

Firepowerデータパスのトラブルシューティング フェーズ6:アクティブ認証

内容

[概要](#)

[前提条件](#)

[アクティブ認証フェーズのトラブルシューティング](#)

[リダイレクト方式の確認](#)

[パケットキャプチャの生成](#)

[パケットキャプチャ\(PCAP\)ファイル分析](#)

[暗号化されたストリームの復号化](#)

[復号化されたPCAPファイルの表示](#)

[緩和手順](#)

[パッシブ認証のみに切り替え](#)

[TACに提供するデータ](#)

[次のステップ](#)

概要

この記事は、Firepowerシステムのデータパスを体系的にトラブルシューティングし、Firepowerのコンポーネントがトラフィックに影響を与えているかどうかを判断する方法を説明する一連の記事の一部です。Firepowerプラットフォームの[アーキテクチャ](#)に関する情報や、その他のデータパスのトラブルシューティングに関する記事へのリンクについては、概要記事を参照してください。

この記事では、Firepowerのデータパスのトラブルシューティングの6番目の段階であるアクティブ認証機能について説明します。



前提条件

- この記事は、現在サポートされているすべてのFirepowerプラットフォームに関連しています
- Firepowerデバイスがルーテッドモードで動作している必要があります

アクティブ認証フェーズのトラブルシューティング

問題がIDによって引き起こされているかどうかを判断する場合は、この機能が影響を与えるトラフィックを理解することが重要です。トラフィックの中断を引き起こす可能性があるアイデンティティ自体の唯一の機能は、アクティブ認証に関連するものです。パッシブ認証では、トラフィックが予期せずドロップされることはありません。アクティブ認証の影響を受けるのは

HTTP(S)トラフィックだけであることを理解することが重要です。IDが動作していないために他のトラフィックが影響を受ける場合、これはポリシーがユーザ/グループを使用してトラフィックを許可/ブロックするため、ID機能がユーザを特定できない場合は予期せぬ事態が発生する可能性が高くなります。このセクションのトラブルシューティングでは、アクティブ認証のみに関連する問題を順に説明します。

リダイレクト方式の確認

アクティブな認証機能には、HTTPサーバを実行するFirepowerデバイスが含まれます。トラフィックがアクティブ認証アクションを含むアイデンティティポリシールールに一致すると、Firepowerは307 (一時的なリダイレクト) パケットをセッションに送信し、クライアントをキャプティブポータルサーバにリダイレクトします。

現在、アクティブ認証には5種類あります。2つのリダイレクトは、センサーのホスト名と、レルムに関連付けられたActive Directoryプライマリドメインで構成されるホスト名に送信され、3つのリダイレクトは、キャプティブポータルリダイレクトを実行するFirepowerデバイスのインターフェイスのIPアドレスに送信されます。

リダイレクトプロセスで何らかの問題が発生した場合、サイトが使用できないため、セッションが中断する可能性があります。そのため、リダイレクションが実行コンフィギュレーションでどのように動作しているかを理解することが重要です。次の図は、この設定の側面を理解するのに役立ちます。

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

アクティブ認証がホスト名にリダイレクトしている場合、クライアントは `ciscoasa.my-ad.domain:<port_used_for_captive_portal>` にリダイレクトされます

パケットキャプチャの生成

パケットキャプチャの収集は、アクティブな認証の問題のトラブルシューティングで最も重要な部分です。パケットキャプチャは、次の2つのインターフェイスで行われます。

1. アイデンティティ/認証の実行時にトラフィックが入力されるFirepowerデバイスのインターフェイス 次の例では、内部インターフェイスが使用されます
2. FirepowerがHTTPSサーバへのリダイレクションに使用する内部トンネルインターフェイス - tun1 このインターフェイスは、トラフィックをキャプティブポータルにリダイレクトするために使用されます。トラフィックのIPアドレスは、出力時に元のアドレスに戻されます

```
> 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 ]
```

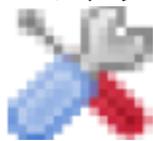
2つのキャプチャが開始され、対象トラフィックがFirepowerデバイスを通じて実行され、キャプチャが停止されます。

内部インターフェイスの packets キャプチャファイル「ins_ntlm」が/mnt/disk0ディレクトリにコピーされることに注目します。次に、デバイスからダウンロードできるように/var/commonディレクトリにコピーできます(すべてのFTDプラットフォームで/ngfw/var/common)。

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

パケットキャプチャファイルは、この記事の指示に従って、>プロンプトからFirepowerデバイスからコピーできます。

または、Firepowerバージョン6.2.0以降のFirepower Management Center(FMC)にはオプションはありません。FMCでこのユーティリティにアクセスするには、[Devices] > [Device



Management]に移動します。次に、 アイコンをクリックし、その後に[Advanced Troubleshooting] > [File Download]をクリックします。その後、該当するファイルの名前を入力し、[Download]をクリックします。



パケットキャプチャ(PCAP)ファイル分析

WiresharkのPCAP分析を実行すると、アクティブな認証操作で問題を特定できます。非標準ポートはキャプティブポータル設定(デフォルトでは885)で使用されるため、SSLなどのトラフィックをデコードするようにWiresharkを設定する必要があります。

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=1445654081 Win=
885	TCP	66	47336->885 [ACK] Seq=1445654082 Ack=1526709789 Win=
885	TCP	583	47336->885 [PSH, ACK] Seq=1445654082 Ack=1526709789 Win=
47336	TCP	66	885->47336 [ACK] Seq=1526709789 Ack=1445654599 Win=
47336	TCP	227	885->47336 [PSH, ACK] Seq=1526709789 Ack=1445654599 Win=
885	TCP	66	47336->885 [ACK] Seq=1445654599 Ack=1526709950 Win=
885	TCP	141	47336->885 [PSH, ACK] Seq=1445654599 Ack=1526709950 Win=
885	TCP	519	47336->885 [PSH, ACK] Seq=1445654674 Ack=1526709950 Win=
47336	TCP	66	885->47336 [ACK] Seq=1526709950 Ack=1445655127 Win=
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526709950 Ack=1445655127 Win=
885	TCP	519	47336->885 [PSH, ACK] Seq=1445655127 Ack=1526710712 Win=
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526710712 Ack=1445655580 Win=
885	TCP	66	47336->885 [ACK] Seq=1445655580 Ack=1526711474 Win=
885	TCP	503	47336->885 [ACK] Seq=1445655580 Ack=1526711474 Win=
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526711474 Ack=1445656017 Win=
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=1445654081 Win=
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=

内部インターフェイスキャプチャとトンネルインターフェイスキャプチャを比較する必要があります。両方のPCAPファイルで問題のセッションを識別する最善の方法は、IPアドレスが異なるため、一意の送信元ポートを見つけることです。

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=1865974
2	00:20:21.384326	192.168.62.1	885	192.168.62.69	47328	TCP	74	885->47328 [SYN, ACK] Seq=3976845
3	00:20:21.384422	192.168.62.69	47328	192.168.62.1	885	TCP	66	47328->885 [ACK] Seq=1865974
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=3976845

No.	Time	Source	src port	Destination	dest port	Prot.	Length	Info
1	00:20:22.879547	169.254.6.96	47328	169.254.6.1	885	TCP	60	47328->885 [SYN] Seq=1865974
2	00:20:22.879623	169.254.6.1	885	169.254.6.96	47328	TCP	60	885->47328 [SYN, ACK] Seq=3976845
3	00:20:22.894570	169.254.6.96	47328	169.254.6.1	885	TCP	52	47328->885 [ACK] Seq=1865974
4	00:20:22.894935	169.254.6.96	47328	169.254.6.1	885	TL..	252	Client Hello
5	00:20:22.894975	169.254.6.1	885	169.254.6.96	47328	TCP	52	885->47328 [ACK] Seq=3976845
6	00:20:22.922856	169.254.6.1	885	169.254.6.96	47328	TL..	1500	Server Hello, Certificate

