Firepower数据路径故障排除第6阶段：主动身份验证

目录

简介

本文是一系列文章的一部分，这些文章说明如何系统地排除Firepower系统上的数据路径故障，以确定Firepower的组件是否可能影响流量。有关Firepower平台架构的信息以及指向其他数据路径故障排除文章的链接，请参阅概述文章。

本文介绍Firepower数据路径故障排除的第六阶段，即主动身份验证功能。

先决条件

- 本文涉及当前支持的所有Firepower平台
- Firepower设备必须在路由模式下运行

主动身份验证阶段故障排除

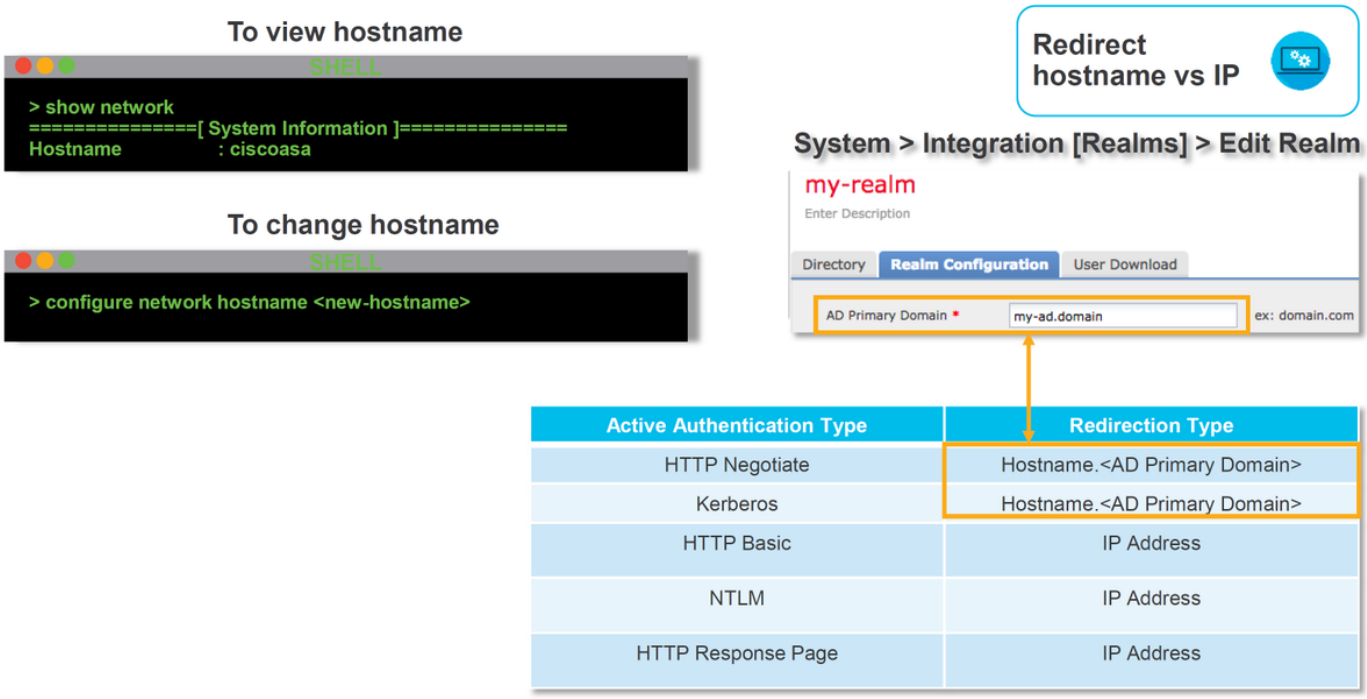
在尝试确定问题是否由身份引起时，了解此功能可能影响的流量非常重要。身份本身中唯一可能导致流量中断的功能是与主动身份验证相关的功能。被动身份验证不能导致流量意外丢弃。必须了解只有HTTP(S)流量受主动身份验证影响。如果其他流量因身份不起作用而受到影响，则更可能是因为策略使用用户/组来允许/阻止流量，因此当身份功能无法识别用户时，可能会发生意外情况，但这取决于设备访问控制策略和身份策略。本节中的故障排除仅介绍与主动身份验证相关的问题。

验证重定向方法

活动身份验证功能涉及运行HTTP服务器的Firepower设备。当流量与包含主动身份验证操作的身份策略规则匹配时，Firepower将307（临时重定向）数据包发送到会话，以将客户端重定向到其强制网络门户服务器。

目前有五种不同类型的主动身份验证。两个重定向到主机名，该主机名由传感器的主机名和与领域关联的Active Directory主域组成，三个重定向到执行强制网络门户重定向的Firepower设备上接口的IP地址。

如果重定向过程中出现问题，会话可能会中断，因为站点不可用。因此，了解重定向在运行配置中如何运行非常重要。下表有助于了解此配置方面。



Active Authentication Type	Redirection Type
HTTP Negotiate	Hostname.<AD Primary Domain>
Kerberos	Hostname.<AD Primary Domain>
HTTP Basic	IP Address
NTLM	IP Address
HTTP Response Page	IP Address

如果主动身份验证重定向到主机名，它将将客户端重定向到**ciscoasa.my-ad.domain:<port_used_for_captive_portal>**

生成数据包捕获

收集数据包捕获是排除主动身份验证问题的最重要部分。数据包捕获在两个接口上进行：

1. 在执行身份/身份验证时，流量正在接收的Firepower设备上的接口 在以下示例中，使**用内**部接口
2. Firepower用于重定向到HTTPS服务器的内部隧道接口 — **tun1** 此接口用于将流量重定向到强制网络门户流量中的IP地址在出口时更改回原始地址

```
> capture ins_ntlm interface inside buffer 1000000 match tcp host 192.168.62.31 any
> expert

# tcpdump -i tun1 -s 1518 -w /var/common/ntlm_tun.pcap

[Test authentication and then stop captures]

# ^C
> capture ins_ntlm stop

> copy /noconfirm /pcap capture:ins_ntlm ins_ntlm.pcap
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
748 packets copied in 0.40 secs


[ File will be copied here: /mnt/disk0/ins_ntlm.pcap ]
```

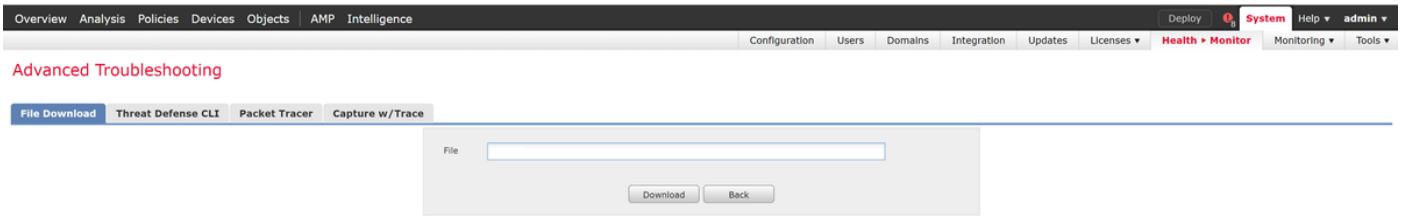
启动两个捕获，相关流量通过Firepower设备运行，然后停止捕获。

请注意，内部接口数据包捕获文件“ins_ntlm”已复制到**/mnt/disk0目**录。然后，可以将其复制到/var/common目录，以便从设备(所有FTD平台上的**/ngfw/var/common**)下载：

```
> expert
# copy /mnt/disk0/<pcap_file> /var/common/
```

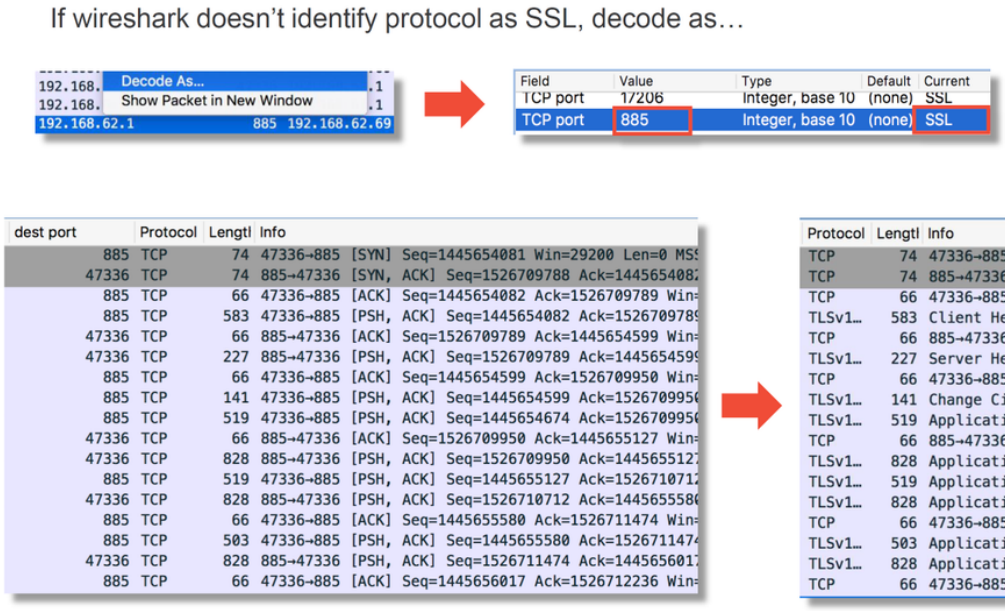
然后，可以使用本文中的说明从>提示符中从Firepower设备复制数据包捕获文件。

或者，Firepower 6.2.0及更高版本的Firepower管理中心(FMC)上没有选项。要在FMC上访问此实用程序，请导航至**Devices > Device Management**。然后，单击  图标，然后是高级故障排除**>文件下载**。然后，可以输入有关文件的名称，然后点击Download。

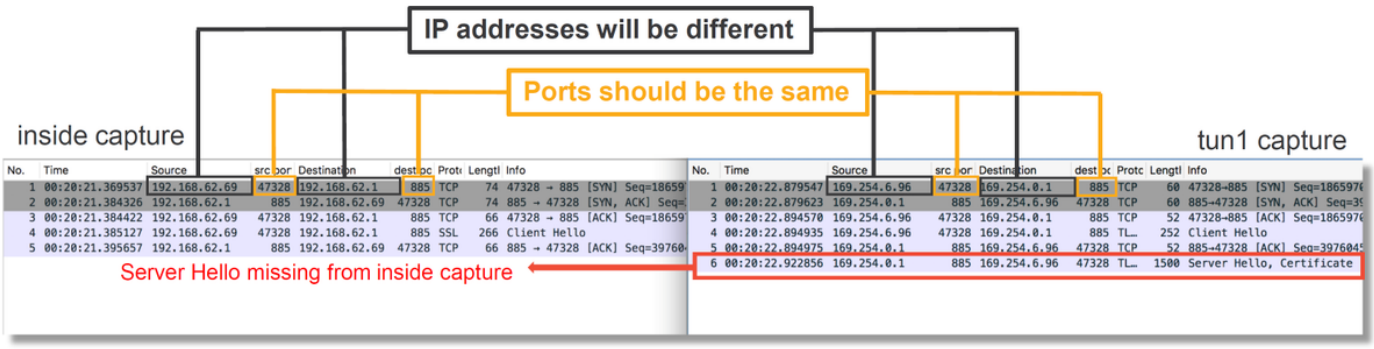


数据包捕获(PCAP)文件分析

可以执行Wireshark中的PCAP分析，以帮助确定主动身份验证操作中的问题。由于强制网络门户配置中使用非标准端口(默**认为**885)，因此需要配置Wireshark来解码SSL等流量。



