La configuración del VPN de sitio a sitio en el contexto múltiple ASA 9.x recibe el mensaje de error

Contenido

Introducción

Se ha alcanzado este documento describe cómo resolver problemas el mensaje de error, “la cuenta máxima del túnel permitida”, cuando usted configura un VPN de sitio a sitio en los dispositivos de seguridad adaptantes del contexto múltiple (ASA) 9.x.

Prerrequisitos

Componentes Utilizados

La información en este documento se basa en la versión de software 9.0 ASA y posterior. Esta configuración introducida versión del VPN de sitio a sitio en el modo de contexto múltiple.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial del comando any.

Problema

Cuando usted intenta traer para arriba el VPN de sitio a sitio múltiple hace un túnel en el ASA, falla y genera el mensaje de Syslog “que la cuenta máxima del túnel permitida se ha alcanzado”.

El mensaje de Syslog específico está abajo:

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

- **<LocalAddr>** - Dirección local para este intento de conexión
- **<RemoteAddr>** - Dirección remota de peer para este intento de conexión
- **<username>** - Nombre de usuario para el par que intenta la conexión
- **<licenseType>** - Tipo de licencia que fue excedido (el otro premio VPN o de AnyConnect/esencial)

Antecedentes

El registro indica que una creación de sesión falló porque el límite máximo de la licencia para los túneles VPN fue excedido que causa un error al iniciado o responde a una petición del túnel.

La implementación del VPN en el modo múltiple requiere la división de las licencias disponibles totales VPN entre los contextos configurados. El administrador ASA puede configurar cuántas licencias se afecta un aparato cada contexto.

Por abandono, no se afecta un aparato ningunas licencias del túnel VPN a los contextos, y la asignación del tipo de licencia se debe hacer manualmente por el administrador.

Acción Recomendada

Asegure que bastantes licencias están disponibles para todos los usuarios permitidos y/o obtenga más licencias de permitir las conexiones rechazadas. Para el multi-contexto, afecte un aparato más licencias al contexto que señaló el error, si es posible.

Solución

La división de las licencias entre los contextos es hecha por el aumento del administrador de recursos con “VPN otro” recurso que maneje la división del pool de la licencia “otro VPN” usado para el VPN de sitio a sitio entre los contextos configurados.

El límite-recurso CLI abajo permite esta configuración dentro del modo de la “clase” del recurso.

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

Donde, rango del **<value>**: 1 límite de la licencia de la plataforma o 1-100% de las licencias instaladas.

Para las explosiones, el rango es 1 a las licencias no asignadas o 1-100% de las licencias no asignadas.
Predeterminado: 0; no se afecta un aparato ningunos recursos VPN a una clase.

Para asignar un contexto hasta el 10% de las licencias instaladas, usted necesita definir una clase de recursos. Después, aplique la clase a los contextos que usted necesita poder conseguir este recurso dentro de la configuración del contexto del sistema.

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

Para asignar un contexto de 250 pares VPN de las licencias instaladas, usted necesita definir un recurso “clase”. Después, aplique la clase a los contextos que usted prefiere poder conseguir a este recurso dentro de la configuración del contexto del sistema.

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

Para aplicar la clase antedicha “vpn” a un contexto llamó al “administrador”, siguen los siguientes pasos:

1. El cambio/el intercambio al contexto del sistema y aplica la clase VPN para el contexto “administrador”. Esto se podía hacer solamente dentro del contexto del sistema.
2. Abajo están los fragmentos de la configuración para afectar un aparato la clase “vpn” al contexto “administrador”.
   ```
   ciscoasa(config)# context administrator
   ciscoasa(config-ctx)# member vpn
   ```

Información Relacionada

- Guías de referencia de los Firewall de la última generación de las 5500 Series de Cisco ASA
- Guías de configuración de los Firewall de la última generación de las 5500 Series de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems