Fase 6 da solução de problemas de caminho de dados do Firepower: Autenticação Ativa

Contents

Introduction

Este artigo faz parte de uma série de artigos que explicam como solucionar problemas sistematicamente no caminho de dados em sistemas Firepower para determinar se os componentes do Firepower podem estar afetando o tráfego. Consulte o artigo Visão geral para obter informações sobre a arquitetura das plataformas Firepower e links para outros artigos de solução de problemas de caminho de dados.

Este artigo aborda o sexto estágio da solução de problemas de caminho de dados do Firepower, o recurso de autenticação ativa.

Prerequisites

- Este artigo se refere a todas as plataformas Firepower suportadas atualmente
- O dispositivo Firepower deve estar em execução no modo roteado

Troubleshooting da Fase de Autenticação Ativa

Ao tentar determinar se um problema é causado pela identidade, é importante entender qual tráfego esse recurso pode afetar. Os únicos recursos na própria identidade que podem causar interrupções de tráfego são os relacionados à autenticação ativa. A autenticação passiva não pode fazer com que o tráfego seja descartado inesperadamente. É importante entender que

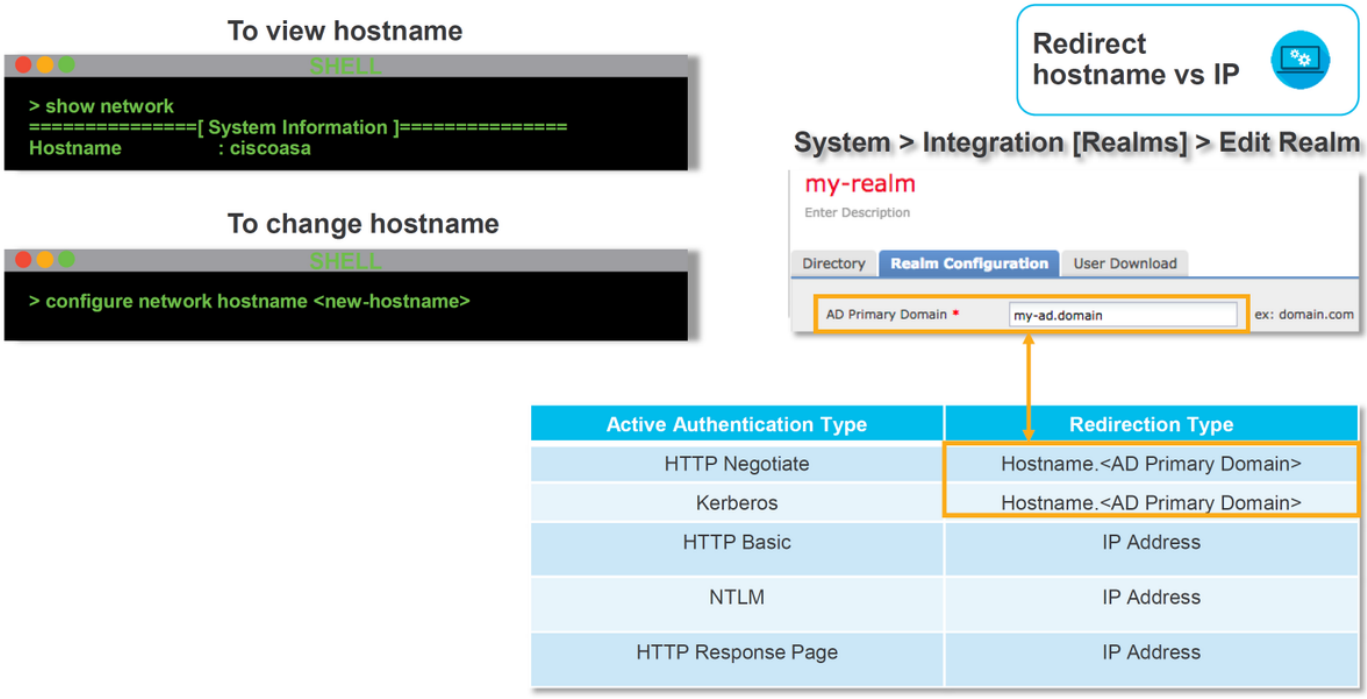
somente o tráfego HTTP(S) é afetado pela autenticação ativa. Se outro tráfego for afetado porque a identidade não está funcionando, isso é mais provável porque a política usa usuários/grupos para permitir/bloquear o tráfego, então quando o recurso de identidade não pode identificar usuários, coisas inesperadas podem ocorrer, mas depende da política de controle de acesso e da política de identidade do dispositivo. A solução de problemas nesta seção apresenta problemas relacionados apenas à autenticação ativa.

