Firepower資料路徑故障排除第6階段：主動驗證

目錄

簡介

本文是一系列文章的一部分，這些文章介紹了如何對Firepower系統的資料路徑進行系統故障排除，以確定Firepower的元件是否影響流量。請參閱概述文章，瞭解有關Firepower平台架構的資訊，以及指向其他資料路徑故障排除文章的連結。

本文介紹Firepower資料路徑故障排除的第六階段，即主動身份驗證功能。

必要條件

- 本文涉及當前支援的所有的Firepower平台
- Firepower裝置必須在路由模式下運行

主動身份驗證階段故障排除

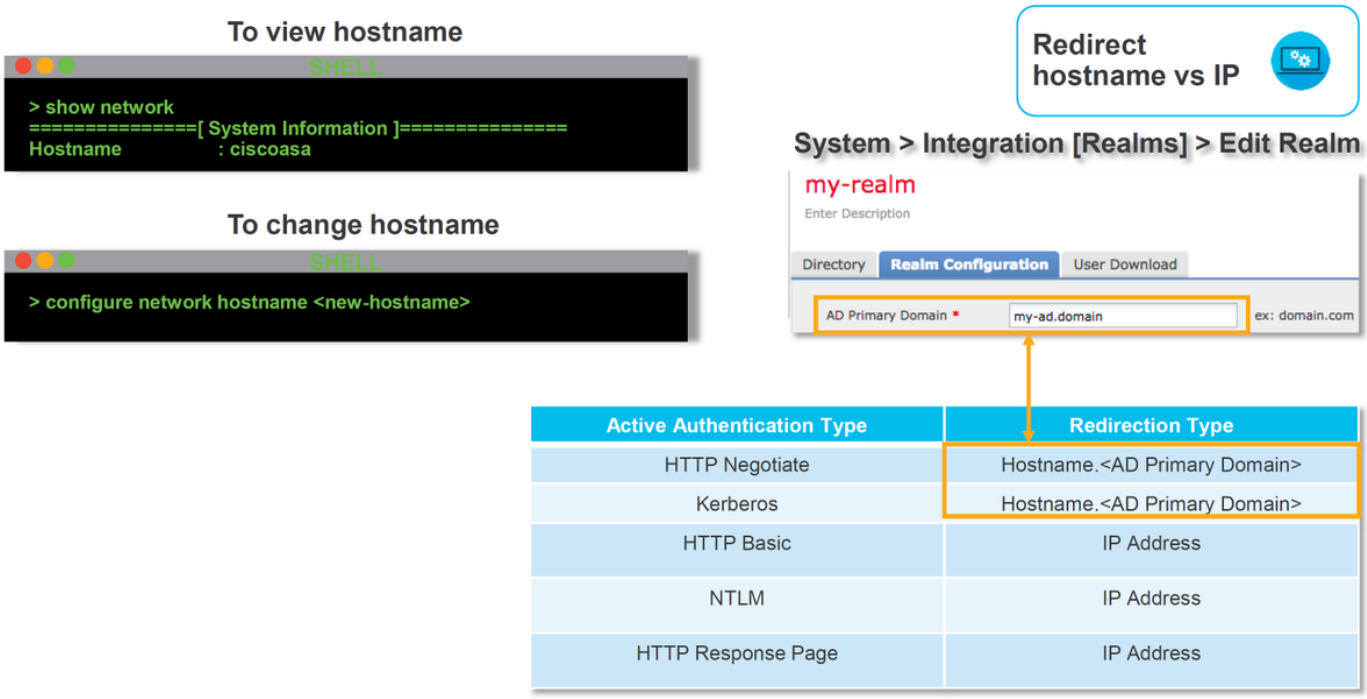
嘗試確定問題是否由身份引起時，瞭解此功能可能影響哪些流量非常重要。身份本身中唯一可能導致流量中斷的功能是與主動身份驗證相關的功能。被動身份驗證無法導致流量被意外丟棄。請務必瞭解，只有HTTP(S)流量受主動驗證的影響。如果其他流量因標識不起作用而受到影響，則更有可能是因為策略使用使用者/組來允許/阻止流量，因此當標識功能無法識別使用者時，會發生意外情況，但這取決於裝置訪問控制策略和身份策略。本節中的故障排除只介紹與主動身份驗證相關的問題。

