Configuración de VPN de Sitio a Sitio en el Contexto Múltiple ASA 9.x Recibe Mensaje de Error

Contenido

Introducción

Este documento describe cómo resolver problemas del mensaje de error "Se ha alcanzado el número máximo de túnel permitido", cuando configura una VPN de sitio a sitio en los dispositivos de seguridad adaptable al contexto múltiple (ASA) 9.x.

Prerequisites

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Cuando intenta activar varios túneles VPN de sitio a sitio en el ASA, éste falla y genera el mensaje syslog "Se ha alcanzado el número máximo de túneles permitido".

El mensaje específico de syslog se muestra a continuación:

```
%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 de peer remota para este intento de conexión
- <username>: Nombre de usuario para la conexión de peer que intenta
- <licenseType>: tipo de licencia excedida (Other VPN o AnyConnect Premium/Essentials)

Antecedentes

El registro indica que una creación de sesión falló porque se excedió el límite máximo de licencia para los túneles VPN, lo que causa una falla al iniciar o responder a una solicitud de túnel.

La implementación de VPN en modo múltiple requiere la división de las licencias VPN disponibles totales entre los contextos configurados. El administrador de ASA puede configurar el número de licencias asignadas a cada contexto.

De forma predeterminada, no se asignan licencias de túnel VPN a los contextos y el administrador debe asignar manualmente el tipo de licencia.

Acción Recomendada

Asegúrese de que haya suficientes licencias disponibles para todos los usuarios permitidos y/o obtenga más licencias para permitir las conexiones rechazadas. Para multicontexto, asigne más licencias al contexto que informó de la falla, si es posible.

Solución

La división de las licencias entre los contextos se realiza mediante el aumento del administrador de recursos con un recurso 'VPN other' que administra la división del conjunto de licencias 'Other VPN' utilizado para VPN de sitio a sitio entre los contextos configurados.

La CLI de limit-resource que se muestra a continuación permite esta configuración en el modo 'class' de recursos.

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

Donde, <valor> rango: 1- Límite de licencia de plataforma o del 1 al 100% de las licencias instaladas.

Para las ráfagas, el rango es de 1 a licencias no asignadas o de 1 a 100% de licencias no asignadas.
Predeterminado: 0; no hay recursos VPN asignados a una clase.

Para asignar un contexto al 10% de las licencias instaladas, debe definir una clase de recurso. A continuación, aplique la clase a los contextos que necesita para poder obtener este recurso dentro de la configuración de 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, debe definir una 'clase' de recurso. A continuación, aplique la clase a los contextos en los que prefiera obtener este recurso dentro de la configuración de contexto del sistema.

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

Para aplicar la clase "vpn" anterior a un contexto llamado "administrator", siga estos pasos:

1. Cambie/Switchover al contexto del sistema y aplique la clase VPN para el "administrador" del contexto. Esto sólo podría hacerse en el contexto del sistema.
2. A continuación se muestra el fragmento de configuración para asignar la clase "vpn" al "administrador" del contexto.

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

Información Relacionada

- Guías de referencia de los firewalls de última generación Cisco ASA serie 5500
- Guías de configuración de firewalls de última generación Cisco ASA serie 5500
- Soporte Técnico y Documentación - Cisco Systems