

Fehlerbehebung für FirePOWER-Datenpfad

Phase 6: Aktive Authentifizierung

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Fehlerbehebung in der Phase der aktiven Authentifizierung](#)

[Überprüfen der Umleitungsmethode](#)

[Paketerfassung erstellen](#)

[Dateianalyse zur Paketerfassung \(PCAP\)](#)

[Entschlüsseln des verschlüsselten Streams](#)

[Anzeigen der entschlüsselten PCAP-Datei](#)

[Schritte zur Risikominimierung](#)

[Nur zur passiven Authentifizierung wechseln](#)

[Daten für TAC](#)

[Nächste Schritte](#)

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.

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

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 top 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):

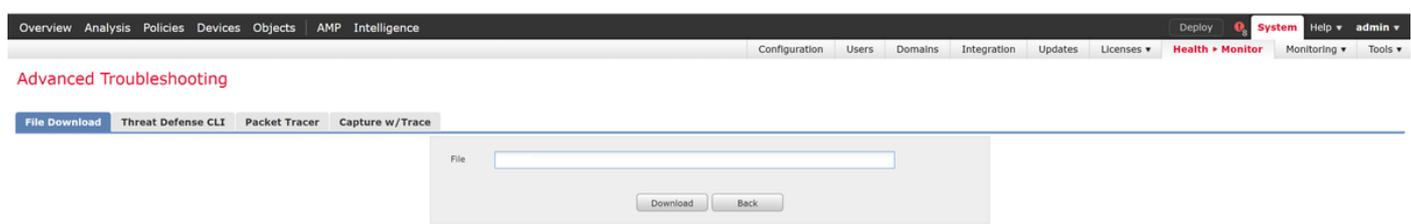
```
> expert
# copy /mnt/disk0/<pcap_file> /var/common/
```

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.

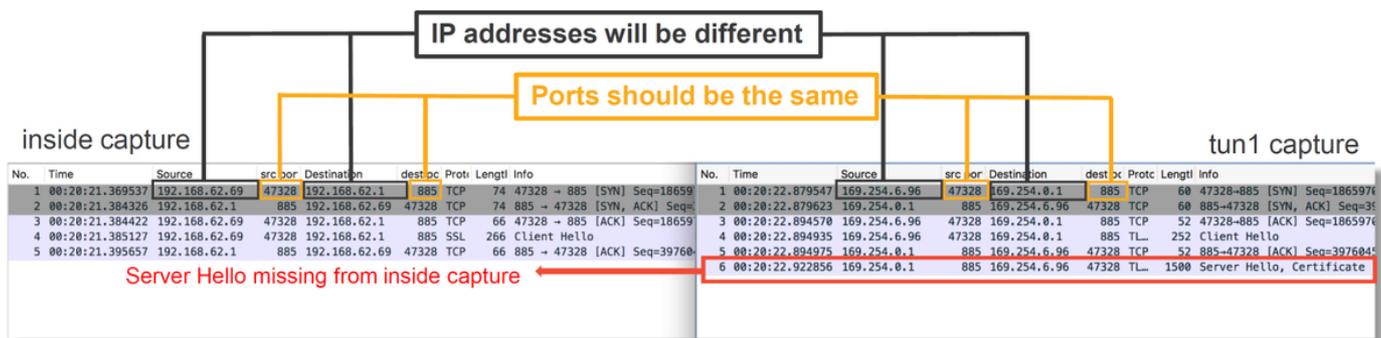
If wireshark doesn't identify protocol as SSL, decode as...