驗證重新導向方法

活動身份驗證功能涉及運行HTTP伺服器的Firepower裝置。當流量與包含主動身份驗證操作的身份策略規則匹配時，Firepower會向會話傳送307（臨時重定向）資料包，以便將客戶端重定向到其強制網路門戶伺服器。

當前有五種不同型別的活動身份驗證。兩個重定向至主機名（由感測器的主機名和與領域關聯的Active Directory主域組成），三個重定向至正在執行強制網路門戶重定向的Firepower裝置上的介面的IP地址。

如果重新導向過程中出現錯誤，會話可能會中斷，因為站點不可用。這就是瞭解重新導向如何在執行組態中運作的原因。下面的圖表有助於理解此配置方面。



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

如果活動身份驗證重定向至主機名，則會將客戶端重定向至**ciscoasa.my-ad.domain:<port_used_for_captive_portal>**

生成資料包捕獲

收集資料包捕獲是解決活動身份驗證問題的最重要部分。封包擷取發生在兩個介面上：

1. 執行身份/身份驗證時，流量正在進入的Firepower裝置上的介面 在下面的示例中，使用**inside**介面
2. Firepower用於重定向到HTTPS伺服器的內部隧道介面**- tun1** 此介面用於將流量重定向到強制網路門戶流量中的IP位址會在輸出時變更回原始位址

```
> 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 ]
```

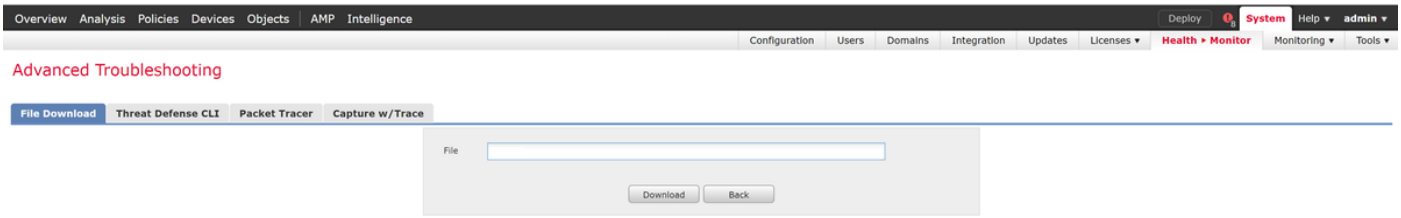
啟動兩個捕獲，通過Firepower裝置運行感興趣的流量，然後停止捕獲。

請注意，內部介面資料包捕獲檔案「ins_ntlm」被複製到**/mnt/disk0** 目錄。然後可以將其複製到/var/common目錄，以便從裝置下載(在所有FTD平台上**/ngfw/var/common**):

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

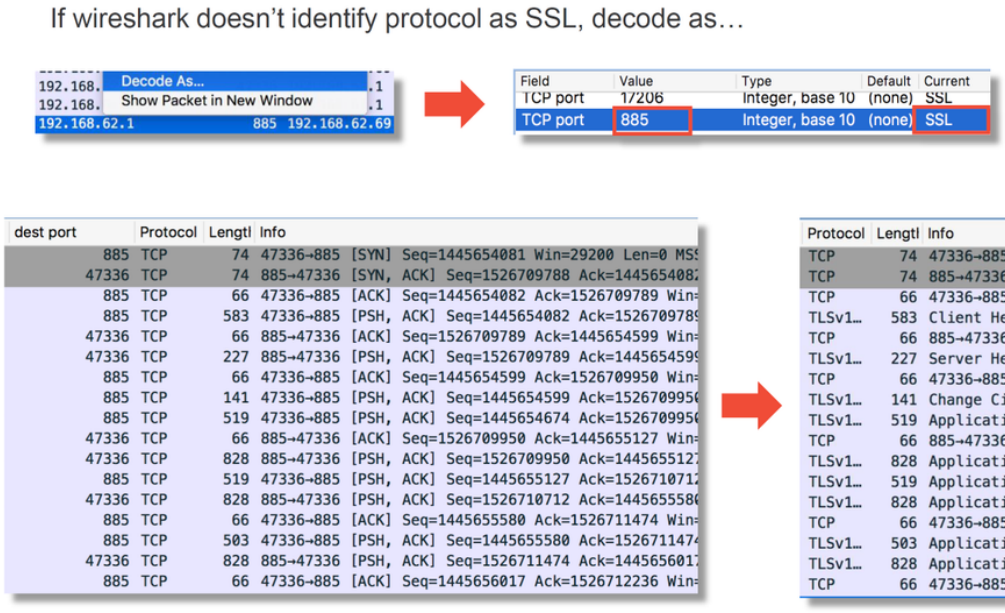
然後，可使用本文中的說明從>提示符處將資料包捕獲檔案從Firepower裝置複製。

