Fehlerbehebung für FirePOWER-Datenpfad Phase 6: Aktive Authentifizierung

Inhalt

Einführung

Dieser Artikel ist Teil einer Reihe von Artikeln, in denen erläutert wird, wie der Datenpfad auf FirePOWER-Systemen systematisch behoben wird, um festzustellen, ob Komponenten von FirePOWER den Datenverkehr beeinträchtigen können. Weitere Informationen zur Architektur von FirePOWER-Plattformen und Links zu anderen Artikeln zur Fehlerbehebung für Datenpfade finden Sie im Übersichtsartikel.

In diesem Artikel wird die sechste Phase der Fehlerbehebung bei Firepower-Datenpfaden beschrieben, die Active Authentication-Funktion.

Voraussetzungen

- Dieser Artikel bezieht sich auf alle derzeit unterstützten Firepower-Plattformen
- Das FirePOWER-Gerät muss im Routing-Modus ausgeführt werden.

Fehlerbehebung in der Phase der aktiven Authentifizierung

Beim Versuch, festzustellen, ob ein Problem durch die Identität verursacht wird, ist es wichtig zu verstehen, welche Auswirkungen diese Funktion auf den Datenverkehr haben kann. Die einzigen Funktionen in der Identität, die Datenverkehrsunterbrechungen verursachen können, sind die Funktionen für die aktive Authentifizierung. Die passive Authentifizierung kann nicht dazu führen,

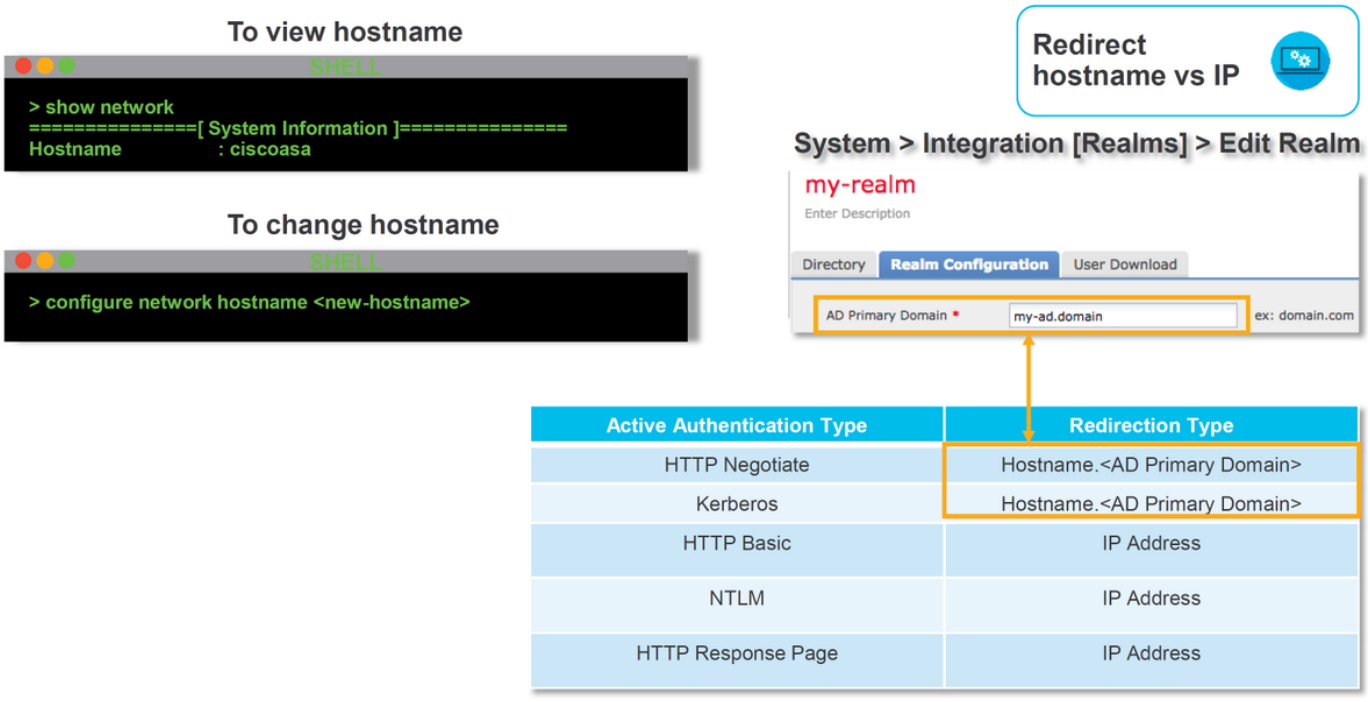
dass Datenverkehr unerwartet verworfen wird. Es ist wichtig zu verstehen, dass nur HTTP(S)-Datenverkehr durch aktive Authentifizierung beeinträchtigt wird. Wenn der andere Datenverkehr beeinträchtigt wird, weil die Identität nicht funktioniert, ist dies wahrscheinlicher, da die Richtlinie Benutzer/Gruppen verwendet, um Datenverkehr zuzulassen/zu blockieren. Wenn die Identitätsfunktion also Benutzer nicht identifizieren kann, können unerwartete Ereignisse auftreten, aber dies hängt von der Richtlinie für die Gerätezugriffskontrolle und der Identitätsrichtlinie ab. Bei der Fehlerbehebung in diesem Abschnitt werden nur Probleme im Zusammenhang mit der aktiven Authentifizierung behandelt.

