

Configuration et dépannage de l'intégration de l'accès sécurisé (SSE) sur le SD-WAN Catalyst

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Accès sécurisé Cisco](#)

[Configurations préliminaires](#)

[Créer des interfaces de bouclage](#)

[Configurer de nouvelles clés API sur le portail SSE](#)

[Configurer SSE sur Catalyst Manager](#)

[Configurer les informations d'identification cloud](#)

[Configuration des tunnels SSE à l'aide du groupe de stratégies](#)

[Configurer le groupe de stratégies](#)

[Configurer le groupe de stratégies pour rediriger le trafic vers SSE](#)

[Vérifier](#)

[Responsable](#)

[Tableau de bord Secure Access](#)

[Commandes CLI \(Command Line Interface\)](#)

Introduction

Ce document décrit comment configurer l'intégration SSE active-active sur le SD-WAN Catalyst et guide son dépannage.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Réseau étendu défini par logiciel (SD-WAN) Cisco
- Groupes de configuration
- Groupes de stratégies

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- C8000V version 17.15.02
- vManage version 20.15.02
- Compte Cisco Secure Access

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Accès sécurisé Cisco

Cisco Secure Access est une solution SSE (Security Service Edge) basée sur le cloud qui fait converger plusieurs services de sécurité réseau, en les fournissant à partir du cloud pour prendre en charge une main-d'oeuvre hybride. Cisco SD-WAN Manager exploite les API REST pour récupérer des informations de stratégie à partir de Cisco Secure Access et les distribue aux périphériques SD-WAN Cisco IOS XE. Cette intégration permet aux utilisateurs de bénéficier d'un accès direct à Internet (DIA) transparent, transparent et sécurisé, leur permettant de se connecter à partir de n'importe quel périphérique, n'importe où et en toute sécurité.

Cisco SSE permet aux périphériques SD-WAN d'établir des connexions avec les fournisseurs SSE à l'aide de tunnels IPsec. Ce document est destiné aux utilisateurs de Cisco Secure Access.

Configurations préliminaires

- Activer la recherche de domaine pour le périphérique : Accédez à Groupes de configuration > Profil système > Global et activez la recherche de domaine.



Remarque : Par défaut, la recherche de domaine est désactivée.

- Configurer DNS : Le routeur peut résoudre le DNS et accéder à Internet sur le VPN 0.
- Configurez NAT DIA : La configuration DIA doit être présente sur le routeur où le tunnel SSE est créé.