或者，在Firepower 6.2.0及更高版本中，Firepower管理中心(FMC)上沒有選項。要在FMC上訪問此實用程式，請導航至**Devices > Device Management**。然後，按一下  圖示位於相關裝置旁，然後是**Advanced Troubleshooting > File Download**。然後，您可以輸入有問題的檔案的名稱，然後按一下「下載」。

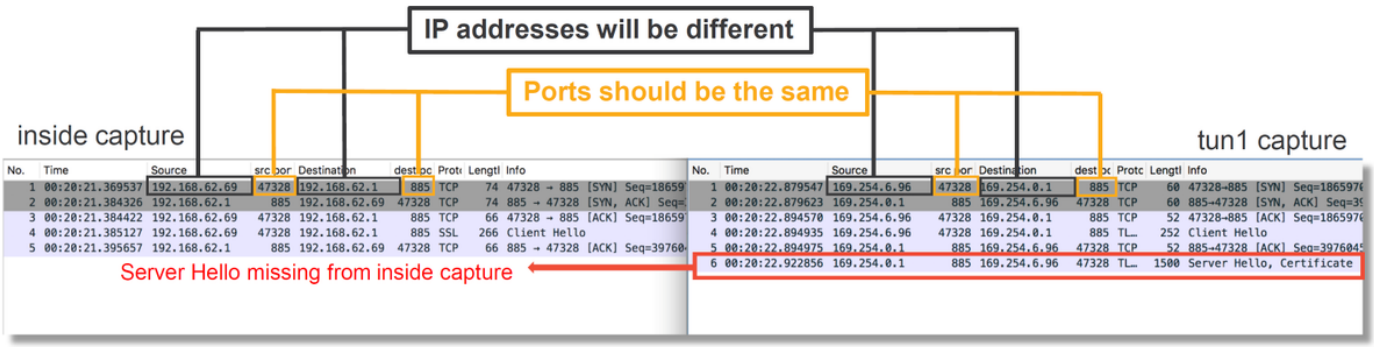


封包擷取(PCAP)檔案分析

可以在Wireshark中執行PCAP分析，以幫助識別活動身份驗證操作中的問題。由於非標準埠用於強制網路門戶配置(預設情況下為**885**)，因此需要將Wireshark配置為像SSL一樣解碼流量。



