Firepower 데이터 경로 문제 해결 6단계: 활성 인증

목차

소개

이 문서는 Firepower 시스템의 데이터 경로 문제를 체계적으로 해결하여 Firepower의 구성 요소가 트래픽에 영향을 미치는지 여부를 확인하는 방법을 설명하는 일련의 문서 중 일부입니다. Firepower 플랫폼의 아키텍처에 대한 자세한 내용은 개요 문서를 참조하고 다른 데이터 경로 문제 해결 문서에 대한 링크를 참조하십시오.

이 문서에서는 Firepower 데이터 경로 문제 해결의 6단계인 활성 인증 기능을 다룹니다.

사전 요구 사항

- 이 문서는 현재 지원되는 모든 Firepower 플랫폼에 적용됩니다.
- Firepower 디바이스는 라우팅 모드에서 실행해야 합니다.

활성 인증 문제 해결 단계

ID로 인해 문제가 발생하는지 확인할 때는 이 기능이 영향을 줄 수 있는 트래픽을 파악하는 것이 중요합니다. 트래픽 중단을 유발할 수 있는 ID 자체의 기능은 활성 인증과 관련된 기능뿐입니다. 패시브 인증으로 인해 트래픽이 예기치 않게 삭제될 수는 없습니다. HTTP(S) 트래픽만 활성 인증의 영향을 받는다는 점을 이해하는 것이 중요합니다. ID가 작동하지 않아 다른 트래픽이 영향을 받는 경우, 이는 정책이 사용자/그룹을 사용하여 트래픽을 허용/차단하기 때문일 가능성이 높습니다. 따라서 ID 기능에서 사용자를 식별할 수 없는 경우 예기치 않은 상황이 발생할 수 있지만, 이는 디바이스

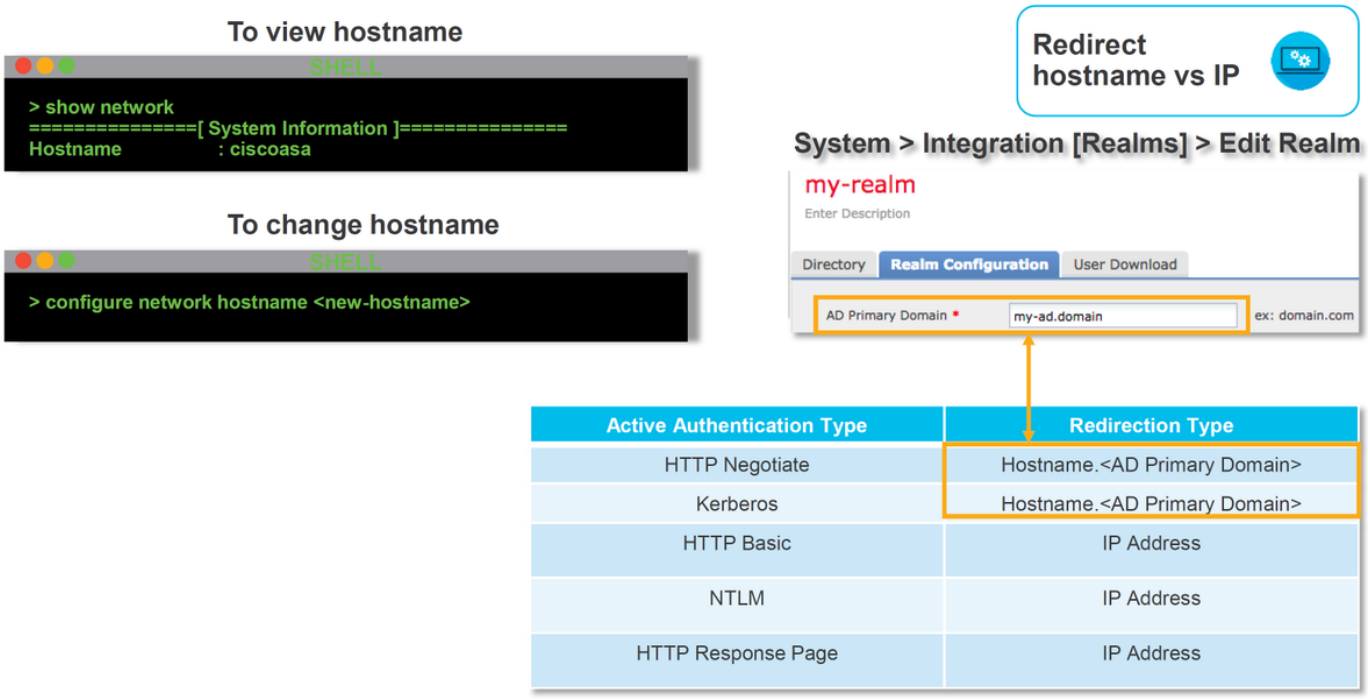
액세스 제어 정책 및 ID 정책에 달려 있습니다. 이 섹션의 문제 해결에서는 활성 인증과 관련된 문제만 안내합니다.

리디렉션 방법 확인

활성 인증 기능에는 HTTP 서버를 실행하는 Firepower 디바이스가 관련됩니다. 트래픽이 활성 인증 작업을 포함하는 ID 정책 규칙과 일치하는 경우, Firepower는 307(임시 리디렉션) 패킷을 세션으로 전송하여 클라이언트를 캡티브 포털 서버로 리디렉션합니다.

현재 5가지 유형의 활성 인증이 있습니다. 두 개 유형은 센서의 호스트 이름 및 영역에 연결된 Active Directory 기본 도메인으로 구성된 호스트 이름으로 리디렉션되고, 세 개 유형은 캡티브 포털 리디렉션을 수행 중인 Firepower 디바이스의 인터페이스 IP 주소로 리디렉션됩니다.

리디렉션 프로세스에서 문제가 발생하면 사이트를 사용할 수 없으므로 세션이 중단될 수 있습니다. 따라서 실행 중인 설정에서 리디렉션이 작동하는 방식을 이해하는 것이 중요합니다. 아래 차트는 이러한 설정 측면을 이해하는 데 도움이 됩니다.



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

활성 인증이 호스트 이름으로 리디렉션되는 경우 클라이언트는 **ciscoasa.my-ad.domain<port_used_for_captive_portal>으로 리디렉션됩니다.**

패킷 캡처 생성

패킷 캡처 수집은 활성 인증 문제를 해결하는 데 있어 가장 중요한 부분입니다. 패킷 캡처는 두 개의 인터페이스에서 발생합니다.

1. ID/인증을 수행할 때 트래픽이 인그레스되는 Firepower 디바이스의 인터페이스 아래 예에서는 **내부** 인터페이스가 사용됩니다
2. Firepower에서 HTTPS 서버로 리디렉션하는 데 사용하는 내부 터널 인터페이스 - **tun1** 이 인터페이스는 캡티브 포털로 트래픽을 리디렉션하는 데 사용됩니다.트래픽의 IP 주소는 이그레스 시 원래 주소로 다시 변경됩니다.

```
> 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 ]
```

두 개의 캡처가 시작되고, 관심 있는 트래픽이 Firepower 디바이스를 통해 실행된 다음 캡처가 중지됩니다.

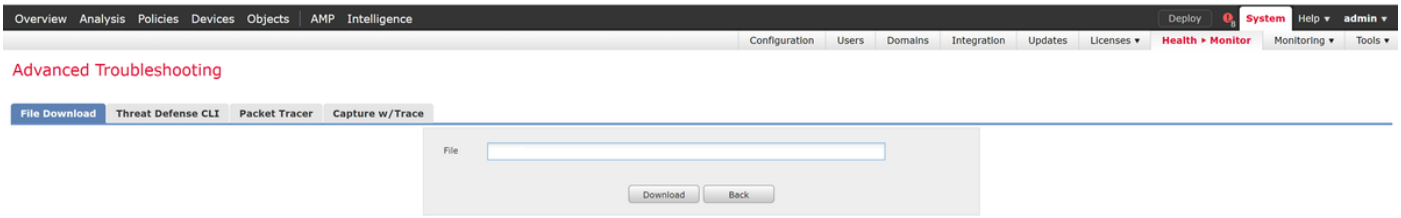
내부 인터페이스 패킷 캡처 파일인 "ins_ntlm"이 **/mnt/disk0** 디렉토리에 복사됩니다. 그런 다음 디바이스에서 다운로드할 수 있도록 /var/common 디렉터리에 복사할 수 있습니다(모든 FTD 플랫폼의 **/ngfw/var/common**).

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

그런 다음 이 문서의 지침에 따라 **>** 프롬프트에서 Firepower 디바이스 외부로 패킷 캡처 파일을 복사할 수 있습니다.

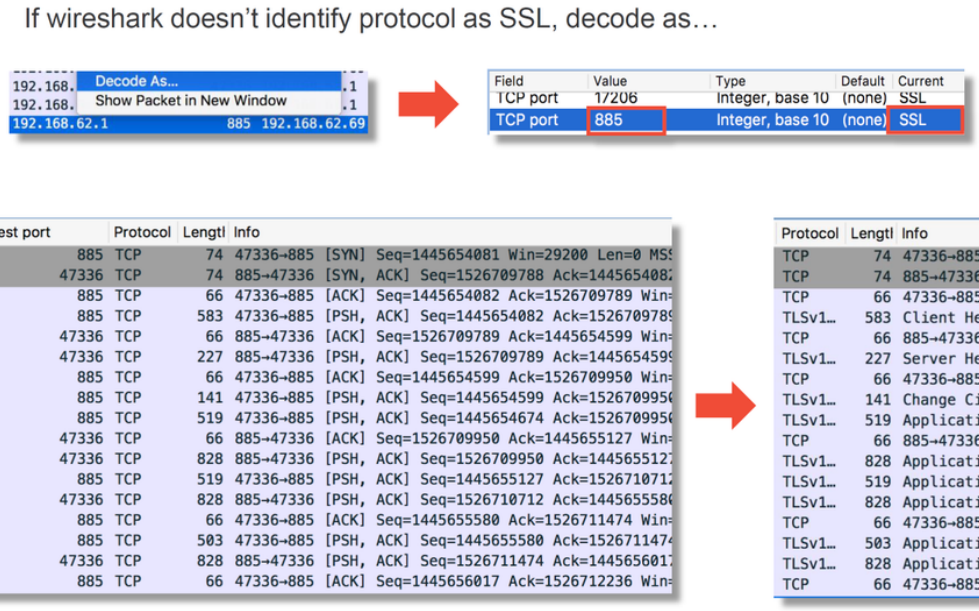
또는 Firepower 버전 6.2.0 이상의 FMC(Firepower Management Center)에는 n 옵션이 있습니다. FMC의 이 유틸리티에 액세스하려면 **디바이스 > 디바이스 관리**로 이동합니다. 그런 다음

해당 디바이스 옆의 아이콘과 **Advanced** Troubleshooting(**고급 문제 해결**) **> File Download(파일 다운로드)가 차례로 나타납니다**. 그런 다음 해당 파일의 이름을 입력하고 다운로드를 클릭할 수 있습니다.

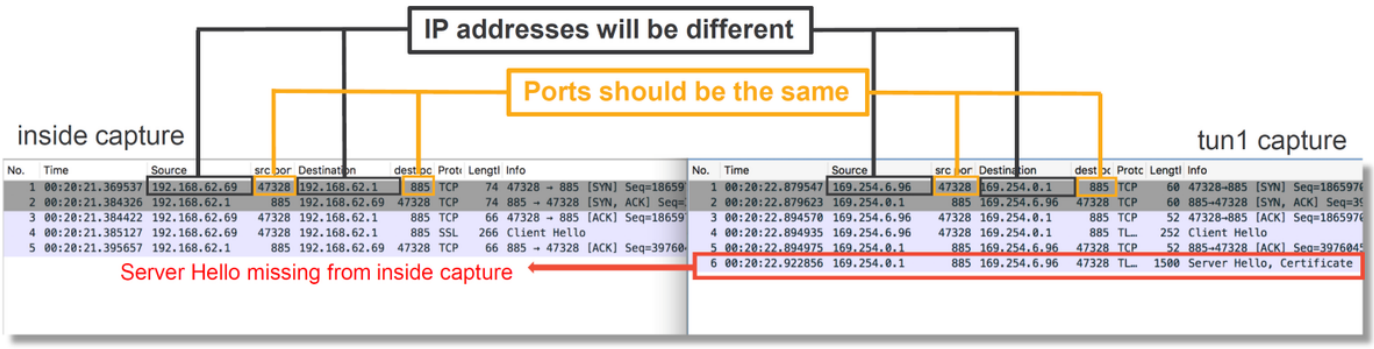


PCAP(Packet Capture) 파일 분석

활성 인증 작업 내에서 문제를 식별하는 데 도움이 되도록 Wireshark의 PCAP 분석을 수행할 수 있습니다. 비표준 포트는 캡티브 포털 설정(기본적으로 **885**)에서 사용되므로 SSL과 같은 트래픽을 디코딩하도록 Wireshark를 설정해야 합니다.



내부 인터페이스 캡처와 터널 인터페이스 캡처를 비교해야 합니다. 두 PCAP 파일에서 해당 세션을 식별하는 가장 좋은 방법은 IP 주소가 다르므로 고유한 소스 포트를 찾는 것입니다.



