Configurer l'équilibrage de charge du client VPN avec DNS Round Robin sur ASA

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configurations
Étape 1. Configurer Anyconnect VPN sur ASA
Étape 2. Configuration du DNS de routage sur le serveur DNS
Vérifier
<u>Dépannage</u>

Introduction

Ce document décrit comment configurer l'équilibrage de charge du client vpn anyconnect avec le round robin DNS sur ASA.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Vous avez attribué des adresses IP à vos ASA et configuré la passerelle par défaut.
- Anyconnect VPN est configuré sur les ASA.
- Les utilisateurs VPN peuvent se connecter à tous les ASA à l'aide de leur adresse IP attribuée individuellement.
- Le serveur DNS des utilisateurs VPN est compatible round robin.

Composants utilisés

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

- Logiciel client VPN Anyconnect versions 4.10.08025
- Logiciel Cisco ASA version 9.18.2
- Windows Server 2019

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.

Configurer

Diagramme du réseau



Diagramme du réseau

Configurations

Étape 1. Configurer Anyconnect VPN sur ASA

Pour savoir comment configurer anyconnect VPN sur ASA, référez-vous à ce document :

 <u>ASA 8.x : Exemple de configuration d'un accès VPN avec le client VPN AnyConnect à l'aide</u> <u>d'un certificat auto-signé</u>

Voici la configuration des deux ASA dans cet exemple :

ASA1 :

ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0

```
interface GigabitEthernet0/0
```

nameif outside security-level 0 ip address 10.1.1.1 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 route outside 0.0.0.0 0.0.0.0 10.1.1.2 1 webvpn enable outside anyconnect enable tunnel-group-list enable group-policy anyconnect internal group-policy anyconnect attributes dns-server value 192.168.1.99 vpn-tunnel-protocol ssl-client default-domain value example.com username example1 password ***** username example1 attributes vpn-group-policy anyconnect service-type remote-access tunnel-group anyconnect-tunnel-group type remote-access tunnel-group anyconnect-tunnel-group general-attributes address-pool anyconnect default-group-policy anyconnect tunnel-group anyconnect-tunnel-group webvpn-attributes group-alias example enable **ASA2**: ip local pool anyconnect 10.4.0.100-10.4.0.200 mask 255.255.255.0 interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.2.1.1 255.255.255.0 interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.1.1 255.255.255.0 route outside 0.0.0.0 0.0.0.0 10.2.1.2 1 webvpn enable outside anyconnect enable tunnel-group-list enable group-policy anyconnect internal group-policy anyconnect attributes dns-server value 192.168.1.99

```
vpn-tunnel-protocol ssl-client
default-domain value example.com
username example1 password *****
username example1 attributes
vpn-group-policy anyconnect
service-type remote-access
tunnel-group anyconnect-tunnel-group type remote-access
tunnel-group anyconnect-tunnel-group general-attributes
address-pool anyconnect
default-group-policy anyconnect
tunnel-group anyconnect-tunnel-group webvpn-attributes
group-alias example enable
```

Vous devez être en mesure de vous connecter aux deux ASA en utilisant leur adresse IP attribuée individuellement avant de passer à l'étape 2.

Étape 2. Configuration du DNS de routage sur le serveur DNS

Vous pouvez utiliser n'importe quel serveur DNS compatible round robin. Dans cet exemple, le serveur DNS sur Windows Server 2019 est utilisé. Pour savoir comment installer et configurer le serveur DNS sur le serveur Windows, reportez-vous à ce document :

Installation et configuration du serveur DNS sur Windows Server

Dans cet exemple, 10.3.1.4 est le serveur Windows avec le serveur DNS activé pour le domaine example.com.

Å	DNS M	anager		_ 🗆 X
File Action View Help				
🗢 🤿 🙇 🖬 🧟 🖬				
🚊 DNS	Name	Туре	Status	DNSSEC Status
 WIN-RTR8ICOV77A Forward Lookup Zones example.com Reverse Lookup Zones Trust Points Conditional Forwarders Global Logs 	example.com	Standard Primary	Running	Not Signed
	<	ш		

Serveur DNS

Assurez-vous que la fonctionnalité Round Robin est activée pour votre serveur DNS :

- 1. Sur le bureau de Windows, ouvrez le menu Démarrer, sélectionnez Outils d'administration > DNS.
- 2. Dans l'arborescence de la console, sélectionnez le serveur DNS que vous souhaitez gérer, cliquez avec le bouton droit de la souris, puis sélectionnez Propriétés.
- 3. Sous l'onglet Advanced, vérifiez que l'option Enable round robin est cochée.

å	DNS Manager 📃 🗖 🗙
File Action Vir	sw Help
🗢 🌩 🖄 📰	
👗 DNS	Name
⊿ 🗄 WIN-R	Configure a DNS Server
a For	New Zone
> 🛄 Rev	Set Aging/Scavenging for All Zones
> 🧰 Tru	Scavenge Stale Resource Records
b Cor b Cor cor cor cor	Update Server Data Files
	Clear Cache
	Launch nsleakup
	All Tasks •
	Yiew •
	Delete
	Refresh
	Export List
	Properties
	Help
Opens the propertie	s dialog box for the current selection.

