

Fase 6 de Troubleshooting de Trayectoria de Datos de Firepower: Autenticación activa

Contenido

[Introducción](#)

[Prerequisites](#)

[Solución de problemas de la fase de autenticación activa](#)

[Verificar el método de redirección](#)

[Generar capturas de paquetes](#)

[Análisis de archivos de captura de paquetes \(PCAP\)](#)

[Descifrado del flujo cifrado](#)

[Visualización del archivo PCAP descifrado](#)

[Pasos de mitigación](#)

[Cambiar sólo a autenticación pasiva](#)

[Datos que se deben proporcionar al TAC](#)

[Pasos siguientes](#)

Introducción

Este artículo forma parte de una serie de artículos que explican cómo resolver sistemáticamente los problemas de la ruta de datos en sistemas Firepower para determinar si los componentes de Firepower pueden estar afectando al tráfico. Consulte el [artículo Descripción general](#) para obtener información sobre la arquitectura de las plataformas Firepower y los enlaces a otros artículos de Troubleshooting de Trayectoria de Datos.

En este artículo se describe la sexta etapa de la solución de problemas de la ruta de datos de Firepower, la función de autenticación activa.



Prerequisites

- Este artículo pertenece a todas las plataformas Firepower soportadas actualmente
- El dispositivo Firepower se debe ejecutar en modo ruteado

Solución de problemas de la fase de autenticación activa

Al intentar determinar si un problema es causado por la identidad, es importante entender qué tráfico puede afectar esta función. Las únicas funciones de la identidad que pueden causar interacciones de tráfico son las relacionadas con la autenticación activa. La autenticación pasiva no puede hacer que el tráfico se descarte inesperadamente. Es importante comprender que sólo

el tráfico HTTP(S) se ve afectado por la autenticación activa. Si hay otro tráfico afectado porque la identidad no funciona, esto es más probable porque la política utiliza usuarios/grupos para permitir/bloquear el tráfico, de modo que cuando la función de identidad no puede identificar a los usuarios, pueden ocurrir cosas inesperadas, pero depende de la política de control de acceso del dispositivo y de la política de identidad. La resolución de problemas de esta sección aborda los problemas relacionados con la autenticación activa solamente.

Verificar el método de redirección

Las funciones de autenticación activas involucran al dispositivo Firepower que ejecuta un servidor HTTP. Cuando el tráfico coincide con una regla de política de identidad que contiene una acción de autenticación activa, Firepower envía un paquete 307 (redirección temporal) a la sesión, para redirigir clientes a su servidor de portal cautivo.

Actualmente hay cinco tipos diferentes de autenticación activa. Dos redirige a un nombre de host que consta del nombre de host del sensor y el dominio primario de Active Directory vinculado al rango, y tres redirige a la dirección IP de la interfaz en el dispositivo Firepower que está realizando la redirección del portal cautivo.

Si algo sale mal en el proceso de redirección, la sesión puede interrumpirse porque el sitio no está disponible. Por este motivo, es importante comprender cómo funciona el redireccionamiento en la configuración en ejecución. El siguiente gráfico ayuda a entender este aspecto de la configuración.

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

Si la autenticación activa se redirige al nombre de host, se redirigiría a los clientes a **ciscoasa.my-ad.domain:<port_used_for_captive_portal>**

Generar capturas de paquetes

La recolección de capturas de paquetes es la parte más importante de la resolución de problemas de autenticación activa. Las capturas de paquetes tienen lugar en dos interfaces:

1. La interfaz en el dispositivo Firepower que el tráfico ingresa cuando se realiza la identidad/autenticación En el siguiente ejemplo, se utiliza la interfaz **interna**
2. La interfaz de túnel interna que Firepower utiliza para redireccionar al servidor HTTPS - **tun1**
Esta interfaz se utiliza para redirigir el tráfico al portal cautivo Las direcciones IP del tráfico se cambian de nuevo a los originales al salir

```

> 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 ]

```

Las dos capturas se inician, el tráfico interesante se ejecuta a través del dispositivo Firepower y luego se detienen las capturas.

Observe que el archivo de captura de paquetes de la interfaz interna, "ins_ntlm", se copia en el directorio **/mnt/disk0**. A continuación, se puede copiar en el directorio **/var/common** para descargarlo del dispositivo (**/ngfw/var/common** en todas las plataformas FTD):

```

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

```

Los archivos de captura de paquetes se pueden copiar del dispositivo Firepower desde el mensaje > usando las direcciones de este [artículo](#).

Alternativamente, no hay opción en Firepower Management Center (FMC) en Firepower versión 6.2.0 y posterior. Para acceder a esta utilidad en el FMC, navegue hasta **Dispositivos >**



Administración de dispositivos. A continuación, haga clic en el botón **Resolución de problemas avanzada > Descarga de archivos.** A continuación, puede introducir el nombre de un archivo en cuestión y hacer clic en Descargar.