위의 예에서는 내부 인터페이스 캡처에서 서버 hello 패킷이 누락되고 있음을 확인할 수 있습니다. 이는 클라이언트에 다시 연결되지 않았음을 의미합니다. 패킷이 Snort에 의해 삭제되었거나 결함이나 잘못된 설정으로 인해 삭제되었을 수 있습니다.

참고: Snort는 HTTP 익스플로잇을 방지하기 위해 자체 캡티브 포털 트래픽을 검사합니다.

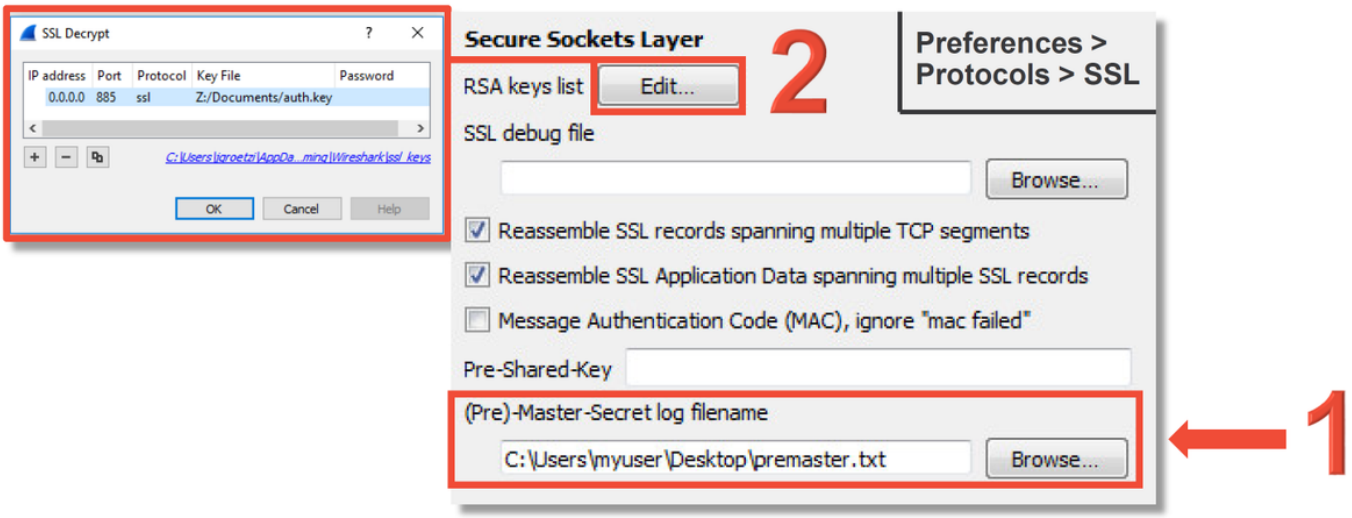
암호화된 스트림 암호 해독

SSL 스택에 문제가 없는 경우 HTTP 스트림을 확인하기 위해 PCAP 파일의 데이터의 암호를 해독하는 것이 도움이 될 수 있습니다. 두 가지 방법으로 이 작업을 수행할 수 있습니다.

1. Windows에서 환경 변수 설정(더 안전함 - 권장) 이 방법에는 프리마스터 암호 파일 생성 작업이 포함됩니다. 이 작업은 다음 명령을 사용하여 수행할 수 있습니다(Windows 명령 터미널에서 실행). **setx SSLKEYlogFILE "%HOMEPATH%\Desktop\premaster.txt"**그런 다음 Firefox에서 비공개 세션을 열어 SSL을 사용하는 해당 사이트로 이동할 수 있습니다.그런 다음 위의 1단계에서 명령에 지정된 파일에 대칭 키가 로그됩니다.Wireshark는 해당 파일을 사용하여 대칭 키를 통해 암호를 해독할 수 있습니다(아래 다이어그램 참조).
2. RSA 개인 키 사용(테스트 인증서 및 사용자를 사용하지 않는 경우 보안 수준 낮음) 사용할 개

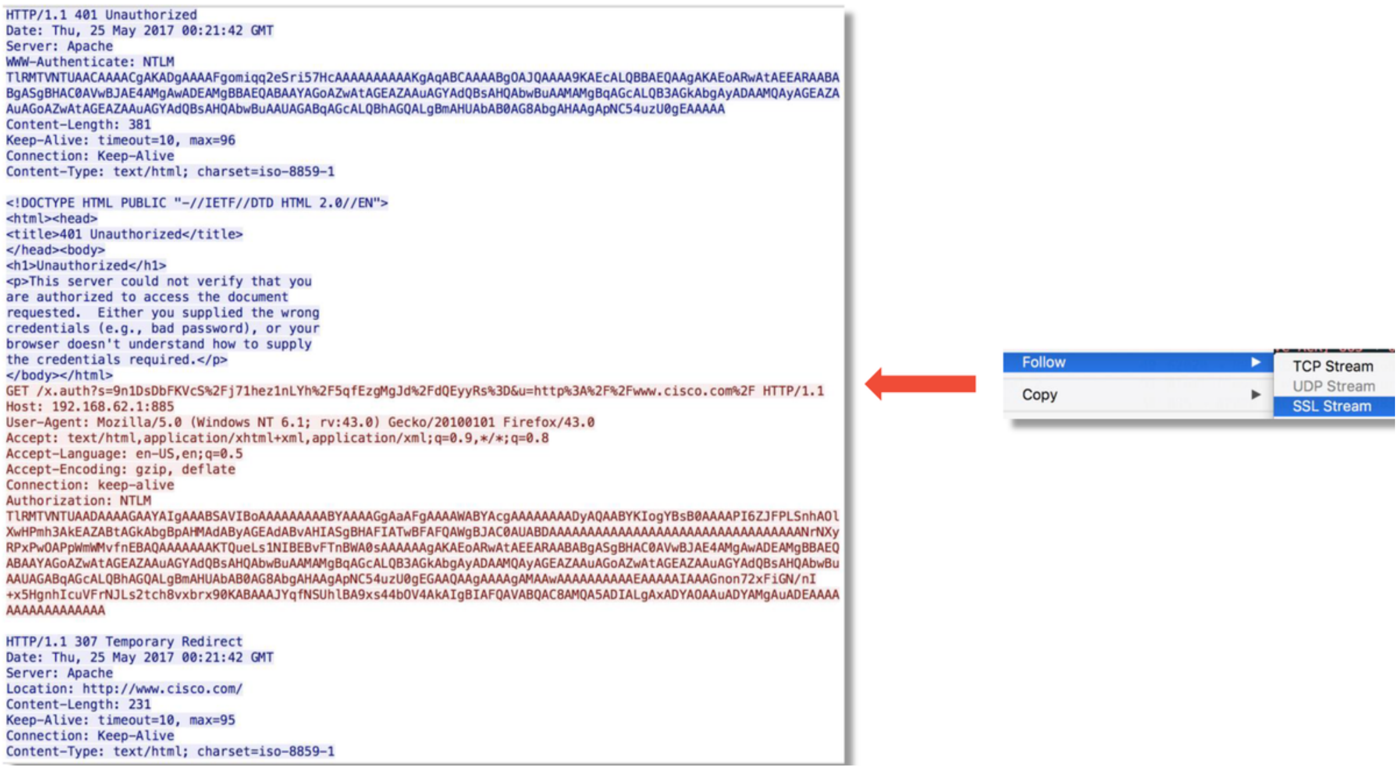
인 키는 캡티브 포털 인증서에 사용됩니다.이는 비 RSA(예: Elliptic Curve) 또는 일회성 항목(예: Diffie-Hellman)에는 작동하지 않습니다.

주의: 방법 2를 사용하는 경우 Cisco TAC(Technical Assistance Center)에 개인 키를 제공하지 마십시오. 그러나 임시 테스트 인증서 및 키를 사용할 수 있습니다. 테스트 사용자도 테스트에 사용해야 합니다.



암호 해독된 PCAP 파일 보기

아래 예에서는 PCAP 파일의 암호가 해독되었습니다. 이는 NTLM이 활성 인증 방법으로 사용되고 있음을 보여줍니다.



```
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
TlRMTVNTUAADAAAAGAAYAIgAAABSAVIBoAAAAAAAAABYAAAAGgAaAFgAAAAWABYAcgAAAAAAAADyAQAABYKIogYBsB0AAAAPI6ZJFPLSnhA0l
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
```