Überprüfen der Umleitungsmethode

Die aktiven Authentifizierungsfunktionen umfassen das FirePOWER-Gerät, auf dem ein HTTP-Server ausgeführt wird. Wenn der Datenverkehr mit einer Identitätsrichtlinie übereinstimmt, die eine Active Authentication-Aktion enthält, sendet Firepower ein 307-Paket (temporäre Umleitung) an die Sitzung, um Clients an den Captive Portal-Server umzuleiten.

Derzeit gibt es fünf verschiedene Arten der aktiven Authentifizierung. Zwei werden an einen Hostnamen umgeleitet, der aus dem Hostnamen des Sensors und der primären Active Directory-Domäne besteht, die mit dem Bereich verknüpft ist, und drei werden zur IP-Adresse der Schnittstelle auf dem FirePOWER-Gerät umgeleitet, das die Umleitung des Captive Portals durchführt.

Wenn bei der Umleitung etwas schief läuft, kann die Sitzung unterbrochen werden, da die Website nicht verfügbar ist. Aus diesem Grund ist es wichtig zu verstehen, wie die Umleitung in der aktuellen Konfiguration funktioniert. Das folgende Diagramm hilft, diesen Konfigurationsaspekt zu verstehen.



Wenn die aktive Authentifizierung zum Hostnamen umgeleitet wird, werden die Clients an **ciscoasa.my-ad.domain** umgeleitet:**<port_used_for_captive_portal>**

Paketerfassung erstellen

Das Sammeln von Paketerfassungen ist der wichtigste Teil bei der Behebung aktiver Authentifizierungsprobleme. Die Paketerfassung erfolgt an zwei Schnittstellen:

1. Die Schnittstelle auf dem FirePOWER-Gerät, über die der Datenverkehr bei der Durchführung von Identität/Authentifizierung abgeht Im folgenden Beispiel wird die **interne** Schnittstelle verwendet
2. Die interne Tunnelschnittstelle, die FirePOWER für die Umleitung zum HTTPS-Server verwendet - **tun1** Diese Schnittstelle wird verwendet, um Datenverkehr an das Captive Portal umzuleiten.Die IP-Adressen im Datenverkehr werden beim Ausgang wieder in die ursprüngliche Adresse geändert.

```
> 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 ]
```

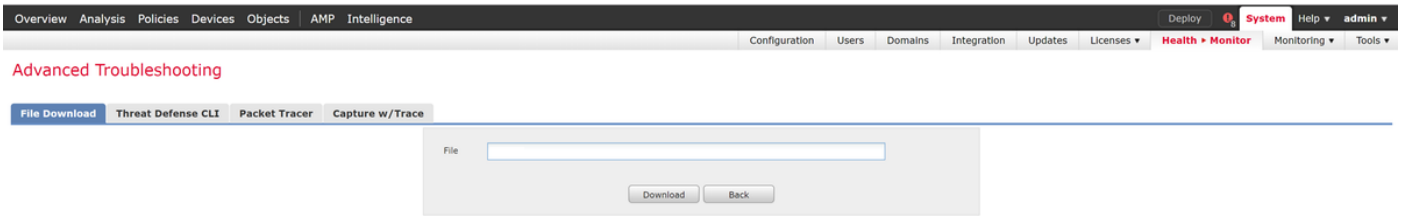
Die beiden Captures werden initiiert, der interessante Datenverkehr wird durch das FirePOWER Gerät, dann werden die Captures gestoppt.

Beachten Sie, dass die interne Schnittstellenpaketerfassungsdatei "ins_ntlm" in das Verzeichnis **/mnt/disk0** kopiert wird. Sie kann dann in das Verzeichnis /var/common kopiert werden, um vom Gerät heruntergeladen zu werden (**/ngfw/var/common** auf allen FTD-Plattformen):

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

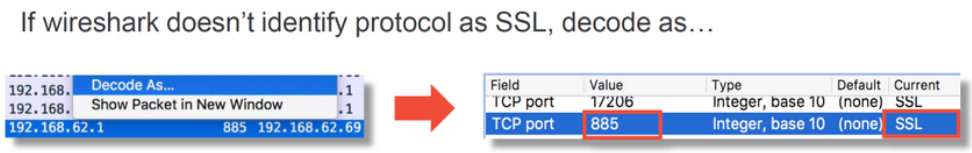
Die Paketerfassungsdateien können dann mithilfe der Anweisungen in diesem Artikel von der Eingabeaufforderung **>** vom FirePOWER-Gerät kopiert werden.

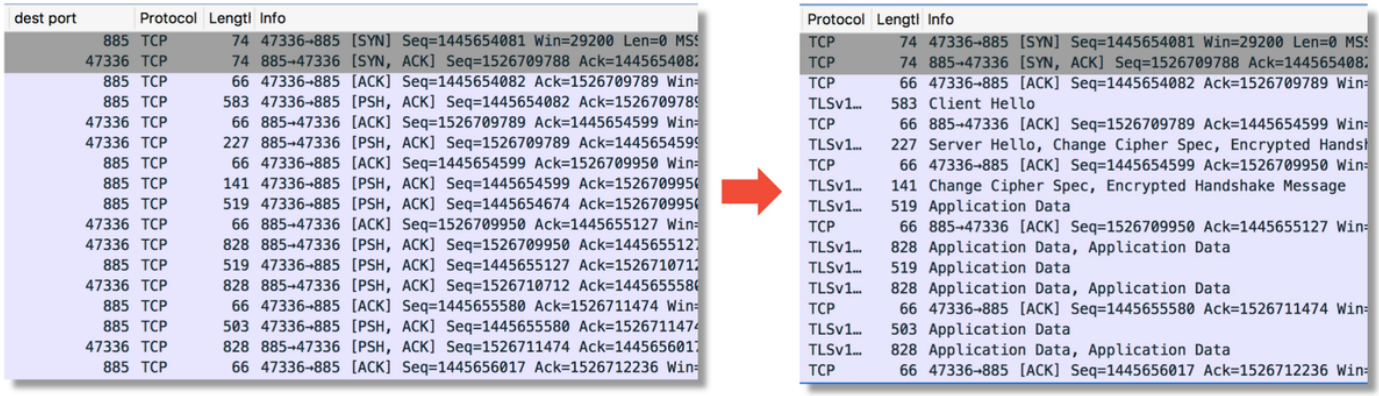
Alternativ gibt es im FirePOWER Management Center (FMC) in FirePOWER 6.2.0 und höher keine Option. Um auf dieses Dienstprogramm im FMC zuzugreifen, navigieren Sie zu **Devices > Device Management (Geräte > Geräteverwaltung)**. Klicken Sie anschließend auf die Schaltfläche  neben dem betreffenden Gerät, gefolgt von **Advanced Troubleshooting > File Download**. Sie können dann den Namen einer Datei eingeben und auf Herunterladen klicken.



