Dépannage du chemin de données Firepower Phase 6 : Authentification active

Contenu

Introduction

Cet article fait partie d'une série d'articles qui expliquent comment dépanner systématiquement le chemin de données sur les systèmes Firepower pour déterminer si les composants de Firepower peuvent affecter le trafic. Reportez-vous à l'article Présentation pour obtenir des informations sur l'architecture des plates-formes Firepower et des liens vers les autres articles de dépannage du chemin de données.

Cet article couvre la sixième étape du dépannage du chemin de données Firepower, la fonctionnalité d'authentification active.

Conditions préalables

- Cet article concerne toutes les plates-formes Firepower actuellement prises en charge
- Le périphérique Firepower doit être exécuté en mode routé

Dépannage de la phase d'authentification active

Lorsque vous essayez de déterminer si un problème est causé par l'identité, il est important de comprendre quel trafic cette fonctionnalité peut avoir un impact. Les seules fonctionnalités de l'identité qui peuvent provoquer des interruptions de trafic sont celles liées à l'authentification active. L'authentification passive ne peut pas entraîner l'abandon inattendu du trafic. Il est

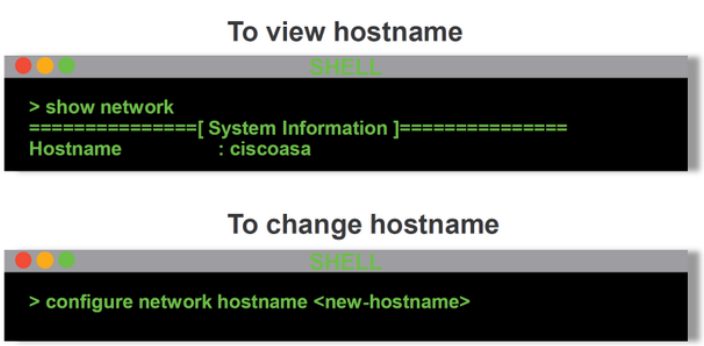
important de comprendre que seul le trafic HTTP(S) est affecté par l'authentification active. Si un autre trafic est affecté parce que l'identité ne fonctionne pas, cela est plus probable car la stratégie utilise des utilisateurs/groupes pour autoriser/bloquer le trafic, de sorte que lorsque la fonctionnalité d'identité ne peut pas identifier les utilisateurs, des choses inattendues peuvent se produire, mais cela dépend de la stratégie de contrôle d'accès du périphérique et de la stratégie d'identité. Le dépannage de cette section passe en revue les problèmes liés à l'authentification active uniquement.

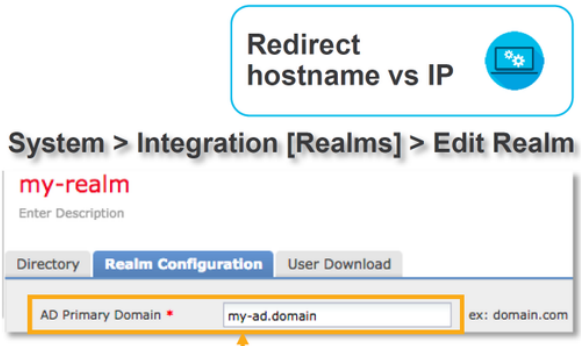
Vérifier la méthode de redirection

Les fonctions d'authentification actives impliquent que le périphérique Firepower exécute un serveur HTTP. Lorsque le trafic correspond à une règle de stratégie d'identité qui contient une action d'authentification active, Firepower envoie un paquet 307 (redirection temporaire) dans la session, afin de rediriger les clients vers son serveur portail captif.

Il existe actuellement cinq types différents d'authentification active. Deux redirigent vers un nom d'hôte qui se compose du nom d'hôte du capteur et du domaine principal Active Directory lié au domaine, et trois redirigent vers l'adresse IP de l'interface sur le périphérique Firepower qui effectue la redirection captive du portail.

Si un problème survient dans le processus de redirection, la session peut se rompre car le site n'est pas disponible. C'est pourquoi il est important de comprendre comment la redirection fonctionne dans la configuration en cours. Le tableau ci-dessous vous aide à comprendre cet aspect de configuration.





