Firepower Data Path Problemen opsporen en verhelpen fase 6: Actieve verificatie

Inhoud

Inleiding

Dit artikel maakt deel uit van een reeks artikelen waarin wordt uitgelegd hoe u het gegevenspad op FirePOWER-systemen systematisch moet oplossen om te bepalen of onderdelen van Firepower invloed kunnen hebben op het verkeer. Raadpleeg het gedeelte Overzicht voor informatie over de architectuur van FirePOWER-platforms en de koppelingen naar de andere artikelen voor probleemoplossing in datacenters.

Dit artikel bestrijkt de zesde fase van de probleemoplossing bij FirePOWER-gegevens, de functie Actieve Verificatie.

Voorwaarden

- Dit artikel heeft betrekking op alle momenteel ondersteunde FirePOWER-platforms
- Het apparaat Firepower moet in Routed Mode worden uitgevoerd

Probleemoplossing voor de actieve verificatiefase

Wanneer je probeert te bepalen of een probleem veroorzaakt is door identiteit, is het belangrijk om te begrijpen welk verkeer deze optie kan beïnvloeden. De enige kenmerken in identiteit zelf die verkeersinterupties kunnen veroorzaken, zijn die welke gerelateerd zijn aan actieve authenticatie. Passieve authenticatie kan geen onverwachts verkeer laten vallen. Het is belangrijk te begrijpen

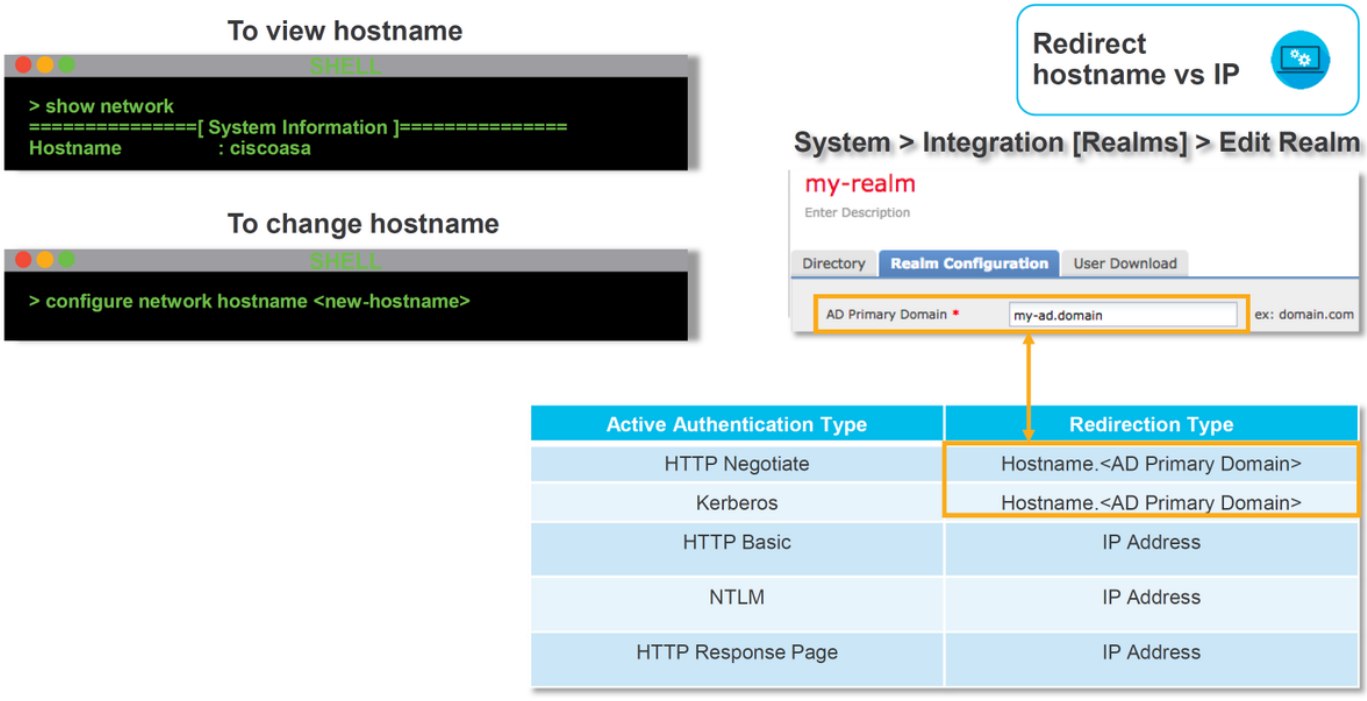
dat alleen HTTP(S)-verkeer wordt beïnvloed door actieve authenticatie. Als ander verkeer wordt beïnvloed omdat de identiteit niet werkt is dit waarschijnlijker omdat het beleid gebruikers/groepen gebruikt om verkeer toe te staan/te blokkeren, zodat wanneer de identiteitsfunctie geen gebruikers kan identificeren, onverwachte dingen kunnen voorkomen, maar het hangt af van het beleid en het identiteitsbeleid van het apparaat. De probleemoplossing in deze sectie doorloopt alleen kwesties die te maken hebben met actieve authenticatie.

