

NGFW服务模块TLS中止错误由于握手失败或证书确认错误

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

本文描述如何通过有启用的解密的Cisco NEXT-GENERATION防火墙(NGFW)服务模块排除故障与访问的一个特定问题到基于HTTPS的网站。

[先决条件](#)

[要求](#)

Cisco 建议您了解以下主题：

- 安全套接字协议层(SSL)握手步骤
- SSL证书

[使用的组件](#)

本文档中的信息根据有Cisco最初安全经理(PRSM)版本9.2.1.2(52)的Cisco NGFW服务模块。

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。

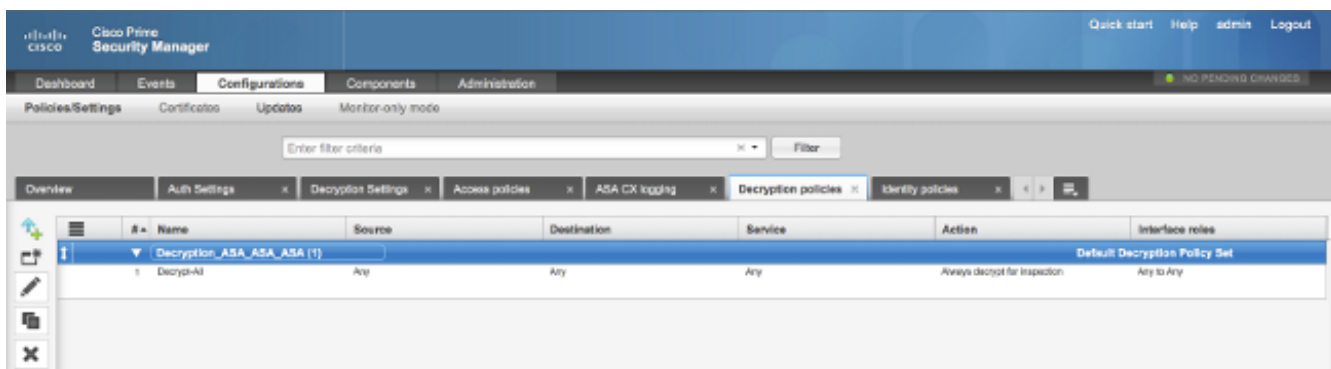
[背景信息](#)

解密是使NGFW服务模块解密SSL加密的流的功能(和检查否则加密)和强制执行在流量的策略的会话。为了配置此功能，管理员必须配置在NGFW模块的解密证书，被提交到访客接入基于HTTPS的网站在原始服务器证书位置。

为了解密能工作，NGFW模块必须委托服务器提交证书。本文解释方案，当SSL握手失效在NGFW服务模块和服务器之间时，造成某些基于HTTPS的网站发生故障，当您尝试到达他们时。

