Esempio di configurazione del traffico VPN SSL senza client ASA su tunnel IPsec da LAN a LAN

Sommario

Introduzione

In questo documento viene descritto come connettersi a un portale SSLVPN senza client di Cisco Adaptive Security Appliance (ASA) e accedere a un server che si trova in una posizione remota connessa tramite un tunnel LAN-LAN IPsec.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN SSL senza client.
- Configurazione VPN da LAN a LAN

Componenti usati

Per la stesura del documento, la serie ASA 5500-X è in esecuzione sulla versione 9.2(1), ma è valida per tutte le versioni ASA.

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. valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi prima di apportare modifiche alla rete.

Premesse

Quando il traffico proveniente da una sessione VPN senza client attraversa un tunnel LAN-LAN, tenere presente che vi sono due connessioni:

- Dal client all'appliance ASA
- Dall'appliance ASA all'host di destinazione.

Per la connessione tra appliance ASA e host di destinazione, viene usato l'indirizzo IP dell'interfaccia ASA "più vicina" all'host di destinazione. Pertanto, il traffico da LAN a LAN deve includere un'identità proxy tra l'indirizzo di interfaccia e la rete remota.

> **Nota:** Se si usa Smart-Tunnel per un segnalibro, viene ancora usato l'indirizzo IP dell'interfaccia ASA più vicina alla destinazione.

Configurazione

Nel diagramma riportato di seguito viene mostrato un tunnel LAN-LAN tra due appliance ASA che consente il passaggio del traffico da 192.168.10.x a 192.168.20.x.

L'elenco degli accessi che determina il traffico interessante per il tunnel:

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

Se l'utente SSLVPN senza client tenta di comunicare con un host sulla rete 192.168.20.x, ASA1 utilizza l'indirizzo 209.165.200.225 come origine del traffico. Poiché l'elenco di controllo di accesso (ACL) da LAN a LAN non contiene 209.168.200.225 come identità proxy, il traffico non viene inviato sul tunnel LAN a LAN.

Per inviare il traffico sulla rete LAN-LAN, è necessario aggiungere una nuova voce di controllo di accesso (ACE) all'ACL del traffico interessato.

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

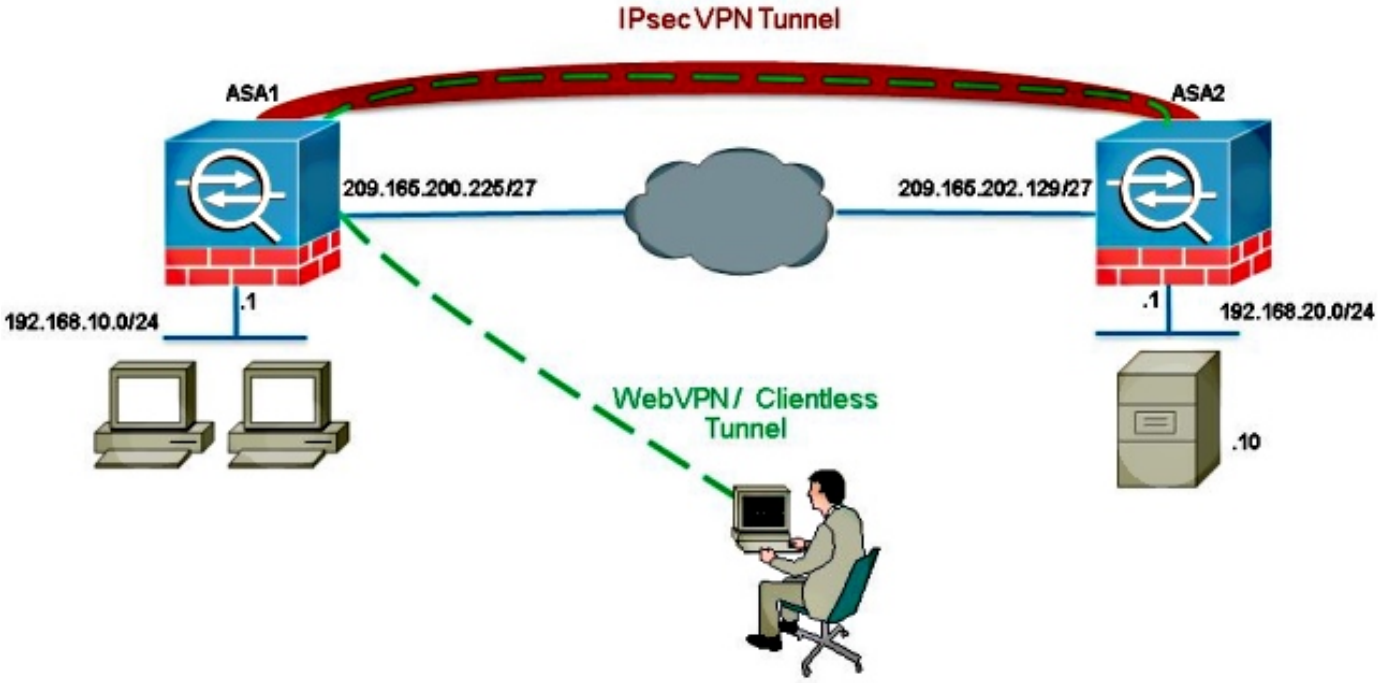
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

Lo stesso principio si applica alle configurazioni in cui il traffico SSL VPN senza client deve **disattivare** l'interfaccia utilizzata, anche se non deve passare attraverso un tunnel LAN-LAN.

> **Nota:** per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete



In genere, ASA2 esegue Port Address Translation (PAT) per 192.168.20.0/24 per fornire l'accesso a Internet. In questo caso, il traffico proveniente da 192.168.20.0/24 su ASA 2 deve essere escluso dal processo PAT quando raggiunge il valore 209.165.200.225. In caso contrario, la risposta non passerà attraverso il tunnel LAN-LAN. Ad esempio:

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi **show.** Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando **show.**

- **show crypto ipsec sa**-Verificare con questo comando che sia stata creata un'associazione di sicurezza (SA) tra l'indirizzo IP del proxy ASA1 e la rete remota. Verificare se i contatori crittografati e decrittografati aumentano quando l'utente SSLVPN senza client accede al server.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Se l'associazione di protezione non è stata creata, è possibile utilizzare il debug IPSec per individuare la causa dell'errore:

- **debug crypto ipsec <livello>**

  Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**