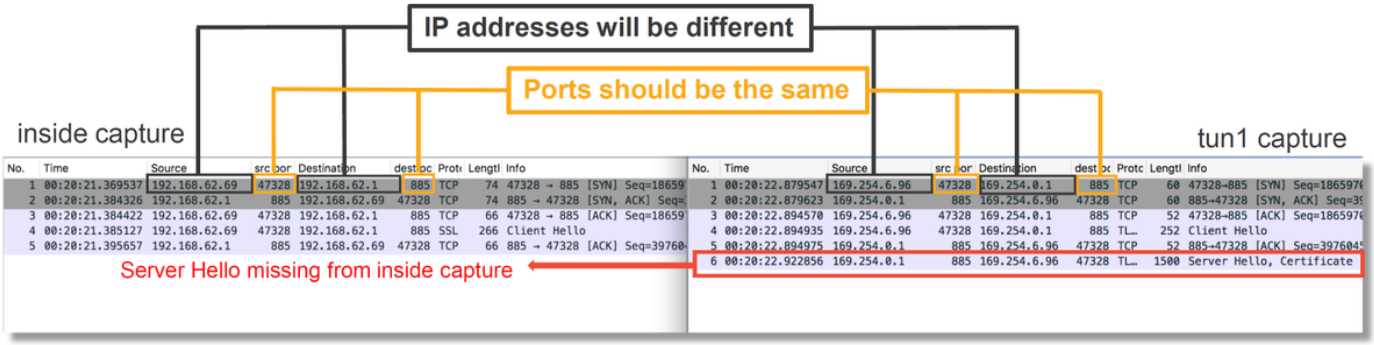
Dateianalyse zur Paketerfassung (PCAP)

Die PCAP-Analyse in Wireshark kann durchgeführt werden, um das Problem innerhalb der aktiven Authentifizierungsvorgänge zu identifizieren. Da ein nicht standardmäßiger Port in der Captive-Portal-Konfiguration verwendet wird (standardmäßig **885**), muss Wireshark so konfiguriert werden, dass der Datenverkehr wie SSL decodiert wird.





Die Erfassung der internen Schnittstelle und die Erfassung der Tunnelschnittstelle sollten verglichen werden. Die beste Möglichkeit, die betreffende Sitzung in beiden PCAP-Dateien zu identifizieren, besteht darin, den eindeutigen Quell-Port zu finden, da die IP-Adressen unterschiedlich sind.



Beachten Sie im obigen Beispiel, dass das Server-Hello-Paket bei der internen Schnittstellenerfassung fehlt. Dies bedeutet, dass es nie wieder zurück zum Kunden. Es ist möglich, dass das Paket nach Sort oder möglicherweise aufgrund eines Fehlers oder einer Fehlkonfiguration verworfen wurde.

