Configuration du basculement pour les tunnels IPSec site à site

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Informations générales
Configurer
Diagramme du réseau
Configuration du FTD
Étape 1 : définition des interfaces ISP principale et secondaire
Étape 2 : définition de la topologie VPN pour l'interface principale du FAI
Étape 3. Définition de la topologie VPN pour l'interface ISP secondaire
Étape 4. Configuration du SLA Monitor
Étape 5. Configuration des routes statiques avec le SLA Monitor
Étape 6. Configuration de l'exemption NAT
Étape 7. Configuration de la stratégie de contrôle d'accès pour le trafic intéressant
Configuration de l'ASA
Vérifier
FTD
Route
Suivre
NAT
Effectuer le basculement
Route
Suivre
NAT
Dépannage

Introduction

Ce document décrit comment configurer le basculement basé sur la crypto-carte avec des liaisons de sauvegarde ISP avec la fonctionnalité IP SLA track sur FTD géré par FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Compréhension de base d'un réseau privé virtuel (VPN)
- Expérience avec FTD
- Expérience avec FMC
- Expérience avec la ligne de commande ASA (Adaptive Security Appliance)

Composants utilisés

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

- FMC version 6.6.0
- FTD version 6.6.0
- ASA version 9.14.1

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.

Informations générales

Ce document décrit comment configurer le basculement basé sur une crypto-carte pour la liaison de secours du fournisseur d'accès Internet (FAI) avec la fonctionnalité de suivi IP SLA (Internet Protocol Service Level Agreement) sur le pare-feu Firepower Threat Defense (FTD) géré par le Centre de gestion Firepower (FMC). Il explique également comment configurer l'exemption de traduction d'adresses de réseau (NAT) pour le trafic VPN lorsqu'il y a deux FAI et qu'il nécessite un basculement transparent.

Dans ce scénario, le VPN est établi du FTD vers l'ASA comme homologue VPN avec une seule interface ISP. Le FTD utilise une liaison FAI à ce moment pour établir le VPN. Lorsque la liaison du FAI principal tombe en panne, le FTD prend le relais avec la liaison du FAI secondaire via le SLA Monitor et le VPN est établi.

Configurer

Diagramme du réseau

Voici la topologie utilisée pour l'exemple dans ce document :



Configuration du FTD

Étape 1 : définition des interfaces ISP principale et secondaire

1. Accédez à Périphériques > Gestion des périphériques > Interfaces comme indiqué dans l'image.

Firepower Management	Center _Q	Overview An	alysis Policies	Devices Objects	AMP	Intelligence	Deploy	¢	\$	admin 🛛	1*			
End of the set o														
				Q Sear	ch by name		Sync Device		Add I	nterfaces 🔻	,			
Interface	Logical Name	Туре	Security Zones	MAC Address (Acti	ve/Standby)	IP Addres	ŝS							
Diagnostic0/0	diagnostic	Physical								/				
GigabitEthernet0/0	Outside	Physical	Outside			10.200.1.	5/24(Static)			/				
GigabitEthernet0/1	Outside2	Physical	Outside2			10.201.1.	5/24(Static)			/				
GigabitEthernet0/2	Inside	Physical	Inside			10.10.10.	5/24(Static)			/				
GigabitEthernet0/3		Physical								/				

Étape 2 : définition de la topologie VPN pour l'interface principale du FAI

1. Accédez à Devices > VPN > Site To Site. Sous Add VPN, cliquez sur Firepower Threat Defense Device, créez le VPN et sélectionnez l'interface externe.

Remarque : Ce document ne décrit pas comment configurer un VPN S2S à partir de zéro. Pour plus de références sur la configuration VPN S2S sur FTD, consultez la page <u>https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html</u>

Edit VPN Topology			G	
Topology Name:* VPN_Outside1 Network Topology: Point to Point Hub and Sp	poke Full Mesh			
IKE Version:* IKE IKEv1	KEv2			
Node A:			+	
Device Name	VPN Interface	Protected Networks		
ASAv	10.100.1.1	10.10.20.0_24	/ 1	
Node B:			+	
Device Name	VPN Interface	Protected Networks]
FTDv	Outside/10.200.1.5	10.10.10.0_24	/ 1	
Ensure the protected netw	vorks are allowed by access o	ontrol policy of each device.		
			Cancel Save	

Étape 3. Définition de la topologie VPN pour l'interface ISP secondaire

1. Accédez à Devices > VPN > Site To Site. Sous Add VPN, cliquez sur Firepower Threat Defense Device, créez le VPN et sélectionnez l'interface Outside2.