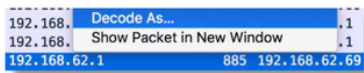


Análisis de archivos de captura de paquetes (PCAP)

El análisis de PCAP en Wireshark se puede realizar para ayudar a identificar el problema dentro de las operaciones de autenticación activas. Dado que un puerto no estándar se utiliza en la configuración del portal cautivo (**885** de forma predeterminada), Wireshark debe configurarse para

decodificar el tráfico como SSL.

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



Field	Value	Type	Default	Current
TCP port	17206	Integer, base 10	(none)	SSL
TCP port	885	Integer, base 10	(none)	SSL

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 Handshake Message
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=

Se deben comparar la captura de la interfaz interna y la captura de la interfaz de túnel. La mejor manera de identificar la sesión en cuestión en ambos archivos PCAP es localizar el puerto de origen único, ya que las direcciones IP son diferentes.

IP addresses will be different

Ports should be the same

inside capture

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
2	00:20:21.384326	192.168.62.1	885	192.168.62.69	47328	TCP	74	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
4	00:20:21.385127	192.168.62.69	47328	192.168.62.1	885	SSL	266	Client Hello
5	00:20:21.395657	192.168.62.1	885	192.168.62.69	47328	TCP	66	885->47328 [ACK] Seq=3976045

Server Hello missing from inside capture

tun1 capture

No.	Time	Source	src port	Destination	dest port	Prot	Length	Info
1	00:20:22.879547	169.254.6.96	47328	169.254.0.1	885	TCP	60	47328->885 [SYN] Seq=1865976
2	00:20:22.879623	169.254.0.1	885	169.254.6.96	47328	TCP	60	885->47328 [SYN, ACK] Seq=3976045
3	00:20:22.894570	169.254.6.96	47328	169.254.0.1	885	TCP	52	47328->885 [ACK] Seq=1865976
4	00:20:22.894935	169.254.6.96	47328	169.254.0.1	885	TL...	252	Client Hello
5	00:20:22.894975	169.254.0.1	885	169.254.6.96	47328	TCP	52	885->47328 [ACK] Seq=3976045
6	00:20:22.922856	169.254.0.1	885	169.254.6.96	47328	TL...	1500	Server Hello, Certificate

En el ejemplo anterior, observe que falta el paquete hello del servidor en la captura de la interfaz interna. Esto significa que nunca regresó al cliente. Es posible que el paquete haya sido descartado por snort, o posiblemente debido a un defecto o configuración incorrecta.

Nota: Snort inspecciona su propio tráfico de portal cautivo para evitar cualquier ataque HTTP.

Descifrado del flujo cifrado

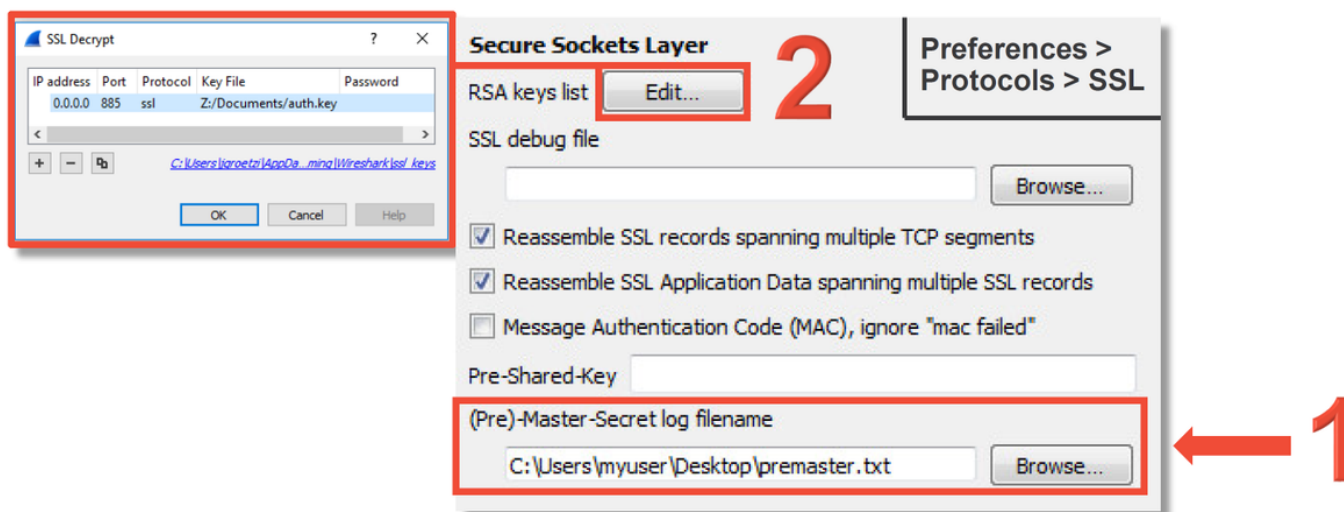
Si el problema no está en la pila SSL, puede ser beneficioso descifrar los datos en el archivo PCAP para ver la secuencia HTTP. Hay dos métodos para lograrlo.

1. Establecer una variable de entorno en Windows (más seguro - recomendado) Este método implica la creación de un archivo secreto premaestro. Esto se puede hacer con el siguiente comando (ejecutar desde el terminal del comando windows): **setx SSLKEYIOGFILE**

"%HOMEPATH%\Desktop\premaster.txt" Una sesión privada se puede entonces abrir en Firefox, en la que se puede navegar hasta el sitio en cuestión, que utiliza SSL. La clave simétrica se registra luego en el archivo especificado en el comando desde el paso 1 anterior. Wireshark puede utilizar el archivo para descifrar mediante la clave simétrica (consulte el diagrama siguiente).

- Utilice la clave privada RSA (menos segura, a menos que utilice un certificado de prueba y un usuario) La clave privada que se utilizará es la utilizada para el certificado del portal cautivo. Esto no funciona para los que no son de RSA (como la curva elíptica) o para nada efímero (Diffie-Hellman, por ejemplo)

Precaución: Si se utiliza el método 2, no proporcione Cisco Technical Assistance Center (TAC) su clave privada. Sin embargo, se puede utilizar un certificado de prueba temporal y una clave. También se debe utilizar un usuario de prueba en las pruebas.



Visualización del archivo PCAP descifrado

En el siguiente ejemplo, se descifró un archivo PCAP. Muestra que NTLM se está utilizando como método de autenticación activo.

```
HTTP/1.1 401 Unauthorized
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
WWW-Authenticate: NTLM
TLRMTVNTUAAACAAAAGAKADgAAAAFgomiqq2eSr157HcAAAAAAAAAAKqAqBCAAAAABg0AJQAAA9KAEcALQBBAEQAAgAKAEoARwAtAEEARAABA
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=9n1DsDbFKVc5%2Fj71hez1nLh%2F5qfEzgmJd%2FdQEyRs%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
TLRMTVNTUADAAAAGAAAYIqAAABSIVBoAAAAAAAAABYAAAAAGqAaAfgAAAAWABYAcgAAAAAAADyAQAAByKIogYBsb0AAAAPI6ZJFPLSnhADl
XuHPmh3AkeAZABtAGkAbgBpAHMAdABYAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPw0APpWmMvfnEBQAQAAAAAAKTQuelS1NIBEBvFTnBHA0sAAAAAGAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAyAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAYAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBu
AAUAGABgAGcALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAQAgAAAwAAAAAAAEAAAAIAAAGnon72xFiGN/nI
+X5Hghn1cuVFRnJLs2tch8Vxbrx9KABAAAjYqfNSUhlBA9xs44b0V4kaIqBIAFQVABQAC8AMQAS5ADIALgAxADYAOAAuADYAMgAuADEAAAA
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
```



Después de que se realice la autorización NTLM, el cliente se redirige a la sesión original, de modo que pueda alcanzar su destino previsto, que es <http://www.cisco.com>.

Pasos de mitigación

Cambiar sólo a autenticación pasiva

Cuando se utiliza en una política de identidad, la autenticación activa tiene la capacidad de descartar tráfico permitido (sólo tráfico HTTP), si algo sale mal en el proceso de redirección. Un paso de mitigación rápido es inhabilitar cualquier regla dentro de la política de identidad con la acción de **Autenticación activa**.

Además, asegúrese de que las reglas con 'Autenticación pasiva' como acción no tengan marcada la opción 'Usar autenticación activa si la autenticación pasiva no puede identificar al usuario'.

Editing Rule - Passive

Name: Enabled Move

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

Zones Networks VLAN Tags Ports **Realm & Settings**

Realm * Make sure passive auth rules don't fall back to active auth

Use active authentication if passive authentication cannot identify user

* Required Field

Save Cancel

Identity Policy Settings

Identity Policy Or remove identity from Advanced tab of ACP

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

Remove or disable active auth rules

Datos que se deben proporcionar al TAC

Datos

Solución de problemas de archivo de Firepower Management Center (FMC)
 Solución de problemas de archivo del dispositivo Firepower que inspecciona el tráfico
 Capturas de paquetes de sesión completa

Instrucciones

<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>

Consulte este artículo para obtener instrucciones

Pasos siguientes

Si se ha determinado que el componente de Autenticación activa no es la causa del problema, el siguiente paso sería resolver el problema de la función Política de intrusiones.

Haga clic [aquí](#) para continuar con el siguiente artículo.