Round Robin 1

WIN-RTR8IC0V77A Properties

2

E

Debug Loggin	9	Even	Logging		Monitoring
Interfaces	Form	rarders	ders Advanced RootH		Root Hints
Server version nu 6.3 9600 (0x258	mber: 0)		νę		
Server options: Disable recursi Enable 50ND or Fail on load if 5 Enable round r	on (also scondark ad zone obin	disables for es clata	warders)		^ =
Enable netmask ordering Secure cache against pollution Enable DNSSEC validation for remote responses					
Name checking:	Name checking: Multibyte (UTP8) V			~	
Load zone data or	Load zone data on startup: From Active Directory and registry 🗸 🗸			registry 🗸 🗸	
Enable automatic scavenging of stale records					
Scavenging pr	ripd:	0	0	tays	v
				Reset	to Default
	ок	Cano	el Ap	ply	Help

Round Robin 2

Créez deux enregistrements d'hôte pour les serveurs VPN ASA :

- 1. Sur le bureau Windows, ouvrez le menu Démarrer, sélectionnez Outils d'administration > DNS.
- 2. Dans l'arborescence de la console, connectez-vous au serveur DNS que vous souhaitez gérer, développez le serveur DNS, développez votre zone de recherche directe, cliquez

avec le bouton droit de la souris, puis sélectionnez Nouvel hôte (A ou AAAA).

- 3. Dans l'écran Nouvel hôte, spécifiez le nom et l'adresse IP de l'enregistrement hôte. Dans cet exemple, vpn et 10.1.1.1.
- 4. Sélectionnez Add Host pour créer l'enregistrement.



Créer un nouvel hôte

New Host
Name (uses parent domain name if blank):
vpn
Fully qualified domain name (FQDN):
vpn.example.com.
IP address:
10.1.1.1
Create associated pointer (PTR) record
R
Add Host Cancel

Enregistrement hôte 1

Répétez les étapes similaires pour créer un autre enregistrement d'hôte et assurez-vous que Nom est identique. Dans cet exemple, Nom est vpn, l'adresse IP est 10.2.1.1.

New Host	x
Name (uses parent domain name if blank):	
vpn	
Fully qualified domain name (FQDN):	_
vpn.example.com.	
IP address:	_
10-2-1-1	
Create associated pointer (PTR) record	
145 1	
Add Host Done	

Enregistrement hôte 2

Vous pouvez trouver deux hôtes 10.1.1.1 et 10.2.1.1 associés au même enregistrement vpn.example.com.

å	DNS M	anager	_ D X
File Action View Help			
🗢 🏟 🙇 🛅 🖾 🙆	2 🗊 🗄 🔲 🕄		
 DNS WIN-RTR8ICOV77A Forward Lookup Zones example.com Reverse Lookup Zones Trust Points Conditional Forwarders Global Logs 	Name (same as parent folder) (same as parent folder) vpn vpn	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A)	Data [6], win-rtr8ic0v77a., host win-rtr8ic0v77a. 10.1.1.1 10.2.1.1

Deux enregistrements d'hôte

Vérifier

Accédez à votre ordinateur client sur lequel le client Cisco AnyConnect Secure Mobility est installé. Dans cet exemple, Test-PC-1, vérifiez que votre serveur DNS est 10.3.1.4.

Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DN	
Description	Intel(R) PRO/1000 MT Network Connecti
Physical Address	52-54-00-0B-68-6F
DHCP Enabled	No
Pv4 Address	10.3.1.2
IPv4 Sultreet Mask	255.255.255.0
Pv4 Default Gateway	10.3.1.1
Pv4 DNS Server	10.3.1.4
IPv4 WINS Server	
NetBIOS over Topip En	Yes
Link-local IPv6 Address	fe80::6147:aeeb:9647:9004%16
IPv6 Default Gateway	
IPv6 DNS Server	
<	>
	Class
	Ciuse

Adresse IP de PC1

 \times



Remarque : un certificat auto-signé étant utilisé pour que le modem routeur s'identifie, plusieurs avertissements de certificat peuvent apparaître lors de la tentative de connexion. Ils sont attendus et doivent être acceptés pour que la connexion puisse continuer. Afin d'éviter ces avertissements de certificat, le certificat auto-signé qui est présenté doit être installé dans le magasin de certificats de confiance de l'ordinateur client, ou si un certificat tiers est utilisé, alors le certificat de l'autorité de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certificats de certification doit être dans le magasin de certificats de certification doit être dans le magasin de certificats de certificats de certification doit etre dan

Connectez-vous à votre tête de réseau VPN vpn.example.com et saisissez le nom d'utilisateur et les informations d'identification.



: sur l'ASA, vous pouvez définir différents niveaux de débogage ; par défaut, le niveau 1 est utilisé. Si vous modifiez le niveau de débogage, le niveau de détail des débogages augmente. Faites-le avec prudence, en particulier dans les environnements de production.

Vous pouvez activer le débogage pour diagnostiquer la connexion VPN sur ASA.

• debug webvpn anyconnect - Affiche des messages de débogage sur les connexions aux clients Anyconnect VPN.

Référez-vous à <u>ce</u> document afin de dépanner les problèmes courants trouvés du côté client.

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.