应比较内部接口捕获和隧道接口捕获。在两个PCAP文件中识别相关会话的最佳方法是查找唯一源端口，因为IP地址不同。



在上例中，请注意内部接口捕获中缺少服务器hello数据包。这意味着它从未返回客户。数据包可能由snort丢弃，或可能由于缺陷或配置错误。

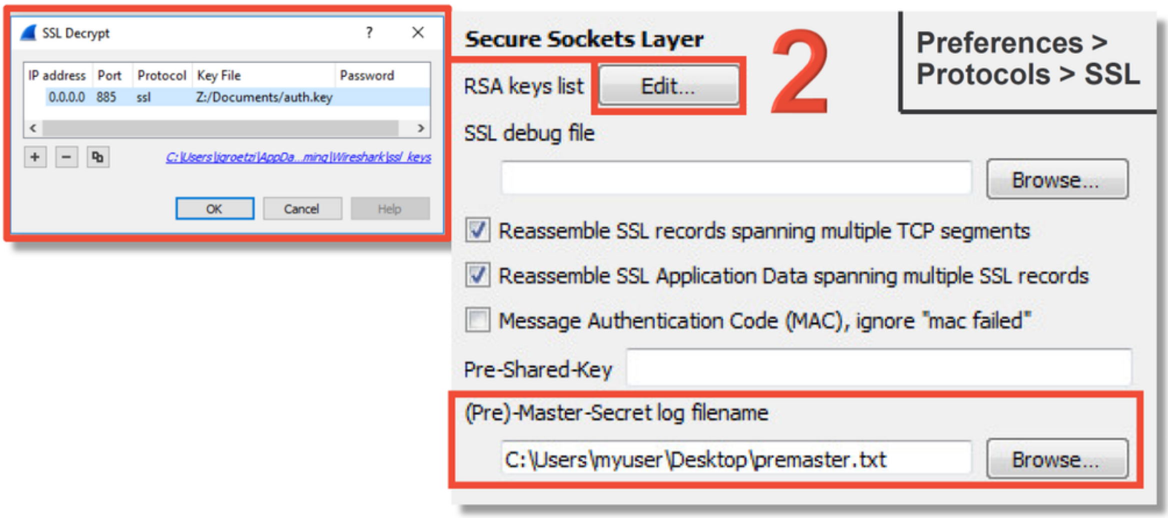
注意：Snort会检查其自己的强制网络门户流量，以防止任何HTTP漏洞。

解密加密流

如果问题不在SSL堆栈中，则解密PCAP文件中的数据以便查看HTTP流可能会有益。有两种方法可以实现此目的。

1. 在Windows中设置环境变量（更安全 — 推荐）此方法包括创建预主机加密文件。这可以通过以下命令（从windows命令终端运行）完成：**setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"**然后，可以在Firefox中打开专用会话，在该会话中，您可以浏览到使用SSL的有关站点。然后，对称密钥将记录到上述步骤1中命令中指定的文件。Wireshark可以使用对称密钥（请参见下图）使用文件解密。
2. 使用RSA私钥（安全性较低，除非使用测试证书和用户）要使用的私钥是用于强制网络门户证书的私钥这对非RSA（如椭圆曲线）或任何短时间（例如Diffie-Hellman）都不起作用

