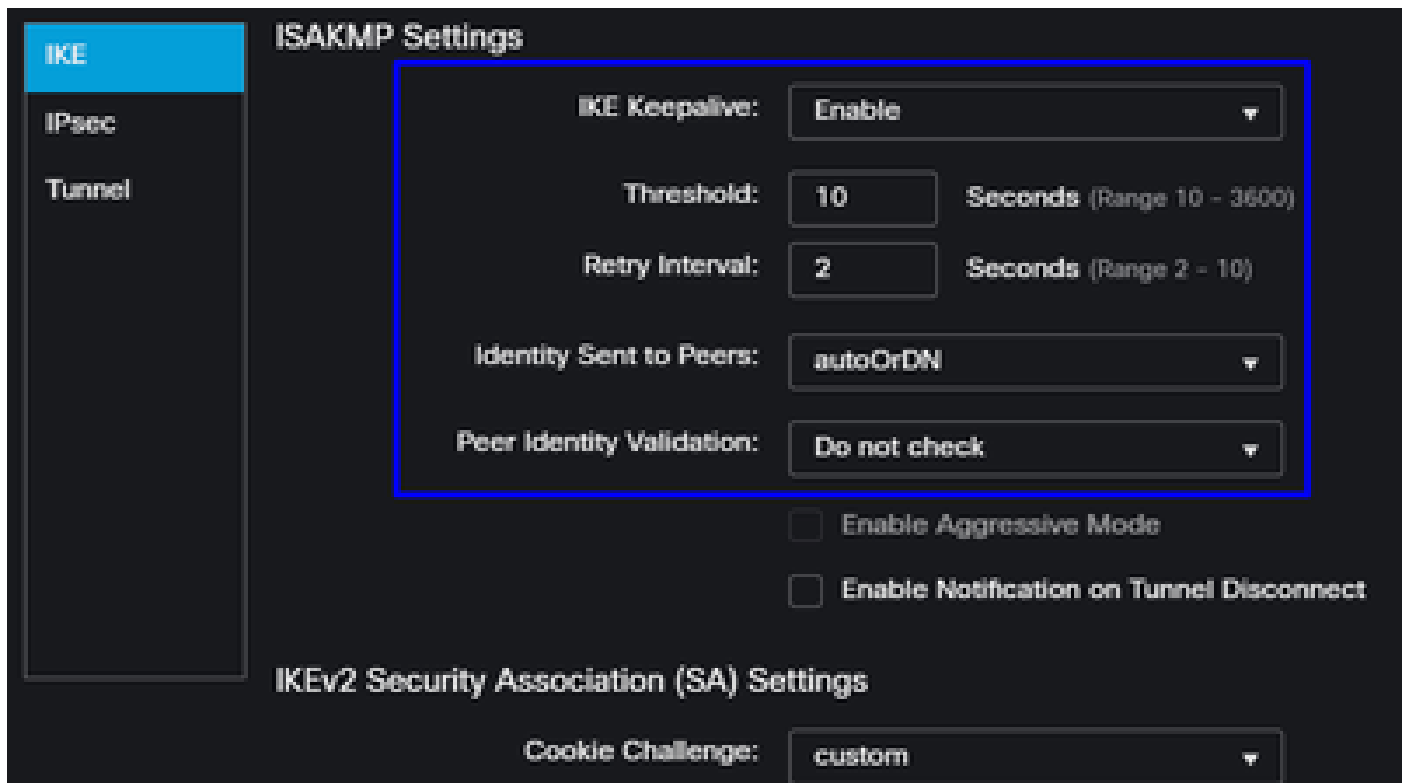
之后，您的配置IPSEC完成，现在您可以转到步骤“高级配置”。

高级配置

要配置高级参数，请点击Advanced。

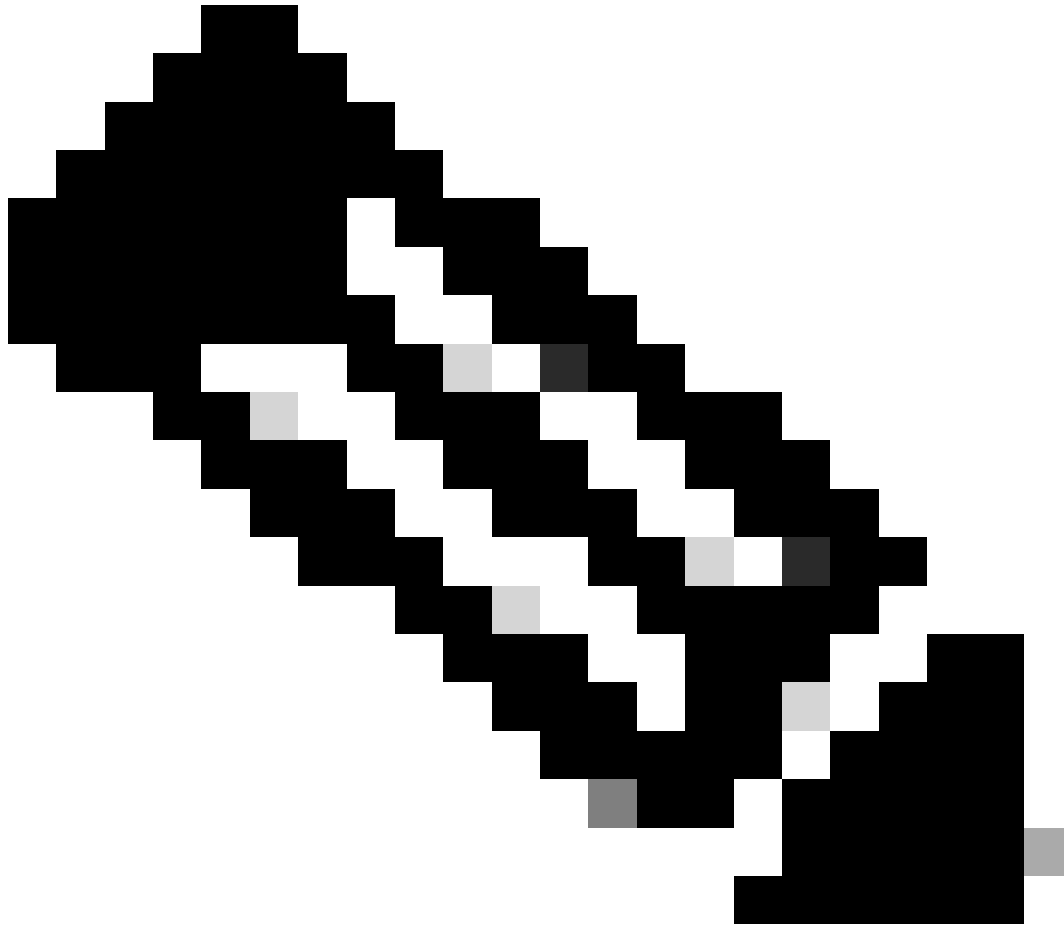


在Advanced, 下，您需要配置以下参数：



- IKE Keepalive:enable
- Threshold:10
- Retry Interval:2
- Identity Sent to Peers:autoOrDN
- Peer Identity Validation:不检查

之后，您可以点击SaveDeploy和。



注意：几分钟后，您会看到两个节点都建立了VPN。

Topology Name	VPN Type	Network Topology	Tunnel Status Distribution	IKEv1	IKEv2
SecureAccess	Route Based (VTI)	Point to Point	2 - Tunnels	✓	✗
Node A			Node B		
Device	VPN Interface	VTI Interface	Device	VPN Interface	VTI Interface
EXTRANET	Extranet	3.120.4... (3.120.45.23)	FTD	FTD_HOME	Secon... (192.168.0.202) Seconda... (169.254.3.1)
EXTRANET	Extranet	18.15... (18.156.145.74)	FTD	FTD_HOME	Primary... (192.168.30.5) PrimaryVTI (169.254.2.1)

之后，配置完VPN to Secure Access in VTI Mode成，现在您可以转到第步Configure Policy Base Routing。



警告：当两个隧道都建立时，安全访问的流量仅转发到主隧道；如果主隧道关闭，安全访问允许通过辅助隧道转发流量。

注意：安全访问站点上的故障切换基于用户指南中记录的DPD值[以获取](#)支持的IPsec值。

访问策略配置场景

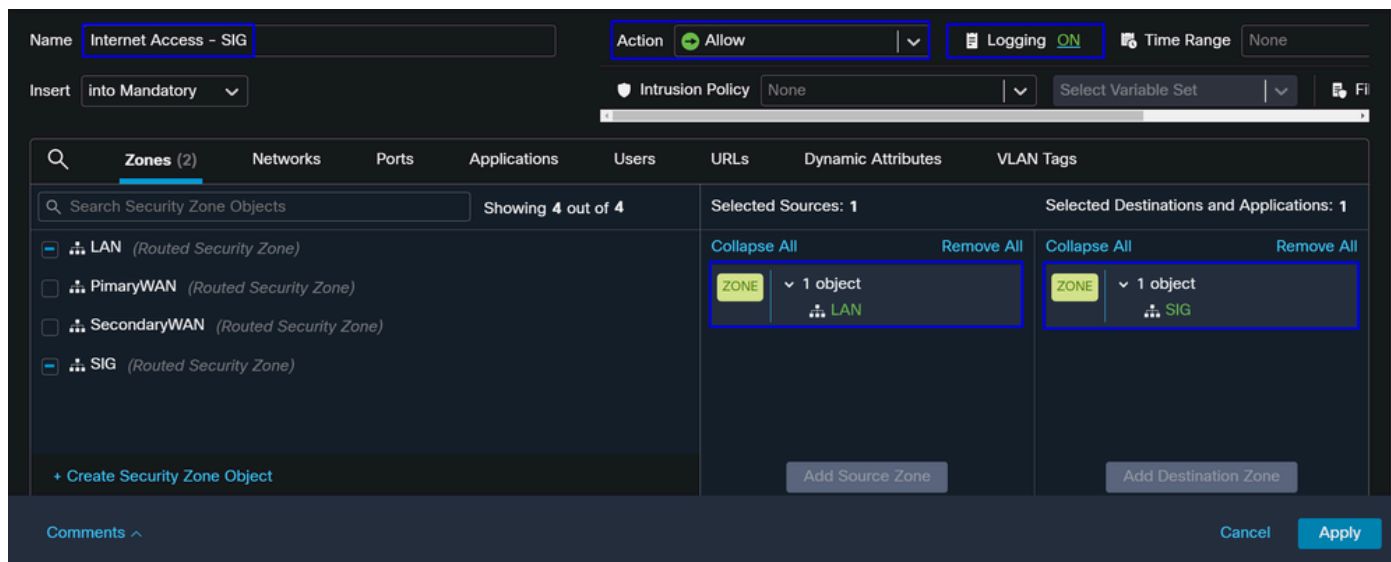
定义的访问策略规则基于：

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
● GigabitEthernet0/0	SecondaryWAN	Physical	SecondaryWAN		192.168.0.202/24(Static)
● Tunnel2	SecondaryVTI	VTI	SIG		169.254.3.1/30(Static)
● GigabitEthernet0/1	LAN	Physical	LAN		192.168.10.1/24(Static)
● GigabitEthernet0/2	PrimaryWAN	Physical	PrimaryWAN		192.168.30.5/24(Static)
● Tunnel1	PrimaryVTI	VTI	SIG		169.254.2.1/30(Static)

接口	区域
主VTI	SIG
辅助VTI	SIG
局域网	局域网

Internet访问场景

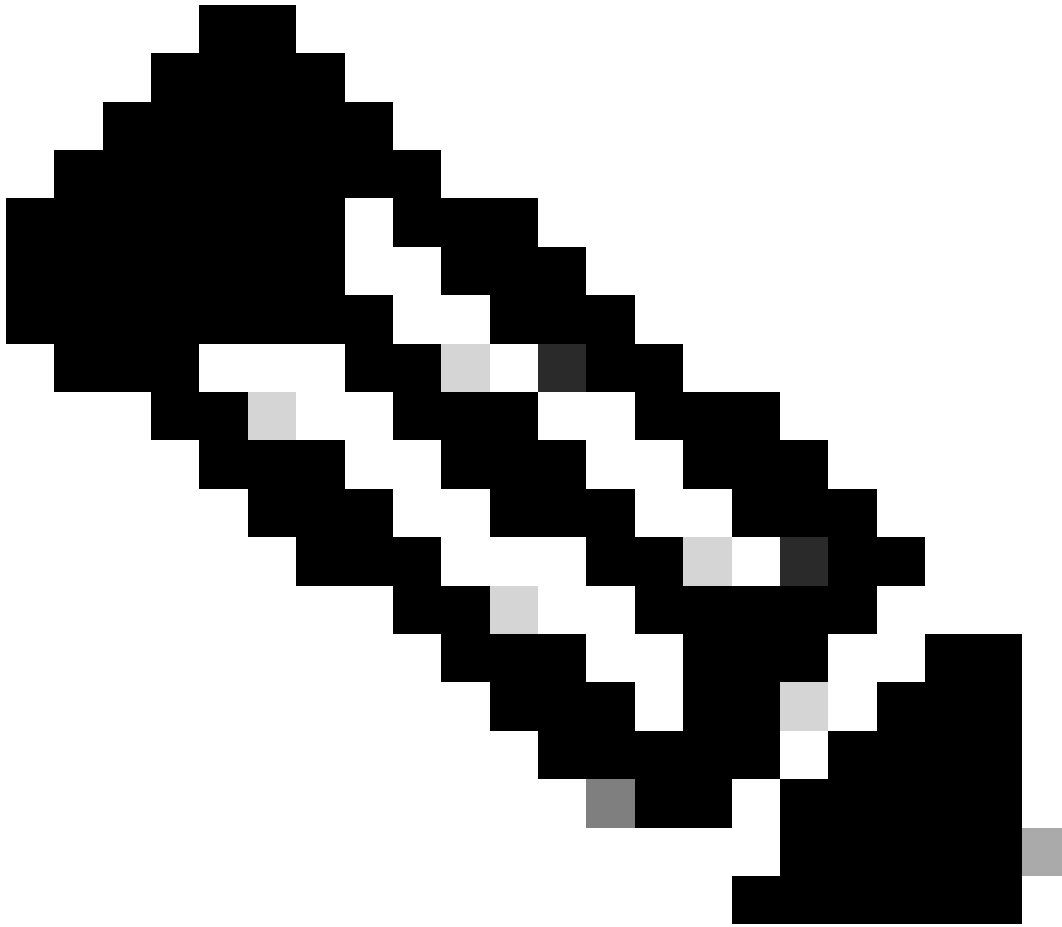
要为您在策略基础路由上配置的所有资源提供对Internet的访问，您需要配置一些访问规则以及安全访问中的某些策略，让我解释一下在此场景下如何实现这一目标：



此规则提供对InternetLAN的访问，在本例中，Internet是SIG的。

RA-VPN环境

要提供来自RA-VPN用户的访问，您需要根据在RA-VPN池上分配的范围对其进行配置。



注意：要配置RA-VPNaaS策略，可以通过[管理虚拟专用网络](#)

如何验证VPNaaS的IP池？

导航到您的[安全访问控制面板](#)

- 点击 **Connect > End User Connectivity**
- 点击 **Virtual Private Network**
- 在**Manage IP Pools**下，点击 **Manage**

End User Connectivity

↓ Cisco Secure Client

Manage DNS Servers (2)

End user connectivity lets you define how your organization's traffic is steered from endpoints to Secure Access or to the internet. [Help](#)

Zero Trust

Virtual Private Network

Internet Security

Global FQDN

fb57.vpn.sse.cisco.com [Copy](#)

Manage IP Pools

2 Regions mapped

[Manage](#)

- 你可以看到你的池子下面 Endpoint IP Pools

Pop Name	Display Name	Endpoint IP Pools	Management IP Pools	DNS Servers
Europe (Germany)	RA VPN 1	192.168.50.0/24 256 user connections	192.168.60.0/24 256 user connections	House

- 您需要在SIG下允许此范围，但还必须将其添加到在PBR中配置的ACL下。

访问规则配置

如果您仅配置安全访问，使其具有访问专用应用程序资源的功能，则您的访问规则可能如下所示：

The screenshot shows a configuration page for a rule named 'Private APP'. The 'Action' is set to 'Allow', 'Logging' is 'ON', and 'Time Range' is 'None'. The rule is inserted 'into Mandatory'. The configuration is based on an 'Intrusion Policy' of 'None' and a 'Variable Set'.

The rule configuration is as follows:

Networks	Geolocations	Selected Sources	Selected Destinations and Applications
<ul style="list-style-type: none"> 192.168.0.150 (Host Object) 192.168.10.153 (Host Object) any (Network Group) any-ipv4 (Network Object) any-ipv6 (Host Object) 	<ul style="list-style-type: none"> 192.168.0.150 192.168.10.153 0.0.0.0/0::/0 0.0.0.0/0 ::/0 	<ul style="list-style-type: none"> ZONE: 1 object (SIG) NET: 1 object (192.168.50.0/24) 	<ul style="list-style-type: none"> ZONE: 1 object (LAN)

Buttons at the bottom include 'Cancel' and 'Apply'.

该规则允许从RA-VPN池192.168.50.0/24到您的LAN的流量；如果需要，可以指定更多。

ACL 配置

要允许从SIG到LAN的路由流量，您必须将其添加到ACL下，使其在PBR下工作。

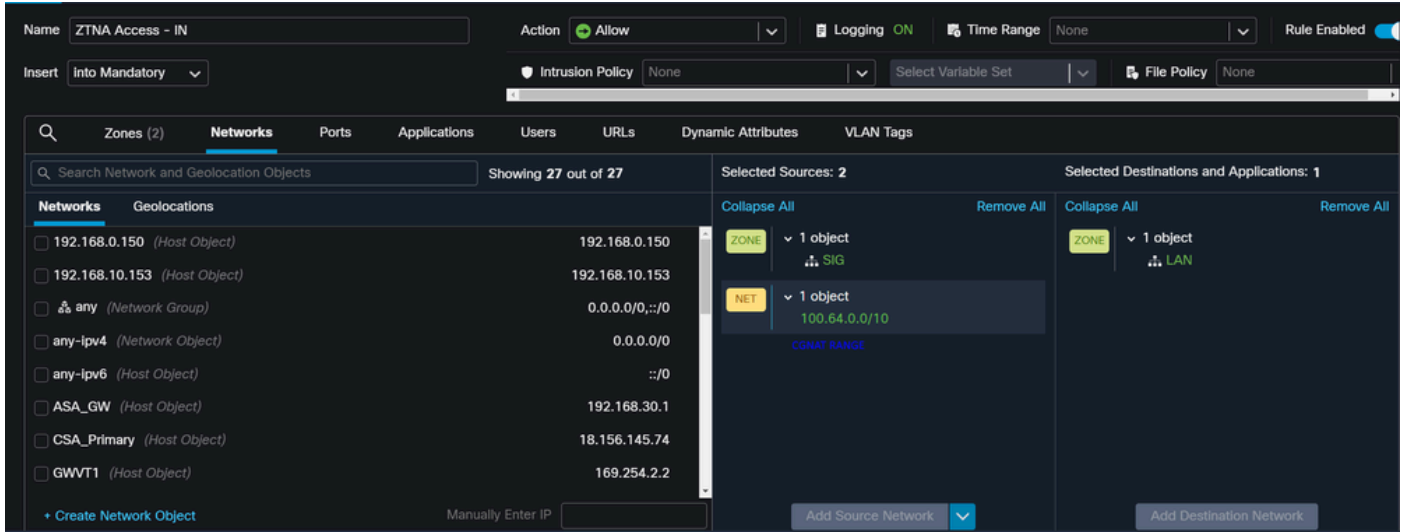
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Allow	192.168.10.0/24	Any	192.168.50.0/24	Any	Any	Any	
2	Block	Any	Any	Any	Any	Any	Any	

CLAP-BAP ZTNA Escenario

您必须根据CGNAT范围100.64.0.0/10配置您的网络，以便从客户端基础ZTA或浏览器基础ZTA用户访问您的网络。

访问规则配置

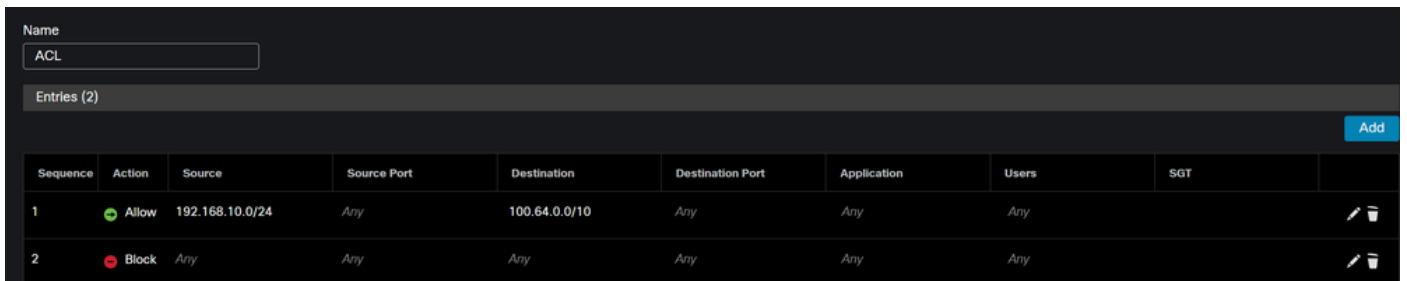
如果您仅配置安全访问，使其具有访问专用应用程序资源的功能，则您的访问规则可能如下所示：



该规则允许从ZTNA CGNAT范围100.64.0.0/10到您的LAN的流量。

ACL 配置

要允许使用CGNAT从SIG到LAN的路由流量，您必须将其添加到ACL下，使其在PBR下工作。



配置策略基础路由

要通过安全访问提供对内部资源和互联网的访问，您必须通过策略基础路由(PBR)创建路由，以便于将流量从源路由到目标。

- 导航至 **Devices > Device Management**
- 选择创建路由的FTD设备

<input type="checkbox"/>	Name	Model	Version
<input type="checkbox"/>	Ungrouped (1)		
<input checked="" type="checkbox"/>	FTD_HOME Snort 3 192.168.0.201 - Routed	FTDv for VMware	7.2.5

- 点击 **Routing**
- 选择 Policy Base Routing
- 点击 Add

Policy Based Routing
Specify Ingress interfaces, match criteria and egress interfaces to route traffic accordingly. Traffic can be routed across Egress Interfaces accordingly

在此场景中，选择所有用作源以路由流量到安全访问的接口，或使用RA-VPN或基于客户端或基于浏览器的ZTA访问对网络内部资源进行安全访问的用户身份验证：

- 在Ingress Interface下，选择通过Secure Access发送流量的所有接口：

Edit Policy Based Route

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*

LAN

- 在“匹配条件和出口接口”(Match Criteria and Egress Interface)下，点击后定义以下参数Add:

Match Criteria and Egress Interface
Specify forward action for chosen match criteria.

Add Forwarding Actions

Match ACL:*

Send To:*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

↑ Internal Sources

Match ACL:*

Send To:*

IPv4 Addresses:

IPv6 Addresses:

Don't Fragment:

- **Match ACL:**对于此ACL，您需要配置要路由到安全访问的所有内容：

Traffic to the destination 208.67.222.222 or 208.67.220.220 over DNS using TCP or UDP will not be routed to Secure Access

✘ REJECT

Name:

Entries (2)

Sequence	Action	Source	Source Port	Destination	Destination Port
1	Block	Any	Any	208.67.222.222 208.67.222.220	Any
2	Allow	192.168.10.0/24	Any	Any	Any

Traffic from the source 192.168.10.0/24 will be routed to Secure Access

Depends how you play with the ACL, you can define how the traffic must be routed to Secure Access

✔ ACCEPT

- **Send To:**选择IP地址
- **IPv4 Addresses:**您必须使用两个VTI上配置的掩码30下的下一个IP;您可以在此步骤中检查[VTI Interface Config](#)

接口	IP	网关
主VTI	169.254.2.1/30	169.254.2.2
辅助VTI	169.254.3.1/30	169.254.3.2



这样配置后，您将得到下一个结果，您可以继续点击Save:

Match ACL:* **ACL** +

Send To:* **IP Address**

IPv4 Addresses: **169.254.2.2,169.254.3.2**

IPv6 Addresses: For example, 2001:db8::, 2002:db8::1:

Don't Fragment: **None**

Default Interface

IPv4 settings IPv6 settings

Recursive: For example, 192.168.0.1

Default: For example, 192.168.0.1, 10.10.10.1

Peer Address

Verify Availability +

Cancel Save

之后，您需要重新配置它Save，然后按照以下方式对其进行配置：

A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces

Ingress Interface*
LAN

Match Criteria and Egress Interface
 Specify forward action for chosen match criteria. Add

Match ACL	Forwarding Action	
ACL	Send through <div style="display: flex; align-items: center;"> <div style="border: 1px solid #0070c0; padding: 2px; margin-right: 5px;">169.254.2.2</div> <div style="border: 1px solid #0070c0; padding: 2px; margin-right: 5px;">169.254.3.2</div> <div style="margin-left: 10px;">→ Send the traffic to the PrimaryVTI</div> </div>	✎ 🗑️

↓
 If PrimaryVTI fail it will send the traffic to the SecondaryVTI

Cancel Save


之后，您可以部署，并且您会看到在ACL上配置的计算机的流量将流量路由到安全访问：



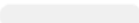





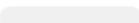


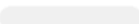


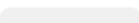


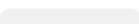




在FMCConexion Events中：

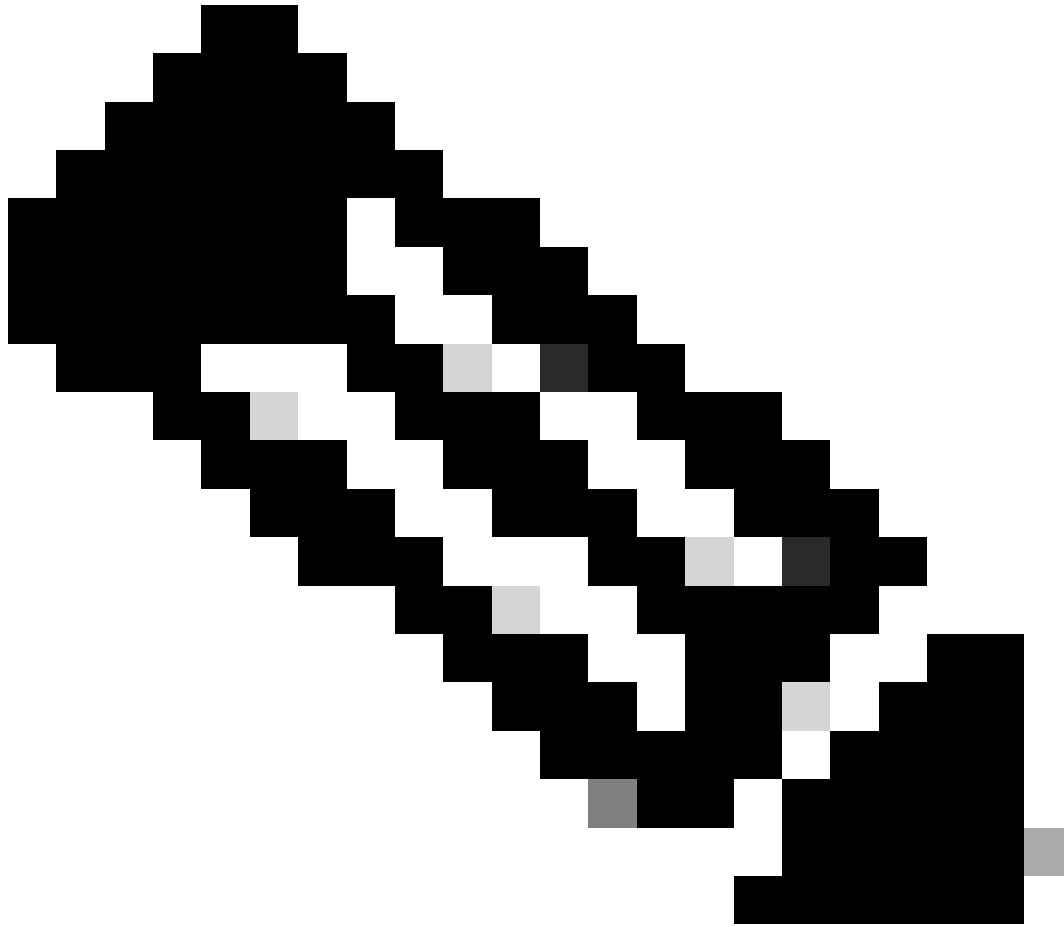
<input type="checkbox"/>	Action ×	Initiator IP ×	Responder IP ×	↓ Application Risk ×	Access Control Policy ×	Ingress Interface ×	Egress Interface ×
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI
▼ <input type="checkbox"/>	Allow	192.168.10.40	8.8.8.8	Medium	HOUSE	LAN	PrimaryVTI

Activity Search Secure Access:

40,678 Total  Viewing activity from Mar 13, 2024 12:30 AM to Mar 14, 2024 12:30 AM

Page: 1  Results per page

Request	Source	Rule Identity 	Destination	Destination IP	Internal IP	External IP	Action	Categories	Res
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	
	⇄ HomeFTD	⇄ HomeFTD		8.8.8.8	192.168.10.40		 Allowed	Uncategorized	



注意：默认情况下，默认安全访问策略允许流量到达互联网。要提供对专用应用的访问，您需要创建专用资源并将其添加到专用资源访问的访问策略。

在安全访问中配置互联网访问策略

要配置互联网访问的访问权限，您需要在[Secure Access Dashboard](#)上创建策略：

- 点击 **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- 点击 [Add Rule > Internet Access](#)

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

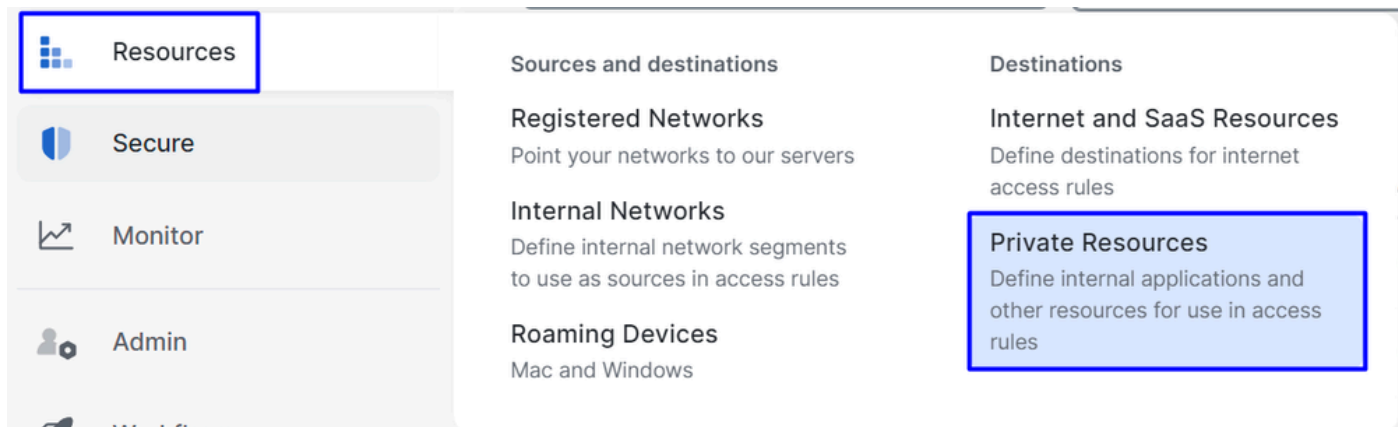
Control and secure access to public destinations from within your network and from managed devices

您可以在此处指定源作为隧道，对于目标，您可以选择任意，具体取决于要在策略上配置的内容。请查看[Secure Access用户指南](#)。

配置ZTNA和RA-VPN的私有资源访问

要配置专用资源的访问，您需要首先在[安全访问控制面板](#)下创建资源：

点击 **Resources > Private Resources**



- ?? 然后单击 **ADD**

在配置下，您可以找到以下要配置的部分：**General, Communication with Secure Access Cloud and Endpoint Connection Methods.**

常规

General

Private Resource Name

Description (optional)

- Private Resource Name :为通过“安全访问”访问您的网络提供的资源创建一个名称

终端连接方法

Zero-trust connections
 Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. [Help](#)

Client-based connection
 Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture).

Remotely Reachable Address (FQDN, Wildcard FQDN, IP Address) ⓘ

[+ FQDN or IP Address](#)

Browser-based connection
 Allow browser-based connections from endpoints that do not have the Secure Client installed. Enable this option when devices that your organization does not manage must connect to this resource. Fewer endpoint security checks are possible.

Public URL for this resource ⓘ
 https:// -8195126.ztna.sse.cisco.io

Protocol Server Name Indication (SNI) (optional) ⓘ

Validate Application Certificate ⓘ

- **Zero Trust Connections:**选中复选框。
- **Client-based connection:**如果启用，可以使用安全客户端 — 零信任模块启用通过基于客户端模式的访问。
- **Remote Reachable Address (FQDN, Wildcard FQDN, IP Address) :**配置资源IP或FQDN;如果配置FQDN，则需要添加DNS以解析名称。
- **Browser-based connection :**如果启用，您可以通过浏览器访问资源（请仅使用HTTP或HTTPS通信添加资源）
- **Public URL for this resource:**通过浏览器配置使用的公共URL;Secure Access可保护此资源。
- **Protocol:**选择协议（HTTP或HTTPS）

VPN connections
 Allow endpoints to connect to this resource when connected to the network using VPN.

VPN Connection:选中此复选框可启用通过RA-VPNaaS的访问。

之后，点击Save即可将该资源添加到Access Policy。

配置访问策略

创建资源时，需要将其分配到安全访问策略之一：

- 点击 **Secure > Access Policy**



Secure



Monitor



Admin



Workflows

Policy

Access Policy

Create rules to control and secure access to private and internet destinations

Data Loss Prevention Policy

Prevent data loss/leakage with policy rules

- 点击 [Add > Private Resource](#)

Add Rule ^

Private Access

Control and secure access to resources and applications that cannot be accessed by the general public.

Internet Access

Control and secure access to public destinations from within your network and from managed devices

对于此专用访问规则，可以配置默认值以提供对资源的访问。要了解有关策略配置的更多信息，请查看[用户指南](#)。

1 Specify Access

Specify which users and endpoints can access which resources. [Help](#)

Action

<input checked="" type="radio"/> Allow Allow specified traffic if security requirements are met.	<input type="radio"/> Block Block specified traffic.
--	--

From

Specify one or more sources.

Information about sources, including selecting multiple sources. [Help](#)

To

Specify one or more destinations.

Information about destinations, including selecting multiple destinations. [Help](#)

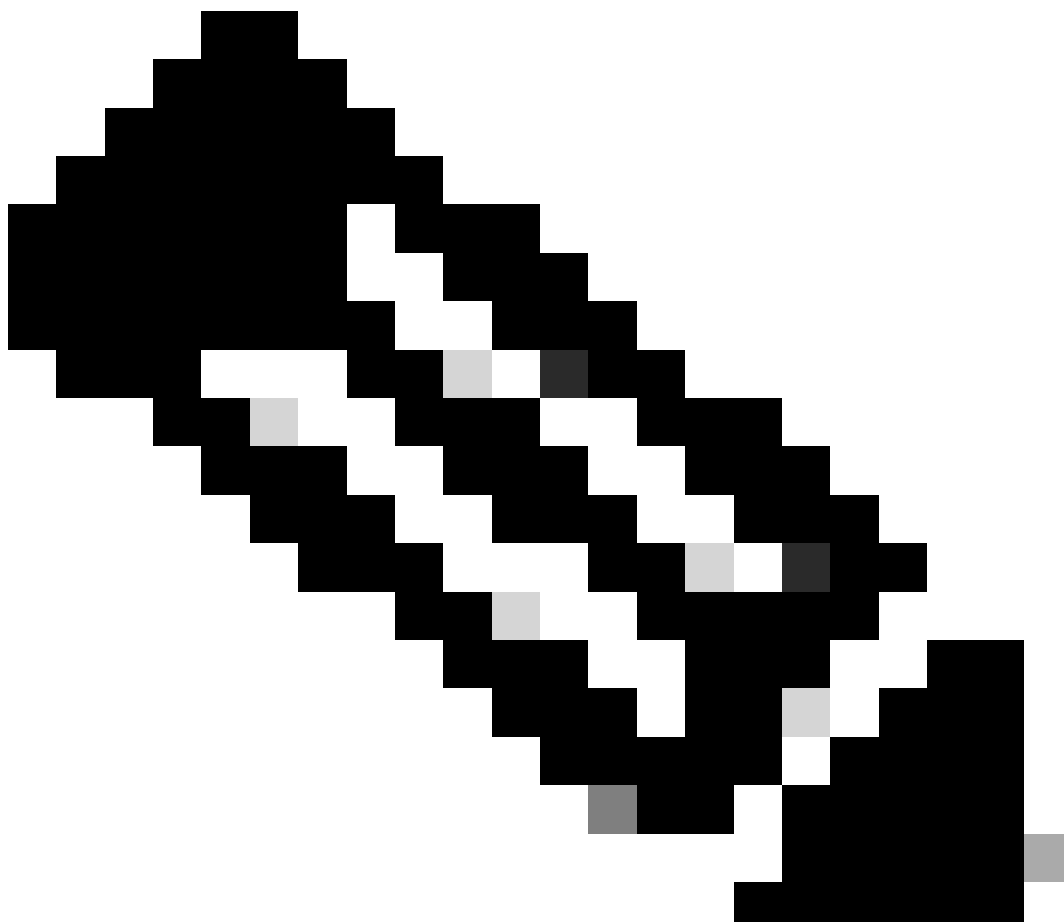
- **Action** :选择Allow以提供对资源的访问。
- **From** :指定可用于登录资源的用户。
- **To** :选择要通过Secure Access访问的资源。

Endpoint Requirements

For zero-trust connections, if endpoints do not meet the specified requirements, this rule will not match the traffic. [Help](#)

<input type="checkbox"/> Zero-Trust Client-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is installed. <input type="text" value="System provided (Client-based)"/>
Private Resources: SplunkFTD
<input type="checkbox"/> Zero Trust Browser-based Posture Profile Rule Defaults Requirements for end-user devices on which the Cisco Secure Client is NOT installed. <input type="text" value="System provided (Browser-based)"/>
Private Resources: SplunkFTD

- **Zero-Trust Client-based Posture Profile**:选择客户端基本访问的默认配置文件
- **Zero-Trust Browser-based Posture Profile** : 选择默认配置文件浏览器基本访问权限



注意：要了解有关安全评估策略的更多信息，请查看[安全访问用户指南](#)。

然后，点击Next和Save 和您的配置，您可以尝试通过RA-VPN和客户端基础ZTNA或浏览器基础ZTNA访问您的资源。

故障排除

要根据安全防火墙和安全访问之间的通信进行故障排除，您可以验证设备之间是否已顺利建立第1阶段(IKEv2)和第2阶段(IPSEC)。

检验第1阶段(IKEv2)

