Esempio di connessione di un client VPN ASA tramite un tunnel L2L

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo da consentire una connessione client VPN remota da un indirizzo peer Lan-to-Lan (L2L).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ASA
- VPN ad accesso remoto
- VPN da LAN a LAN

Componenti usati

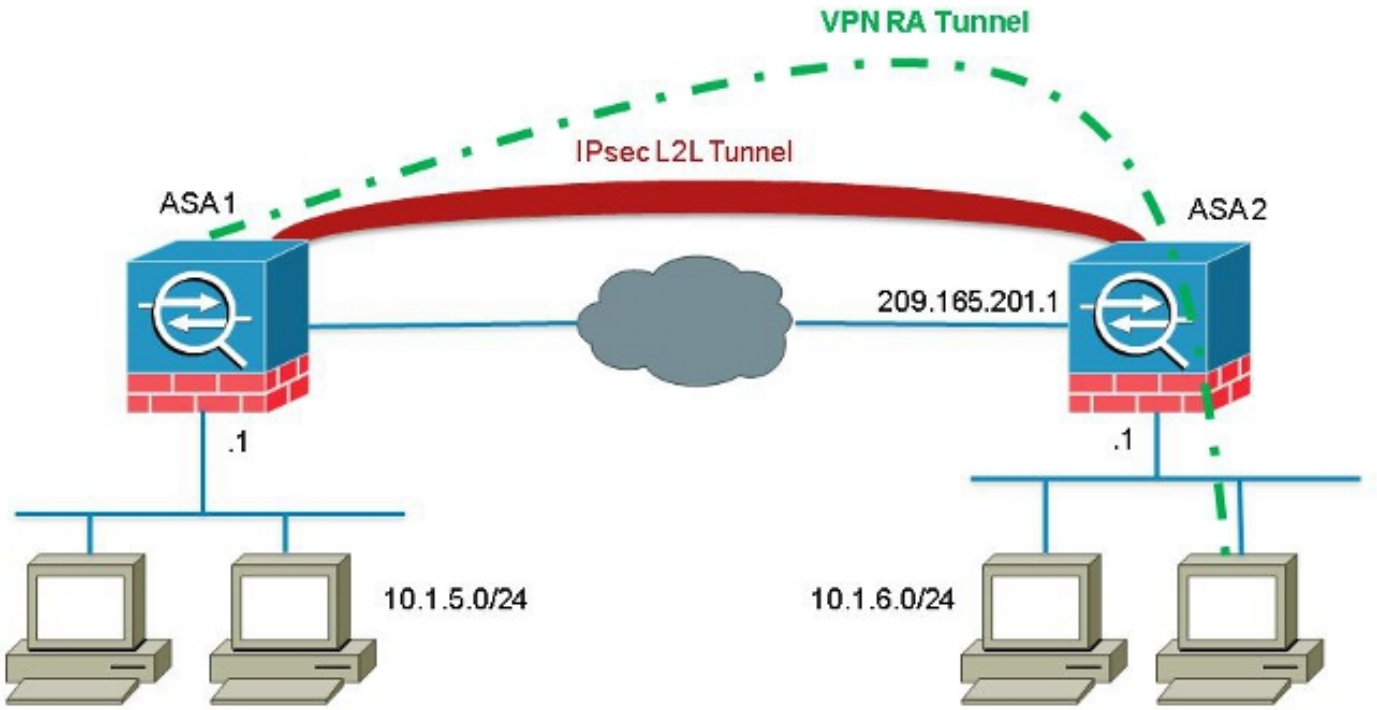
Per la stesura del documento, è stata usata un'appliance ASA Cisco serie 5520 con software versione 8.4(7).

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.

Premesse

Sebbene non sia comune trovarsi in uno scenario in cui un client VPN tenta di stabilire una connessione tramite un tunnel L2L, gli amministratori potrebbero voler assegnare privilegi specifici o restrizioni di accesso a determinati utenti remoti e istruirli a utilizzare il client software quando è necessario accedere a queste risorse.

> **Nota:** Questo scenario funzionava in passato, ma dopo un aggiornamento dell'headend ASA alla versione 8.4(6) o successive, il client VPN non è più in grado di stabilire la connessione.



L'ID bug Cisco CSCuc75090 ha introdotto una modifica nel comportamento. In precedenza, con Private Internet Exchange (PIX), quando il proxy IPSec (Internet Protocol Security) non corrispondeva a un elenco di controllo di accesso (ACL, Access Control List) con mappa crittografica, continuava a controllare le voci più in basso nell'elenco. Sono incluse le corrispondenze con una mappa crittografica dinamica senza peer specificato.

Questa operazione è stata considerata una vulnerabilità, in quanto gli amministratori remoti potevano accedere a risorse non previste dall'amministratore headend durante la configurazione dell'L2L statico.

Èstata creata una correzione che ha aggiunto un controllo per impedire corrispondenze con una voce di mappa crittografica senza un peer quando è già stata selezionata una voce di mappa corrispondente al peer. Tuttavia, ciò ha influito sullo scenario descritto in questo documento. In particolare, un client VPN remoto che tenta di connettersi da un indirizzo peer L2L non è in grado di connettersi all'headend.

Configurazione

Utilizzare questa sezione per configurare l'ASA in modo da consentire una connessione client VPN remota da un indirizzo peer L2L.

Aggiungi nuova voce dinamica

Per consentire connessioni VPN remote da indirizzi peer L2L, è necessario aggiungere una nuova voce dinamica contenente lo stesso indirizzo IP peer.

> **Nota:** È inoltre necessario lasciare un'altra voce dinamica senza un peer in modo che qualsiasi client da Internet possa connettersi.

Di seguito è riportato un esempio della precedente configurazione operativa della mappa crittografica dinamica:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Di seguito è riportata la configurazione della mappa crittografica dinamica con la nuova voce dinamica configurata:

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.