

NAT basato sulla destinazione sul lato servizio su vEdge Router

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare NAT (Network Address Translation) basato sulla destinazione nella VPN di servizio sul router vEdge.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di Cisco SD-WAN.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

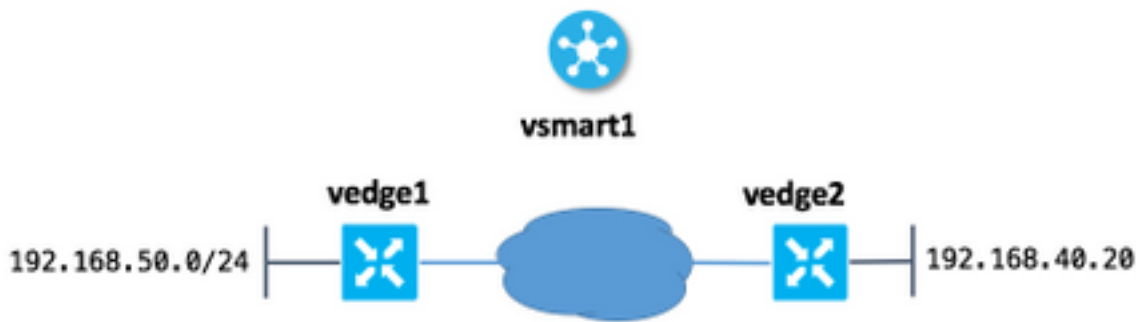
- Router vEdge
- vSmart Controller con versione software 18.3.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete

Di seguito è riportato il diagramma di rete.



In questo caso, l'idea principale è che gli utenti del sito 50 (vedge1) possano raggiungere l'host 192.168.40.20 da un altro lato, utilizzando l'indirizzo IP 192.168.140.20.

Analoga alla seguente istruzione di configurazione IOS:

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

Configurazioni

1. Configurare il pool NAT su vEdge nel sito 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. Configurare e applicare i criteri dati su 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
```

!
!

Verifica

1. Verificare che la traduzione sia presente in una VPN di servizio corrispondente.

```
vedgel# 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. Verificare che il criterio sia stato applicato a vEdge da vSmart.

```
vedgel# 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
```

Risoluzione dei problemi

Se il protocollo NAT basato sulla destinazione non funziona, è importante verificare che l'indirizzo IP del pool NAT sia raggiungibile dall'host di destinazione. Questa operazione è importante perché, come per l'implementazione NAT basata su destinazione vEdge, anche l'indirizzo IP di origine NAT viene associato all'indirizzo IP del pool.

Ad esempio, in base all'indirizzo di destinazione 192.168.140.20 della configurazione di esempio, l'indirizzo IP reale viene sostituito con l'indirizzo IP reale 192.168.40.20, ma anche l'indirizzo dell'host dalla subnet 192.168.50.0/24 al sito 50 viene sostituito con l'indirizzo NAT 192.168.140.5, quindi è necessario disporre comunque di un percorso per tornare a questo indirizzo altrimenti i pacchetti di risposta non raggiungeranno l'host di origine (richiedente). A tale scopo, è possibile utilizzare la pubblicità per la subnet del pool NAT. Nell'esempio, la subnet è costituita da un solo indirizzo e pubblicizzata tramite il protocollo OMP (Overlay Management Protocol).

Di seguito è possibile verificare che il percorso sia presentato su vEdge1 nel sito remoto:

```
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