

Configurar o Timeout de Conexão para Tráfego Específico no ASA com ASDM

Contents

[Introdução](#)

- [Requisitos](#)
- [Componentes Utilizados](#)
- [Defaults](#)

[Configurar tempo limite da conexão](#)

- [ASDM](#)
- [CLI do ASA](#)

[Verificar](#)

[Referências](#)

Introdução

Este documento descreve a configuração do timeout do Connection no ASA e no ASDM para um protocolo de aplicação específico, como HTTP, HTTPS, FTP ou qualquer outro protocolo. O tempo limite da conexão é o período de inatividade após o qual um firewall ou dispositivo de rede encerra uma conexão ociosa para liberar recursos e aumentar a segurança. Com antecedência, a primeira pergunta é: qual é o requisito para essa configuração? Se os aplicativos tiverem configurações de manutenção de atividade TCP apropriadas, a configuração do tempo limite de conexão em um firewall é frequentemente desnecessária. No entanto, se os aplicativos não tiverem as configurações de keepalive ou de timeout, nesse caso, configurar o timeout de conexão em um firewall é crucial para gerenciar recursos, melhorar a segurança, melhorar o desempenho da rede, garantir a conformidade e otimizar a experiência do usuário.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Lista de controle de acesso (ACL)
- Política de serviço

- Tempo Limite da Conexão

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 9.17(1)
- ASDM 7.17(1)

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 a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Defaults

 Observação: Tempo limite padrão

O tempo limite padrão de embrionário é de 30 segundos.

O tempo limite padrão de half-closed ocioso é de 10 minutos.

O valor padrão de dcd max_retries é 5.

O valor padrão de dcd retry_interval é de 15 segundos.

O tempo limite padrão de tcp ocioso é de 1 hora.

O tempo limite de udp ocioso padrão é de 2 minutos.

O tempo limite padrão de icmp ocioso é de 2 segundos.

O tempo limite padrão de sip ocioso é de 30 minutos.

O tempo limite de ociosidade padrão de sip_media é de 2 minutos.

O tempo limite de esp e ha ocioso padrão é de 30 segundos.

Para todos os outros protocolos, o timeout de ociosidade padrão é de 2 minutos.

Para nunca atingir o tempo limite, digite 0:0:0.

Configurar tempo limite da conexão

ASDM

Se um tráfego específico tiver uma tabela de conexão, ele terá um timeout ocioso específico; por

exemplo, neste artigo, alteramos o timeout de conexão para tráfego DNS.

Aqui estão várias opções para configurar o tempo limite da conexão para tráfego específico, considerando o diagrama de rede desse tráfego:

Cliente ----- [Interface: MNG] Firewall [Interface: OUT] ----- Servidor

Há a possibilidade de atribuir uma ACL à interface.

Etapa 1: Criar uma ACL

Podemos atribuir Origem, Destino ou Serviço

ASDM > Configuração > Firewall > Avançado > ACL Manager

The screenshot shows the 'Edit ACE' dialog box. The 'Action' is set to 'Permit'. Under 'Source Criteria', 'Source' is 'any', 'User' is empty, and 'Security Group' is empty. Under 'Destination Criteria', 'Destination' is 'any', 'Security Group' is empty, and 'Service' is 'udp/domain'. The 'Description' field is empty. 'Enable Logging' is checked, and 'Logging Level' is 'Default'. There are 'Help', 'Cancel', and 'OK' buttons at the bottom.

Etapa 2: Criar regra de política de serviço

Você pode pular a última etapa se já tiver a ACL ou pode atribuir um desses parâmetros (origem, destino ou serviço) à Política de serviço da interface.

ASDM > Configuração > Firewall > Regras de Política de Serviço

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Global - applies to all interfaces

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Etapa 3: Criar classe de tráfego

Há uma possibilidade de escolher o endereço IP origem e destino (usa ACL)

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP or SCTP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.

< Back Next > Cancel Help

Etapa 4: Atribuir ACL

Nesta etapa, você pode atribuir a ACL existente ou selecionar condições de correspondência (origem, destino ou serviço)

Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address

Action: Match Do not match

Existing ACL: ExistingACL 

Source Criteria

Source: 

User: 

Security Group: 

Destination Criteria

Destination: 

Security Group: 