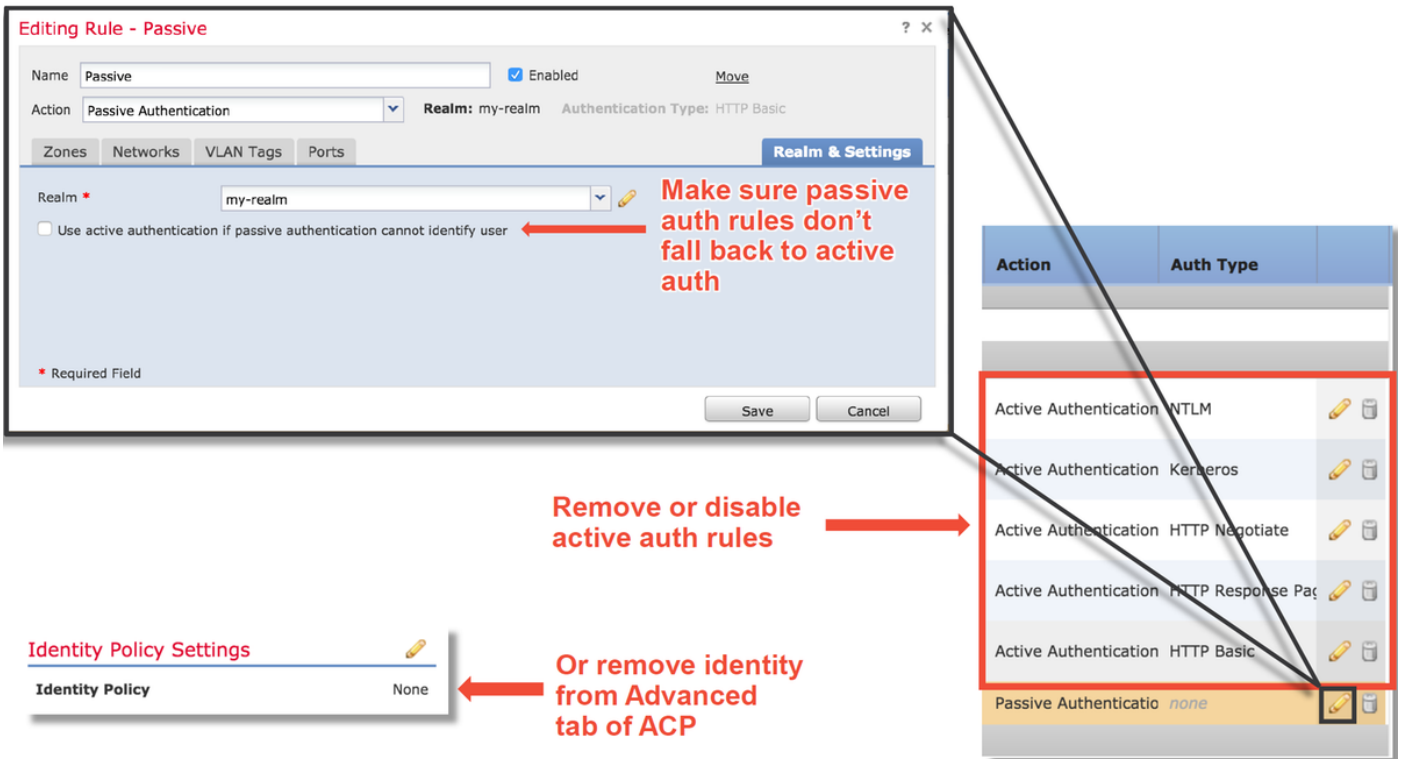

NTLM 권한 부여가 수행된 후 클라이언트가 원래 세션으로 다시 리디렉션되므로 의도된 대상인 http://www.cisco.com에 연결할 수 있습니다.

완화 단계

패시브 인증 전용으로 전환

ID 정책에서 사용할 경우, 활성 인증은 리디렉션 프로세스에서 문제가 발생하는 경우 허용된 항목을(HTTP 트래픽만) 삭제할 수 있습니다. 빠른 완화 단계는 **활성 인증** 작업을 사용하여 ID 정책 내에서 모든 규칙을 비활성화하는 것입니다.

또한 '패시브 인증' 작업이 포함된 규칙에서 '패시브 인증이 사용자를 식별할 수 없는 경우 활성 인증 사용' 옵션이 선택되어 있지 않은지 확인합니다.



TAC에 제공할 데이터

데이터	지침
FMC(Firepower Management Center)에서 파일 문제 해결	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
트래픽을 검사하는 Firepower 디바이스에서 파일 문제 해결	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
전체 세션 패킷 캡처	지침은 이 문서를 참조하십시오.

다음 단계

활성 인증 구성 요소가 문제의 원인이 아닌 것으로 확인된 경우, 다음 단계로 침입 정책 기능의 문제 해결을 수행합니다.

다음 문서로 이동하려면 여기를 클릭하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.