應對內部介面捕獲和隧道介面捕獲進行比較。在兩個PCAP檔案中標識相關會話的最佳方式是找到唯一的源埠，因為IP地址不同。



在上方示例中，請注意，內部介面捕獲中缺少伺服器hello資料包。這意味著它從未返回客戶端。資料包可能被snort丟棄，也可能是因為存在缺陷或配置錯誤。

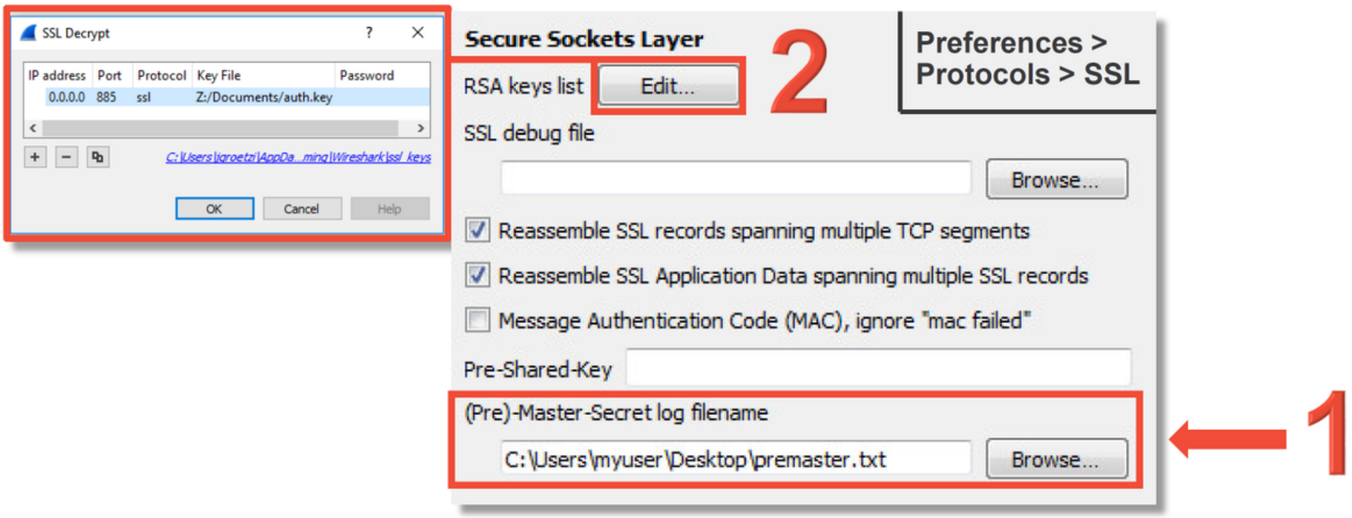
附註：Snort會檢查其自身的強制網路門戶流量，從而防止任何HTTP漏洞。

解密加密的流

如果問題不在SSL堆疊中，則最好將PCAP檔案中的資料解密，以便檢視HTTP流。有兩種方法可以實現這一點。

1. 在Windows中設定環境變數（更安全 — 推薦）此方法包括建立主控程式加密檔案。這可以通過以下命令完成（從windows命令終端運行）：**setx SSLKEYIOGFILE「%HOMEPATH%\Desktop\premaster.txt」**然後，可以在Firefox中開啟一個專用會話，在該會話中您可以瀏覽到相關站點，該站點使用SSL。然後，將對稱金鑰記錄到上述步驟1命令中指定的檔案。Wireshark可以使用對稱金鑰使用該檔案進行解密（請參閱下圖）。
2. 使用RSA私鑰（安全性較低，除非使用測試證書和使用者）要使用的私鑰是強制網路門戶證書使用的私鑰這不適用於非RSA（如Elliptic Curve）或任何短暫（例如Diffie-Hellman）的情形

注意：如果使用方法2，請勿向思科技術協助中心(TAC)提供您的私鑰。但可以使用臨時測試證書和金鑰。測試使用者也應用於測試。



檢視已解密的PCAP檔案

在以下示例中，PCAP檔案已解密。它顯示NTLM正被用作主動身份驗證方法。

```
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
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEGAAQAAgAAAAgAMAAwAAAAAAAAAAAEAAAAAIAAAGnon72xFiGN/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
```

進行NTLM授權後，使用者端將重新導向回原始作業階段，以便其可以到達其預期目的地，即http://www.cisco.com。

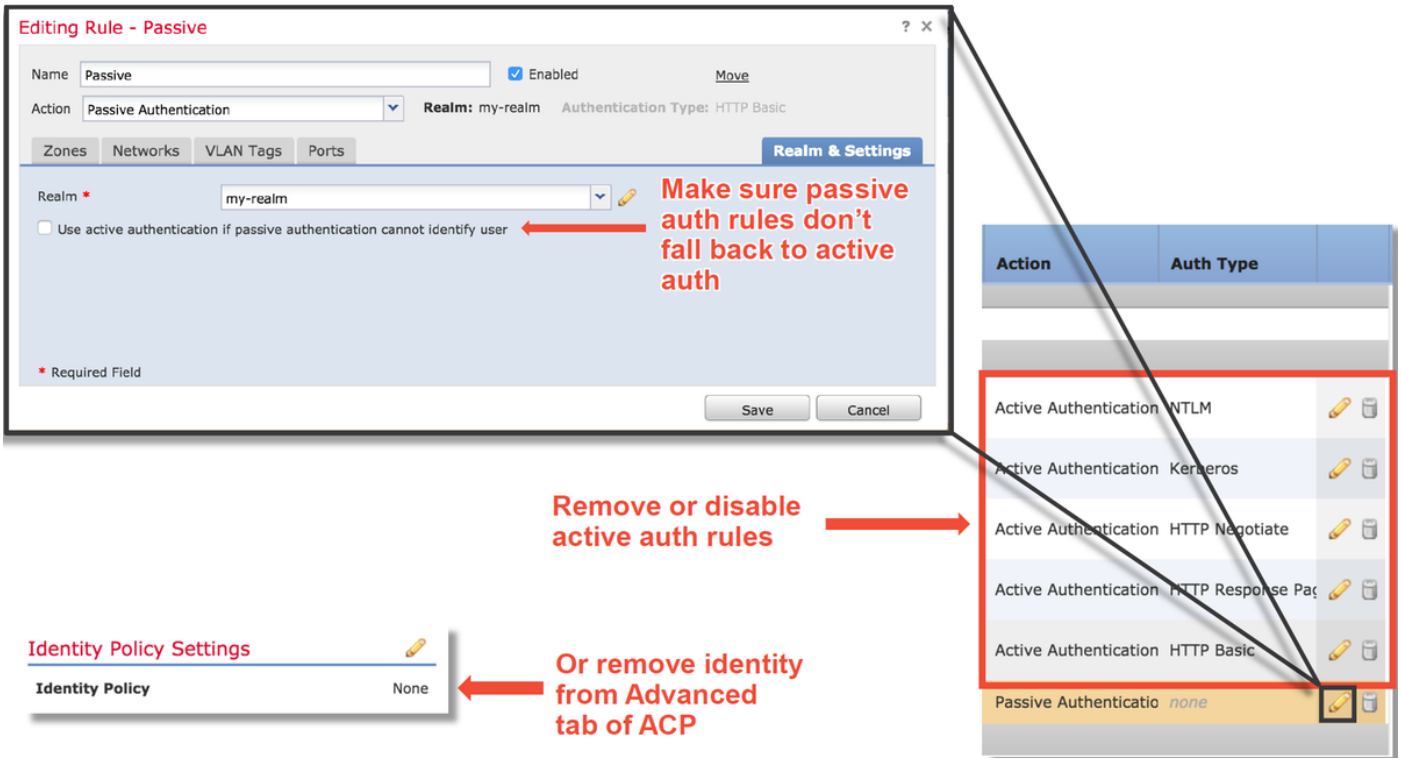
緩解步驟

切換到僅被動身份驗證

在身份策略中使用時，如果重定向過程中出現問題，活動身份驗證能夠丟棄允許的(僅限HTTP(s)流

量)。快速緩解步驟是使用Active Authentication操作禁用身份策略中的任何規則。

此外，請確保將「被動身份驗證」作為操作的任何規則均未選中「如果被動身份驗證無法識別使用者，則使用主動身份驗證」選項。



要提供給TAC的資料

資料	說明
Firepower管理中心(FMC)中的故障排除檔案	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
檢查流量的Firepower裝置的故障排除檔案	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
完整會話資料包捕獲	有關說明，請參閱本文

後續步驟

如果已確定活動身份驗證元件不是問題的原因，則下一步是排除入侵策略功能的故障。

按一下here繼續閱讀下一篇文章。