Controleer de omleidingsmethode

De actieve authenticatie functies omvatten het Firepower apparaat dat een HTTP server runt. Wanneer het verkeer overeenkomt met een regel voor het identiteitsbeleid die een actie voor actieve verificatie bevat, verstuurt Firepower een 307 (tijdelijke herleiding) pakket naar de sessie zodat klanten naar hun server in gevangenschap kunnen worden doorgestuurd.

Momenteel zijn er vijf verschillende soorten actieve authenticatie. Twee keren terug naar een hostname die uit de hostname van de sensor en het primaire domein van de Actieve Map gebonden aan het gebied bestaat, en drie keren terug naar het IP adres van de interface op het Firepower apparaat dat het gevangen portaal herricht.

Als er iets verkeerd gaat in het herleidingsproces, kan de sessie breken omdat de site niet beschikbaar is. Dit is waarom het belangrijk is om te begrijpen hoe de omleiding in de actieve configuratie werkt. Aan de hand van het schema hieronder kunt u dit configuratieaspect begrijpen.



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

Als actieve authenticatie naar de hostname overhevelt, zou dit het omleiden van de clients naar **ciscoasa.my-ad.domein** zijn:**<port_use_for_host_portal_portal>**

pakketvastlegging genereren

Het verzamelen van pakketvastlegging is het belangrijkste deel van het oplossen van actieve authenticiteitskwesties. De pakketvastlegging vindt op twee interfaces plaats:

1. De interface op het FirePOWER-apparaat dat het verkeer kenmerkt wanneer de identiteit/verificatie wordt uitgevoerd In het onderstaande voorbeeld wordt de **interne** interface gebruikt
2. De interne tunnelinterface die Firepower gebruikt voor omleiding naar de HTTPS-server - **noot 1** Deze interface wordt gebruikt om verkeer terug te sturen naar het portalDe IP-adressen in het verkeer worden bij aanvang terugveranderd in de originals

```
> 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 ]
```

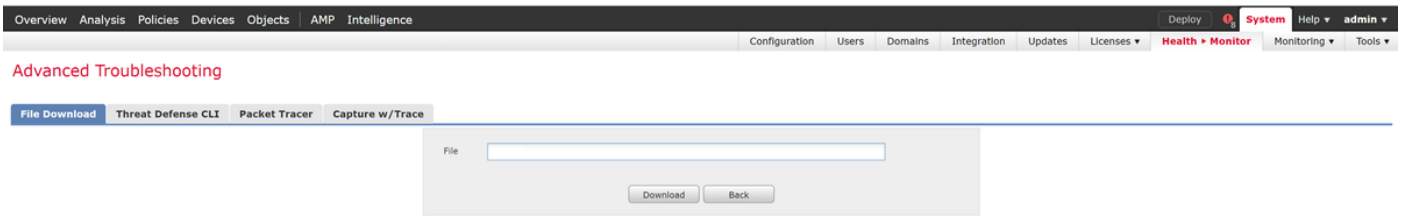
De twee opnamen worden geïnitieerd, het interessante verkeer wordt uitgevoerd door het Firepower apparaat en de opnamen worden gestopt.