Créer des interfaces de bouclage

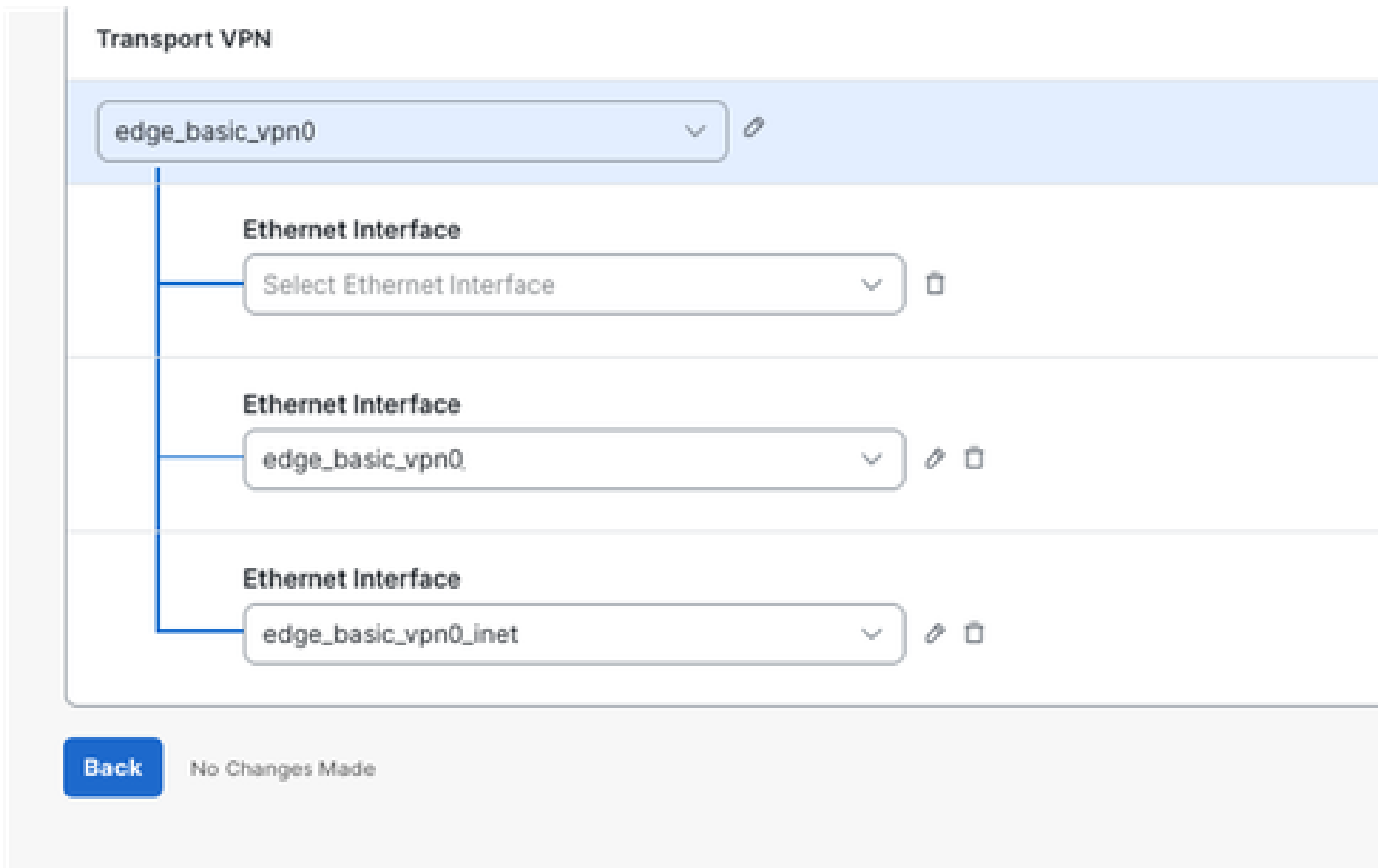
Si les deux tunnels d'une configuration active/active se connectent au même data center de destination et utilisent la même interface WAN que la source, deux adresses IP de bouclage doivent être créées.



Remarque : Lorsque deux tunnels sont configurés avec la même source et la même destination, IKEv2 forme une paire d'identités composée d'un ID local et d'un ID distant. Par défaut, l'ID local est l'adresse IP de l'interface source du tunnel. Cette paire d'identités doit être unique et ne peut pas être partagée entre deux tunnels. Pour éviter toute confusion dans l'état IKEv2, chaque tunnel utilise une interface de bouclage différente comme source.

 Bien que les paquets IKE soient traduits (NATed) sur l'interface DIA, l'ID local reste inchangé et conserve l'adresse IP de bouclage d'origine.

1. Accédez à Configuration > Configuration Groups > Configuration Group Name> Transport & Management Profile > cliquez sur Edit.
2. Cliquez sur le signe plus (+) à droite du profil VPN de transport (profil principal). Le menu Ajouter une fonction (Add Feature) situé à l'extrême droite s'ouvre.
3. Cliquez sur Ethernet Interface. Il ajoute une nouvelle interface Internet sous Transport VPN.



4. Créez les deux interfaces de bouclage à l'aide des adresses IPv4 RFC1918, comme l'exemple Loopback0 dans l'image.

Ethernet Interface

Name: Loopback0

Description(optional):

Basic Configuration | Ether Channel | Tunnel | NAT | ARP | ACL/QoS | Advanced

Shutdown: ☐ ☒

Interface Name: Loopback0

Description: <SYSTEM DEFAULT>

Service Provider: <SYSTEM DEFAULT>

Bandwidth Upstream: <SYSTEM DEFAULT>

Bandwidth Downstream: <SYSTEM DEFAULT>

Auto Detect Bandwidth: ☐ ☒

IPv4 Settings

☐ Dynamic ☒ Static

IP Address: 10.1.1.1

Subnet Mask: /32 255.255.255.255

Cancel Save

Transport VPN

edge_basic_vpn0

Ethernet Interface: Loopback1

Ethernet Interface: Loopback0

Ethernet Interface: edge_basic_vpn0_mpls

Ethernet Interface: edge_basic_vpn0_inet

New Loopback interfaces

Back All Changes Saved

5. Après avoir appliqué la configuration de bouclage, poursuivez le déploiement de la modification de configuration sur le périphérique. Notez que l'état d'approvisionnement passe de 1/1 à 0/1.

Name	Type	Profile	Provisioning Status ¹ Sync Devices / Associated Devices	Origin	Updated By
Hub2-SIG	Single Router	4	 0 / 1	user	cisco

Configurer de nouvelles clés API sur le portail SSE

1. Accès au portail SSE <https://login.sse.cisco.com/>
2. Accédez à Admin > Clés API



Home



Experience
Insights



Connect



Resources



Secure



Monitor

Admin



Account Settings

Accounts

Authentication

Management

API Keys

Third-party Integrations

Log Management

Subscription

Integrations

6. Copiez la clé API et la clé secrète dans un bloc-notes et sélectionnez ACCEPT AND CLOSE (ACCEPTER ET FERMER)

Click Refresh to generate a new key and secret.

API Key [Redacted]	Key Secret [Redacted]
-----------------------	--------------------------

Copy the Key Secret. For security reasons, it is only displayed once. If lost, it cannot be retrieved.

ACCEPT AND CLOSE

7. Sous l'URL <https://dashboard.sse.cisco.com/#some-numbers#/admin/apikeys#some-numbers#> est votre ID d'organisation. Copiez également ces informations dans votre bloc-notes.



Discover your SSE organization ID

Configurer SSE sur Catalyst Manager

Configurer les informations d'identification cloud

1. Accédez à Administration > Settings > Cloud Credentials > Cloud Provider Credentials, et activez l'accès sécurisé Cisco et entrez les détails.

Settings / External Services

Cloud Credentials

Cloud Provider Credentials Umbrella DNS Certificate

Configure Cisco Umbrella, Zscaler, and Cisco Secure Access credentials to enable Cisco Catalyst SD-WAN Manager to create automatic SIG tunnels to Cisco Umbrella or Zscaler endpoints.

☐ Umbrella

☐ Zscaler

☒ Cisco SSE

Organization Id

Api Key

Secret

☒ Context Sharing

2. Facultatif : Vous pouvez activer le partage de contexte pour une fonctionnalité améliorée. Pour plus d'informations, reportez-vous au [Guide de l'utilisateur Cisco SSE sur le partage de contexte](#).

Configuration des tunnels SSE à l'aide du groupe de stratégies

Dans le gestionnaire SD-WAN, accédez à Configuration > Policy Groups > Secure Internet Gateway/Secure Service Edge et cliquez sur Add Secure Service Edge (SSE) .

Remarque : si les informations d'identification du cloud n'ont pas encore été configurées, vous pouvez les ajouter à cette étape. Si les informations d'identification ont déjà été configurées, elles sont chargées automatiquement.

Add cisco-sse Credentials



Cisco SSE Organization Id*

[Redacted]

Cisco SSE API Key*

[Redacted]

Cisco SSE API Secret*

..... [SHOW](#)



Context Sharing

[Cancel](#)

[Add](#)

1. Configurez le dispositif de suivi SSE. Dans cet exemple, l'URL du dispositif de suivi est définie sur <http://www.cisco.com>, et l'adresse IP source est attribuée à partir de l'une des interfaces de bouclage.

Add Tracker



Name



cisco-tracker

API URL Of Endpoint



<http://www.cisco.com>

Threshold



300

Probe Interval



60

Multiplier



3

[Cancel](#)

[Add](#)

SSE-Policy

SSE Provider
☒ Cisco Secure Access ☐ Zscaler

Context Sharing
☒ VPN ☐ SGT

Tracker
Source IP address: 10.0.0.10

+ Add Tracker

Name	Threshold	Interval	Multiplier	API URL Of Endpoint	Action
cisco-tracker	300	60	3	http://www.cisco.com	

1 Record

Comme le partage de contexte a été activé lorsque les informations d'identification du cloud ont été configurées, le VPN est sélectionné comme option facultative dans cet exemple.

