

# Aborto do Módulo de serviços TLS NGFW erros devido ao erro da falha ou da validação certificada do aperto de mão

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve como pesquisar defeitos um problema particular com acesso aos Web site HTTPS-baseados através do Módulo de serviços do Firewall da próxima geração de Cisco (NGFW) com a descriptografia permitida.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Procedimentos de aperto de mão do secure sockets layer (SSL)
- Certificados SSL

### [Componentes Utilizados](#)

A informação neste documento é baseada no Módulo de serviços de Cisco NGFW com versão 9.2.1.2(52) do gerenciador de segurança da prima de Cisco (PRSM).

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Informações de Apoio

A descryptografia é uma característica que permita o Módulo de serviços NGFW de decifrar fluxos SSL-cifrados (e para inspecionar a conversação que é cifrada de outra maneira) e de reforçar políticas no tráfego. A fim configurar esta característica, os administradores devem configurar um certificado da descryptografia no módulo NGFW, que é apresentado aos Web site HTTPS-baseados acesso do cliente no lugar do certificado de servidor original.

Para que a descryptografia trabalhe, o módulo NGFW deve confiar o certificado server-apresentado. Este documento explica as encenações quando a saudação de SSL falha entre o Módulo de serviços NGFW e o server, que faz com que determinados Web site HTTPS-baseados falhem quando você tenta os alcançar.

Com a finalidade deste documento, estas políticas são definidas no Módulo de serviços NGFW com PRSM:

- **Políticas da identidade:** Não há nenhuma política definida da identidade.
- **Políticas de descryptografia:** **Decrypt-toda** política usa esta configuração:
- **Políticas de acesso:** Não há nenhuma política de acesso definida.
- **Ajustes da descryptografia:** Este documento supõe que um **certificado da descryptografia** está configurado no Módulo de serviços NGFW e que os clientes o confiam.

Quando uma política de descryptografia é definida no Módulo de serviços NGFW e configurada como descrito anteriormente, o Módulo de serviços NGFW tenta interceptar todo o tráfego SSL-cifrado através do módulo e decifrá-lo.

Nota: Uma explicação passo a passo deste processo está disponível na seção [decifrada do fluxo de tráfego do Guia do Usuário para ASA CX e o gerenciador de segurança principal 9.2 de Cisco](#).

Esta imagem descreve a sequência de evento:

Nesta imagem, **A** é o cliente, **B** é o Módulo de serviços NGFW, e o **C** é o servidor HTTPS. Para os exemplos fornecidos neste documento, o server HTTPS-baseado é um Cisco Adaptive Security Device Manager (ASDM) em uma ferramenta de segurança adaptável de Cisco (ASA).

Há dois fatores importantes sobre este processo que você deve considerar:

- No segundo passo do processo, o server deve aceitar uma das séries da cifra SSL que são apresentadas pelo Módulo de serviços NGFW.

- Na quarta etapa do processo, o Módulo de serviços NGFW deve confiar o certificado que é apresentado pelo server.

## Problema

Se o server não pode aceitar algumas das cifras SSL que estão apresentadas pelo Módulo de serviços NFGW, você recebe um Mensagem de Erro similar a este:

É importante tomar a nota da informação de detalhes do erro (destacada), que mostra:

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

Quando você vê o arquivo de `/var/log/cisco/tls_proxy.log` no arquivo dos diagnósticos do módulo, estes Mensagens de Erro aparecem:

```
2014-02-05 05:21:42,189 INFO TLS_Proxy - SSL alert message received from  
server (0x228 = "fatal : handshake failure") in Session: x2fd1f6
```

```
2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:  
SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while  
connecting to server for Session: x2fd1f6
```

## Solução

Uma causa possível para este problema é que uma licença do Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) (referida frequentemente como o K9) não está instalada no módulo. Você pode [transferir a licença K9](#) para o módulo sem carga e transferir a arquivos pela rede através de PRSM.