要验证Phase1，您需要在FTD的CLI上运行下一命令：

```
show crypto isakmp sa
```


在这种情况下，所需的输出是建立到数IKEv2 SAs据中心IP的安全访问和所需的状态中的两个READY输出：

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:3, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52346451 192.168.0.202/4500 3.120.45.23/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/4009 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0xfb34754c/0xc27fd2ba
```

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

```
Tunnel-id Local Remote
52442403 192.168.30.5/4500 18.156.145.74/4500
Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/3891 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
remote selector 0.0.0.0/0 - 255.255.255.255/65535
ESP spi in/out: 0x4af761fd/0xfbca3343
```

检验第2阶段(IPSEC)

要验证Phase2，您需要在FTD的CLI上运行下一命令：

```
interface: PrimaryVTI
Crypto map tag: __vti-crypto-map-Tunnel1-0-1, seq num: 65280, local addr: 192.168.30.5

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 18.156.145.74

#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965
#pkts decaps: 91325, #pkts decrypt: 91325, #pkts verify: 91325
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.30.5/4500, remote crypto endpt.: 18.156.145.74/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
```

PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: FBCA3343
current inbound spi : 4AF761FD

inbound esp sas:

spi: 0x4AF761FD (1257726461)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (3916242/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF

outbound esp sas:

spi: 0xFBCA3343 (4224332611)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 2, crypto-map: __vti-crypto-map-Tunnel1-0-1
sa timing: remaining key lifetime (kB/sec): (4239174/27571)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

interface: SecondaryVTI

Crypto map tag: __vti-crypto-map-Tunnel2-0-2, seq num: 65280, local addr: 192.168.0.202

Protected vrf (ivrf): Global
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer: 3.120.45.23

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.0.202/4500, remote crypto endpt.: 3.120.45.23/4500
path mtu 1500, ipsec overhead 63(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: C27FD2BA
current inbound spi : FB34754C

inbound esp sas:

spi: 0xFB34754C (4214519116)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4101120/27412)
IV size: 8 bytes

```
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
outbound esp sas:
spi: 0xC27FD2BA (3263156922)
SA State: active
transform: esp-aes-gcm-256 esp-null-hmac no compression
in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, VTI, }
slot: 0, conn_id: 20, crypto-map: __vti-crypto-map-Tunnel2-0-2
sa timing: remaining key lifetime (kB/sec): (4239360/27412)
IV size: 8 bytes
replay detection support: Y
Anti replay bitmap:
 0x00000000 0x00000001
```

在最后一个输出中，您可以看到两个隧道均已建立；不需要的只是数据包和数据包下的下一个输出 encapsdecaps。

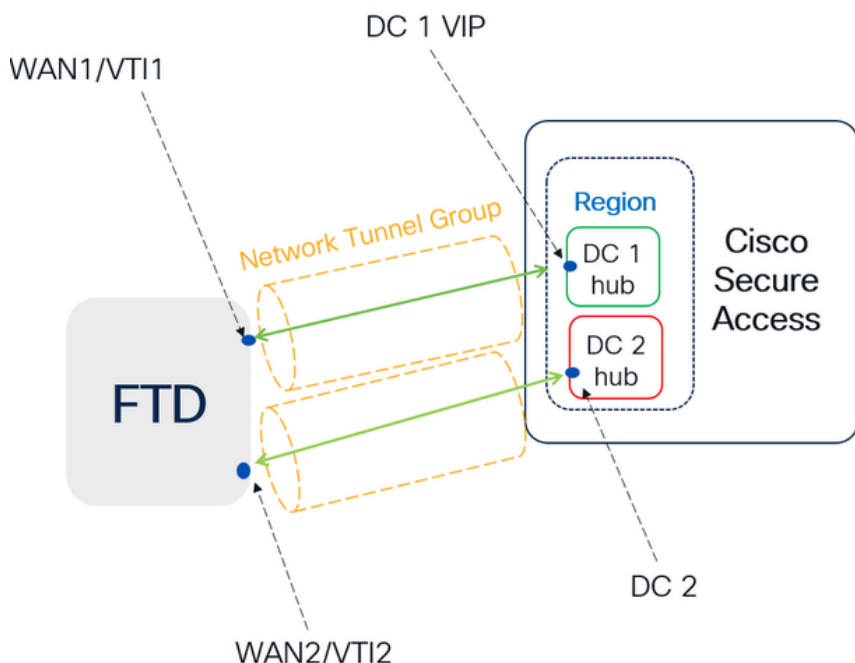
```
#pkts encaps: 71965, #pkts encrypt: 71965, #pkts digest: 71965 → Packets forwarded to Secure Access
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0 → No packets forwarded from Secure
#pkts compressed: 0, #pkts decompressed: 0 → Access to your firewall
#pkts not compressed: 71965, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

如果您有此场景，请通过TAC提交案例。

高可用性功能

具有安全访问功能的隧道与云中的数据中心通信是主动/被动的，这意味着只有DC 1的门才会打开以接收流量；dc 2的门一直关闭，直到1号隧道关闭。

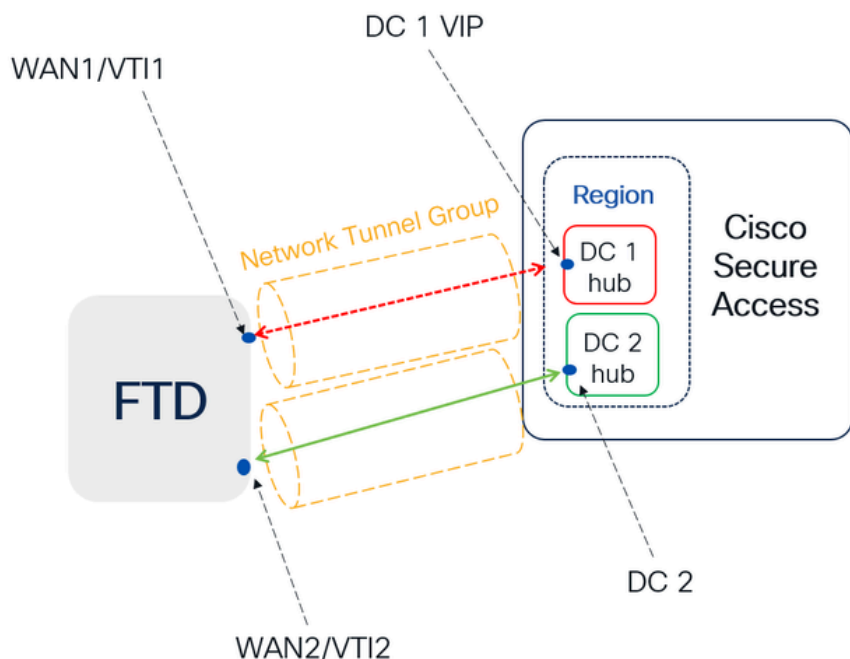
Normal Behavior



Secure Access default behavior

- DC2 is **passive** when DC1 is **active**
- Data Centers operating in High Availability (HA) mode ensure that only one tunnel receives traffic at a time. The other tunnel remains on standby and will drop any packets sent through it while in standby mode.

