La configurazione della VPN da sito a sito su ASA 9.x a contesto multiplo riceve un messaggio di errore

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi al messaggio di errore "È stato raggiunto il numero massimo di tunnel consentiti" quando si configura una VPN da sito a sito su ASA (Multiple Context Adaptive Security Appliance) 9.x.

Prerequisiti

Componenti usati

Per questo documento, è stato usato il software ASA versione 9.0 e successive. In questa versione è stata introdotta la configurazione della VPN da sito a sito in modalità contesto multiplo.

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.

Problema

Quando si tenta di attivare più tunnel VPN da sito a sito sull'appliance ASA, l'operazione non riesce e viene generato il messaggio syslog "È stato raggiunto il numero massimo di tunnel consentiti".

Il messaggio syslog specifico è il seguente:

```
%ASA-4-751019: Local:<LocalAddr> Remote:<RemoteAddr> Username:<username> Failed to obtain a
<licenseType> license.
```

- <LocalAddr> - Indirizzo locale per il tentativo di connessione
- <IndirizzoRemoto> - Indirizzo peer remoto per questo tentativo di connessione
- <nomeutente> - Nome utente per il peer che tenta la connessione
- <licenseType> - Tipo di licenza superato (altra VPN o AnyConnect Premium/Essentials)

Premesse

Il log indica che la creazione di una sessione non è riuscita perché è stato superato il limite massimo di licenze per i tunnel VPN e di conseguenza non è possibile avviare o rispondere a una richiesta tunnel.

L'implementazione della VPN in modalità multipla richiede la divisione del totale di licenze VPN disponibili tra i contesti configurati. L'amministratore ASA può configurare il numero di licenze che devono essere allocate per ciascun contesto.

Per impostazione predefinita, nessuna licenza per tunnel VPN viene allocata ai contesti e l'allocazione del tipo di licenza deve essere eseguita manualmente dall'amministratore.

Azione consigliata

Accertarsi che siano disponibili licenze sufficienti per tutti gli utenti autorizzati e/o ottenere più licenze per consentire le connessioni rifiutate. In caso di più contesti, allocare più licenze al contesto che ha segnalato l'errore, se possibile.

Soluzione

La divisione delle licenze tra i contesti viene eseguita aumentando il gestore delle risorse con una risorsa 'VPN other' che gestisce la divisione del pool di licenze 'Other VPN' utilizzato per la VPN da sito a sito tra i contesti configurati.

La CLI limit-resource riportata di seguito consente questa configurazione nella modalità 'class' della risorsa.

```
Limit-resource vpn [burst] other <value> | <value>%
```

Dove, <valore> intervallo: 1- Limite di licenze per piattaforma o 1-100% delle licenze installate.

Per i burst, l'intervallo è compreso tra 1 e 100% delle licenze non assegnate.
Predefinito: 0; nessuna risorsa VPN allocata a una classe.

Per assegnare un contesto al 10% delle licenze installate, è necessario definire una classe di risorse. Successivamente, applicare la classe ai contesti che devono essere in grado di ottenere questa risorsa all'interno della configurazione del contesto di sistema.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 10%
```

Per assegnare un contesto di 250 peer VPN delle licenze installate, è necessario definire una "classe" di risorse. Applicare quindi la classe ai contesti che si desidera possano ottenere questa risorsa nella configurazione del contesto di sistema.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 250
```

Per applicare la classe "vpn" a un contesto denominato "administrator", attenersi alla seguente procedura:

1. Cambiare/passare al contesto di sistema e applicare la classe VPN per il contesto "amministratore". Questa operazione può essere eseguita solo nel contesto di sistema.
2. Di seguito è riportato il frammento di configurazione per allocare la classe "vpn" al contesto "administrator".

   ```
   ciscoasa(config)# context administrator
   ciscoasa(config-ctx)# member vpn
   ```

Informazioni correlate

- Guide di riferimento per i firewall Cisco ASA serie 5500 di nuova generazione
- Guide alla configurazione dei firewall di nuova generazione Cisco ASA serie 5500
- Documentazione e supporto tecnico – Cisco Systems