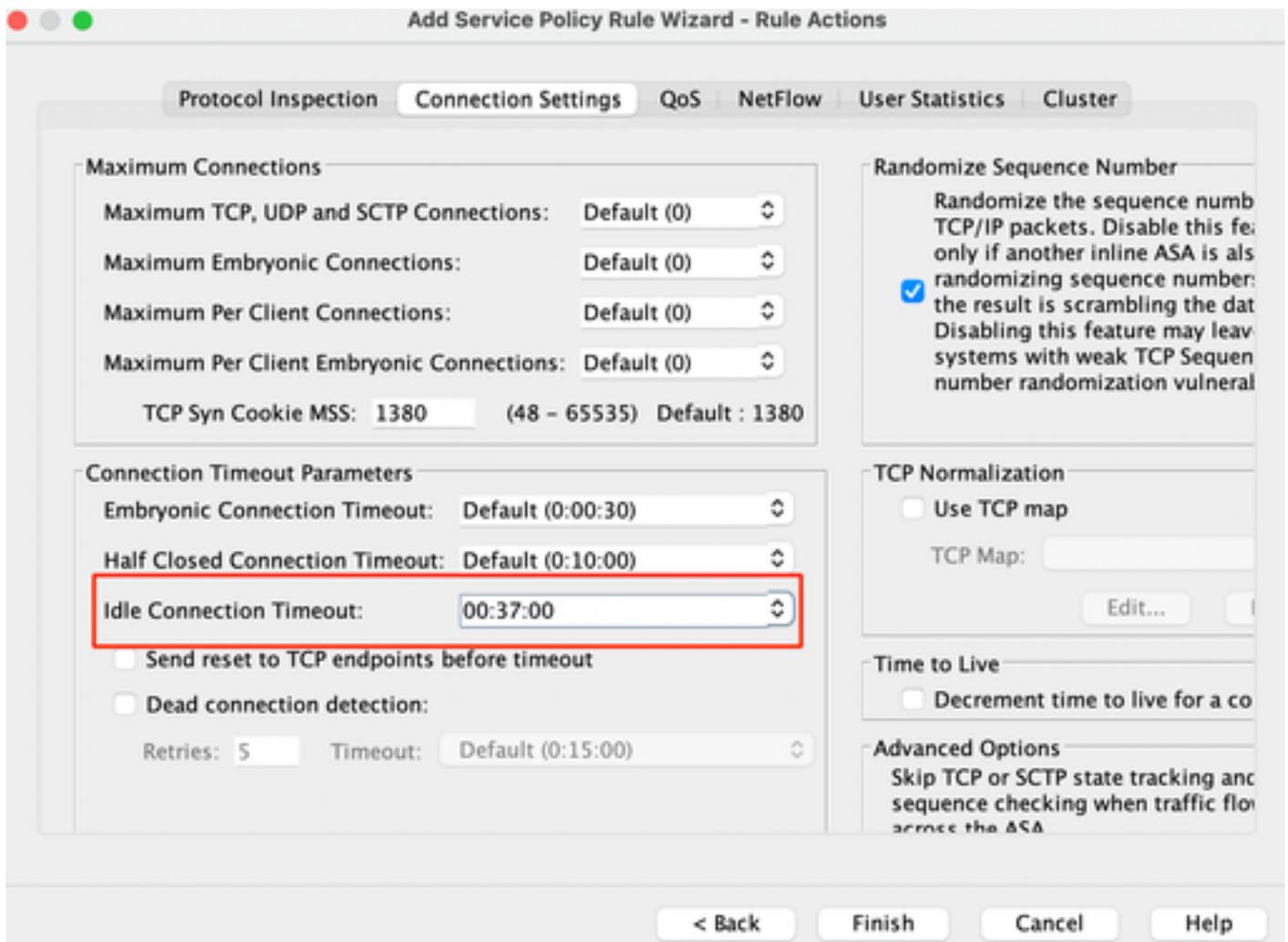
Service: 

Description:

More Options

Etapa 5: Configurar o parâmetro Idle Timeout

Com base no formato válido HH:MM:SS, configure o tempo limite de Ociosidade.



Limpe as conexões para esse tráfego específico:

```
#clear endereço IPdigite um endereço IP ou um intervalo de endereços IP
```

```
#clear conn protocoloDigite esta palavra-chave para limpar somente conexões SCP/TCP/UDP
```

CLI do ASA

Você pode definir todas essas configurações por meio da CLI:

ACL:

```
access-list DNS_TIMEOUT extended permit udp any any eq domain
```

Mapa de classe:

```
class-map MNG-class  
match access-list DNS_TIMEOUT
```

Policy-map:

```
policy-map MNG-policy
class MNG-class
set connection timeout idle 0:37:00
```

Aplicue o mapa de políticas na interface:

```
service-policy MNG-policy interface MNG
```

Verificar



Dica: se executarmos esse comando, podemos confirmar o tempo limite da conexão do tráfego DNS:

ASA CLI > modo de ativação > show conn long

Exemplo: show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63327 (10.10.10.30/63327), flags
- , idle 17s, uptime 17s, timeout 2m0s, bytes 36
```

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/62558 (10.10.10.30/62558), flags
- , idle 40s, uptime 40s, timeout 2m0s, bytes 36
```

Depois da configuração, podemos confirmar a configuração de timeout de ociosidade:

Exemplo: show conn long address 192.168.1.1

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63044 (10.10.10.30/63044), flags
- , idle 8s, uptime 8s, timeout 37m0s, bytes 37
```

```
UDP MNG: 192.168.1.1/53 (192.168.1.1/53) OUT: 10.10.10.30/63589 (10.10.10.30/63589), flags
- , idle 5s, uptime 5s, timeout 37m0s, bytes 41
```

Referências

[O que são configurações de conexão](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.