dest port	Protocol	Length	Info
885	TCP	74	47336->885 [SYN, ACK] Seq=1445654081 Win=29200 Len=0 MSS=1460
47336	TCP	74	885->47336 [SYN, ACK] Seq=1526709788 Ack=1445654081 Win=29200 Len=0 MSS=1460
885	TCP	66	47336->885 [ACK] Seq=1445654082 Ack=1526709789 Win=29200 Len=0 MSS=1460
885	TCP	583	47336->885 [PSH, ACK] Seq=1445654082 Ack=1526709789 Win=29200 Len=579
47336	TCP	66	885->47336 [ACK] Seq=1526709789 Ack=1445654599 Win=29200 Len=0 MSS=1460
47336	TCP	227	885->47336 [PSH, ACK] Seq=1526709789 Ack=1445654599 Win=29200 Len=211
885	TCP	66	47336->885 [ACK] Seq=1445654599 Ack=1526709950 Win=29200 Len=0 MSS=1460
885	TCP	141	47336->885 [PSH, ACK] Seq=1445654599 Ack=1526709950 Win=29200 Len=135
885	TCP	519	47336->885 [PSH, ACK] Seq=1445654674 Ack=1526709950 Win=29200 Len=485
47336	TCP	66	885->47336 [ACK] Seq=1526709950 Ack=1445655127 Win=29200 Len=0 MSS=1460
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526709950 Ack=1445655127 Win=29200 Len=812
885	TCP	519	47336->885 [PSH, ACK] Seq=1445655127 Ack=1526710712 Win=29200 Len=485
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526710712 Ack=1445655580 Win=29200 Len=812
885	TCP	66	47336->885 [ACK] Seq=1445655580 Ack=1526711474 Win=29200 Len=0 MSS=1460
885	TCP	503	47336->885 [PSH, ACK] Seq=1445655580 Ack=1526711474 Win=29200 Len=485
47336	TCP	828	885->47336 [PSH, ACK] Seq=1526711474 Ack=1445656017 Win=29200 Len=812
885	TCP	66	47336->885 [ACK] Seq=1445656017 Ack=1526712236 Win=29200 Len=0 MSS=1460

Protocol	Length	Info
TCP	74	47336->885 [SYN] Seq=1445654081 Win=29200 Len=0 MSS=1460
TCP	74	885->47336 [SYN, ACK] Seq=1526709788 Ack=1445654081 Win=29200 Len=0 MSS=1460
TCP	66	47336->885 [ACK] Seq=1445654082 Ack=1526709789 Win=29200 Len=0 MSS=1460
TLSv1...	583	Client Hello
TCP	66	885->47336 [ACK] Seq=1526709789 Ack=1445654599 Win=29200 Len=0 MSS=1460
TLSv1...	227	Server Hello, Change Cipher Spec, Encrypted Handshake Message
TCP	66	47336->885 [ACK] Seq=1445654599 Ack=1526709950 Win=29200 Len=0 MSS=1460
TLSv1...	141	Change Cipher Spec, Encrypted Handshake Message
TLSv1...	519	Application Data
TCP	66	885->47336 [ACK] Seq=1526709950 Ack=1445655127 Win=29200 Len=0 MSS=1460
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=29200 Len=0 MSS=1460
TLSv1...	503	Application Data
TLSv1...	828	Application Data, Application Data
TCP	66	47336->885 [ACK] Seq=1445656017 Ack=1526712236 Win=29200 Len=0 MSS=1460

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.