2. Cliquez sur Add Tunnel

Configuration
+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
There is no data.					

0 Record

Region: Auto

3. Dans cet exemple, l'interface Loopback0 est utilisée comme source du tunnel, tandis que l'interface GigabitEthernet1 sert d'interface WAN pour acheminer le trafic.

Add Tunnel



Tunnel Type
☒ ipsec

Interface Name(1..255)

Tunnel Source Interface*

Tracker

Tunnel Route-via Interface

Data Center
☒ Primary ☐ Secondary

> Advanced Options

Cancel Add

Comme le tracker a été configuré dans cet exemple, le paramètre est changé en Global, et le tracker cisco préconfiguré est sélectionné.

4. Pour le deuxième tunnel, répétez les mêmes étapes en utilisant les mêmes paramètres, mais changez le nom d'interface de ipsec1 à ipsec2, et le nom d'interface source à Loopback1.



Add Tunnel

Tunnel Type

☒ ipsec

Interface Name(1..255)



ipsec2

Tunnel Source Interface*



Loopback1

Tracker



cisco-tracker



Tunnel Route-via Interface



GigabitEthernet1

Data Center

☒ Primary

☐ Secondary

> Advanced Options

Cancel

Add

Les deux tunnels sont configurés pour être actifs simultanément, sans sauvegarde.

5. Cliquez sur Add Interface Pair.

6. Cliquez sur Ajouter. L'interface active est définie sur ipsec1 et aucune interface de sauvegarde n'est spécifiée.



Add Interface Pair

Active Interface



ipsec1



Active Interface Weight



1

Backup Interface



None



Backup Interface Weight



1

Cancel

Add

7. La même opération est répétée pour le deuxième tunnel, ipsec2.

Configuration

+ Add Tunnel

Interface Name	Description	Shutdown	TCP MSS	IP MTU	Action
ipsec1		☒ false	☒	☒ 1400	✎ ✕
ipsec2		☒ false	☒	☒ 1400	✎ ✕

2 Records

Items per page: 5 1 - 2 of 2 < > >>

Region

☒ Auto

High Availability

+ Add Interface Pair

Active Interface	Active Interface Weight	Backup Interface	Backup Interface Weight	Action
ipsec1	☒ 1	☒ None	☒ 1	✎ ✕
ipsec2	☒ 1	☒ None	☒ 1	✎ ✕

2 Records

Items per page: 5 1 - 2 of 2 < > >>

8. Enregistrez la configuration.

Configurer le groupe de stratégies

1. Il vous suffit de sélectionner la règle précédemment créée dans le groupe de règles et de l'enregistrer.

Policy Groups

Policy Group 1 Application Priority & SLA 0 NGFW 0 Secure Internet Gateway / Secure Service Edge 2 DNS Security 0

+ Add Policy Group Export Import

As of: 29 de julio de 2025, 1:09 p.m.

Q Search

Name	Description	Number of Policies	Number of Devices	Devices Up to Date	Updated By	Last Updated On	Actions
PG-SSE-C8V							⋮ ↑

Policy Group Name

PG-SSE-C8V

Description(optional)

Application Priority

Please Select one

NGFW

Please Select one

Secure Internet Gateway / Secure Service Edge

SSE-Policy

DNS Security

Please Select one

Device Solution

Type sdwan

Deployment

Associated + Add

Save

Deploy

2. Une fois que le ou les périphériques ont été associés au groupe de stratégies, poursuivez le déploiement du groupe de stratégies.

PG-SSE-C8V

Policy Group Name

PG-SSE-C8V

Description(optional)

Application Priority

Please Select one

NGFW

Please Select one

Secure Internet Gateway / Secure Service Edge

SSE-Policy

DNS Security

Please Select one

Device Solution

Type sdwan

Deployment

Associated 1 device

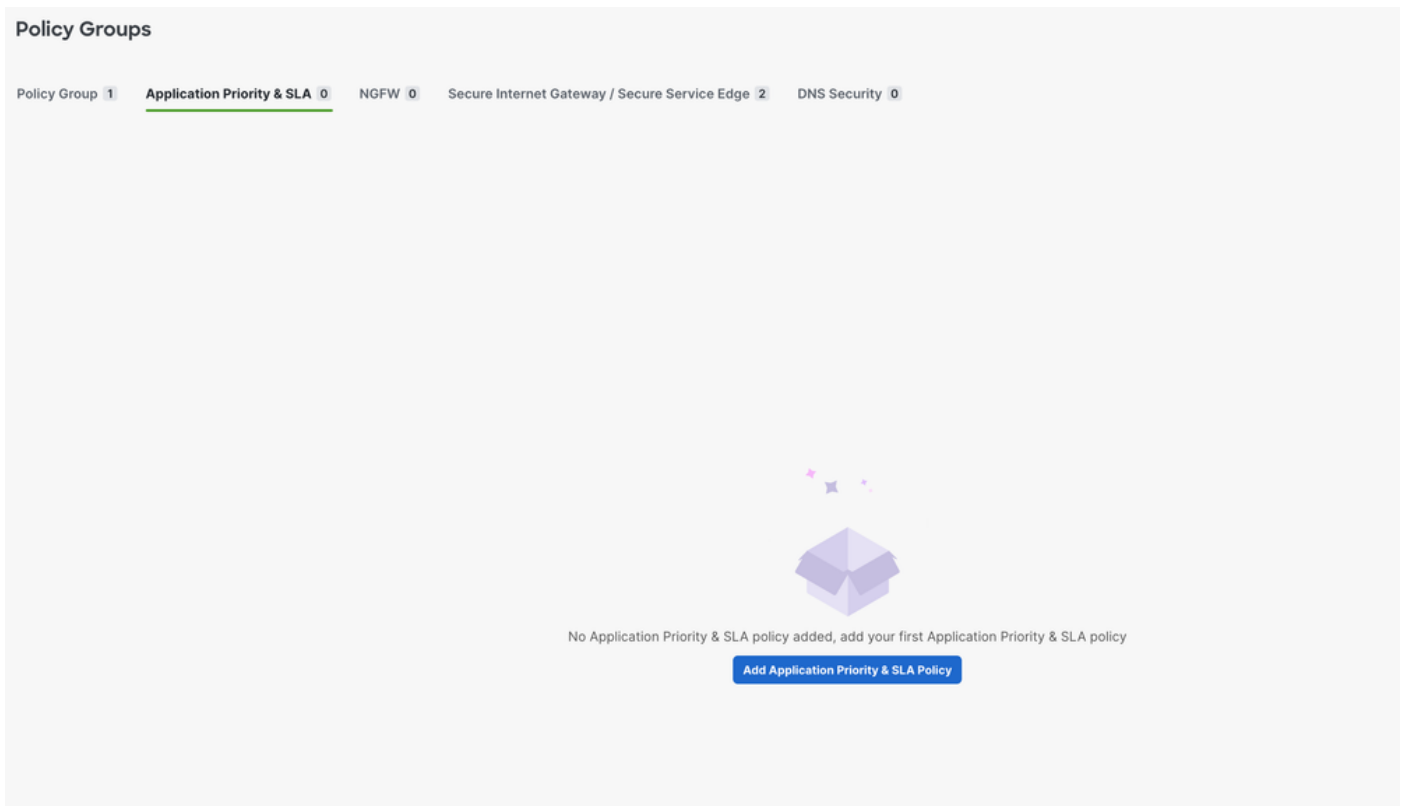
Save

Deploy

Configurer le groupe de stratégies pour rediriger le trafic vers SSE

1. Sur le gestionnaire SD-WAN, accédez à Configuration > Policy Groups > Application Priority & SLA.

- Sélectionnez Ajouter une priorité d'application et une politique SLA
- Spécifiez un nom pour la stratégie.



2. Une fois la nouvelle stratégie affichée, sélectionnez la bascule Mise en page avancée.



3. Sélectionnez Add Traffic Policy List.

- Configurez les VPN pour rediriger le trafic vers le tunnel SSE.
- Définissez la direction et l'action par défaut selon vos besoins, puis enregistrez.