上記の例では、サーバのhelloパケットが内部インターフェイスキャプチャから欠落していることに注意してください。これは、クライアントに戻されなかったことを意味します。パケットがSnortによってドロップされた可能性があります。また、パケットまたは設定の誤りが原因である可能性もあります(不具合または設定の誤り)。

注：Snortは、HTTPの不正利用を防ぐために、自身のキャプティブポータルトラフィックを検査します。

暗号化されたストリームの復号化

SSLスタックに問題がない場合は、PCAPファイルのデータを復号化してHTTPストリームを表示することが有益な場合があります。これを実現する方法は2つあります。

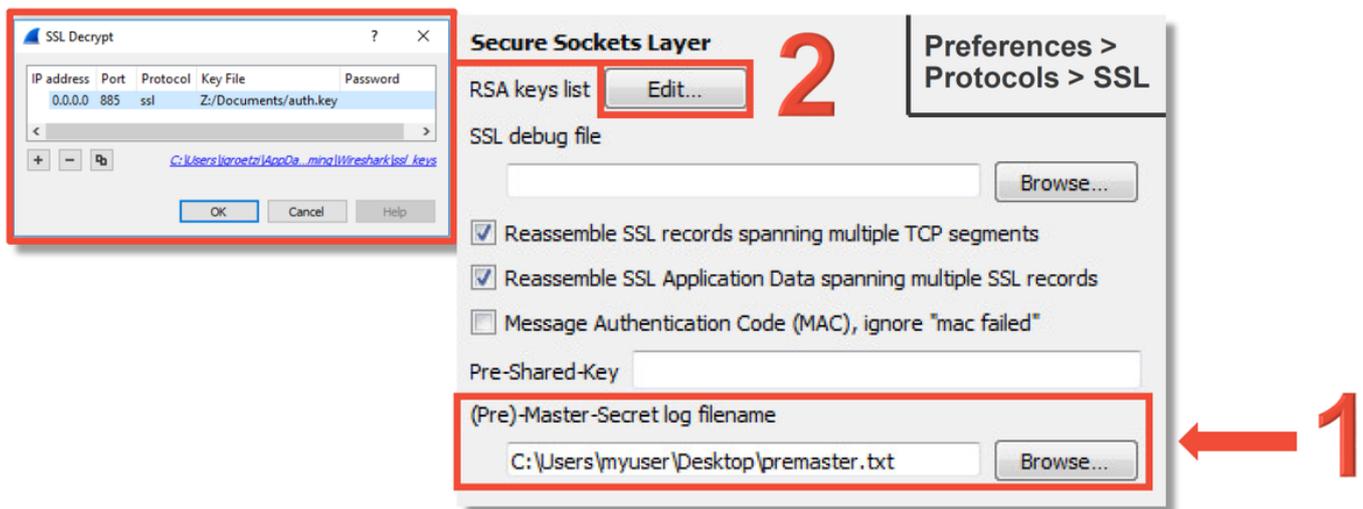
1. Windowsで環境変数を設定する(より安全-推奨) この方法では、プリマスターシークレットファイルを作成します。これは、次のコマンドを使用して実行できます(Windowsのコマンド端末から実行)。`setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"`その後、Firefoxでプライベートセッションを開き、SSLを使用して対象のサイトを参照できま

す。対称キーは、上記のステップ1でコマンドで指定したファイルに記録されます。

Wiresharkは、ファイルを使用して対称キーを使用して復号化できます（次の図を参照）。

2. RSA秘密キーを使用する（テスト証明書とユーザを使用しない限り、セキュリティが低い）
使用する秘密キーは、キャプティブポータル証明書に使用される秘密キーですこれは、非RSA（楕円曲線など）やephemeral（Diffie-Hellmanなど）では動作しません

注意：方法2を使用する場合は、Cisco Technical Assistance Center(TAC)に秘密キーを提供しないでください。ただし、一時的なテスト証明書とキーを使用できます。テストユーザは、テストにも使用する必要があります。