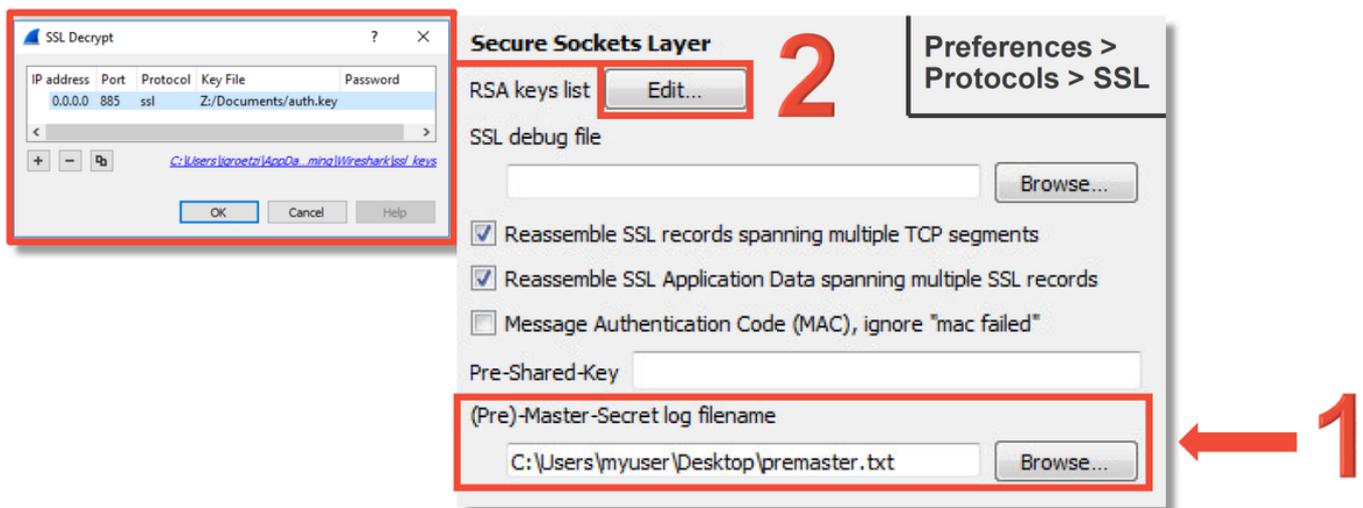
Hinweis: Snort prüft seinen eigenen Captive-Portal-Datenverkehr, um HTTP-Exploits zu verhindern.

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 SSLKEYIOGFILE "%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.



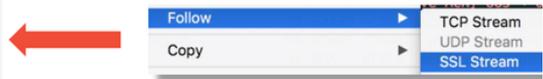
Anzeigen der entschlüsselten PCAP-Datei

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

```
HTTP/1.1 401 Unauthorized
Date: Thu, 25 May 2017 00:21:42 GMT
Server: Apache
WWW-Authenticate: NTLM
TLRMTVNTUAAACAAACgAKADgAAAAFgomiqq2eSr157HcAAAAAAAAAKgAqBCAAAAABg0AJQAAA9KAecALQBBAEQAAgAKAEoARwAtAEEARAABA
BgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQABAAYGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAUAGABgAGALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAA
AuAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAUAGABgAGALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAA
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%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
TLRMTVNTUADAAAGAAAYIqAAABSaVIBoAAAAAAAAABYAAAAAGgAaAFgAAAAWABYAcgAAAAAADyAQAAByKIogYBsb0AAAAPI6ZJFPLSnhAD1
XaHPmh3AkeAZBtAGkAbgBpAHMAdABYAGEAdABvAHIASgBHAFIATwBFAFQAWgBJAC0AUABDAAAAAAAAAAAAAAAAAAAAAAAAANrNXy
RPxPw0APpMmMvfnEBAQAAAAAAKTQuelS1NIBEBvFTnBH0sAAAAAAGAKAEoARwAtAEEARAABABgASgBHAC0AVwBJAE4AMgAwADEAMgBBAEQ
ABAAyAGoAZwAtAGEAZAAuAGYAdQBShAQAbwBuAAUAGABgAGALQBhAGQALgBmAHUAbAB0AG8ABgAHAAGApNC54uzU0gEAAAQAAgAAAwAAAAA
AAAEAAAAIAAGn0n72xFiGN/ni
+x5HghnlcuVFRNjLs2tch8Vxbrx9KABAAAjYqfNSUhl1BA9xs44b0V4kaIgbIAFQVABQAC8AMQASADIALgAxADYAOAAuADYAMgAuADEAAAA
AAAAAAAAAAAA

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
```



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 identify user' nicht aktiviert ist.

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 * my-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 None 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	

Daten für TAC

Daten

Fehlerbehebungsdatei vom FirePOWER Management Center (FMC)
 Fehlerbehebungsdatei vom FirePOWER-Gerät, die den Datenverkehr prüft
 Paketerfassung für vollständige Sitzungen

Anweisungen

<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>

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.