Merk op dat het binnenkant van de interface pakketvastlegging bestand, "ins_ntlm", naar de **/mnt/disk0** directory wordt gekopieerd. Het kan vervolgens worden gekopieerd naar de /var/common folder zodat het van het apparaat kan worden gedownload (**/ngfw/var/common** op alle FTD-platforms):

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

De bestanden met de pakketvastlegging kunnen vervolgens uit het FirePOWER-apparaat van de **>**-prompt worden gekopieerd met behulp van de aanwijzingen in dit artikel.

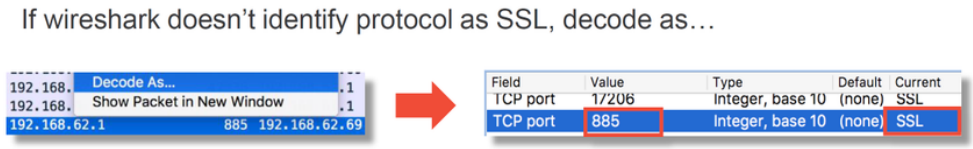
In plaats hiervan is er ook geen optie in het FireSIGHT Management Center (FMC) in Firepower versie 6.2.0 en hoger. Om toegang tot dit hulpprogramma op het FMC te krijgen, navigeer naar **Apparaten > Apparaatbeheer**. Klik vervolgens op de  pictogram naast het apparaat in kwestie, gevolgd door **Advanced Problemen opsporen en verhelpen > Bestand downloaden**. U kunt vervolgens de naam van een bestand in kwestie invoeren en op Downloaden klikken.

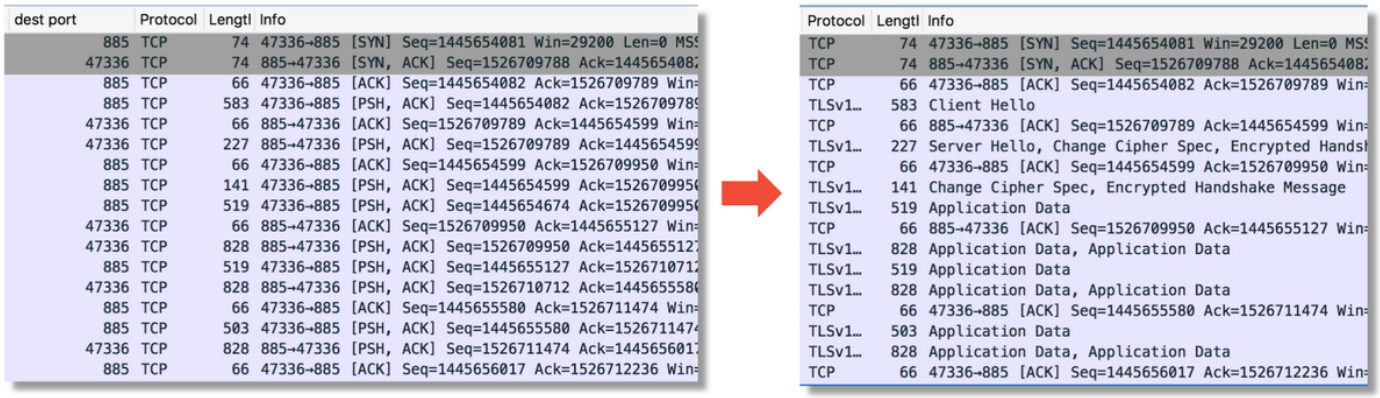


Packet Capture (PCAP) bestandsanalyse

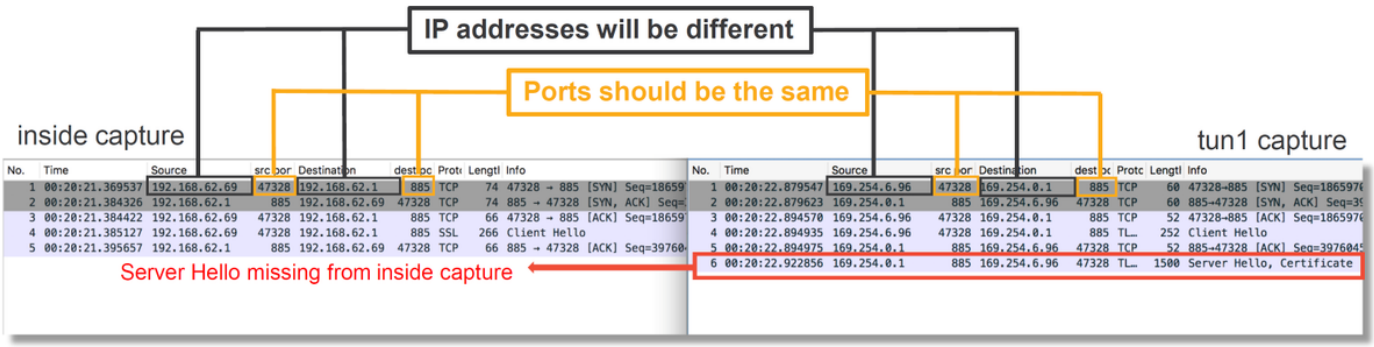
PCAP-analyse in Wireshark kan worden uitgevoerd om het probleem te helpen identificeren

binnen de actieve authenticatieoperaties. Aangezien een niet-standaard poort wordt gebruikt in de configuratie van het gevangen portaal (standaard **885**), moet Wireless-shark worden geconfigureerd om het verkeer als SSL te decoderen.





De interne interface-opname en de tunnelinterface-opname moeten worden vergeleken. De beste manier om de sessie in kwestie in beide PCAP bestanden te identificeren is de unieke bronpoort te vinden omdat de IP-adressen anders zijn.



In het bovenstaande voorbeeld, merk op dat het server hallo pakket ontbreekt in de interne interface-opname. Dit betekent dat het nooit terug is gekomen naar de cliënt. Het is mogelijk dat de pakking door de slang is gevallen of dat dit mogelijk is veroorzaakt door een defect of een defect.

Opmerking: Snort inspecteert haar eigen portaalverkeer om HTTP-exploitatie te voorkomen.

De versleutelde stromen decrypteren

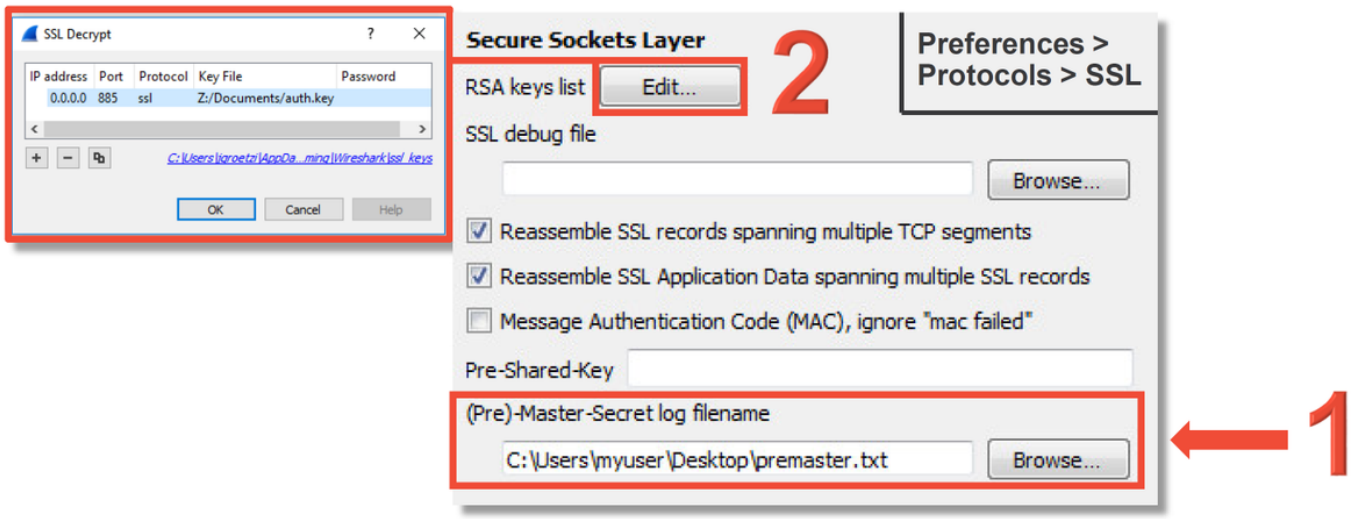
Als het probleem niet in de SSL-stack ligt, kan het voordelig zijn de gegevens in het PCAP-bestand te decrypteren om de HTTP-stream te zien. Er zijn twee methoden om dit te bereiken.

1. Stel een omgevingsvariabele in Windows in (veiliger - aanbevolen) Deze methode houdt in

dat er een geheim bestand wordt gemaakt. Dit kan worden gedaan met de volgende opdracht (vanuit de Windows-opdrachtterminal): **setx SSLKEYOGFILE "%HOMEPATH%\Desktop\premaster.txt"**Een privésessie kan dan worden geopend in Firefox, waarin u naar de site in kwestie kunt bladeren, wat SSL gebruikt.De symmetrische toets wordt vervolgens gelogd naar het bestand dat in de opdracht uit stap 1 hierboven is gespecificeerd.Wireshark kan het bestand gebruiken om te decrypteren met behulp van de symmetrische toets (zie diagram hieronder).

2. Gebruik de privé-toets van RSA (minder veilig, tenzij met een testcertificaat en een gebruiker) De te gebruiken particuliere sleutel is die die wordt gebruikt voor het certificaat voor het gevangen portaalDit werkt niet voor niet-RSA (zoals Elliptische Curve) of voor wat dan ook (Diffie-Hellman, bijvoorbeeld)

Voorzichtig: Als methode 2 wordt gebruikt, zorg dan niet voor Cisco Technical Assistance Center (TAC) op uw privé-toets. Er kan echter een tijdelijk testcertificaat en -sleutel worden gebruikt. Ook bij de tests moet een testgebruiker worden gebruikt.



Het gedecrypteerde PCAP-bestand bekijken

In het onderstaande voorbeeld is een PCAP-bestand versleuteld. Hieruit blijkt dat NTLM wordt gebruikt als de actieve authenticatiemethode.

```
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
```