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 l'authentification active redirige vers le nom d'hôte, elle redirige les clients vers **ciscoasa.my-ad.domain : <port_used_for_captive_portal>**

Générer des captures de paquets

La collecte de captures de paquets est la partie la plus importante du dépannage des problèmes

d'authentification active. Les captures de paquets ont lieu sur deux interfaces :

1. L'interface sur le périphérique Firepower que le trafic utilise lors de l'identification/authentification Dans l'exemple ci-dessous, l'interface **interne** est utilisée
2. Interface de tunnel interne utilisée par Firepower pour la redirection vers le serveur HTTPS - **tun1** Cette interface est utilisée pour rediriger le trafic vers le portail captifLes adresses IP du trafic sont reconverties en adresses originales en sortie

```
> 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 ]
```

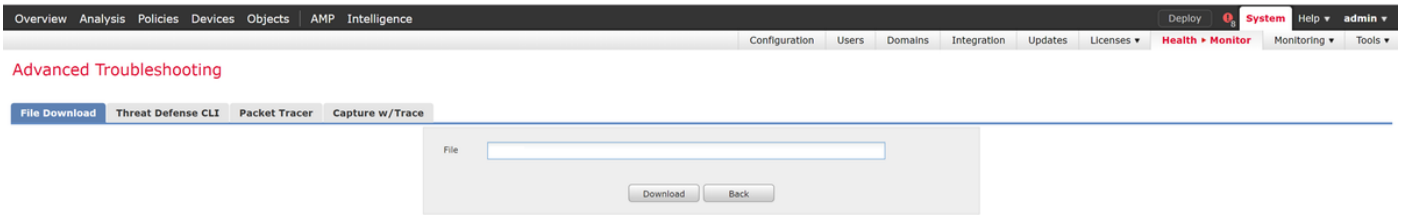
Les deux captures sont initiées, le trafic intéressant est exécuté via le périphérique Firepower, puis les captures sont arrêtées.

Notez que le fichier de capture de paquets de l'interface interne, « ins_ntlm », est copié dans le répertoire **/mnt/disk0**. Il peut ensuite être copié dans le répertoire /var/common afin d'être téléchargé hors du périphérique (**/ngfw/var/common** sur toutes les plates-formes FTD) :

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

Les fichiers de capture de paquets peuvent ensuite être copiés hors du périphérique Firepower à partir de l'invite **>** en suivant les instructions de cet article.

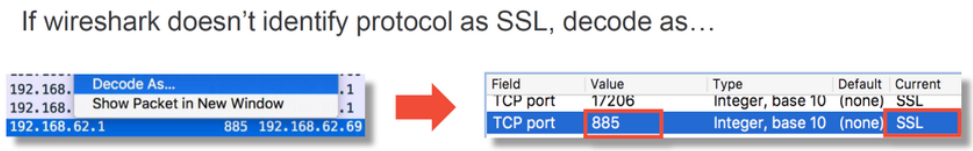
Vous pouvez également choisir Firepower Management Center (FMC) dans Firepower version 6.2.0 et ultérieure. Pour accéder à cet utilitaire sur le FMC, accédez à **Périphériques > Gestion des périphériques**. Cliquez ensuite sur le bouton  en regard du périphérique en question, puis **Dépannage avancé > Téléchargement de fichier**. Vous pouvez ensuite entrer le nom d'un fichier en question et cliquer sur Télécharger.

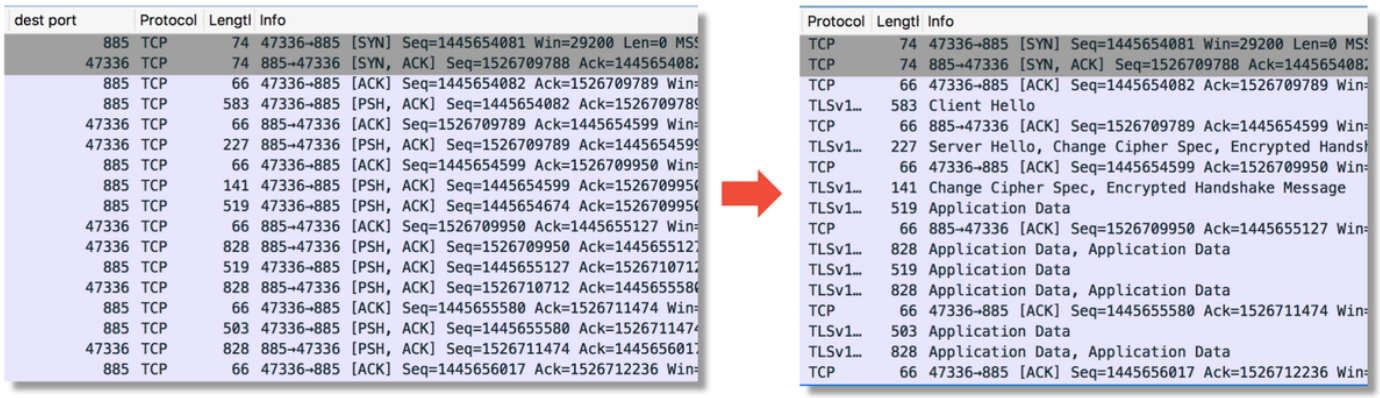


Analyse des fichiers PCAP (Packet Capture)

