

由于握手失败或证书验证错误，NGFW服务模块TLS中止错误

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[解决方案](#)

[问题](#)

[解决方案](#)

[相关信息](#)

简介

本文档介绍如何在启用解密的情况下通过思科下一代防火墙(NGFW)服务模块对基于HTTPS的网站的访问进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全套接字层(SSL)握手过程
- SSL证书

使用的组件

本文档中的信息基于思科NGFW服务模块(带思科Prime安全管理器(PRSM)版本9.2.1.2(52))。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

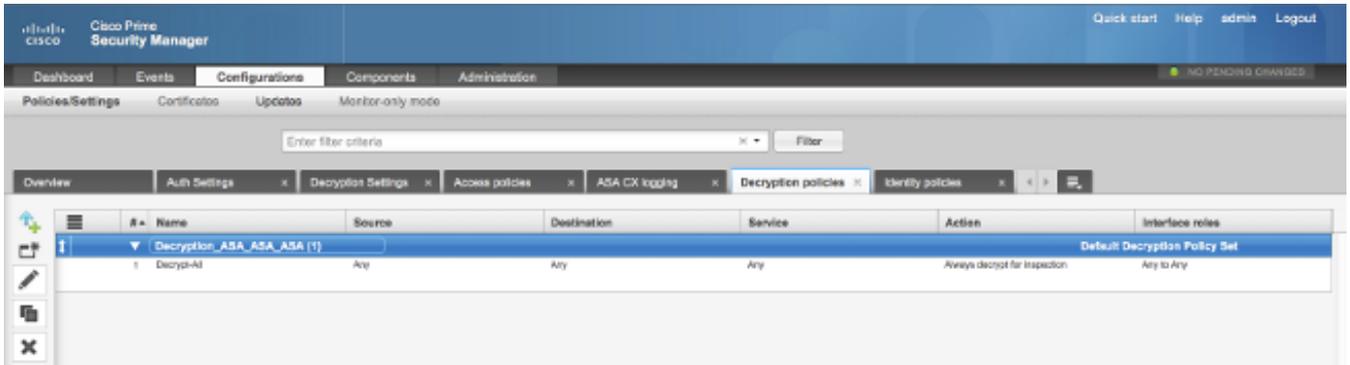
解密功能使NGFW服务模块能够解密SSL加密流(并检查其他加密的会话)并对流量实施策略。要配置此功能，管理员必须在NGFW模块上配置解密证书，该证书将呈现给客户端访问基于HTTPS的网站，以取代原始服务器证书。

