Konfigurieren des VPN-Client-Lastenausgleichs mit DNS Round Robin auf der ASA

Inhalt

Einleitung
<u>Voraussetzungen</u>
Anforderungen
Verwendete Komponenten
Konfigurieren
Netzwerkdiagramm
Konfigurationen
Schritt 1: Konfigurieren von AnyConnect VPN auf ASA
Schritt 2: Round-Robin-DNS auf DNS-Server konfigurieren
Überprüfung
Fehlerbehebung

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Lastenausgleich des AnyConnect VPN-Clients mit dem DNS-Round-Robin auf der ASA konfigurieren.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie diese Konfiguration ausprobieren:

- Sie haben den ASAs IP-Adressen zugewiesen und das Standard-Gateway konfiguriert.
- AnyConnect VPN wird auf den ASAs konfiguriert.
- VPN-Benutzer können sich über ihre jeweils zugewiesene IP-Adresse mit allen ASAs verbinden.
- Der DNS-Server der VPN-Benutzer ist Round-Robin-fähig.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- AnyConnect VPN Client Software-Versionen 4.10.08025
- Cisco ASA Software-Versionen 9.18.2
- Windows Server 2019

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm

Konfigurationen

Schritt 1: Konfigurieren von AnyConnect VPN auf ASA

Informationen zur Konfiguration von AnyConnect VPN auf ASA finden Sie in diesem Dokument:

 <u>ASA 8.x : VPN-Zugriff mit dem AnyConnect VPN-Client unter Verwendung eines</u> selbstsignierten Zertifikats - Konfigurationsbeispiel

Nachfolgend finden Sie die Konfiguration der beiden ASAs in diesem Beispiel:

ASA 1:

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 ASA 2: 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
```

Bevor Sie mit Schritt 2 fortfahren, müssen Sie in der Lage sein, eine Verbindung zu beiden ASAs unter Verwendung der jeweils zugewiesenen IP-Adresse herzustellen.

Schritt 2: Round-Robin-DNS auf DNS-Server konfigurieren

Sie können einen beliebigen Round-Robin-fähigen DNS-Server verwenden. In diesem Beispiel wird der DNS-Server auf dem Windows-Server 2019 verwendet. Informationen zur Installation und Konfiguration von DNS-Servern auf Windows-Servern finden Sie in diesem Dokument:

Installieren und Konfigurieren des DNS-Servers auf Windows Server

In diesem Beispiel ist 10.3.1.4 der Windows-Server mit aktiviertem DNS-Server für die Domäne 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
	<			>

DNS-Server

Stellen Sie sicher, dass Round Robin für Ihren DNS-Server aktiviert ist:

- 1. Öffnen Sie auf dem Windows-Desktop das Menü Start, und wählen Sie Verwaltung > DNS aus.
- 2. Wählen Sie in der Konsolenstruktur den DNS-Server aus, den Sie verwalten möchten, klicken Sie mit der rechten Maustaste, und wählen Sie dann Eigenschaften aus.
- 3. Vergewissern Sie sich unter der Registerkarte Erweitert, dass Rundlauf aktivieren aktiviert ist.

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		Event	Logging		Monitoring	
Interfaces	Forwar	ders	Advance	s	Root Hints	
Server version nu 6.3 9600 (0x258	mber: 0)		νę]
Server options:	on (also dis conderies ed zone da obin	ables forv ta	(arders)		-	
Secure cache a Prosble Dasser	igainst polk	ition for remol	e restanses		v	
Name checking:		Mult	byte (UTH8)		Ŷ	
Load zone data or	startup:	From	Active Dire	clory an	dregistry 🗸 🗸]
thable automatic scavenging of stale records						
Scavenging pr	ripd:	0		days	Ŷ	
				Rese	t to Default	
	ж	Cance	A	oply	Help	

Round Robin 2

Erstellen Sie zwei Host-Datensätze für ASA VPN-Server:

- 1. Öffnen Sie auf dem Windows-Desktop das Menü Start, und wählen Sie Verwaltung > DNS aus.
- 2. Stellen Sie in der Konsolenstruktur eine Verbindung mit dem DNS-Server her, den Sie verwalten möchten, erweitern Sie den DNS-Server, erweitern Sie die

Weiterleitungssuchzone, klicken Sie mit der rechten Maustaste, und wählen Sie dann Neuer Host (A oder AAAA).

- 3. Geben Sie im Bildschirm New Host (Neuer Host) den Namen und die IP-Adresse des Host-Datensatzes an. In diesem Beispiel vpn und 10.1.1.1.
- 4. Wählen Sie Host hinzufügen, um den Datensatz zu erstellen.

👗 DNS Manager 📃 🗖 🗙			
File Action View Help			
🗢 🄿 🖄 📷 🗶 🗊 🧟 🗉	1 🖬 🖬 🗐		
2 DNS	Name	Туре	Data
⊿	(same as parent folder)	Start of Authority (SOA)	[3], win-rtr8ic0v77a., host
Forward Lookup Zones	🗐 (same as parent folder)	Name Server (NS)	win-rtr8ic0v77a.
E example com	rver Data File		
heverse oppose of			
Conditie New Hort	(A or AAAA)		
Dig Global L New Alia	(CNAME)		
New Mail	Exchanger (MV)		
New Mail	Exchanger (MA)		
New Dom	ain		
New Dele	gation		
Other New	v Records		
DNSSEC	•		
All Tasks	•		
View	•		
Delete			
Refresh			
Export Lis	L		
Properties			
Create a new host n Help			

Neuen Host erstellen

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
- 10
Add Host Cancel

Host-Datensatz 1

Wiederholen Sie ähnliche Schritte, um einen weiteren Hostdatensatz zu erstellen, und stellen Sie sicher, dass Name identisch ist. In diesem Beispiel ist Name vpn, die IP-Adresse ist 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	
R	
Add Host Done	

Host-Datensatz 2

Es gibt zwei Hosts, die 10.1.1.1 und 10.2.1.1 mit demselben Datensatz vpn.example.com verknüpft sind.

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

Zwei Host-Datensätze

Überprüfung

Navigieren Sie zu dem Client-Computer, auf dem der Cisco AnyConnect Secure Mobility Client installiert ist. In diesem Beispiel wird Test-PC-1 verwendet. Stellen Sie sicher, dass der DNS-Server 10.3.1.4 lautet.

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	
<	>
	Close

PC1-IP-Adresse

 \times



Hinweis: Da das Gateway zur Identifizierung eines selbst signierten Zertifikats verwendet wird, können während des Verbindungsversuchs mehrere Zertifikatwarnungen angezeigt werden. Diese werden erwartet und müssen akzeptiert werden, damit die Verbindung fortgesetzt werden kann. Um diese Zertifikatwarnungen zu vermeiden, muss das bereitgestellte selbstsignierte Zertifikat im vertrauenswürdigen Zertifikatspeicher des Clientcomputers installiert sein. Wenn ein Zertifikat eines Drittanbieters verwendet wird, muss sich das Zertifikat der Zertifizierungsstelle im vertrauenswürdigen Zertifikatspeicher befinden.

Stellen Sie eine Verbindung mit Ihrem VPN-Headend vpn.example.com her, und geben Sie den Benutzernamen und die Anmeldeinformationen ein.



: Auf der ASA können verschiedene Debug-Ebenen festgelegt werden. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, wird die Ausführlichkeit der Debugs erhöht. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

Sie können das Debugging aktivieren, um die VPN-Verbindung auf der ASA zu diagnostizieren.

• debug webvpn anyconnect - Zeigt Debug-Meldungen über Verbindungen zu AnyConnect VPN-Clients an.

Lesen Sie dieses Dokument, um häufige Probleme auf der Client-Seite zu beheben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.