

Erros de aborto TLS do módulo de serviços NGFW devido a falha de handshake ou erro de validação de certificado

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Problema](#)

[Solução](#)

[Problema](#)

[Solução](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como solucionar um problema específico com o acesso a sites baseados em HTTPS por meio do módulo de serviços do Cisco Next-Generation Firewall (NGFW) comcriptografia habilitada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Procedimentos de handshake SSL (Secure Sockets Layer)
- certificados SSL

Componentes Utilizados

As informações neste documento são baseadas no módulo de serviços Cisco NGFW com o Cisco Prime Security Manager (PRSM) versão 9.2.1.2(52).

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. If your network is live, make sure that you understand the potential impact of any command.

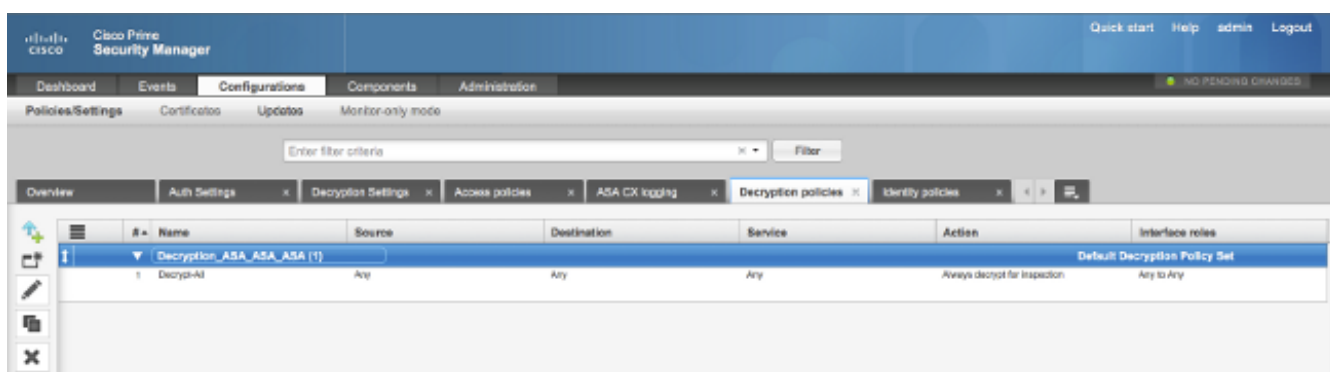
Informações de Apoio

A descryptografia é um recurso que permite que o módulo de serviços NGFW descryptografe fluxos criptografados por SSL (e inspecione a conversação que, de outra forma, é criptografada) e aplique políticas no tráfego. Para configurar esse recurso, os administradores devem configurar um certificado de descryptografia no módulo NGFW, que é apresentado aos sites baseados em HTTPS de acesso do cliente no lugar do certificado do servidor original.

Para que a descryptografia funcione, o módulo NGFW deve confiar no certificado apresentado pelo servidor. Este documento explica os cenários em que o handshake SSL falha entre o módulo de serviços NGFW e o servidor, o que faz com que determinados sites baseados em HTTPS falhem quando você tenta alcançá-los.

Para os fins deste documento, essas políticas são definidas no módulo de serviços NGFW com PRSM:

- **Políticas de identidade:** Não há políticas de identidade definidas.
- **Políticas de descryptografia:** A política **Descryptografar tudo** usa esta configuração:

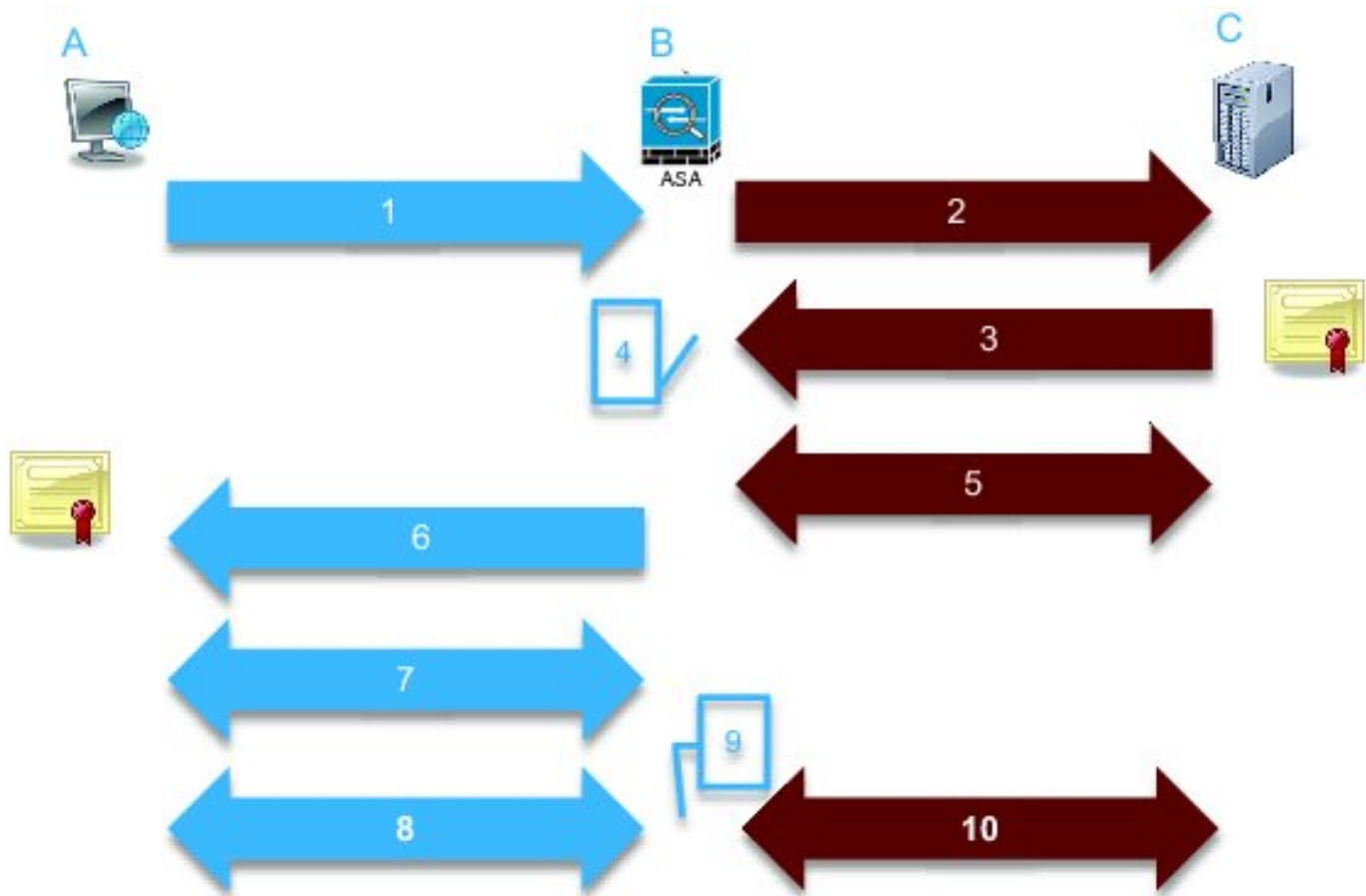


- **Políticas de acesso:** Não há políticas de acesso definidas.
- **Configurações de descryptografia:** Este documento pressupõe que um **certificado de descryptografia** está configurado no módulo de serviços NGFW e que os clientes confiam nele.

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 criptografado por SSL através do módulo e descryptografar.

Note: Uma explicação passo a passo desse processo está disponível na seção [Fluxo de tráfego descryptografado](#) do [Guia do usuário do ASA CX e do Cisco Prime Security Manager 9.2](#).

Esta imagem descreve a sequência de eventos:



334569

Nesta imagem, **A** é o cliente, **B** é o módulo de serviços NGFW e **C** é o servidor HTTPS. Para os exemplos fornecidos neste documento, o servidor baseado em HTTPS é um Cisco Adaptive Security Device Manager (ASDM) em um Cisco Adaptive Security Appliance (ASA).

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

- Na segunda etapa do processo, o servidor deve aceitar um dos conjuntos de cifras SSL que são apresentados pelo módulo de serviços NGFW.
- Na quarta etapa do processo, o módulo de serviços NGFW deve confiar no certificado apresentado pelo servidor.

Problema

Se o servidor não puder aceitar nenhuma das cifras SSL apresentadas pelo módulo de serviços NFGW, você receberá uma mensagem de erro semelhante a esta:

TLS Abort Event ID Time stamp: Wed 05 Feb 2014, 5:05 AM [Close](#)

A TLS or SSL flow was aborted due to a handshake failure or certificate validation error.

▼ **Event details**

Source		Destination		Transaction	
User		IP address	172.16.1.1	Connection ID	390891
Realm		Port	443	Transaction ID	
IP address	10.1.1.10	Interface	Idap	Component name	TLS Proxy
Port	64193	Service	tcp/443	Bytes sent	179
Interface	inside	Host		Bytes received	7
Identity		URL:		Total bytes	186
Remote device	No	URL category		Request content type	
Client OS name		Web reputation		Response content type:	
Context name		Threat type		HTTP response status	
				HTTP app detected phase	
				Configuration version	89
				Error details	

TLS		Application	
Encrypted flow:	Yes	Name	Transport Layer Security Protocol
Decrypted flow	No	Type	IP Protocol
Requested domain		Behavior	
Ambiguous destination			
Server certificate name			
Server certificate issuer			
TLS version			
Server cipher suite			
Error Details	error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure		

► **Policy**

É importante anotar as informações de Detalhes do Erro (destacadas), que mostram:

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

Quando você visualiza o arquivo `/var/log/cisco/tls_proxy.log` no arquivo de diagnóstico do módulo, estas mensagens de erro são exibidas:

```
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 possível causa desse problema é que uma licença Triple Data Encryption Standard/Advanced Encryption Standard (3DES/AES) (geralmente chamada de K9) não está instalada no módulo. Você pode [baixar a licença do K9](#) para o módulo sem custo e carregá-la via PRSM.

Se o problema persistir após a instalação da licença 3DES/AES, obtenha capturas de pacotes para o handshake SSL entre o módulo de serviços NGFW e o servidor e entre em contato com o administrador do servidor para habilitar as cifras SSL apropriadas no servidor.

Problema

Se o módulo de serviços NGFW não confiar no certificado apresentado pelo servidor, você receberá uma mensagem de erro semelhante a esta:

The screenshot shows a network device event log for a 'TLS Abort' event. The event ID is not specified, and the timestamp is 'Wed 05 Feb 2014, 5:04 AM'. The message states: 'A TLS or SSL flow was aborted due to a handshake failure or certificate validation error.' The event details are organized into several sections:

- Source:** User, Realm, IP address (10.1.1.10), Port (64186), Interface (inside), Identity, Remote device (No), Client OS name, Context name.
- Destination:** IP address (172.16.1.1), Port (443), Interface (ldap), Service (tcp/443), Host, URL, URL category, Web reputation, Threat type.
- Transaction:** Connection ID (390874), Transaction ID, Component name (TLS Proxy), Bytes sent (186), Bytes received (523), Total bytes (709), Request content type, Response content type, HTTP response status, HTTP app detected phase, Configuration version (89), Error details.
- TLS:** Encrypted flow (Yes), Decrypted flow (No), Requested domain, Ambiguous destination, Server certificate name, Server certificate issuer (/unstructuredName=ciscoasa), TLS version (TLSv1), Server cipher suite.
- Application:** Name (Transport Layer Security Protocol), Type (IP Protocol), Behavior.
- Device:** Name (ASA - CX), Type (ASA-CX).

The 'Error Details' section is highlighted with a red box and contains the following text:

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

É importante anotar as informações de Detalhes do Erro (destacadas), que mostram:

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

Quando você visualiza o arquivo `/var/log/cisco/tls_proxy.log` no arquivo de diagnóstico do módulo, estas mensagens de erro são exibidas:

```
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 não puder confiar no certificado SSL do servidor, você deve importar o certificado do servidor para o módulo com PRSM para garantir que o processo de handshake SSL seja bem-sucedido.

Conclua estes passos para importar o certificado do servidor:

1. Ignore o módulo de serviços NGFW quando você acessa o servidor para baixar o certificado por meio de um navegador. Uma maneira de ignorar o módulo é criar uma política decriptografia que não descriptografe o tráfego para esse servidor específico. Este vídeo mostra como criar a política:

Estas são as etapas mostradas no vídeo:

Para acessar o PRSM no CX, navegue até https://<IP_ADDRESS_OF_PRSM>. Este exemplo usa <https://10.106.44.101>.

Navegue até **Configurações > Políticas/Configurações > Políticas de descriptografia** no PRSM.

Clique no ícone localizado próximo ao canto superior esquerdo da tela e escolha a opção **Adicionar acima da política** para adicionar uma política ao topo da lista.

Nomeie a diretiva, deixe a Origem como **Qualquer** e crie um objeto de grupo de rede **CX**. **Note:** Lembre-se de incluir o endereço IP do servidor baseado em HTTPS. Neste exemplo, um endereço IP **172.16.1.1** é usado. Escolha **Não descriptografar** para a ação.

Salve a diretiva e confirme as alterações.

2. Baixe o certificado do servidor por meio de um navegador e carregue-o no módulo de serviços NGFW por meio do PRSM, como mostrado neste vídeo:

Estas são as etapas mostradas no vídeo:

Depois que a política mencionada anteriormente for definida, use um navegador para navegar até o servidor baseado em HTTPS que abre pelo módulo de serviços NGFW. **Note:** Neste exemplo, o Mozilla Firefox Versão 26.0 é usado para navegar para o servidor (um ASDM em um ASA) com o URL <https://172.16.1.1>. Aceite o aviso de segurança se aparecer uma mensagem e adicione uma exceção de segurança.

Clique no pequeno ícone em forma de bloqueio localizado à esquerda da barra de endereços. O local desse ícone varia com base no navegador usado e na versão.

Clique no botão **Exibir certificado** e, em seguida, no botão **Exportar** na guia Detalhes após selecionar o certificado do servidor.

Salve o certificado em sua máquina pessoal em um local de sua escolha.

Faça login no PRSM e vá até **Configurações > Certificados**.

Clique em **Quero... > Importar certificado** e escolher o certificado do servidor baixado anteriormente (da Etapa 4).

Salve e confirme as alterações. Depois de concluído, o módulo de serviços NGFW deve confiar no certificado apresentado pelo servidor.

3. Remova a política que foi adicionada na Etapa 1. O módulo de serviços NGFW agora pode concluir o handshake com êxito com o servidor.

Informações Relacionadas

- [Guia do usuário do ASA CX e Cisco Prime Security Manager 9.2](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)