Fase 6 della risoluzione dei problemi relativi al percorso dei dati di Firepower: Autenticazione attiva

Sommario

Introduzione

Questo articolo fa parte di una serie di articoli che spiegano come risolvere in modo sistematico i problemi relativi al percorso dei dati nei sistemi Firepower per determinare se i componenti di Firepower possono influire sul traffico. Per informazioni sull'architettura delle piattaforme Firepower e per i collegamenti agli altri articoli sulla risoluzione dei problemi relativi ai percorsi di dati, consultare l'articolo di panoramica.

In questo articolo viene illustrata la sesta fase della risoluzione dei problemi relativi al percorso dati di Firepower, la funzionalità di autenticazione attiva.

Prerequisiti

- Questo articolo riguarda tutte le piattaforme Firepower attualmente supportate
- Il dispositivo Firepower deve essere in esecuzione in modalità di routing

Risoluzione dei problemi relativi alla fase di autenticazione attiva

Quando si cerca di stabilire se un problema è causato da un'identità, è importante capire quale traffico può avere effetto questa funzionalità. Le uniche funzionalità dell'identità che possono

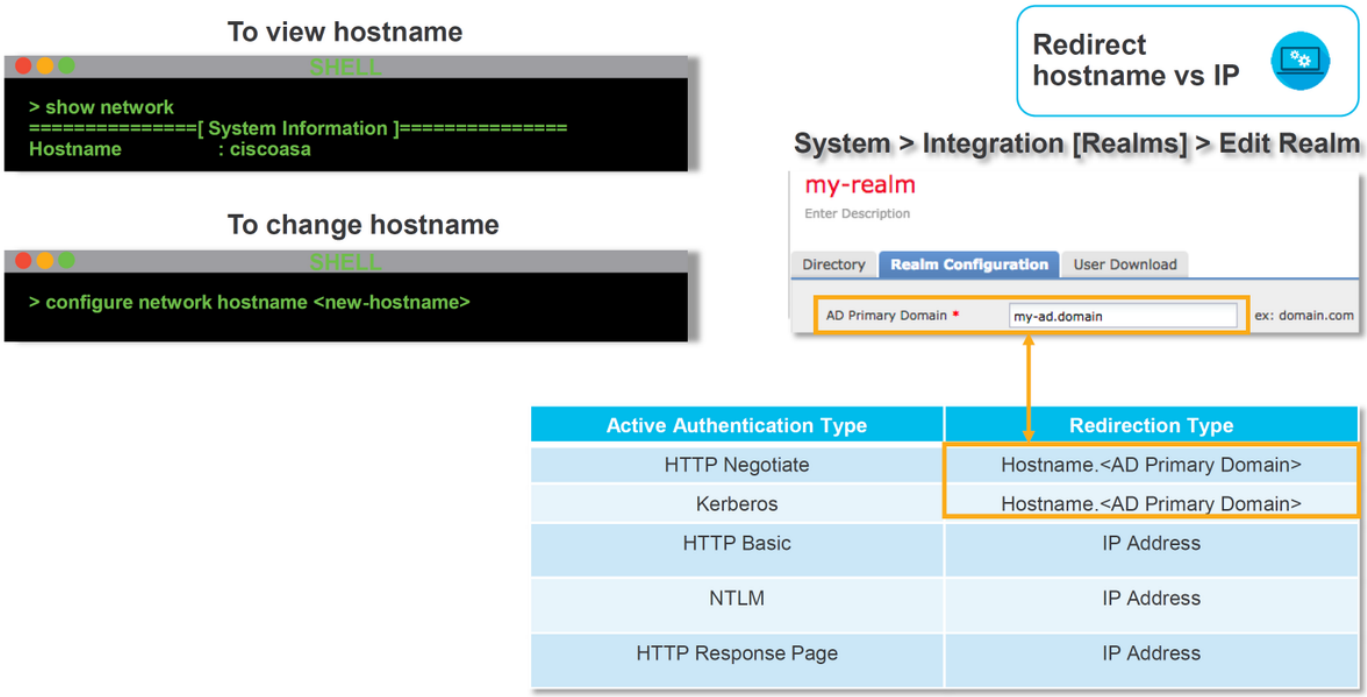
causare interruzioni del traffico sono quelle relative all'autenticazione attiva. L'autenticazione passiva non può causare la perdita imprevista del traffico. È importante tenere presente che solo il traffico HTTP(S) è interessato dall'autenticazione attiva. Se il traffico di altro tipo è influenzato dal mancato funzionamento dell'identità, è più probabile che il criterio utilizzi utenti/gruppi per consentire/bloccare il traffico, pertanto quando la funzionalità di identità non è in grado di identificare gli utenti, possono verificarsi eventi imprevisti, ma questi dipendono dal criterio di controllo di accesso e dal criterio di identità del dispositivo. La risoluzione dei problemi in questa sezione esamina solo i problemi relativi all'autenticazione attiva.