Remarque : la configuration VPN qui utilise l'interface Outside2 doit être exactement identique à la topologie Outside VPN, à l'exception de l'interface VPN.

Edit VPN Topology				9							
Topology Name:* VPN_Outside2 Network Topology: Point to Point Hub and Spoke Full Mesh IKE Version:* IKEv1											
Endpoints IKE IPsec	Advanced										
Node A:				+							
Device Name	VPN Interface	Protected Networks									
ASAv	10.100.1.1	10.10.20.0_24	/ 1								
Node B:				+							
Device Name	VPN Interface	Protected Networks									
FTDv	Outside2/10.201.1.5	10.10.10.0_24	/ 1								
Ensure the protected network	vorks are allowed by access o	control policy of each device.									
			Cancel	ve							

Les topologies VPN doivent être configurées comme indiqué dans l'image.

Firepower Management Center Devices / VPN / Site To Site	Q	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	Deploy	¢	٥	0	admin 🗸
									Add VPN				Ŧ
Node A				Node B									
✓ ↔ VPN_Outside1													/=
extranet : ASAv / 10.100.1.1				FTDv /	Outside / 10.2	00.1.5							
✓ ↔ VPN_Outside2													/ 1
extranet : ASAv / 10.100.1.1				FTDv /	Outside2 / 10.	201.1.5							

Étape 4. Configuration du SLA Monitor

1. Accédez à Objects > SLA Monitor > Add SLA Monitor. Sous Add VPN, cliquez sur Firepower Threat Defense Device, et configurez le SLA Monitor comme indiqué dans l'image.

CISCO Objects / Object Manageme	ment Center	۹	Overview	Analysis	Policies	Devices	Objec	ts	AMP	Intelligence	Deploy	¢	\$	9	admin 🗸
Access List Address Pools Application Filters	SLA MON SLA monitor de Tracking field of	itor fines a c f an IPv4	onnectivity po Static Route F	licy to a monit Policy. IPv6 ro	tored address a utes do not hav	and tracks the ve the option t	availabil to use SL	ity of a A moni	Ad route to t tor via roo	d SLA Monitor he address. The SL ute tracking.	Q, Filter A Monitor ob	oject is	used i	n the	Route
As Paul Cipher Suite List Community List	Name							Value Secur	ity Zone: (Dutside				,	_
Distinguished Name DNS Server Group	ISP_Outside1							Monit	or ID: 10 or Addres	s: 10.200.1.1				/	•
FlexConfig Geolocation															
Interface Key Chain Network															
PKI Policy List															
Port Prefix List RADIUS Server Group															
Route Map Security Group Tag															
Security Intelligence Sinkhole															
Time Range Time Zone															
Tunnel Zone URL															
Variable Set VLAN Tag VPN															

- 2. Pour le champ SLA Monitor ID*, les valeurs peuvent aller de 1 à 2147483647
- 3. Pour le champ Monitor Address*, utilisez l'adresse IP du tronçon suivant externe.

N	Edit SLA Monitor (Object				0	L
nitc I fie	Name: ISP_Outside1]	Descript	ion:		ak tr
uts	Frequency (seconds): SLA Monitor ID*: 10	60			(1-604800)		sic D.
	Threshold (milliseconds):	5000			(0-60000)		
L	Timeout (milliseconds):	5000			(0-604800000)		l
	Data Size (bytes):	28			(0-16384)		I
	ToS:		Number of Pa	ackets:			
	Monitor Address*: 10.200.1.1 Available Zones C Q Search Inside Outside Outside2		Add	Selected	I Zones/Interfaces	3	
l					Cancel	Save	

Étape 5. Configuration des routes statiques avec le SLA Monitor

1. Accédez à Périphériques > Routage > Route statique. Sélectionnez Add Route et configurez la route par défaut pour l'interface externe (principale) avec les informations de surveillance SLA (Créé à l'étape 4) dans le champ Route tracking.

Type: IPv4 (_ IPv6		
Interface*			
Outside1	*		
(Interface starting with this icc	on 🔞 signifies it is av	ailable for route leak)	
Available Network C	+	Selected Network	
Q Search	Add	any-ipv4	Ì
10.10.10.0		·	
192.168.100.1			
192.168.200.0			
any-ipv4			
IPv4-Benchmark-Tests			
IPv4-Link-Local	-		
Gatewav*			
10.200.1.1	• +		
Metric:			
1			
(1 - 254)			
Tunneled: 🗌 (Used only for	default Route)		
Route Tracking:			
ISP_Outside1	• +		

2. Configurez la route par défaut pour l'interface Outside2 (secondaire). La valeur de la mesure

doit être supérieure à la route par défaut principale. Aucun champ de suivi de route n'est nécessaire dans cette section.

Edit Static Route Config	uration		0
Type: IPv4) IPv6		
Interface*	~		
Outside2	*		
(Interface starting with this icon	n 🔊 signifies it is av	vailable for route leak)	
Available Network C	+	Selected Network	
Q Search	Add	any-ipv4	Ì
10.10.10.0	<u> </u>		-
192.168.100.1			
192.168.200.0			
anv-ipv4			
IPv4-Benchmark-Tests			
IPv4-Link-Local	-		
Cataurant			
10 201 1 1	*		
Metric	•		
2			
(1 - 254)			
Tunneled: (Used only for a	default Route)		
Route Tracking:			
	• +		
		Canc	el OK

Les routes doivent être configurées comme indiqué dans l'image.

Firepower Managem Devices / NGFW Routing	ent Center _Q	Overview Analysis	Policies Devices	Objects AMP	Intelligence [Deploy 🔮 🌣 🕲	admin 🗸
FTDV Cisco Firepower Threat Defense for VI Device Routing Interfaces	MWare Inline Sets DHCF					Save	Cancel
OSPF						+ Ad	d Route
OSPFv3 RIP	Network 🔺	Interface	Gateway	Tunneled	Metric	Tracked	
√ BGP	▼ IPv4 Routes						
IPv6 Static Route	any-ipv4	Outside2	10.201.1.1	false	2		/1
✓ Multicast Routing							
IGMP PIM	any-ipv4	Outside	10.200.1.1	false	1	ISP_Outside1	/1
Multicast Routes Multicast Boundary Filter	▼ IPv6 Routes						

Étape 6. Configuration de l'exemption NAT

1. Accédez à Devices > NAT > NAT Policy et sélectionnez la politique qui cible le périphérique FTD. Sélectionnez Add Rule et configurez une exemption NAT par interface ISP (Outside et Outside2). Les règles NAT doivent être identiques, sauf pour l'interface de destination.

cisco	Firepower M Devices / NGFW	Manage NAT Polic	ment Center y Editor	۹	Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	ence		Deploy	e 0	0	admin 🗸
NAT Enter De	_FTDv escription											Show Warnings	S	ve	Cancel		
Rules	_														Policy	Assigi	nments (1)
Filter b	<u>y Device</u>															+ /	Add Rule
								Original Packet					Translated Packet				
	Direction	Туре	Source	Desti	nation	Original Sources		Original Destinations		Original Services	Tr	Translated Sources	Translated Destinations	Translated Services	Option	15	
NAT	Rules Before																
1	4	Static	Inside	Outs	ide	월 10.10.10.0		192.168.10	0.1		ą	10.10.10.0	Page 192.168.100.1		route no-p	-looku oxy-a	p /i
2	4	Static	Inside	Outs	ide2	F a 10.10.10.0		B 192.168.10	0.1		Ę	10.10.10.0	192.168.100.1		route	-looku	p /1
Auto	NAT Rules																
NAT	Rules After																

Remarque : Pour ce scénario, les deux règles NAT nécessitent l'activation de la recherche de route. Sinon, le trafic atteindrait la première règle et ne se cantonnerait pas aux routes de basculement. Si la recherche de route n'est pas activée, le trafic est toujours envoyé à l'aide de l'interface externe (première règle NAT). Lorsque la recherche de route est activée, le trafic reste toujours dans la table de routage qui est contrôlée par le biais du SLA Monitor.

Étape 7. Configuration de la stratégie de contrôle d'accès pour le trafic intéressant

1. Accédez à Stratégies > Contrôle d'accès > Sélectionnez la stratégie de contrôle d'accès. Afin

d'ajouter une règle, cliquez sur Ajouter une règle, comme indiqué dans l'image ici.

Configurez une règle des zones Interne vers Externe (Outside1 et Outside2) qui autorise le trafic intéressé de 10.10.10.0/24 à 192.168.100/24.

Configurez une autre règle de Outside zones (Outside1 et Outside 2) à Inside qui autorise le trafic intéressant de 192.168.100/24 à 10.10.10.0/24.