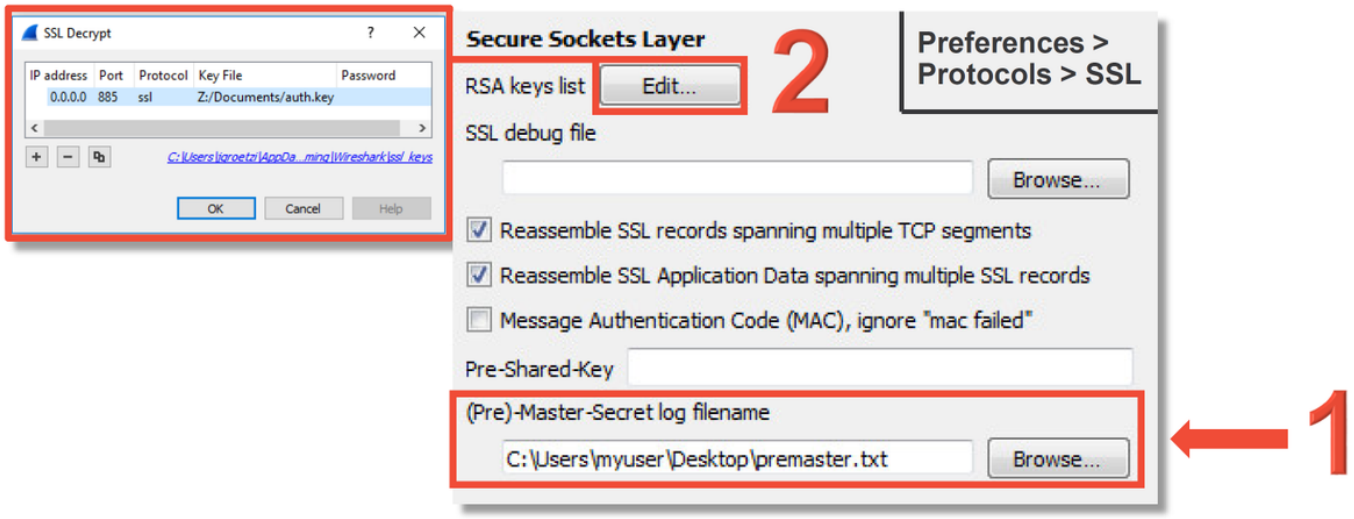
> **Hinweis**: Snort prüft seinen eigenen Captive-Portal-Datenverkehr, um HTTP-Exploits zu verhindern.

Entschlüsseln des verschlüsselten Streams

Wenn das Problem nicht im SSL-Stack vorliegt, kann es von Vorteil sein, die Daten in der PCAP-Datei zu entschlüsseln, um den HTTP-Stream anzuzeigen. Es gibt zwei Methoden, um dies zu erreichen.