Edit Traffic Policy List

Policy Name

SSE-Redirect

VPN(s)

edge_basic_vpn1

Direction

Service

Default Action

☒ Accept ☐ Drop

Cancel

Save

4. Sélectionnez + Ajouter une règle.

SSE-Redirect (0) [Edit Policy](#) [Delete Policy](#) [Copy Policy](#) [+ Add Rules](#) [Delete All Rules](#)

VPN: edge_basic_vpn1 Direction: Service Default Action: Accept

No Rules Added

5. Configurez vos critères de trafic de correspondance pour rediriger le trafic vers le SSE.

6. Sélectionnez Accepter comme action de base, puis cliquez sur + Action.

7. Recherchez l'action Secure Internet Gateway / Secure Service Edge et définissez-la sur Secure Service Edge.

Action + Add Action

- ☐ LOCAL TLOC
- ☐ Remote Preferred Color
- ☐ Preferred Color group
- ☐ NAT Pool
- ☐ NAT VPN
- ☐ Next Hop
- ☐ Policer
- ☐ Redirect DNS
- ☐ TLOC
- ☐ Service
- ☐ Service Chain
- ☒ Secure Internet Gateway / Secure Service Edge
- ☐ AppQoS Optimization
- ☐ Loss Correction

Service Edge ☐ Fall Back to Routing

1 / 1

App Store

SSE-Redirect (1) [Edit Policy](#) [Delete Policy](#) [Copy Policy](#) + Add Rules [Delete All Rules](#)