为了使解密工作，NGFW模块必须信任服务器提供的证书。本文档介绍NGFW服务模块与服务器之

间的SSL握手失败时的场景，当您尝试访问某些基于HTTPS的网站时，这些场景会导致这些网站失败。

在本文档中，这些策略在NGFW服务模块上通过PRSM定义：

- **身份策略**:没有已定义的身份策略。
- **解密策略**:Decrypt-All策略使用以下配置：



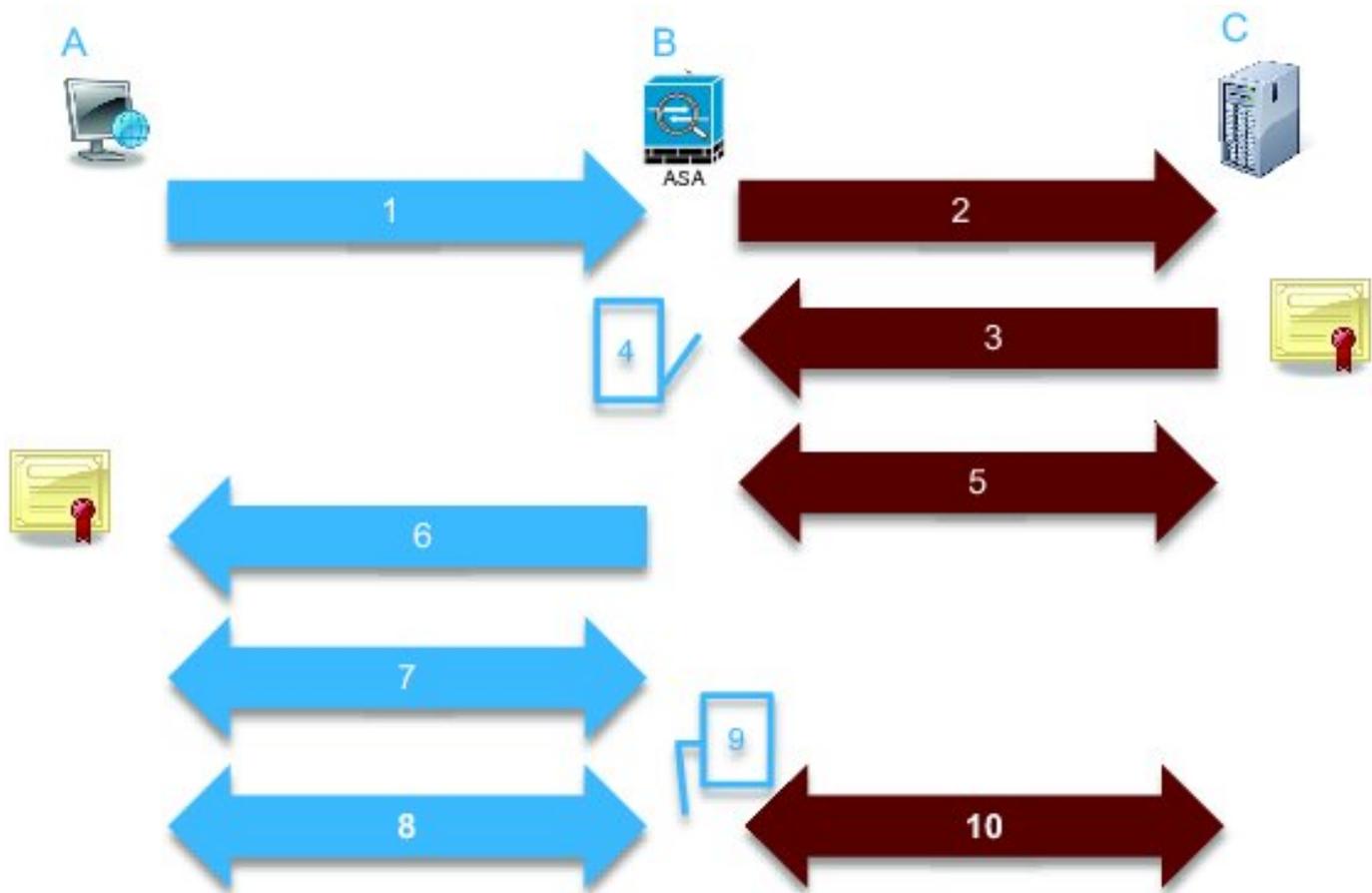
- **访问策略**:没有定义的访问策略。

- **解密设置**:本文档假设在NGFW服务模块上配置了解密证书，并且客户端信任该证书。

当解密策略在NGFW服务模块上定义并按照前面所述进行配置时，NGFW服务模块会尝试拦截通过模块的所有SSL加密流量并解密。

注意：有关此过程的分步说明，请参阅[ASA CX和Cisco Prime Security Manager 9.2用户指南的解密流量部分](#)。

此图显示事件顺序：



在此映像中,A是客户端，B是NGFW服务模块，C是HTTPS服务器。对于本文档中提供的示例，基于HTTPS的服务器是思科自适应安全设备(ASA)上的思科自适应安全设备管理器(ASDM)。

此过程有两个重要因素，您应该考虑：

- 在流程的第二步中，服务器必须接受NGFW服务模块提供的SSL密码套件之一。
- 在流程的第四步中，NGFW服务模块必须信任服务器提供的证书。

问题

如果服务器无法接受NFGW服务模块提供的任何SSL密码，您会收到类似以下的错误消息：

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	
TLS		Application		Transaction	
Encrypted flow:	Yes	Name	Transport Layer Security Protocol	Configuration version	89
Decrypted flow	No	Type	IP Protocol	Error details	
Requested domain		Behavior			
Ambiguous destination		Device			
Server certificate name		Name	ASA - CX		
Server certificate issuer		Type	ASA-CX		
TLS version					
Server cipher suite					
Error Details	error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure				

