

Service Side Destination Based NAT auf dem vEdge-Router

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurationen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie die zielbasierte Network Address Translation (NAT) im Service-VPN auf dem vEdge-Router konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie mit Cisco SD-WAN vertraut sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

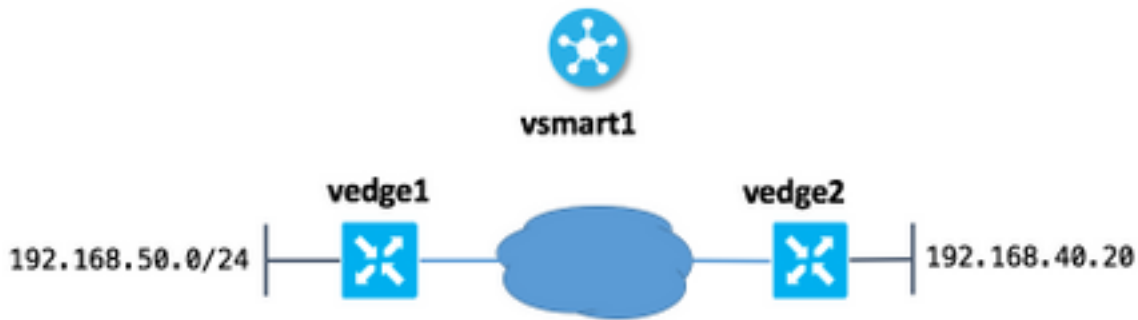
- vEdge-Router
- vSmart Controller mit Softwareversion 18.3.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm

Das Netzwerkdiagramm wird hier angezeigt.



Die Hauptsorge hier, dass Benutzer von Standort 50 (vedge1) über die IP-Adresse 192.168.140.20 erreichen können, um 192.168.140.20 zu hosten.

Dies ist eine Analogie dieser IOS-Konfigurationsanweisung:

```
ip nat outside source static 192.168.40.20 192.168.140.20
```

Konfigurationen

1. Konfigurieren Sie den NAT-Pool auf dem vEdge an der Site 50.

```
vedge1#show running-config vpn 40 interface natpool31
vpn 40
 interface natpool31
  ip address 192.168.140.5/32
  nat
   static source-ip 192.168.40.20 translate-ip 192.168.140.20 outside
  !
 no shutdown
 !
 !
```

2. Konfigurieren und Anwenden von Datenrichtlinien auf vSmart

```
vsmart1# show running-config policy data-policy DNAT
policy
 data-policy DNAT
  vpn-list CORP
  sequence 10
  match
   destination-ip 192.168.140.20/32
  !
  action accept
   nat pool 31
  !
 !
 default-action accept
 !
 !
 !

vsmart1# show running-config apply-policy site-list site_50
apply-policy
 site-list site_50
 data-policy DNAT all
```

!
!

Überprüfen

1. Überprüfen Sie, ob die Übersetzung in einem entsprechenden Service-VPN vorhanden ist.

```
vedge1# show ip nat interface nat-vpn 40
```

```

                                     FIB
NUMBER                               FILTER  FILTER
IP
VPN  IFNAME      MAP TYPE          FILTER TYPE      COUNT  COUNT  IP
POOLS
-----
-----
40   natpool31    endpoint-independent  address-port-restricted  0      0      192.168.140.5/32
1
```

2. Überprüfen Sie, ob die Richtlinie auf vEdge von vSmart angewendet wurde.

```
vedge1# show policy from-vsmart
from-vsmart data-policy ENK_NAT
direction all
vpn-list CORP
sequence 10
match
  destination-ip 192.168.140.20/32
action accept
  nat pool 31
default-action accept
from-vsmart lists vpn-list CORP
vpn 40
```

Fehlerbehebung

Wenn die zielbasierte NAT nicht funktioniert, müssen Sie sicherstellen, dass die IP-Adresse des NAT-Pools vom Ziel-Host aus erreichbar ist. Dies ist wichtig, da die IP-Adresse für die NAT-Implementierung je nach Ziel des vEdge-Routers auch über NAT an die IP-Adresse des Pools geleitet wird.

Die auf der Beispiel-Konfigurationsziel-Adresse 192.168.140.20 basierende Adresse wird durch die tatsächliche IP-Adresse 192.168.40.20 ersetzt, aber die Adresse des Hosts des Subnetzes 192.168.50.0/24 an Standort 50 ist ebenfalls NATed auf 192.168.1 40.5 verwenden, sodass Sie sowieso eine Route zurück zu dieser Adresse haben müssen, oder Antwortpakete erreichen den Quellhost (anfordernde Datei) nicht. Dies kann mithilfe der Anzeige für das NAT-Pool-Subnetz erreicht werden. In diesem Beispiel besteht das Subnetz aus nur einer Adresse und wird über das Overlay Management Protocol (OMP) angekündigt.

Hier können Sie überprüfen, ob die Route auf dem vEdge1 am Remote-Standort angezeigt wird:

```
vedge2# show ip routes vpn 40 omp | i 192.168.140.5
40      192.168.140.5/32      omp      -      -      -      -
```

192.168.30.5

mpls

ipsec F,S