VPN: edge_basic_vpn1 Direction: Service Default Action: Accept

Search Rule by Name or Order

NAME	MATCH	ACTION
1 Rule1		

Sequence: 1 Name(optional): SSE-Traffic Protocol: IPv4

Match + Add Match

Action + Add Action

Base Action

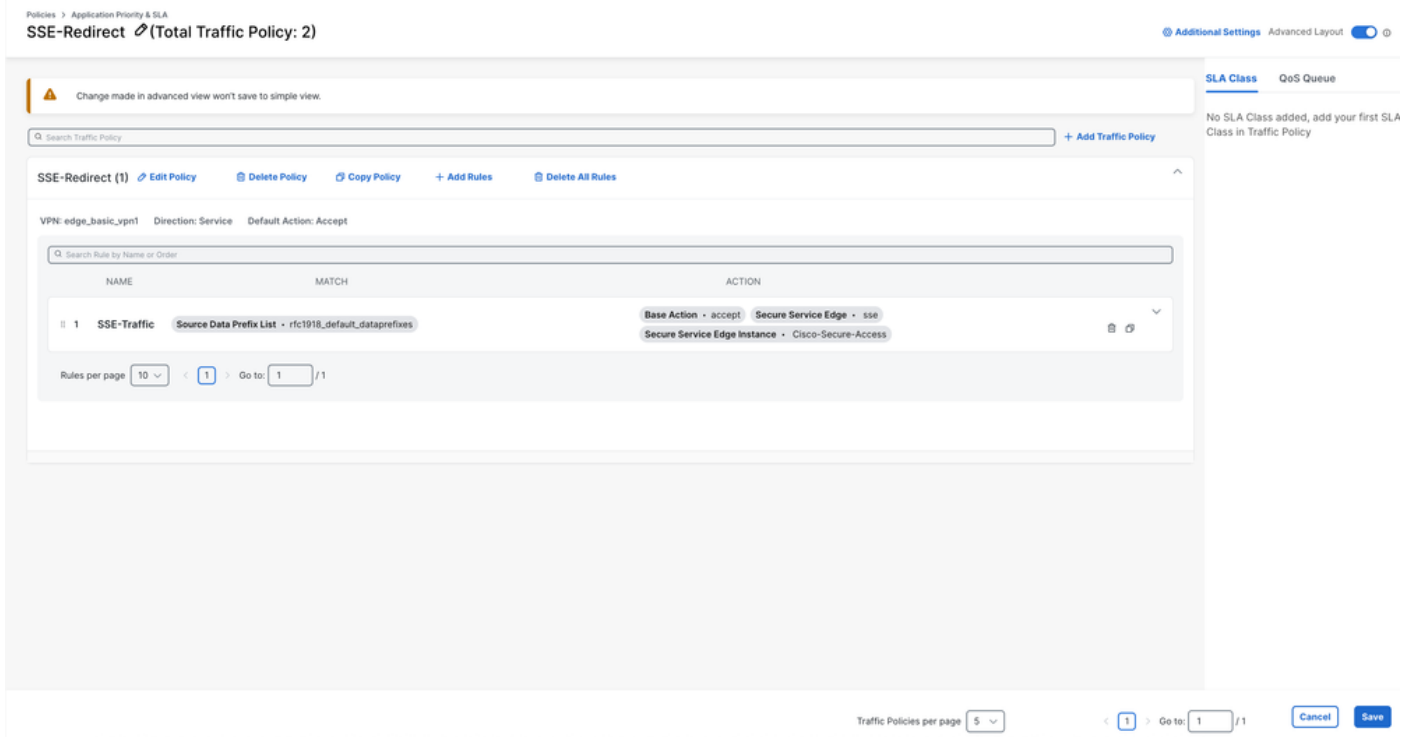
☒ Accept ☐ Drop

Secure Internet Gateway / Secure Service Edge

☐ Secure Internet Gateway ☒ Secure Service Edge Cisco Secure Access ☒ Fall Back to Routing

Cancel Save Match and Actions

8. Cliquez sur Enregistrer la correspondance et les actions



9. Cliquez sur Enregistrer.

10. Accédez à Configuration > Policy Groups et sélectionnez la stratégie Application Priority que vous venez de créer. Enregistrez, puis déployez.

PG-SSE-CBV

Policy Group Name PG-SSE-CBV Description(optional)

Application Priority SSE-Redirect NGFW Please Select one

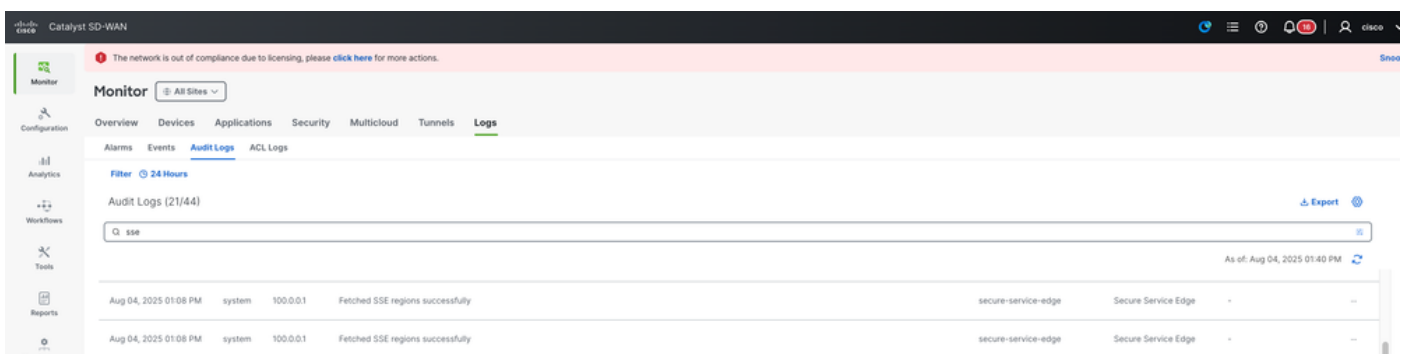
Secure Internet Gateway / Secure Service Edge SSE-Policy DNS Security Please Select one

Device Solution Type sdwan Deployment Associated 1 device Save Deploy

Vérifier

Responsable

1. Surveiller > Journaux > Journaux d'audit et recherchez « sse ».



2. Vous pouvez vérifier si le VPN de partage de contexte est activé correctement en cochant la

case Manager.