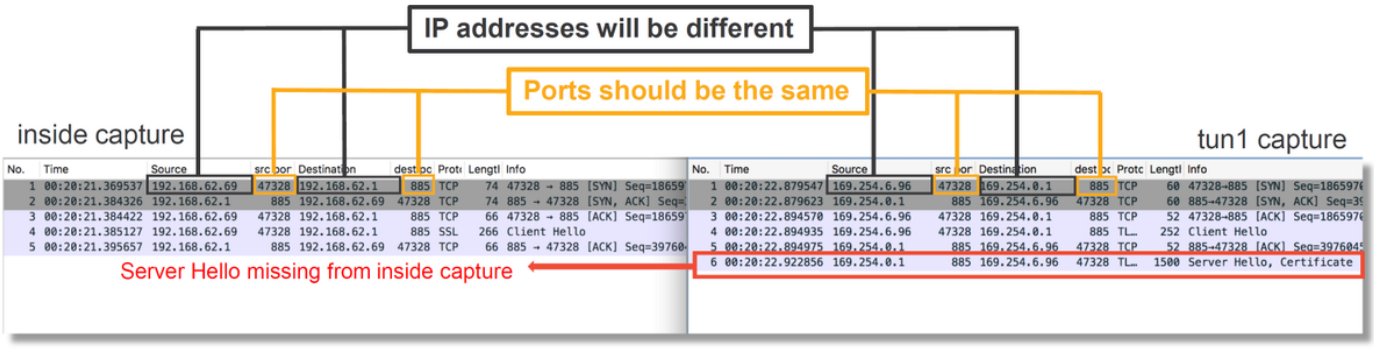
L'analyse PCAP dans Wireshark peut être effectuée pour aider à identifier le problème dans les

opérations d'authentification actives. Comme un port non standard est utilisé dans la configuration du portail captif (**885** par défaut), Wireshark doit être configuré pour décoder le trafic comme SSL.





La capture d'interface interne et la capture d'interface de tunnel doivent être comparées. La meilleure façon d'identifier la session en question dans les deux fichiers PCAP est de localiser le port source unique car les adresses IP sont différentes.



Dans l'exemple ci-dessus, notez que le paquet Hello du serveur est manquant dans la capture d'interface interne. Cela signifie qu'il n'a jamais été rendu au client. Il est possible que le paquet ait été abandonné par snort, ou peut-être en raison d'un défaut ou d'une mauvaise configuration.

> **Note**: Snort inspecte son propre trafic de portail captif afin d'empêcher toute exploitation HTTP.

Décryptage du flux chiffré

Si le problème ne se trouve pas dans la pile SSL, il peut être utile de déchiffrer les données dans le fichier PCAP afin de voir le flux HTTP. Il existe deux méthodes pour y parvenir.

1. Définir une variable d'environnement dans Windows (plus sécurisée - recommandé) Cette méthode implique la création d'un fichier secret de prémaître. Pour cela, utilisez la

commande suivante (exécutez-la à partir du terminal de commande windows) : **setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt "**Une session privée peut alors être ouverte dans Firefox, dans laquelle vous pouvez naviguer jusqu'au site en question, qui utilise SSL.La clé symétrique est ensuite consignée dans le fichier spécifié dans la commande à l'étape 1 ci-dessus.Wireshark peut utiliser le fichier pour le déchiffrement à l'aide de la clé symétrique (voir le schéma ci-dessous).

2. Utiliser la clé privée RSA (moins sécurisée, sauf si vous utilisez un certificat de test et un utilisateur) La clé privée à utiliser est celle utilisée pour le certificat de portail captifCela ne fonctionne pas pour les non-RSA (comme Elliptic Curve) ou tout autre élément éphémère (Diffie-Hellman, par exemple)

Attention : Si la méthode 2 est utilisée, ne fournissez pas votre clé privée au centre d'assistance technique Cisco (TAC). Un certificat et une clé de test temporaires peuvent toutefois être utilisés. Un utilisateur de test doit également être utilisé dans le test.

Affichage du fichier PCAP décrypté

Dans l'exemple ci-dessous, un fichier PCAP a été décrypté. Il montre que NTLM est utilisé comme méthode d'authentification active.

```
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
XwHPmh3AkEAZABtAGkAbgBpAHMAdAByAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPwOAPpWmWMvfnEBAQAAAAAAAKTQueLs1NIBEBvFTnBWA0sAAAAAAgAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAYAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAyAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBsAHQAbwBu
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEGAAQAAgAAAAgAMAAwAAAAAAAAAAEAAAAAIAAAGnon72xFiGN/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
```