Verificare il metodo di reindirizzamento

Le funzionalità di autenticazione attiva riguardano il dispositivo Firepower che esegue un server HTTP. Quando il traffico soddisfa una regola dei criteri di identità che contiene un'azione di autenticazione attiva, Firepower invia un pacchetto 307 (reindirizzamento temporaneo) nella sessione, in modo da reindirizzare i client al relativo server di portale passivo.

Al momento esistono cinque diversi tipi di autenticazione attiva. Due reindirizzamenti a un nome host costituito dal nome host del sensore e dal dominio primario di Active Directory associato al realm e tre reindirizzamenti all'indirizzo IP dell'interfaccia sul dispositivo Firepower che esegue il reindirizzamento del portale vincolato.

Se si verifica un problema nel processo di reindirizzamento, la sessione può interrompersi in quanto il sito non è disponibile. Per questo motivo è importante comprendere come funziona il reindirizzamento nella configurazione corrente. Il grafico seguente spiega questo aspetto della configurazione.



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

Se l'autenticazione attiva esegue il reindirizzamento al nome host, i client verranno reindirizzati a **cisco.my-ad.domain:<port_used_for_captive_portal>**

Genera acquisizioni pacchetti

La raccolta delle acquisizioni dei pacchetti è la parte più importante della risoluzione dei problemi di autenticazione attiva. L'acquisizione del pacchetto ha luogo su due interfacce:

1. L'interfaccia della periferica Firepower su cui il traffico è in entrata quando si esegue l'autenticazione/identità Nell'esempio seguente, viene usata l'interfaccia **interna**
2. Interfaccia del tunnel interno utilizzata da Firepower per il reindirizzamento al server HTTPS - **tun1** Questa interfaccia viene utilizzata per reindirizzare il traffico al portale vincolatoGli indirizzi IP nel traffico vengono ripristinati agli originali all'uscita

```
> 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 ]
```

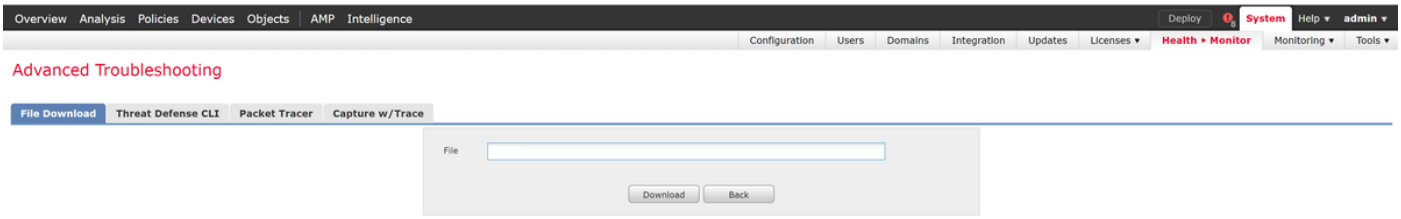
Le due clip vengono avviate, il traffico interessante viene eseguito attraverso il dispositivo Firepower, quindi le clip vengono interrotte.

Il file di acquisizione del pacchetto dell'interfaccia interna, "ins_ntlm", viene copiato nella directory **/mnt/disk0**. Può quindi essere copiato nella directory /var/common in modo da essere scaricato dal dispositivo (**/ngfw/var/common** su tutte le piattaforme FTD):

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

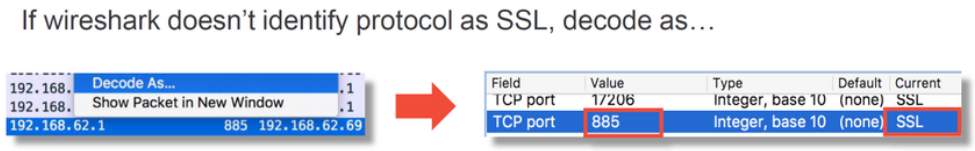
I file di acquisizione dei pacchetti possono quindi essere copiati dal prompt **>** del dispositivo Firepower usando le istruzioni riportate in questo articolo.