警告：如果使用方法2，请勿向思科技术支持中心(TAC)提供您的私钥。但是，可以使用临时测试证书和密钥。测试用户也应用于测试。



查看解密的PCAP文件

在以下示例中，PCAP文件已解密。它显示NTLM正用作主动身份验证方法。

```
HTTP/1.1 401 Unauthorized
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
WWW-Authenticate: NTLM
TlRMTVNTUAACAAAACgAKADgAAAAFgomiqq2eSri57HcAAAAAAAAAAKgAqABCAAAABgOAJQAAAA9KAEcALQBBAEQAAgAKAEoARwAtAEEARAABA
BgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQABAAYAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAyAGEAZA
AuAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEAAAAA
Content-Length: 381
Keep-Alive: timeout=10, max=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
GET /x.auth?s=9n1DsDbFKVcS%2Fj71hez1nLYh%2F5qfEzgMgJd%2FdQEyyRs%3D&u=http%3A%2F%2Fwww.cisco.com%2F HTTP/1.1
Host: 192.168.62.1:885
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:43.0) Gecko/20100101 Firefox/43.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Authorization: NTLM
TlRMTVNTUAADAAAAGAAYAIgAAABSAVIBoAAAAAAAAABYAAAAGgAaAFgAAAAWABYAcgAAAAAAAADyAQAABYKIogYBsB0AAAAPI6ZJFPLSnhAOl
XwHPmh3AkEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPwOAPpWmWMvfnEBAQAAAAAAAKTQueLs1NIBEBvFTnBWA0sAAAAAAgAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAYAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAyAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBu
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEGAAQAAgAAAAgAMAAwAAAAAAAAAAAAEAAAAAIAAAGnon72xFiGN/nI
+x5HgnhIcuVFrNJLs2tch8vxbrx90KABAAAJYqfNSUhlBA9xs44bOV4AkAIgBIAFQAVABQAC8AMQA5ADIALgAxADYAOAAuADYAMgAuADEAAAA
AAAAAAAAAAAAA

HTTP/1.1 307 Temporary Redirect
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
Location: http://www.cisco.com/
Content-Length: 231
Keep-Alive: timeout=10, max=95
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```

在NTLM授权后，客户端将重定向回原始会话，以便其能够到达其预期目标(http://www.cisco.com)。

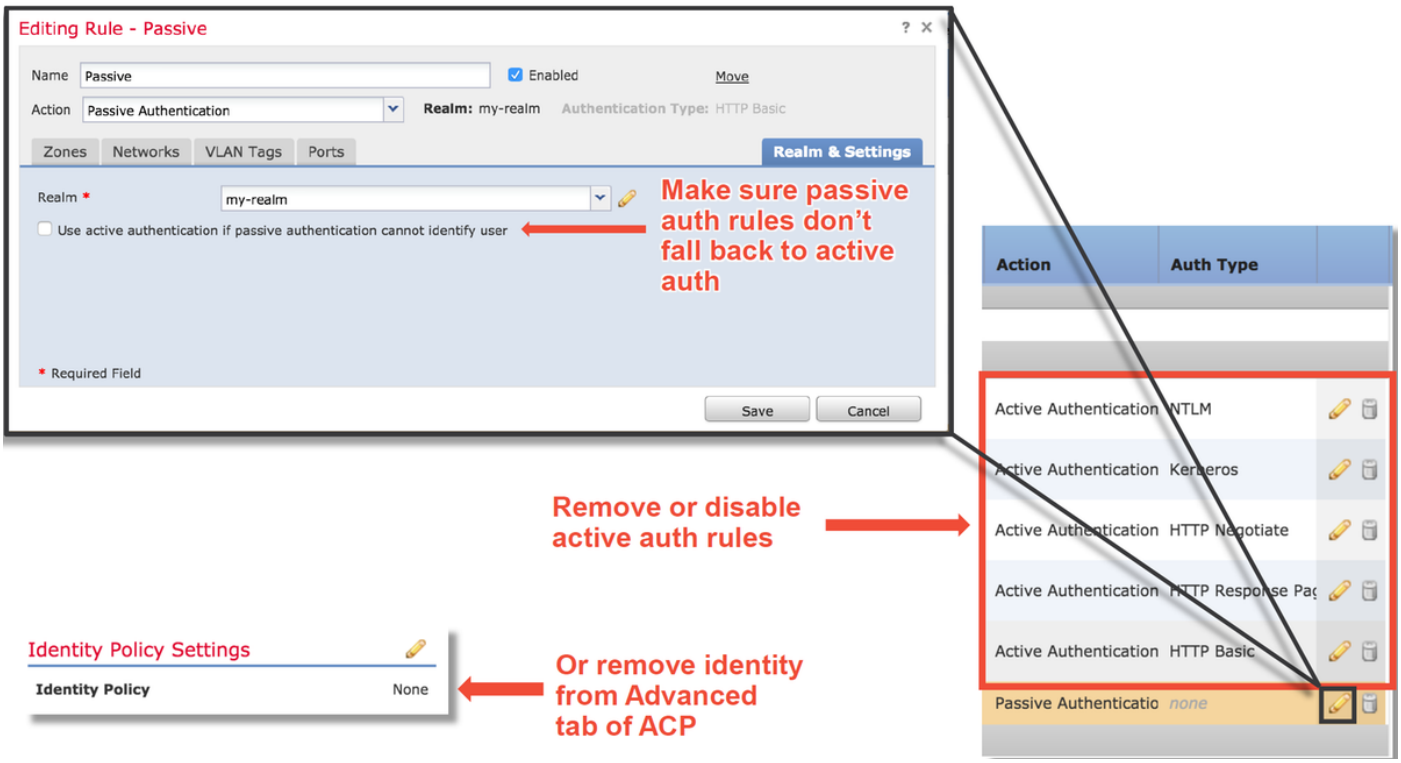
缓解步骤

仅切换到被动身份验证

当在身份策略中使用时，如果重定向过程中出现问题，活动身份验证可以丢弃允许的(仅HTTP(s)流

量)。快速缓解步骤是使用主动身份验证操作禁用身份策略中的任**何规则**。

此外，确保任何具有“被动身份验证”(Passive Authentication)作为操作的规则都未选中“如果被动身份验证无法识别用户，则使用主动身份验证”(Use active authentication if passive authentication cannot identify user)选项。



向TAC提供的数据

数据	说明
从Firepower管理中心(FMC)排除文件故障	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
从Firepower设备检查流量的文件故障排除	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
完整会话数据包捕获	有关说明，请参阅本文

后续步骤

如果已确定主用身份验证组件不是问题的原因，则下一步是排除入侵策略功能故障。

单击此处继续下一篇文章。