► **Policy**

请务必注意错误详细信息（突出显示），其中显示：

error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
在模块诊断归档文件中查看/var/log/cisco/tls_proxy.log文件时，会显示以下错误消息：

```
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
```

解决方案

此问题的一个可能原因是模块上未安装三重数据加密标准/高级加密标准(3DES/AES)许可证（通常称为K9）。您可以[下载模块的K9许可](#)证，无需收费，并通过PRSM上传。

如果在安装3DES/AES许可证后问题仍然存在，请获取NGFW服务模块与服务器之间SSL握手的数据包捕获，然后与服务器管理员联系以在服务器上启用适当的SSL密码。

问题

如果NGFW服务模块不信任服务器提供的证书，则您会收到类似如下的错误消息：

TLS Abort Event ID Time stamp: Wed 05 Feb 2014, 5:04 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	390874
Realm		Port	443	Transaction ID	
IP address	10.1.1.10	Interface	Idap	Component name	TLS Proxy
Port	64186	Service	tcp/443	Bytes sent	186
Interface	inside	Host		Bytes received	523
Identity		URL:		Total bytes	709
Remote device	No	URL category		Request content type	
Client OS name		Web reputation		Response content type:	
Context name		Threat type		HTTP response status	
TLS		Application		Transaction	
Encrypted flow:	Yes	Name	Transport Layer Security Protocol	HTTP app detected phase	
Decrypted flow	No	Type	IP Protocol	Configuration version	89
Requested domain		Behavior		Error details	
Ambiguous destination		Device			
Server certificate name		Name	ASA - CX		
Server certificate issuer	/unstructuredName=ciscoasa	Type	ASA-CX		
TLS version	TLSv1				
Server cipher suite					
Error Details	error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed				

Policy

请务必注意错误详细信息（突出显示），其中显示：

error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
 在模块诊断归档文件中查看/var/log/cisco/tls_proxy.log文件时，会显示以下错误消息：

```
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
```

解决方案

如果模块无法信任服务器SSL证书，则必须将服务器证书导入带PRSM的模块中，以确保SSL握手过程成功。

要导入服务器证书，请完成以下步骤：

1. 访问服务器时，请绕过NGFW服务模块，以便通过浏览器下载证书。绕过模块的一种方法是创建解密策略，该策略不解密流向该特定服务器的流量。此视频显示如何创建策略：

以下是视频中显示的步骤：

要访问CX上的PRSM，请导航至https://<IP_ADDRESS_OF_PRSM>。本示例使用<https://10.106.44.101>。

在PRSM中导航到**Configurations > Policies/Settings > Decryption policies**。

单击位于屏幕左上角的图标，然后选择**Add above policy**选项以将策略添加到列表顶部。

将策略命名，将Source保留为Any，然后创建CX网络组对象。

注意：请记住，应包括基于HTTPS的服务器的IP地址。在本例中，使用IP地址**172.16.1.1**。为**操作选择不解密**。

保存策略并提交更改。

2. 通过浏览器下载服务器证书，并通过PRSM将其上传到NGFW服务模块，如以下视频所示：

以下是视频中显示的步骤：

定义上述策略后，使用浏览器导航至通过NGFW服务模块打开的基于HTTPS的服务器。

注意：在本示例中，使用Mozilla Firefox版本26.0来导航到URL为<https://172.16.1.1>的服务器(ASA上的ASDM)。如果出现安全警告并添加安全异常，请接受该警告。

单击地址栏左侧的小锁形图标。此图标的位置因所使用的浏览器和版本而异。

选择**服务器证书**后，单击**View Certificate**按钮，然后单击**Details**选项卡下的**Export**按钮。

将证书保存到您选择的个人计算机上。

登录PRSM并浏览到**Configurations > Certificates**。

单击**I want to... > Import certificate (我想.....)**，然后选择之前下载的服务器证书(从步骤4)。

保存并提交更改。完成后，NGFW服务模块应信任服务器提供的证书。

3. 删除步骤1中添加的策略。NGFW服务模块现在能够成功完成与服务器的握手。

相关信息

- [ASA CX和Cisco Prime Security Manager 9.2用户指南](#)
- [技术支持和文档 - Cisco Systems](#)