_	cisco Policies /	Ner Manag Access Contro	Jement Cen	Editor	Overview	Analysis	Policies	Devices	Objects	AMP In	telligence			Dep	oloy	¢	adr	min 🔻
	ACP-FTDV Enter Description Rules Secur	ity Intelligence	HTTP Resp	onses Logg	jing Advan	ced					Prefilter Policy	r: Default Prefiite	r Policy	Disn Policy Pre-I Pre-deploy Do Start device pa	Deployme ovice Conf	tification: ent guration f	or FTDv	
1	Filter by Device	Y Search R	ules									X 🗌 sh	ow Rule Conflic	cts 🛛 🕂 🖌	Add Cate	gory	+ Add I	Rule
;	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati	Source Ports	Dest Por	ts URLs	Source SGT	Dest SGT	Action	F0 🛡	B & E	. F ,	æ
	Mandatory - ACP	-FTDv (1-2)																
1	VPN_1_out	Inside	Outside Outside2	10.10.10.0	192.168.100.	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15 0	民名	0 []	/=
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.1	10.10.10.0	Any	Any	Any	Any	Any	Any	Any	Any	Allow	15.0	6.20	_ ∎ 0	/1
Ŧ	Default - ACP-FT	Dv (-)																
TI	nere are no rules in	this section. A	Add Rule or Add	Category														
D	efault Action												Access Control	Block All Tr	affic			•

Configuration de l'ASA

Remarque : Pour ce scénario spécifique, un homologue de sauvegarde est configuré sur la crypto-carte IKEv2. Cette fonctionnalité nécessite que l'ASA soit sur la version 9.14.1 ou ultérieure. Si votre ASA exécute une version antérieure, utilisez IKEv1 comme solution de contournement. Pour plus de référence, allez à l'ID de bogue Cisco <u>CSCud22276.</u>

1. Activez IKEv2 sur l'interface externe de l'ASA :

Crypto ikev2 enable Outside

2. Créez la stratégie IKEv2 qui définit les mêmes paramètres configurés sur le FTD :

crypto ikev2 policy 1 encryption aes-256 integrity sha256 group 14 prf sha256 lifetime seconds 86400

3. Créez une stratégie de groupe pour autoriser le protocole ikev2 :

```
group-policy IKEV2 internal
group-policy IKEV2 attributes
vpn-tunnel-protocol ikev2
```

4. Créez un groupe de tunnels pour chaque adresse IP FTD externe (Outside1 et Outside2). Faites référence à la stratégie de groupe et spécifiez la clé pré-partagée :

tunnel-group 10.200.1.5 type ipsec-121 tunnel-group 10.200.1.5 general-attributes default-group-policy IKEV2 tunnel-group 10.200.1.5 ipsec-attributes ikev2 remote-authentication pre-shared-key Cisco123 ikev2 local-authentication pre-shared-key Cisco123 tunnel-group 10.201.1.5 type ipsec-121 tunnel-group 10.201.1.5 general-attributes default-group-policy IKEV2 tunnel-group 10.201.1.5 ipsec-attributes ikev2 remote-authentication pre-shared-key Cisco123 ikev2 local-authentication pre-shared-key Cisco123

5. Créez une liste de contrôle d'accès qui définit le trafic à chiffrer : (FTD-Subnet 10.10.10.0/24) (ASA-Subnet 192.168.100.0/24) :

```
Object network FTD-Subnet
Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6. Créez une proposition ipsec ikev2 pour référencer les algorithmes spécifiés sur le FTD :

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
protocol esp encryption aes-256
protocol esp integrity sha-256
```

7. Créez une entrée de crypto-carte qui lie la configuration et ajoutez les adresses IP FTD

Outside1 et Outside2 :

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map interface Outside
```

8. Créez une instruction d'exemption NAT qui empêche le trafic VPN d'être NATTED par le parefeu :

Nat (inside,Outside) 1 source static ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

FTD

Dans la ligne de commande, utilisez la commande show crypto ikev2 sa pour vérifier l'état du VPN.

Remarque : le VPN est établi avec l'adresse IP de Outside1 (10.200.1.5) comme adresse locale.

La route par défaut affiche l'adresse IP du tronçon suivant de Outside1.

firepower# sh route

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.200.1.1 to network 0.0.0.0
S*
        0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
С
        10.10.10.0 255.255.255.0 is directly connected, Inside
        10.10.10.5 255.255.255 is directly connected, Inside
L
С
        10.200.1.0 255.255.255.0 is directly connected, Outside1
L
        10.200.1.5 255.255.255.255 is directly connected, Outside1
С
        10.201.1.0 255.255.255.0 is directly connected, Outside2
```

```
L 10.201.1.5 255.255.255 is directly connected, Outside2
```

Suivre

Comme on le voit dans la sortie de show track 1, "Reachability is Up".