为本文的目的，这些策略在有PRSM的NGFW服务模块定义：

- **标识策略**：没有定义标识策略。
- **解密策略**：解密所有策略使用此配置：



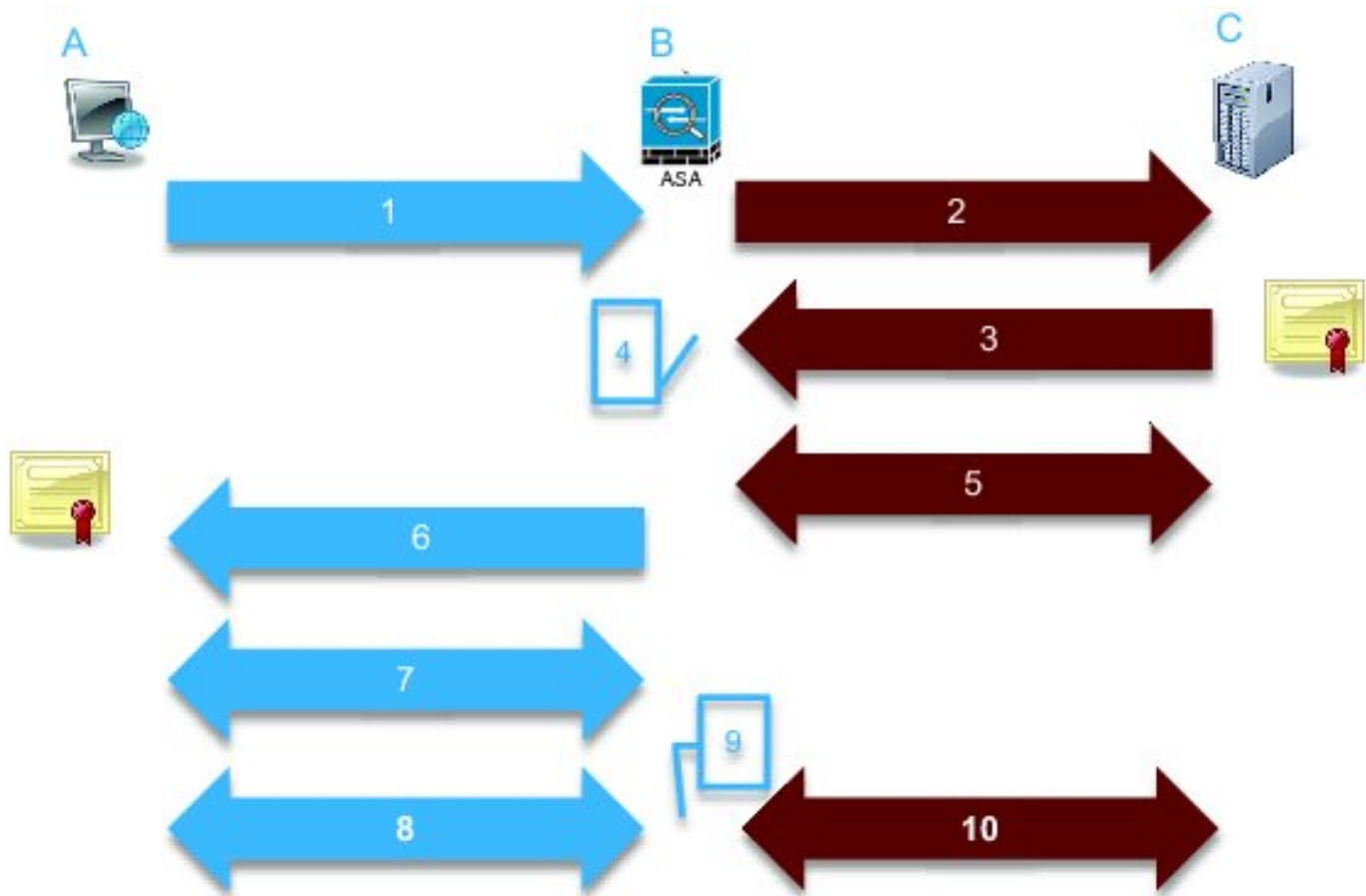
- **访问策略**：没有定义访问策略。

- **解密设置**：本文假设，解密证书在NGFW服务模块配置，并且客户端委托它。

当解密策略在NGFW服务模块定义和如前所述时配置，NGFW服务模块设法通过模块拦截所有SSL加密的流量和解密。

注意：此进程的一逐步说明是可用的在[用户指南为ASA CX和思科头等安全经理9.2的解密的通信流](#)部分。

此镜像表示事件顺序：



在此镜像，A是客户端，B是NGFW服务模块，并且C是HTTPS服务器。对于在本文提供的示例，基于HTTPS的服务器是一Cisco Adaptive Security Device Manager (ASDM)思科可适应安全工具的(ASA)。

有关于您应该考虑的此进程的两个重要因素：

- 在进程的第二步，服务器必须接受NGFW服务模块提交的其中一个SSL密码器套件。
- 在进程的第四步，NGFW服务模块必须委托服务器提交的证书。

问题

如果服务器不能接受NFGW服务模块提交的其中任一SSL密码器，您收到错误消息类似于此：

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**

注意到错误详细信息(被选定)是重要的，显示：

error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
 当您在模块诊断存档时查看/var/log/cisco/tls_proxy.log文件，这些错误消息出现：

```
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

此问题的一个可能的原因是三重数据加密标准/Advanced加密标准(3DES/AES)许可证(经常指K9)在模块没有安装。您能[下载](#)模块的[K9许可证](#)免费和通过PRSM上传它。

如果问题持续，在您安装3DES/AES许可证后，则请得到SSL握手的数据包捕获在NGFW服务模块和服务器之间，并且与服务器管理员联系为了启用在服务器的适当的SSL密码器。

问题

如果NGFW服务模块不委托服务器提交的证书，则您接收错误消息类似于此：

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**

注意到错误详细信息(被选定)是重要的，显示：

error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
 当您在模块诊断存档时查看/var/log/cisco/tls_proxy.log文件，这些错误消息出现：

```
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

如果模块无法委托服务器SSL证书，您必须导入服务器证书到有PRSM的模块为了保证SSL握手过程是成功的。

完成这些步骤为了导入服务器证书：

1. 当您访问服务器为了通过浏览器时，下载证书请绕过NGFW服务模块。一种方式绕过模块将创

建不解密流量到该特定服务器的解密策略。此视频显示您如何创建策略：

这些是在视频显示的步骤：

为了访问在CX的PRSM，请导航对[https:// <IP_ADDRESS_OF_PRSM>](https://<IP_ADDRESS_OF_PRSM>)。此示例使用<https://10.106.44.101>。

导航对在PRSM的**配置>策略/设置>解密策略**。

点击在屏幕的左上角附近查找的图标并且选择在**策略**选项上的**添加**为了添加策略到列表的顶部。

给出策略，留下来源作为其中任一，并且创建**CX网络组**对象。

注意：切记包括基于HTTPS的服务器的IP地址。在本例中，使用**172.16.1.1**的IP地址。choose不为操作**解密**。

保存策略并且确认更改。

2. 如此视频所显示，通过浏览器下载服务器证书并且上传它到NGFW服务模块通过PRSM，：

这些是在视频显示的步骤：

一旦早先被提及的策略定义，请使用一个浏览器为了导航到通过NGFW服务模块打开的基于HTTPS的服务器。

注意：在本例中，Mozilla Firefox版本26.0用于为了导航到服务器(在ASA的一ASDM)有URL的<https://172.16.1.1>。接受安全警告一个是否冒出并且添加安全例外。

点击在地址栏左边查找的小LOCK成形图标。此图标的位置变化基于使用的浏览器和版本。

在您选择服务器证书后，请单击**查看证书**按钮然后**Export**按钮在详细信息选项卡下。

在您的选择的位置保存在您的个人计算机的证书。

登录PRSM并且浏览对**配置>证书**。

点击**我希望对...>进口证明书**和选择早先下载的服务器证书(从步骤4)。

保存并且确认更改。一旦完整，NGFW服务模块应该委托服务器提交的证书。

3. 取消在Step1被添加的策略。NGFW服务模块当前能用服务器成功地完成握手。

相关信息

- [ASA的CX用户指南和思科最初安全经理9.2](#)
- [技术支持和文档 - Cisco Systems](#)