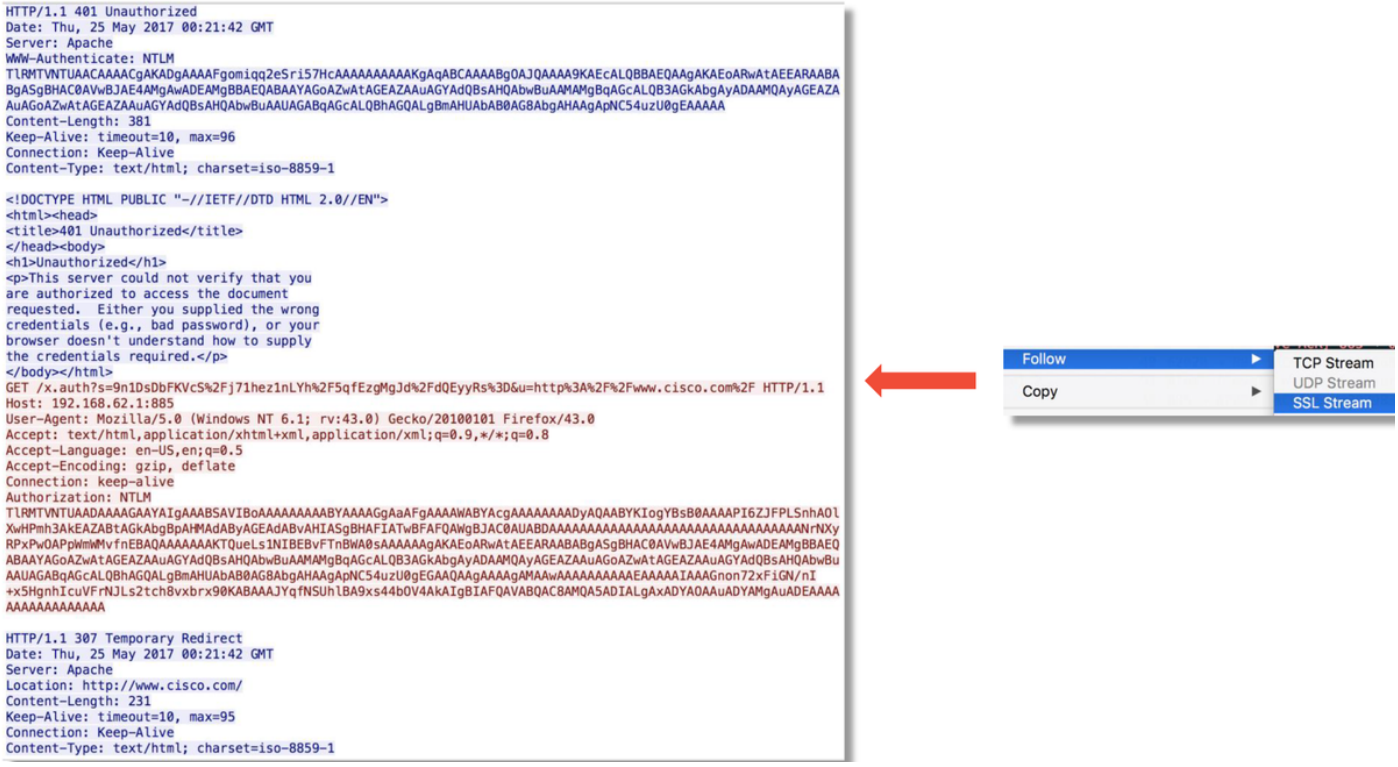
1. Festlegen einer Umgebungsvariablen in Windows (sicherer - empfohlen) Diese Methode umfasst das Erstellen einer geheimen Vormaster-Datei. Dies kann mit dem folgenden Befehl durchgeführt werden (Ausführung über das Windows-Befehlsterminal): **setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"**Eine private Sitzung kann dann in Firefox geöffnet werden, in der Sie zu der betreffenden Website, die SSL verwendet, durchsuchen können.Der symmetrische Schlüssel wird dann in der in Schritt 1 angegebenen Datei protokolliert.Wireshark kann die Datei zum Entschlüsseln mit dem symmetrischen Schlüssel verwenden (siehe Diagramm unten).
2. Verwenden des privaten RSA-Schlüssels (weniger sicher, außer mit einem Testzertifikat und Benutzer) Der verwendete private Schlüssel ist der für das Captive Portal-Zertifikat verwendete Schlüssel.Dies funktioniert nicht für Nicht-RSA (wie Elliptic Curve) oder andere kurzlebige (z. B. Diffie-Hellman)

Vorsicht: Wenn Methode 2 verwendet wird, geben Sie Ihren privaten Schlüssel nicht im Cisco Technical Assistance Center (TAC) an. Es können jedoch ein temporäres Testzertifikat und ein temporärer Schlüssel verwendet werden. Beim Testen sollte auch ein Testbenutzer verwendet werden.



Anzeigen der entschlüsselten PCAP-Datei

Im folgenden Beispiel wurde eine PCAP-Datei entschlüsselt. Es zeigt, dass NTLM als aktive Authentifizierungsmethode verwendet wird.