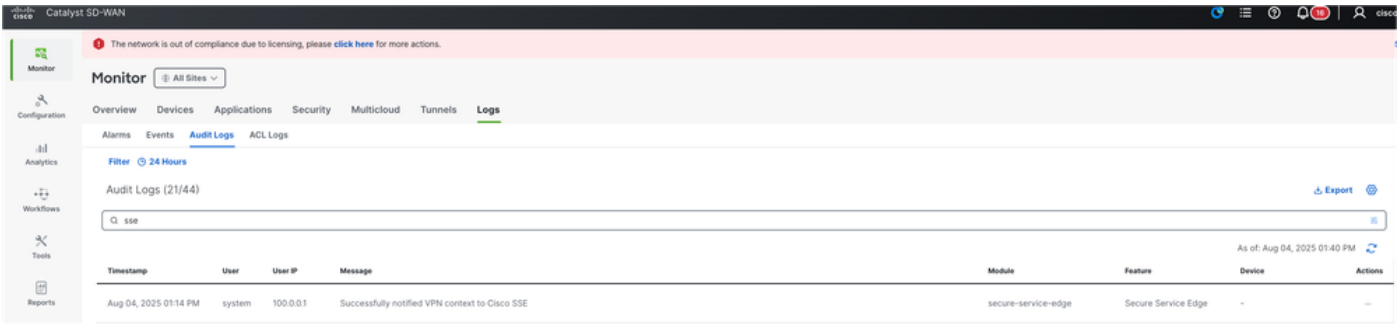
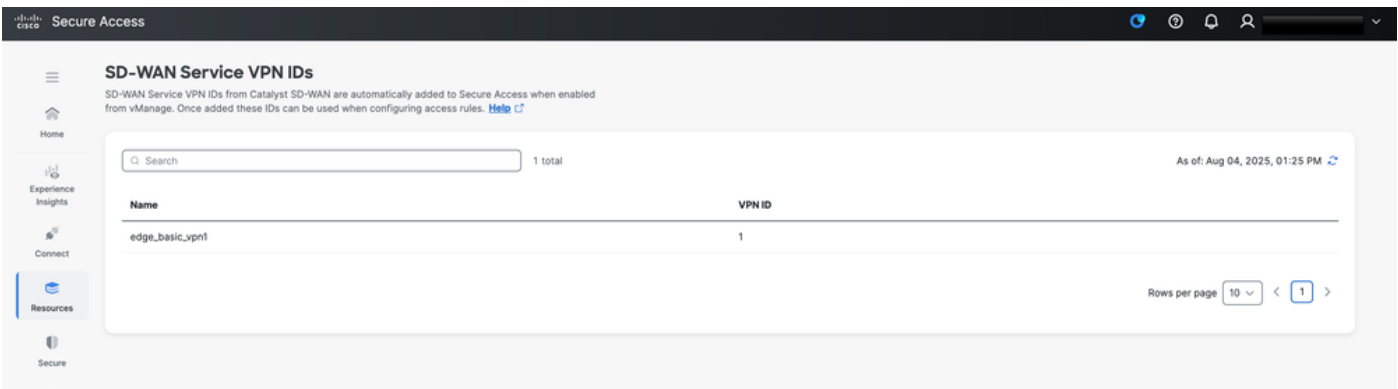


Tableau de bord Secure Access

Partage de contexte

Vous pouvez vérifier si le VPN de partage de contexte est activé correctement en vérifiant le tableau de bord SSE,Ressources > ID VPN du service SD-WAN



Tunnel vers le haut

Lorsque le tunnel est actif et que le traqueur est opérationnel avec le trafic circulant à travers le tunnel, vous pouvez le valider en naviguant vers Monitor > Activity Search. Dans cet écran, vous voyez le trafic qui traverse le tunnel, comme les requêtes vers www.cisco.com générées par le traqueur. Cette visibilité confirme que le traqueur est actif et surveille activement le trafic à travers le tunnel

Request	Source	Rule Identity	Destination	Destination IP	Destination Port	Destination Country	Int.
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...
FW	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD	http://www.cisco.com/	23.33.181.29-80		United States	10.1...

Commandes CLI (Command Line Interface)

```
<#root>
```

```
Hub2-SIG#show sse all
```

```
*****
```

```
SSE Instance Cisco-Secure-Access
```

```
*****
```

```
Tunnel name : Tunnel16000001
```

```
Site id: 2
```

```
Tunnel id: 655184839
```

```
SSE tunnel name: C8K-D4CE7174-5261-7E6F-91EA-4926BCF4C2DD
```

```
HA role: Active
```

```
Local state: Up
```

```
Tracker state: Up
```

```
Destination Data Center: 44.217.195.188
```

```
Tunnel type: IPSEC
```

```
Provider name: Cisco Secure Access
```

```
Context sharing: CONTEXT_SHARING_SRC_VPN
```

Informations connexes

- [Configuration du partage de contexte SD-WAN](#)
- [Intégration de Cisco Secure Access avec le routage SD](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.