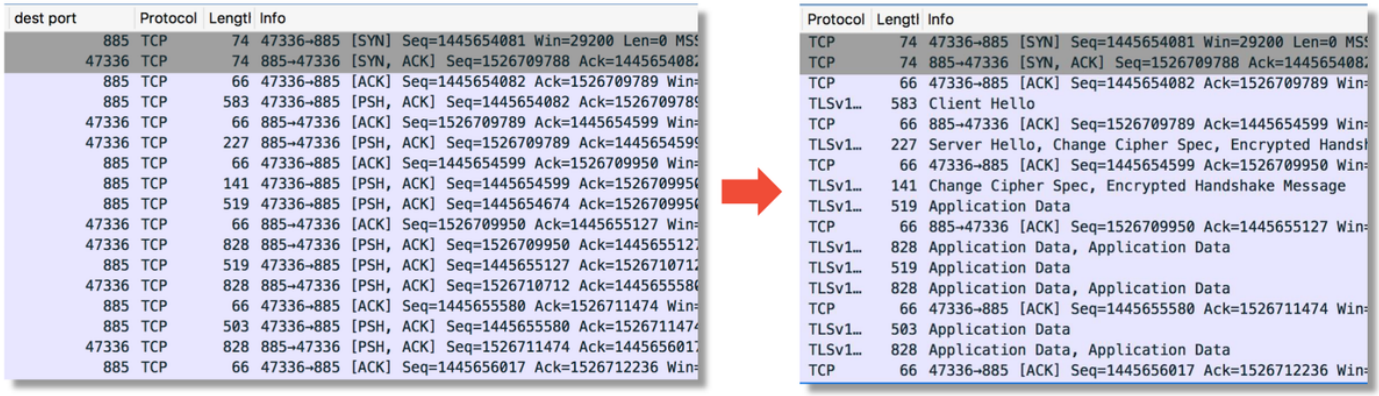
In alternativa, non è disponibile alcuna opzione in Firepower Management Center (FMC) versione 6.2.0 e successive. Per accedere a questa utilità nel FMC, selezionare **Dispositivi > Gestione dispositivi**. Quindi, fare clic sul pulsante  accanto al dispositivo in questione, quindi selezionare **Advanced Troubleshooting > File Download**. È quindi possibile immettere il nome del file in questione e fare clic su Download.



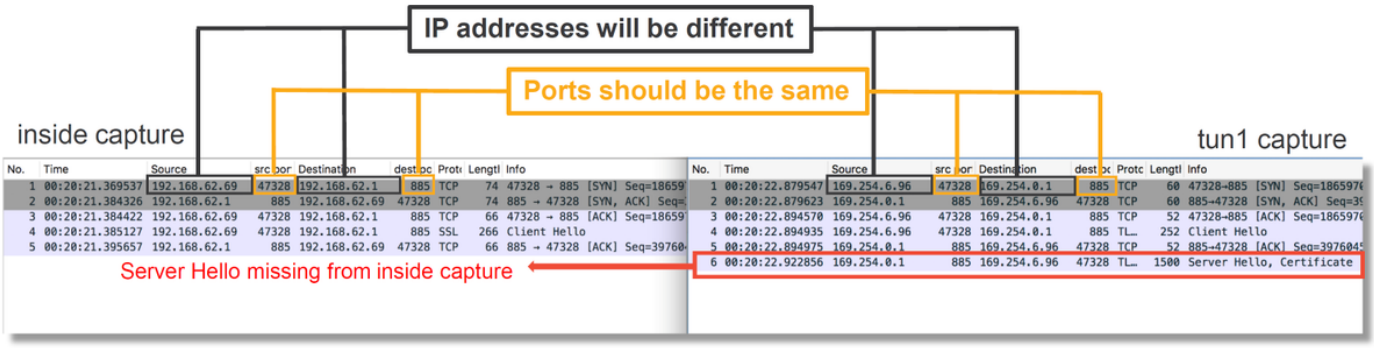
Analisi dei file Packet Capture (PCAP)

L'analisi PCAP in Wireshark può essere eseguita per identificare il problema all'interno delle operazioni di autenticazione attive. Poiché nella configurazione del portale vincolato viene utilizzata una porta non standard (**885** per impostazione predefinita), è necessario configurare Wireshark in modo da decodificare il traffico come SSL.





Ènecessario confrontare l'acquisizione dell'interfaccia interna con l'acquisizione dell'interfaccia del tunnel. Il modo migliore per identificare la sessione in questione in entrambi i file PCAP è individuare la porta di origine univoca, poiché gli indirizzi IP sono diversi.



Nell'esempio precedente, il pacchetto hello del server non è presente nell'acquisizione dell'interfaccia interna. Questo significa che non è mai tornato indietro al cliente. È possibile che il pacchetto sia stato scartato per snort, o forse a causa di un difetto o una configurazione errata.

Nota: Snort controlla il proprio traffico di portale in modo da prevenire attacchi HTTP.

Decrittografia del flusso crittografato

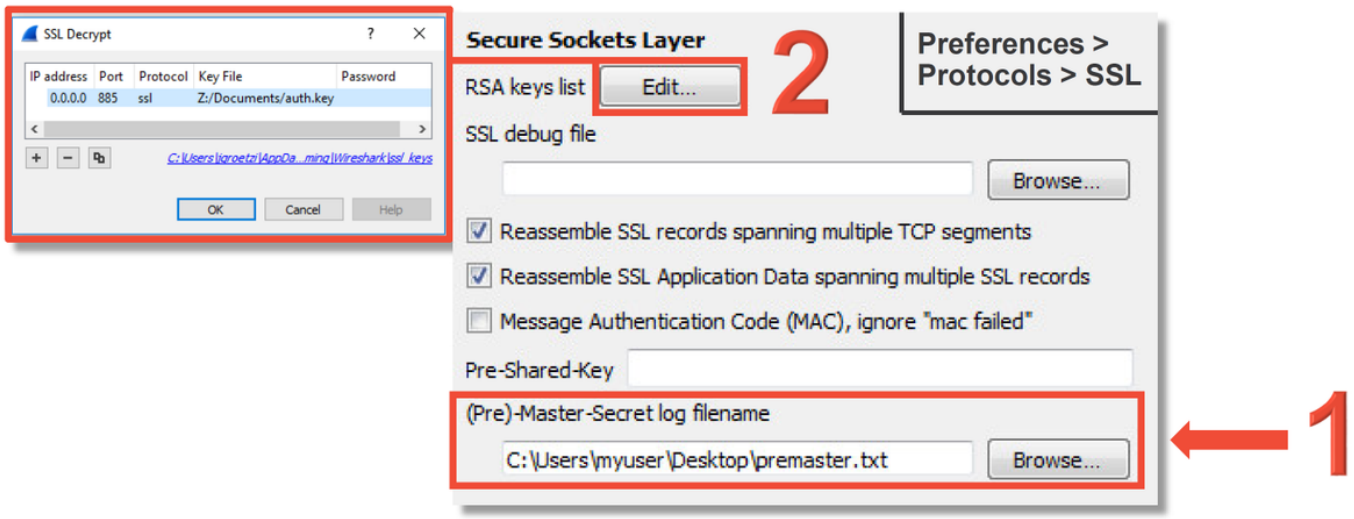
Se il problema non è presente nello stack SSL, potrebbe essere utile decrittografare i dati nel file PCAP in modo da visualizzare il flusso HTTP. Ci sono due metodi per raggiungere questo scopo.

1. Impostazione di una variabile di ambiente in Windows (scelta consigliata, maggiore

protezione) Questo metodo prevede la creazione di un file segreto premaster. A tale scopo, è possibile eseguire il comando seguente (eseguire dal terminale comandi di Windows): **setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"**Una sessione privata può quindi essere aperta in Firefox, in cui è possibile navigare fino al sito in questione, che utilizza SSL.La chiave simmetrica viene quindi registrata nel file specificato nel comando dal passaggio 1 precedente.Wireshark può utilizzare il file per decrittografare utilizzando la chiave simmetrica (vedere il diagramma seguente).

2. Utilizzare la chiave privata RSA (meno sicura, a meno che non si utilizzi un certificato di prova e un utente) La chiave privata da utilizzare è quella utilizzata per il certificato del portale vincolatoQuesta operazione non funziona con dispositivi non RSA (come la curva ellittica) o con dispositivi effimeri (ad esempio Diffie-Hellman)

Attenzione: Se si utilizza il metodo 2, non fornire la chiave privata al Cisco Technical Assistance Center (TAC). È tuttavia possibile utilizzare un certificato di prova temporaneo e una chiave. È inoltre consigliabile utilizzare un utente di prova per il test.