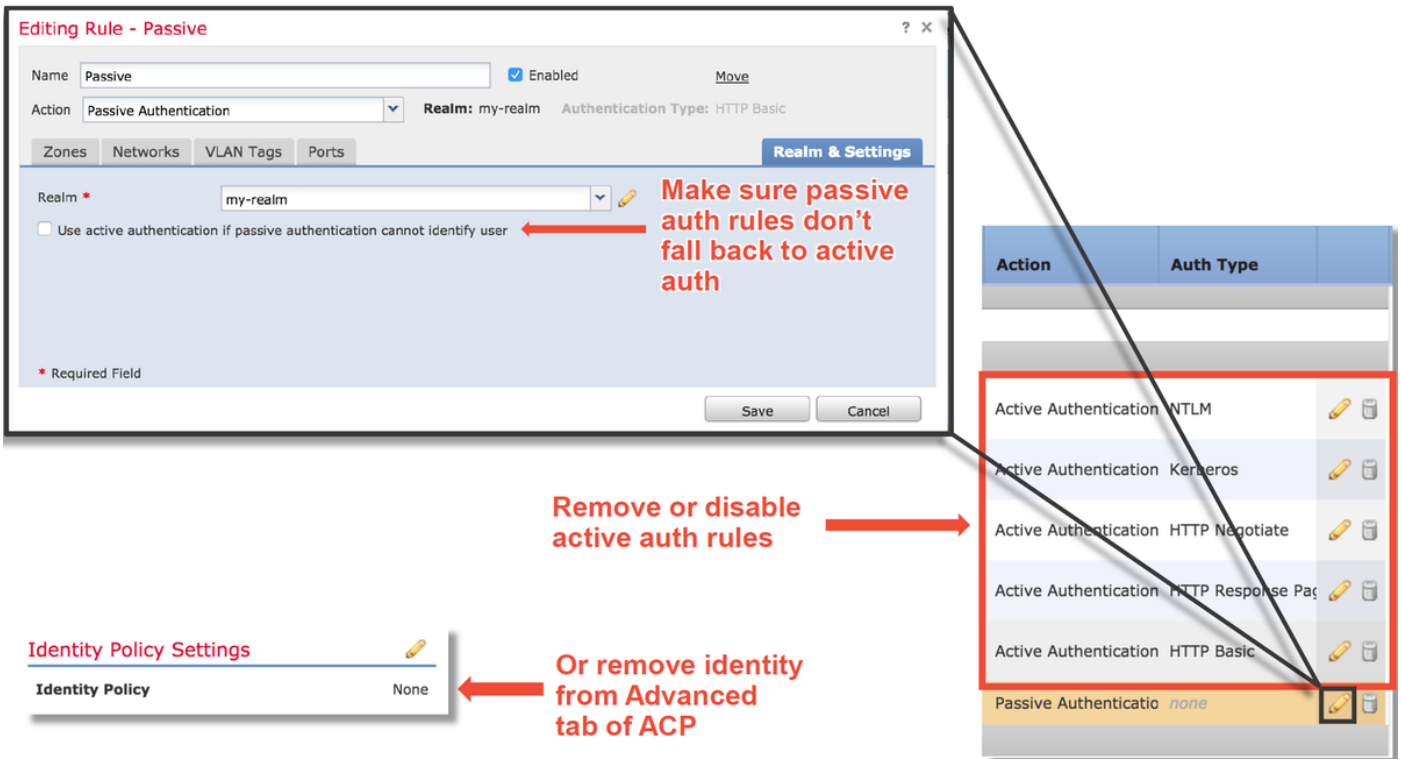
Nach der NTLM-Autorisierung wird der Client zur ursprünglichen Sitzung umgeleitet, sodass er sein beabsichtigtes Ziel erreichen kann, nämlich http://www.cisco.com.

Schritte zur Risikominimierung

Nur zur passiven Authentifizierung wechseln

Bei Verwendung in einer Identitätsrichtlinie kann bei der aktiven Authentifizierung der zulässige (nur HTTP-(s)) Datenverkehr verworfen werden, wenn beim Umleitungsprozess etwas schief läuft. Ein schneller Eindämmungsschritt besteht darin, jede Regel innerhalb der Identitätsrichtlinie mit der Aktion **Active Authentication** zu deaktivieren.

Stellen Sie außerdem sicher, dass bei allen Regeln mit der Aktion 'Passive Authentication' die Option 'Use active authentication if passive authentication cannot identification user' nicht aktiviert ist.



Daten für TAC

Daten	Anweisungen
Fehlerbehebungsdatei vom FirePOWER Management Center (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Paketerfassung für vollständige Sitzungen	Anweisungen hierzu finden Sie in diesem Artikel

Nächste Schritte

Wenn festgestellt wurde, dass die Komponente "Active Authentication" nicht die Ursache des Problems ist, besteht der nächste Schritt darin, eine Fehlerbehebung für die Funktion "Intrusion Policy" (Intrusionsrichtlinie) durchzuführen.

Klicken Sie hier, um mit dem nächsten Artikel fortzufahren.