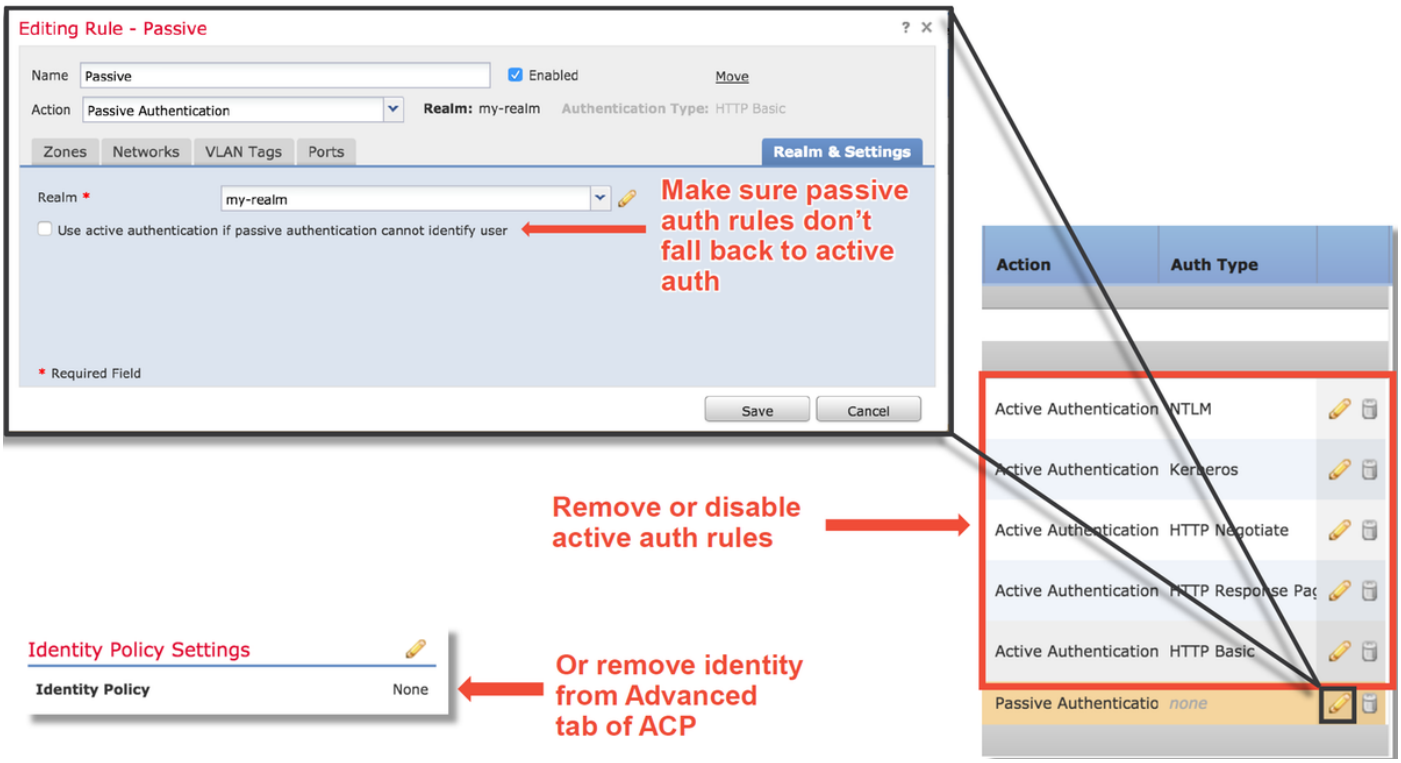
Une fois l'autorisation NTLM effectuée, le client est redirigé vers la session d'origine, afin d'atteindre sa destination prévue, à savoir http://www.cisco.com.

Étapes d'atténuation

Basculer vers l'authentification passive uniquement

Lorsqu'elle est utilisée dans une stratégie d'identité, l'authentification active a la possibilité d'abandonner le trafic autorisé (trafic HTTP(s) uniquement), en cas de problème dans le processus de redirection. Une étape de réduction rapide consiste à désactiver toute règle dans la stratégie d'identité avec l'action d'**Authentification active**.

Assurez-vous également que l'option Utiliser l'authentification active si l'authentification passive ne permet pas d'identifier l'utilisateur n'est pas activée pour toutes les règles avec l'action 'Authentification passive'.



Données à fournir au TAC

Données	Instructions
Dépannage du fichier à partir du Centre de gestion de Firepower (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Dépannage du fichier à partir du périphérique Firepower inspectant le trafic	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Captures de paquets de session complète	Reportez-vous à cet article pour obtenir des instructions.

Étapes suivantes

S'il a été déterminé que le composant Authentification active n'est pas la cause du problème, l'étape suivante consiste à dépanner la fonctionnalité Stratégie d'intrusion.

Cliquez ici pour passer à l'article suivant.