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Up <-----
36 changes, last change 00:00:04
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
STATIC-IP-ROUTING 0</pre>
```

NAT

Il est nécessaire de confirmer que le trafic intéressant atteint la règle d'exemption NAT avec l'interface Outside1.

Utilisez la commande « packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail » pour vérifier la règle NAT appliquée au trafic intéressant.

firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det

-----OMITTED OUTPUT -----

Type: UN-NAT Subtype: static Result: ALLOW Config: nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100. Additional Information: NAT divert to egress interface Outside1(vrfid:0) Untranslate 192.168.100.1/0 to 192.168.100.1/0 -----OMITTED OUTPUT -----Phase: 7 Type: NAT Subtype: Result: ALLOW Config: nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100. Additional Information: Static translate 10.10.10.1/0 to 10.10.10.1/0 Forward Flow based lookup yields rule: in id=0x2b3e09576290, priority=6, domain=nat, deny=false hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0) Phase: 8 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true in hits=3596, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0 input_ifc=any, output_ifc=any -----OMITTED OUTPUT ------Phase: 12 Type: VPN Subtype: encrypt Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=any(vrfid:65535), output_ifc=Outside1 Phase: 13 Type: NAT Subtype: rpf-check Result: ALLOW Config: nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100. Additional Information: Forward Flow based lookup yields rule: out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false

hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0) Phase: 14 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information: Reverse Flow based lookup yields rule: in id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0 src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Outside1(vrfid:0), output_ifc=any Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Reverse Flow based lookup yields rule: in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true hits=3598, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0 input_ifc=any, output_ifc=any -----OMITTED OUTPUT -----Result: input-interface: Inside(vrfid:0) input-status: up input-line-status: up output-interface: Outside1(vrfid:0) output-status: up output-line-status: up Action: allow

Effectuer le basculement

Dans cet exemple, le basculement est effectué par un arrêt sur le tronçon suivant Outside1 utilisé dans la configuration du moniteur IP SLA.

firepower# sh sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.200.1.1
Interface: Outside1
Number of packets: 1

Request size (ARR data portion): 28 Operation timeout (milliseconds): 5000 Type Of Service parameters: 0x0 Verify data: No Operation frequency (seconds): 60 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:

Route

La route par défaut utilise désormais l'adresse IP du tronçon suivant de Outside2 et l'accessibilité est désactivée.

firepower# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF
Gateway of last resort is 10.201.1.1 to network 0.0.0.0
S* 0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C 10.10.10.0 255.255.255.0 is directly connected, Inside
L 10.10.10.5 255.255.255.255 is directly connected. Inside

```
C 10.200.1.0 255.255.255.0 is directly connected, Outside1
```

```
L 10.200.1.5 255.255.255 is directly connected, Outside1
C 10.201.1.0 255.255.255.0 is directly connected, Outside2
```

```
L 10.201.1.5 255.255.255 is directly connected, Outside2
```

Suivre

Comme on le voit dans la sortie de show track 1, "Reachability is Down" à ce point.

firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <---37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0</pre>

firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det -----OMITTED OUTPUT -----Phase: 4 Type: NAT Subtype: Result: ALLOW Confia: nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100. Additional Information: Static translate 10.10.10.1/0 to 10.10.10.1/0 Forward Flow based lookup yields rule: in id=0x2b3e0c67d470, priority=6, domain=nat, deny=false hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0) -----OMITTED OUTPUT -----Phase: 9 Type: VPN Subtype: encrypt Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=any(vrfid:65535), output_ifc=Outside2 Phase: 10 Type: NAT Subtype: rpf-check Result: ALLOW Config: nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100. Additional Information: Forward Flow based lookup yields rule: out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0) Phase: 11 Type: VPN Subtype: ipsec-tunnel-flow Result: ALLOW Config: Additional Information: Reverse Flow based lookup yields rule: in id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0 src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any

dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0 input_ifc=Outside2(vrfid:0), output_ifc=any Phase: 12 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Reverse Flow based lookup yields rule: in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true hits=3669, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0 input_ifc=any, output_ifc=any -----OMITTED OUTPUT -----Result: input-interface: Inside(vrfid:0) input-status: up input-line-status: up output-interface: Outside2(vrfid:0) output-status: up output-line-status: up Action: allow

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.