Visualizzazione del file PCAP decrittografato

Nell'esempio seguente, un file PCAP è stato decrittografato. Indica che NTLM è utilizzato come metodo di autenticazione attivo.

```
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
XwHPmh3AkEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
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
```

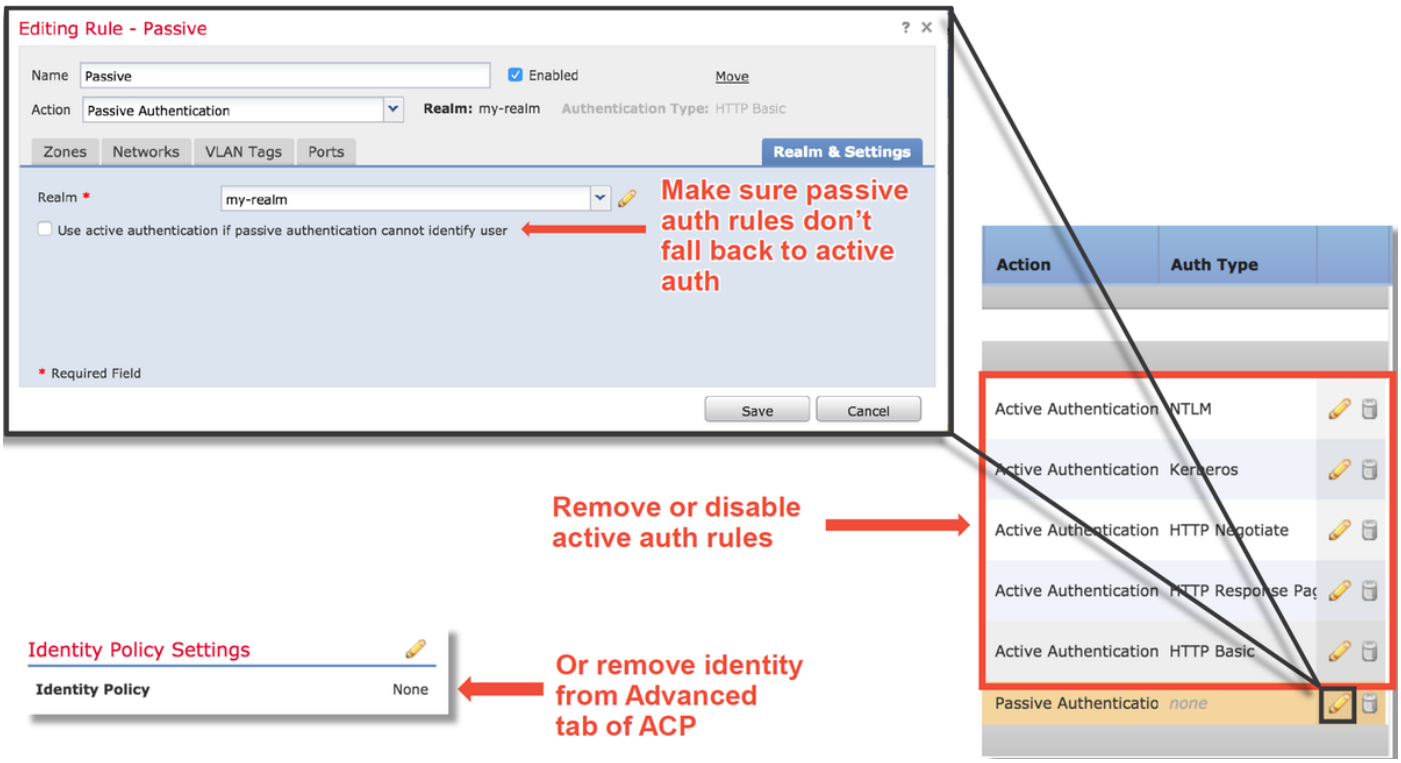
Dopo aver eseguito l'autorizzazione NTLM, il client viene reindirizzato alla sessione originale in modo che possa raggiungere la destinazione prevista, ovvero http://www.cisco.com.

Fasi di mitigazione

Passa solo all'autenticazione passiva

Se utilizzata in un criterio di identità, l'autenticazione attiva è in grado di eliminare il traffico consentito (solo HTTP) in caso di problemi nel processo di reindirizzamento. Per ridurre rapidamente i rischi, è possibile disabilitare qualsiasi regola inclusa nei criteri di identità con l'azione **Autenticazione attiva**.

Verificare inoltre che per le regole con l'opzione 'Autenticazione passiva' come azione non sia selezionata l'opzione 'Utilizza autenticazione attiva se l'autenticazione passiva non è in grado di identificare l'utente'.



Dati da fornire a TAC

Dati	Istruzioni
Risoluzione dei problemi relativi al file da Firepower Management Center (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Risoluzione dei problemi relativi al file dal dispositivo Firepower per il controllo del traffico	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Acquisizioni pacchetti sessione completa	Per istruzioni, vedere questo articolo

Fasi successive

Se è stato determinato che il componente Autenticazione attiva non è la causa del problema, il passaggio successivo consiste nella risoluzione dei problemi relativi alla funzionalità Criteri intrusione.

Fare clic qui per passare all'articolo successivo.