A configuração do VPN de Site-para-Site no contexto múltiplo ASA 9.x recebe o Mensagem de Erro

Índice

Introdução

Este documento descreve como pesquisar defeitos o Mensagem de Erro, “a contagem máxima do túnel permitida esteve alcançado”, quando você configura um VPN de Site-para-Site nas ferramentas de segurança adaptáveis do contexto múltiplo (ASA) 9.x.

Pré-requisitos

Componentes Utilizados

A informação neste documento é baseada na versão de software 9.0 ASA e mais atrasado. Esta configuração introduzida versão do VPN de Site-para-Site no modo de contexto múltiplo.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se sua rede está viva, assegure-se de que você compreenda o impacto potencial do comando any.

Problema

Quando você tenta trazer acima o VPN de Site-para-Site múltiplo escava um túnel no ASA, falha e gerencie o mensagem do syslog “que a contagem máxima do túnel permitida foi alcançada”.

O mensagem do syslog específico está abaixo:

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

- **<LocalAddr>** - Endereço local para esta tentativa de conexão
- **<RemoteAddr>** - Endereço de peer remoto para esta tentativa de conexão
- **<username>** - Username para o par que tenta a conexão
- **<licenseType>** - Tipo de licença que foi excedido (o outro prêmio VPN ou de AnyConnect/fundamentos)

Informações de Apoio

O log indica que uma criação de sessão falhou porque o limite máximo da licença para túneis VPN foi excedido que causa uma falha ao novato ou responde a uma requisição de túnel.

A aplicação do VPN no modo múltiplo exige a divisão das licenças disponíveis totais VPN entre os contextos configurados. O administrador ASA pode configurar quantas licenças cada contexto é atribuído.

Àrevelia, nenhuma licença do túnel VPN é atribuída aos contextos, e a atribuição do tipo de licença deve ser feita manualmente pelo administrador.

Ação recomendada

Assegure que bastante licenças estão disponíveis para todos os usuários permitidos e/ou obtenha mais licenças permitir as conexões rejeitadas. Para o multi-contexto, atribua mais licenças ao contexto que relatou a falha, se possível.

Solução

Dividir as licenças entre os contextos é feito pelo aumento do gerenciador de recurso com “VPN um outro” recurso que controle a divisão “do pool da licença outro VPN” usado para o VPN de Site-para-Site entre os contextos configurados.

O limite-recurso CLI abaixo permite esta configuração dentro do modo da “classe” do recurso.

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

Onde, escala do **<value>**: 1 limite da licença da plataforma ou 1-100% de licenças instaladas.

Para explosões, a escala é 1 às licenças unassigned ou 1-100% de licenças unassigned. Padrão: 0; nenhum recurso VPN é atribuído a uma classe.

A fim atribuir um contexto a 10% das licenças instaladas, você precisa de definir uma classe do recurso. Em seguida, aplique a classe aos contextos que você precisa de poder obter este recurso dentro da configuração do contexto do sistema.

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

A fim atribuir um contexto de 250 pares VPN das licenças instaladas, você precisa de definir um recurso “classe”. Em seguida, aplique a classe aos contextos que você prefere poder obter a este recurso dentro da configuração do contexto do sistema.

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

A fim aplicar a classe acima “vpn” a um contexto chamou o “administrador”, seguem estas etapas:

1. A mudança/Switchover ao contexto do sistema e aplica a classe VPN para o contexto “administrador”. Isto podia ser feito somente dentro do contexto do sistema.
2. Está abaixo o snippet de configuração para atribuir a classe “vpn” ao contexto “administrador”.

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

Informações Relacionadas

- Guias de referência dos Firewall da próxima geração do 5500 Series de Cisco ASA
- Manuais de configuração dos Firewall da próxima geração do 5500 Series de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems