

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

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Probleemoplossing voor de actieve verificatiefase](#)

[Controleer de omleidingsmethode](#)

[pakketvastlegging genereren](#)

[Packet Capture \(PCAP\) bestandsanalyse](#)

[De versleutelde stromen decrypteren](#)

[Het gedecrypteerde PCAP-bestand bekijken](#)

[Beperkingsstappen](#)

[Alleen overschakelen naar passieve verificatie](#)

[Gegevens om te leveren aan TAC](#)

[Volgende stappen](#)

## 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.

**To view hostname**

```

SHELL
> show network
===== [ System Information ] =====
Hostname           : ciscoasa
                
```

**To change hostname**

```

SHELL
> configure network hostname <new-hostname>
                
```

**Redirect hostname vs IP**

**System > Integration [Realms] > Edit Realm**

my-realm  
Enter Description

Directory **Realm Configuration** User Download

AD Primary Domain \*  ex: domain.com

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.

If wireshark doesn't identify protocol as SSL, decode as...



dest port	Protocol	Length	Info
885	TCP	74	47336->885 [SYN] Seq=1445654081 Win=29200 Len=0 MSS=
47336	TCP	74	885->47336 [SYN, ACK] Seq=1526709788 Ack=1445654082
885	TCP	66	47336->885 [ACK] Seq=1445654082 Ack=1526709789 Win=
885	TCP	583	47336->885 [PSH, ACK] Seq=1445654082 Ack=1526709789
47336	TCP	66	885->47336 [ACK] Seq=1526709789 Ack=1445654599 Win=
47336	TCP	227	885->47336 [PSH, ACK] Seq=1526709789 Ack=1445654599
885	TCP	66	47336->885 [ACK] Seq=1445654599 Ack=1526709950 Win=
885	TCP	141	47336->885 [PSH, ACK] Seq=1445654599 Ack=1526709950
885	TCP	519	47336->885 [PSH, ACK] Seq=1445654674 Ack=1526709950
47336	TCP	66	885->47336 [ACK] Seq=1526709950 Ack=1445655127 Win=
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526709950 Ack=1445655127
885	TCP	519	47336->885 [PSH, ACK] Seq=1445655127 Ack=1526710712
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526710712 Ack=1445655580
885	TCP	66	47336->885 [ACK] Seq=1445655580 Ack=1526711474 Win=
885	TCP	503	47336->885 [PSH, ACK] Seq=1445655580 Ack=1526711474
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526711474 Ack=1445656017
885	TCP	66	47336->885 [ACK] Seq=1445656017 Ack=1526712236 Win=

Protocol	Length	Info
TCP	74	47336->885 [SYN] Seq=1445654081 Win=29200 Len=0 MSS=
TCP	74	885->47336 [SYN, ACK] Seq=1526709788 Ack=1445654082
TCP	66	47336->885 [ACK] Seq=1445654082 Ack=1526709789 Win=
TLSv1...	583	Client Hello
TCP	66	885->47336 [ACK] Seq=1526709789 Ack=1445654599 Win=
TLSv1...	227	Server Hello, Change Cipher Spec, Encrypted Handsh
TCP	66	47336->885 [ACK] Seq=1445654599 Ack=1526709950 Win=
TLSv1...	141	Change Cipher Spec, Encrypted Handshake Message
TLSv1...	519	Application Data
TCP	66	885->47336 [ACK] Seq=1526709950 Ack=1445655127 Win=
TLSv1...	828	Application Data, Application Data
TLSv1...	519	Application Data
TLSv1...	828	Application Data, Application Data
TCP	66	47336->885 [ACK] Seq=1445655580 Ack=1526711474 Win=
TLSv1...	503	Application Data
TLSv1...	828	Application Data, Application Data
TCP	66	47336->885 [ACK] Seq=1445656017 Ack=1526712236 Win=

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.

**IP addresses will be different**

**Ports should be the same**

inside capture					tun1 capture												
No.	Time	Source	src port	Destination	dest port	Prot	Length	Info	No.	Time	Source	src port	Destination	dest port	Prot	Length	Info
1	00:20:21.369537	192.168.62.69	47328	192.168.62.1	885	TCP	74	47328 -> 885 [SYN] Seq=1865976	1	00:20:22.879547	169.254.6.96	47328	169.254.0.1	885	TCP	60	47328->885 [SYN] Seq=1865976
2	00:20:21.384326	192.168.62.1	885	192.168.62.69	47328	TCP	74	885 -> 47328 [SYN, ACK] Seq=3976045	2	00:20:22.879623	169.254.6.96	885	169.254.6.96	47328	TCP	60	885->47328 [SYN, ACK] Seq=3976045
3	00:20:21.384422	192.168.62.69	47328	192.168.62.1	885	TCP	66	47328 -> 885 [ACK] Seq=1865976	3	00:20:22.894570	169.254.6.96	47328	169.254.0.1	885	TCP	52	47328->885 [ACK] Seq=1865976
4	00:20:21.385127	192.168.62.69	47328	192.168.62.1	885	SSL	266	Client Hello	4	00:20:22.894935	169.254.6.96	47328	169.254.0.1	885	TL	252	Client Hello
5	00:20:21.395657	192.168.62.1	885	192.168.62.69	47328	TCP	66	885 -> 47328 [ACK] Seq=3976045	5	00:20:22.894975	169.254.6.96	885	169.254.6.96	47328	TCP	52	885->47328 [ACK] Seq=3976045
								<b>Server Hello missing from inside capture</b>	6	00:20:22.922856	169.254.6.96	885	169.254.6.96	47328	TL	1500	Server Hello, Certificate

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 versleten 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.

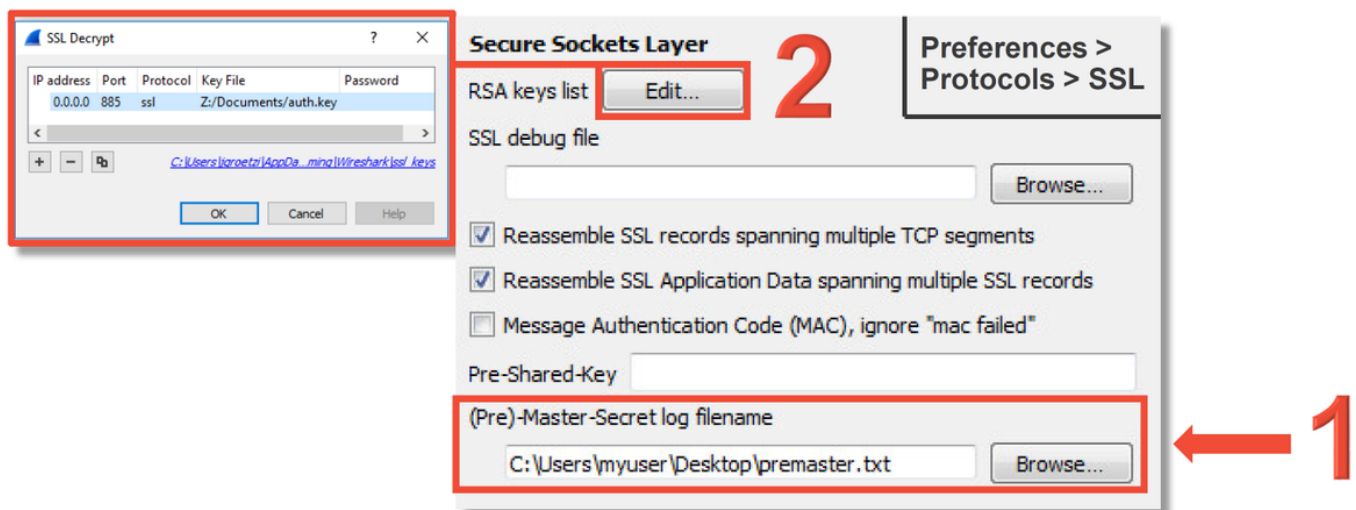
1. Stel een omgevingsvariabele in Windows in (veiliger - aanbevolen) Deze methode houdt in

dat er een geheim bestand wordt gemaakt. Dit kan worden gedaan met de volgende opdracht (vanuit de Windows-opdrachterminal): **setx SSLKEYLOGFILE**

**"%HOMEPATH%\Desktop\premaster.txt"**Een privéessie 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 portaal Dit 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
TLRMTVNTUAAACAAACgAKADgAAAAFgomiqq2eSr157HcAAAAAAAAAKgAqBCAAAAABg0AJQAAAA9KAEcALQBBAEQAAgAKAEoARwAtAEEARAABA
BgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQABAAYGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAYAGEAZA
AuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAUAUAGABgAGcALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAA
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%2Fj71hez1nLh%2F5qfEzgmGjD%2FdQ0EyyRs%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
TLRMTVNTUAAADAAAAGAAAYIqAAABSIVBoAAAAAAAAABYAAAAAGgAaFgAAAAWABYAcgAAAAAAADyAQAAByKIogYBsb0AAAAPI6ZJFPLSnhADl
XaHPmh3AkeAZABtAgkAbgBpAHMAdABYAGEAdABvHIAsgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPw0APpWmMvfnEBQAQAAAAAAKTQuelS1NIBEBvFTnBH0sAAAAAGAKAEoARwAtAEEARAABAgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAyAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAYAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBu
AAUAGABgAGcALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAQAAgAAAwAAAAAAAEAAAAIAAAGnon72xFiGN/nI
+X5HghnlCuVFRnJLs2tch8Vxbrx90KBABAAAJYqfNSUhl1BA9xs44b0V4AkAIgBIAFQVABQAC8AMQg5ADIALgAxADYAOAAuADYAMgAuADEAAAA
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.

**Editing Rule - Passive**

Name: Passive  Enabled Move

Action: Passive Authentication Realm: my-realm Authentication Type: HTTP Basic

Zones Networks VLAN Tags Ports Realm & Settings

Realm \*  Use active authentication if passive authentication cannot identify user **Make sure passive auth rules don't fall back to active auth**

\* Required Field Save Cancel

**Identity Policy Settings**

Identity Policy

Action	Auth Type
Active Authentication	NTLM
Active Authentication	Kerberos
Active Authentication	HTTP Negotiate
Active Authentication	HTTP Response Pa
Active Authentication	HTTP Basic
Passive Authenticatio	none

**Remove or disable active auth rules**

**Or remove identity from Advanced tab of ACP**

## Gegevens om te leveren aan TAC

### Gegevens

Probleemoplossing via het FireSIGHT Management Center (FMC)

Probleemoplossing bestand via het FirePOWER-apparaat dat het verkeer controleert  
Volledige pakketvastlegging voor sessie

### Instructies

<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

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.