HA Behavior



Secure Access HA Behavior

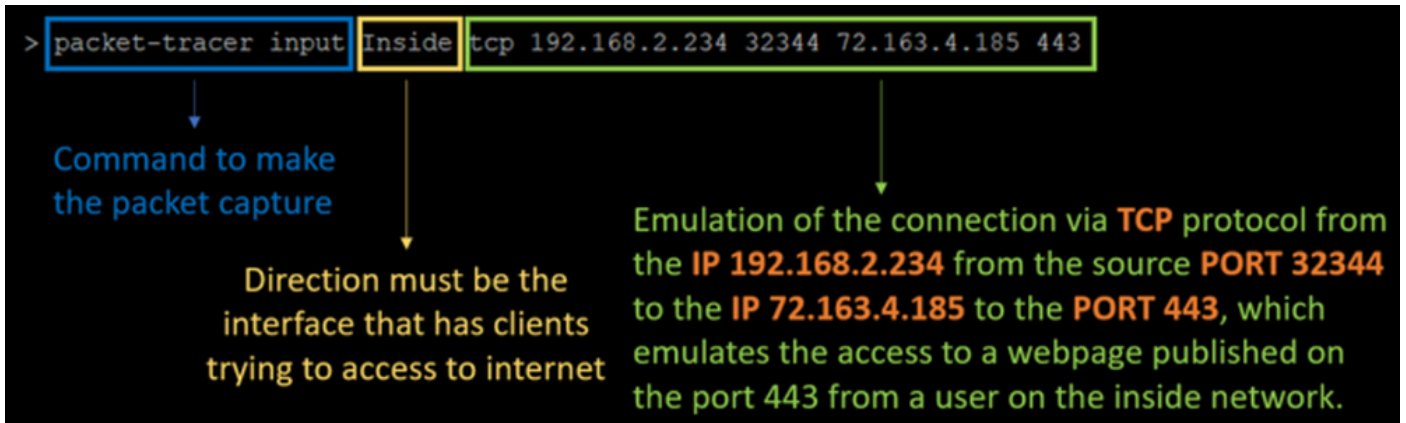
- DC2 is **Active** when DC1 or WAN1 peer is **Down**
- High availability is implemented to address failures in the WAN1 channel on the Firewall, ensuring operational continuity in the **region** and mitigating potential issues in DC1

检验流量路由以实现安全访问

在本示例中，我们将源用作防火墙网络上的计算机：

- 来源：192.168.10.40
- 目的：146.112.255.40 (安全访问监控IP)

示例：



命令：

```
packet-tracer input LAN tcp 192.168.10.40 3422 146.112.255.40 80
```

输出：

```
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 14010 ns
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

```
Phase: 3
Type: OBJECT_GROUP_SEARCH
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:
  Source Object Group Match Count: 0
  Destination Object Group Match Count: 0
```

Object Group Search: 0

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Elapsed time: 233 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any ifc PrimaryVTI any rule-id 268434435
access-list CSM_FW_ACL_ remark rule-id 268434435: ACCESS POLICY: HOUSE - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434435: L7 RULE: New-Rule-#3-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 5
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
class-map class_map_Any
match access-list Any
policy-map policy_map_LAN
class class_map_Any
set connection decrement-ttl
service-policy policy_map_LAN interface LAN
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 233 ns
Config:
Additional Information:

Phase: 8
Type: VPN
Subtype: encrypt
Result: ALLOW
Elapsed time: 18680 ns
Config:
Additional Information:

Phase: 9
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Elapsed time: 25218 ns
Config:
Additional Information:

Phase: 10

Type: NAT
Subtype: per-session
Result: ALLOW
Elapsed time: 14944 ns
Config:
Additional Information:

Phase: 11
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Elapsed time: 0 ns
Config:
Additional Information:

Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Elapsed time: 19614 ns
Config:
Additional Information:
New flow created with id 23811, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 27086 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 28820 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Phase: 15
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 450193 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268434435
Additional Information:
Starting rule matching, zone 1 -> 3, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0,
Matched rule ids 268434435 - Allow

Result:
input-interface: LAN(vrfid:0)
input-status: up
input-line-status: up
output-interface: PrimaryVTI(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 620979 ns

在这里，许多事情都可以为我们提供有关通信的情景，并了解PBR配置下的所有内容是否正确，以便正确地将流量路由到安全访问：

```
Phase: 2
Type: PBR-LOOKUP
Subtype: policy-route
Result: ALLOW
Elapsed time: 21482 ns
Config:
route-map FMC_GENERATED_PBR_1707686032813 permit 5
  match ip address ACL
  set ip next-hop 169.254.2.2 169.254.3.2
Additional Information:
  Matched route-map FMC_GENERATED_PBR_1707686032813, sequence 5, permit
  Found next-hop 169.254.2.2 using egress ifc PrimaryVTI
```

第2阶段表示流量正转发到接口，这是正确PrimaryVTI的，因为根据此场景中的配置，必须通过VTI将互联网流量转发到安全访问。

Phase: 8

Type: VPN

Subtype: encrypt

Result: ALLOW

Elapsed time: 18680 ns

Config:

Additional Information:

Phase: 9

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Elapsed time: 25218 ns

Config:

Additional Information:

连接中的加密阶段，在该阶段，将评估和授权流量进行加密，以确保可以安全地传输数据。另一方面，第9阶段重点关注VPN IPSec隧道内流量流的特定管理，确认已加密流量正确路由并允许通过已建立的隧道。

Result:

input-interface: LAN(vrfid:0)

input-status: up

input-line-status: up

output-interface: PrimaryVTI(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 620979 ns

要最终确定，在流结果的末尾，您可以看到从到的流量将流LAN量PrimaryVTI转发到安全访问。该操作allow可确认流量路由没有问题。

相关信息

- [思科技术支持和下载](#)
- [思科安全访问帮助中心](#)
- [虚拟可信平台模块概述](#)
- [零信任访问模块](#)
- [对安全访问错误“注册服务未响应”进行故障排除。联系您的IT服务中心”](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。