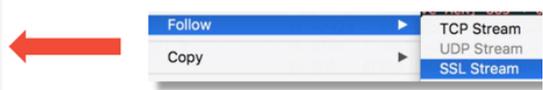
復号化されたPCAPファイルの表示

次の例では、PCAPファイルが復号化されています。NTLMがアクティブ認証方式として使用されていることを示します。

```
HTTP/1.1 401 Unauthorized
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
WWW-Authenticate: NTLM
TLRMTVNTUAAACAAACgAKADgAAAAFgomiqq2eSr157HCAAAAAAAAAAKgAqBCAABAg0AJQAAAA9KAeCALQBBAEQAAKAEoARwAtAEEARAABA
BgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQABAAYGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAYAGEAZA
AuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAAA
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%2F71hezInLh%2F5qfEzgmJd%2FdQYyyRs%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
TLRMTVNTUADAAAGAAAYAIgAAABSAVIBoAAAAAAAAABYAAAAAGgAaAFgAAAAWABYAgAAAAAAADyAQAAABYIogYBsB0AAAAPI6ZJFPLSnhADl
XvHPmh3AKEAZABtAGkAbgBpAHMAdABYAGEAdABVHIASgBHAFIATvBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPwQAPpMmMvfnEBAQAAAAAAAAAKTQuelS1NIBEBvFTnBWA0SAAAAAAGAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAAYAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAMAMgBqAGcALQB3AGkAbgAyADAAMQAYAGEAZAAuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBu
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAGAAQgAAAAAAMAAwAAAAAAAAAAAAAAIAAAGnon72xfIGN/ni
+X5HghnIcUvFRnLs2tch8vrx9KABAAAjYqfNSuHl1BA9xs44b0V4KaIqBIAFQAVABQAC8AMQAS5ADILgAxADYAOAAuADYAMgAuADEAAAA
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=96
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
```



NTLM認証が行われた後、クライアントは元のセッションにリダイレクトされ、意図した宛先

(<http://www.cisco.com>)に到達できるように[なります](#)。

緩和手順

パッシブ認証のみに切り替え

アイデンティティポリシーでアクティブ認証を使用すると、リダイレクトプロセスで何らかの問題が発生した場合に、許可(HTTP(s)トラフィックのみ)をドロップできます。迅速な緩和策は、アクティブ認証のアクションを使用してアイデンティティポリシー内のルールを無効にすることです。

また、[Passive Authentication]がアクションとして設定されているルールで、[Use active authentication if passive authentication cannot identify user]オプションがオンになっていないことを確認します。

The image shows a configuration window titled "Editing Rule - Passive". The "Action" is set to "Passive Authentication" and the "Authentication Type" is "HTTP Basic". A red arrow points to the checkbox "Use active authentication if passive authentication cannot identify user", which is currently unchecked. A red text box next to it says "Make sure passive auth rules don't fall back to active auth". Below this, a table lists authentication rules:

Action	Auth Type	
Active Authentication	NTLM	[edit] [delete]
Active Authentication	Kerberos	[edit] [delete]
Active Authentication	HTTP Negotiate	[edit] [delete]
Active Authentication	HTTP Response Pac	[edit] [delete]
Active Authentication	HTTP Basic	[edit] [delete]
Passive Authentication	none	[edit] [delete]

Red arrows point from the "Remove or disable active auth rules" text to the first five rows of the table. Another red arrow points from the "Or remove identity from Advanced tab of ACP" text to the "Identity Policy" dropdown menu, which is currently set to "None".

TACに提供するデータ

Data
Firepower Management
Center(FMC)からのトラブルシューティングファイル
トラフィックを検査する
Firepowerデバイスからのファイルのトラブルシューティング
フルセッションパケットキャプチャ

手順
<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>

手順については、この記事を参照してください

次のステップ

アクティブ認証コンポーネントが問題の原因ではないと判断された場合、次のステップは、侵入ポリシー機能のトラブルシューティングです。

ここを[クリック](#)して、次の記事に進んでください。