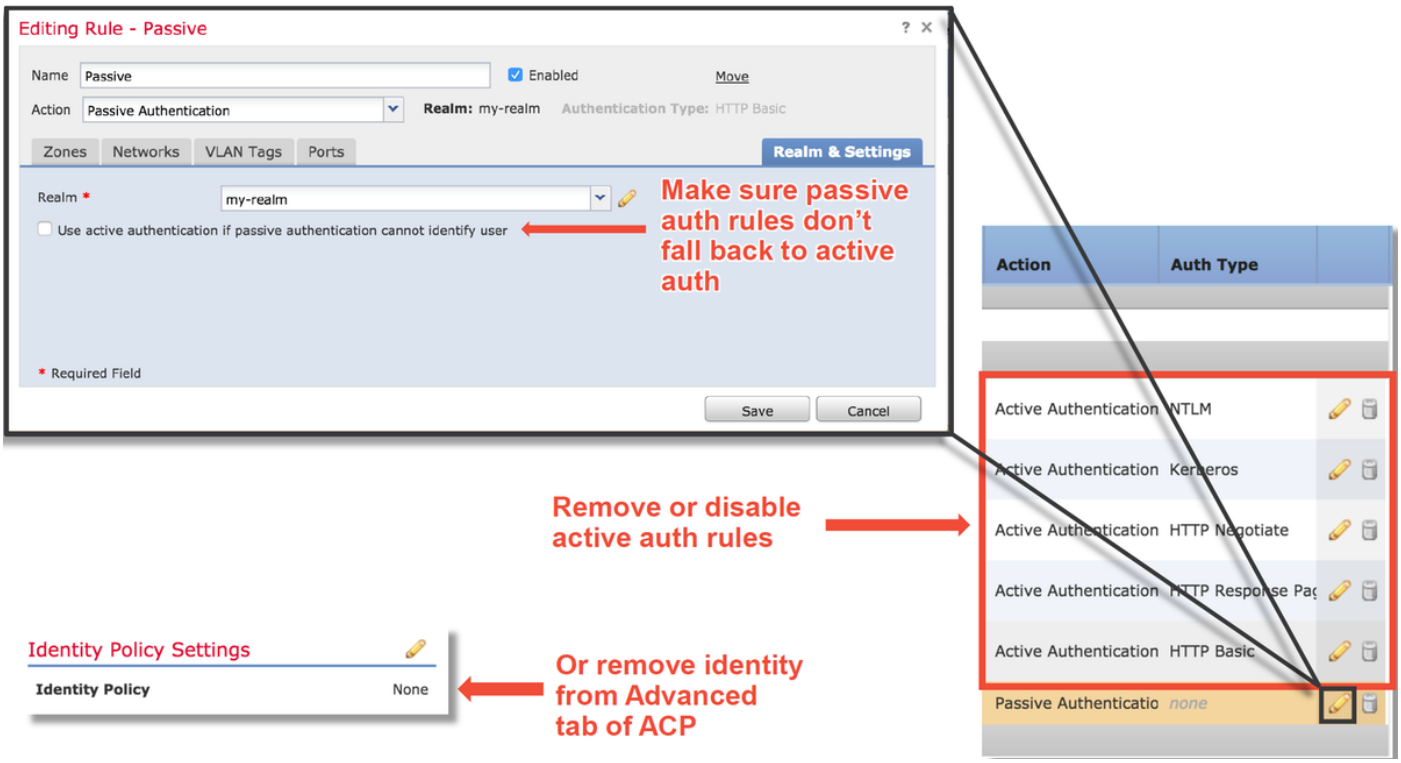
Nadat de NTLM-vergunning heeft plaatsgevonden, wordt de cliënt terugverwezen naar de oorspronkelijke sessie, zodat hij zijn beoogde bestemming, http://www.cisco.com, kan bereiken.

Beperkingsstappen

Alleen overschakelen naar passieve verificatie

Wanneer gebruikt in een identiteitsbeleid, heeft actieve verificatie de mogelijkheid om toegestaan (HTTP(s)-verkeer alleen te laten vallen) als er iets verkeerd gaat in het herleidingsproces. Een snelle matigingsstap is om om het even welke regel binnen het Beleid van de Identiteit met de actie van **Actieve Verificatie** uit te schakelen.

Zorg er ook voor dat alle regels met 'Passive Verificatie' als actie niet de optie 'Actieve authenticatie gebruiken indien passieve authenticatie geen gebruiker kan identificeren' hebben ingeschakeld.



Gegevens om te leveren aan TAC

Gegevens	Instructies
Probleemoplossing via het FireSIGHT Management Center (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Probleemoplossing bestand via het FirePOWER-apparaat dat het verkeer controleert	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Volledige pakketvastlegging voor sessie	Zie dit artikel voor instructies

Volgende stappen

Als is vastgesteld dat de component Actieve Verificatie niet de oorzaak van de kwestie is, dan zou de volgende stap de optie Inbraakbeleid oplossen.

Klik hier om verder te gaan naar het volgende artikel.