Se o problema persiste depois que você instala a licença 3DES/AES, a seguir obtenha capturas de pacote de informação para a saudação de SSL entre o Módulo de serviços NGFW e o server, e contacte o administrador do servidor a fim permitir as cifras apropriadas SSL no server.

## Problema

Se o Módulo de serviços NGFW não confia o certificado que está apresentado pelo server, a seguir você recebe um Mensagem de Erro similar a este:

É importante tomar a nota da informação de detalhes do erro (destacada), que mostra:

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Quando você vê o arquivo de `/var/log/cisco/tls_proxy.log` no arquivo dos diagnósticos do módulo, estes Mensagens de Erro aparecem:

```
2014-02-05 05:22:11,505 INFO TLS_Proxy - Certificate verification failure:  
self signed certificate (code 18, depth 0)
```

```
2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa
```

```
2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa
```

```
2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from  
server (0x230 = "fatal : unknown CA") in Session: x148a696e
```

```
2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
connecting to server for Session: x148a696e
```

## Solução

Se o módulo é incapaz de confiar o certificado do server SSL, você deve importar o certificado de servidor no módulo com PRSM a fim assegurar-se de que o processo da saudação de SSL seja bem sucedido.

Termine estas etapas a fim importar o certificado de servidor:

1. Contorneie o Módulo de serviços NGFW quando você alcança o server a fim transferir o certificado através de um navegador. Uma maneira de contornar o módulo é criar uma política de descryptografia que não decifre o tráfego a esse servidor particular. Este vídeo mostra-lhe como criar a política:

Estas são as etapas que são mostradas no vídeo:

A fim alcançar o PRSM no CX, navegue a **https:// <IP\_ADDRESS\_OF\_PRSM>**. Este exemplo usa **https://10.106.44.101**.

Navegue às **configurações > às políticas/ajustes > às políticas de descryptografia no PRSM**.

Clique o ícone que é ficado situado perto do canto esquerdo superior da tela e escolha **adicionar acima da** opção da **política** a fim adicionar uma política à parte superior da lista.

Nomeie a política, deixe a fonte como **alguns**, e crie um objeto do **grupo de rede CX**.

Nota: Recorde incluir o endereço IP de Um ou Mais Servidores Cisco ICM NT do server HTTPS-baseado. Neste exemplo, um endereço IP de Um ou Mais Servidores Cisco ICM NT de **172.16.1.1** é usado. Choose **não decifra** para a ação.

Salvar a política e comprometa as mudanças.

2. Transfira o certificado de servidor através de um navegador e transfira-o arquivos pela rede ao Módulo de serviços NGFW através de PRSM, segundo as indicações deste vídeo:

Estas são as etapas que são mostradas no vídeo:

Uma vez que a política precedente-mencionada é definida, use um navegador a fim navegar ao server HTTPS-baseado que abre através do Módulo de serviços NGFW.

Nota: Neste exemplo, a versão 26.0 de Mozilla Firefox é usada a fim navegar ao server (um ASDM em um ASA) com a URL **https://172.16.1.1**. Aceite o aviso da Segurança se um estala acima e adicionar uma exceção da Segurança.

Clique o ícone fechamento-dado forma pequeno situado à esquerda da barra de endereços. O lugar deste ícone varia baseado no navegador que é usado e na versão.

Clique o botão do **certificado da vista** e então o botão da **exportação** sob a aba dos detalhes depois que você seleciona o certificado de servidor.

Salvar o certificado em sua máquina pessoal em um lugar de sua escolha.

O log no PRSM e consulta às **configurações > aos Certificados**.

Clique que **eu quero a... > o certificado de importação** e escolheu o certificado de servidor precedente-transferido (de etapa 4).

Salvar e comprometa as mudanças. Uma vez que completo, o Módulo de serviços NGFW deve confiar o certificado que é apresentado pelo server.

3. Remova a política que foi adicionada em etapa 1. O Módulo de serviços NGFW pode agora terminar com sucesso o aperto de mão com o server.

## Informações Relacionadas

- [Guia do Usuário para ASA CX e gerenciador de segurança 9.2 da prima de Cisco](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)