Verifique o método de redirecionamento

Os recursos de autenticação ativa envolvem o dispositivo Firepower executando um servidor HTTP. Quando o tráfego corresponde a uma regra de política de identidade que contém uma ação de autenticação ativa, o Firepower envia um pacote 307 (redirecionamento temporário) para a sessão, para redirecionar os clientes para seu servidor de portal cativo.

Existem atualmente cinco tipos diferentes de autenticação ativa. Dois redirecionamentos para um nome de host que consiste no nome de host do sensor e no domínio primário do Ative Diretory vinculado ao território, e três redirecionamentos para o endereço IP da interface no dispositivo Firepower que está executando o redirecionamento do portal cativo.

Se algo der errado no processo de redirecionamento, a sessão pode ser interrompida porque o site não está disponível. É por isso que é importante entender como o redirecionamento está operando na configuração em execução. O gráfico abaixo ajuda a entender esse aspecto de configuração.



Se a autenticação ativa estiver sendo redirecionada para o nome do host, ela redirecionará os clientes para **ciscoasa.my-ad.domain:<port_used_for_cativo_portal>**

Gerar capturas de pacote

A coleta de capturas de pacotes é a parte mais importante da solução de problemas de autenticação ativa. As capturas de pacotes ocorrem em duas interfaces:

1. A interface no dispositivo Firepower que o tráfego está ingressando quando a identidade/autenticação está sendo executada No exemplo abaixo, a interface **interna** é usada
2. A interface de túnel interna que o Firepower usa para redirecionamento para o servidor HTTPS - **tun1** Esta interface é usada para redirecionar o tráfego para o portal cativoOs endereços IP no tráfego são alterados de volta aos originais na saída

```
> 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 ]
```

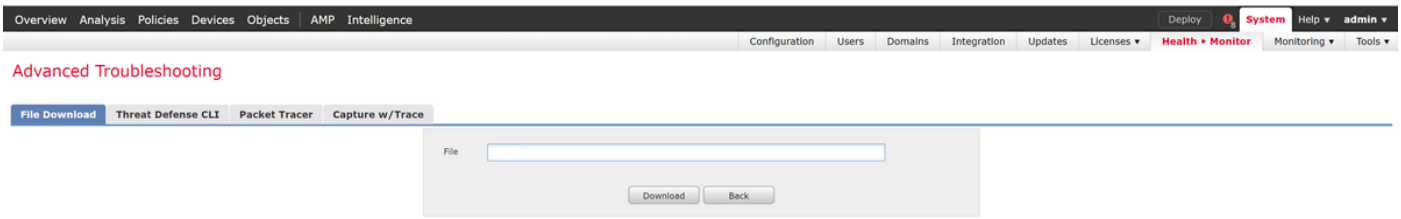
As duas capturas são iniciadas, o tráfego interessante é executado pelo dispositivo Firepower e as capturas são interrompidas.

Observe que o arquivo de captura de pacote da interface interna, "ins_ntlm", é copiado para o diretório **/mnt/disk0**. Em seguida, ele pode ser copiado para o diretório /var/common para ser baixado do dispositivo (**/ngfw/var/common** em todas as plataformas FTD):

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

Os arquivos de captura de pacote podem ser copiados do dispositivo Firepower do prompt **>** usando as instruções neste artigo.

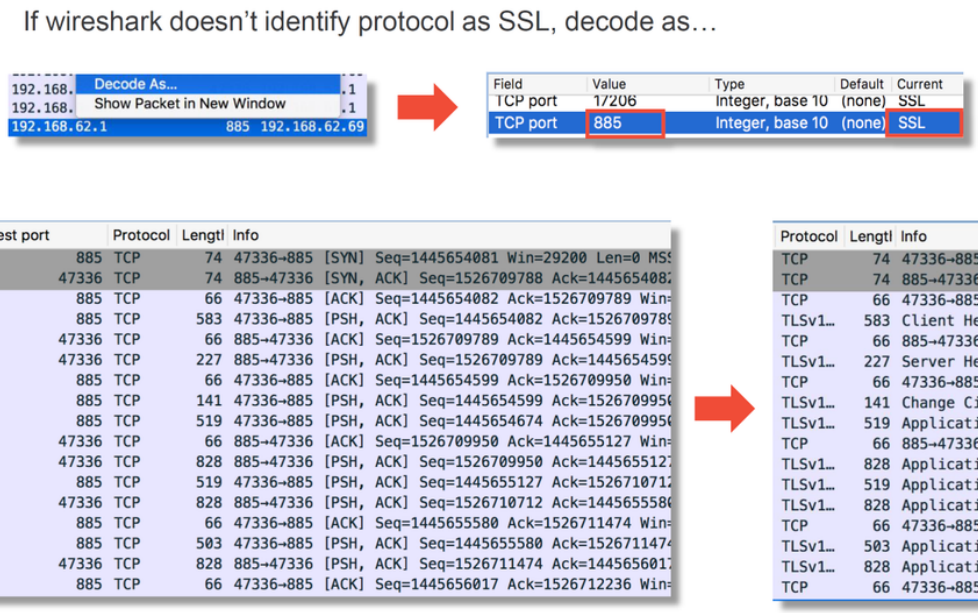
Como alternativa, não há uma opção no Firepower Management Center (FMC) no Firepower versão 6.2.0 e posterior. Para acessar esse utilitário no FMC, navegue para **Dispositivos > Gerenciamento de dispositivos**. Em seguida, clique no botão  ao lado do dispositivo em questão, seguido por **Advanced Troubleshooting > File Download**. Em seguida, você pode digitar o nome de um arquivo em questão e clicar em Download.



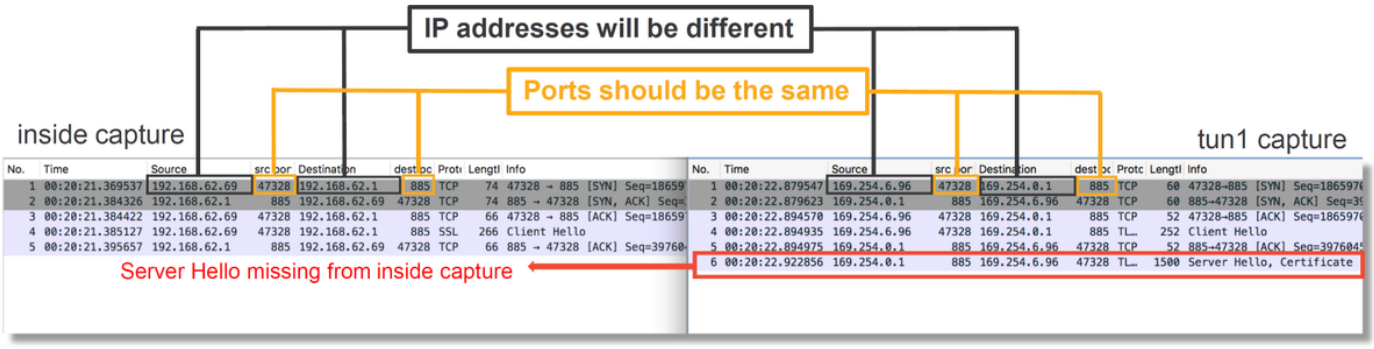
Análise de arquivo de captura de pacote (PCAP)

A análise de PCAP no Wireshark pode ser realizada para ajudar a identificar o problema nas operações de autenticação ativas. Como uma porta fora do padrão é usada na configuração do

portal cativo (**885** por padrão), o Wireshark precisa ser configurado para decodificar o tráfego como SSL.



A captura da interface interna e a captura da interface do túnel devem ser comparadas. A melhor maneira de identificar a sessão em questão em ambos os arquivos PCAP é localizar a porta de origem exclusiva, já que os endereços IP são diferentes.



No exemplo acima, observe que o pacote de saudação do servidor está ausente da captura da interface interna. Isso significa que nunca voltou para o cliente. É possível que o pacote tenha sido descartado pelo snort, ou possivelmente devido a um defeito ou erro de configuração.

> **Note**: O Snort inspeciona seu próprio tráfego de portal cativo para evitar qualquer exploração HTTP.

Descriptografando o fluxo criptografado

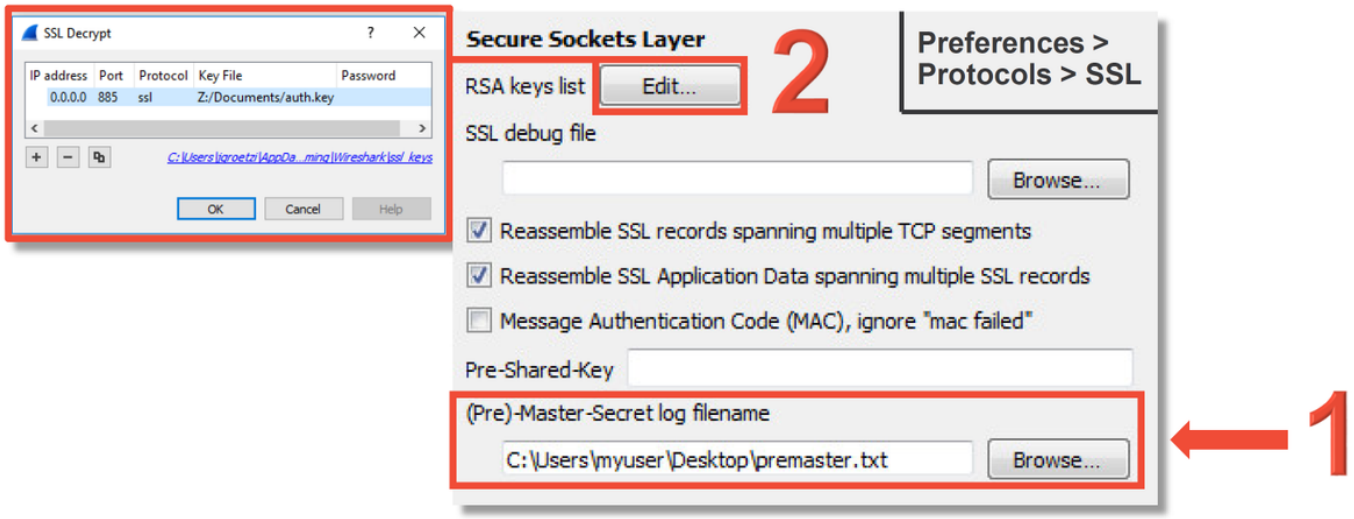
Se o problema não estiver na pilha SSL, pode ser útil descriptografar os dados no arquivo PCAP para ver o fluxo HTTP. Existem dois métodos para isso.

1. Definir uma variável de ambiente no Windows (mais seguro - recomendado) Esse método envolve a criação de um arquivo secreto pré-mestre. Isso pode ser feito com o seguinte

comando (executar a partir do terminal de comando do windows): **setx SSLKEYLOGFILE "%HOMEPATH%\Desktop\premaster.txt"**Uma sessão privada pode ser aberta no Firefox, no qual você pode navegar até o site em questão, que usa SSL.A chave simétrica é então registrada no arquivo especificado no comando da etapa 1 acima.O Wireshark pode usar o arquivo para descriptografar usando a chave simétrica (consulte o diagrama abaixo).

2. Usar a chave privada RSA (menos segura, a menos que use um certificado de teste e um usuário) A chave privada a ser usada é a usada para o certificado do portal cativoIsso não funciona para não-RSA (como a Curva Elíptica) ou para nada efêmero (Diffie-Hellman, por exemplo)

Caution: Se o método 2 for usado, não forneça ao Cisco Technical Assistance Center (TAC) sua chave privada. Entretanto, um certificado de teste temporário e uma chave podem ser usados. Um usuário de teste também deve ser usado em testes.



Exibição do arquivo PCAP descriptografado

No exemplo abaixo, um arquivo PCAP foi descriptografado. Ele mostra que o NTLM está sendo usado como o método de autenticação ativa.


```
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
AAUAGABqAGcALQBhAGQALgBmAHUAbAB0AG8AbgAHAAgApNC54uzU0gEGAAQAAgAAAAgAMAAwAAAAAAAAAAAEAAAAAIAAAGnon72xFiGN/nI
+x5HgnhIcuVFrNJLs2tch8vxbrx90KABAAAJYqfNSUhlBA9xs44bOV4AkAIgBIAFQAVABQAC8AMQA5ADIALgAxADYAOAAuADYAMgAuADEAAAA
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
```

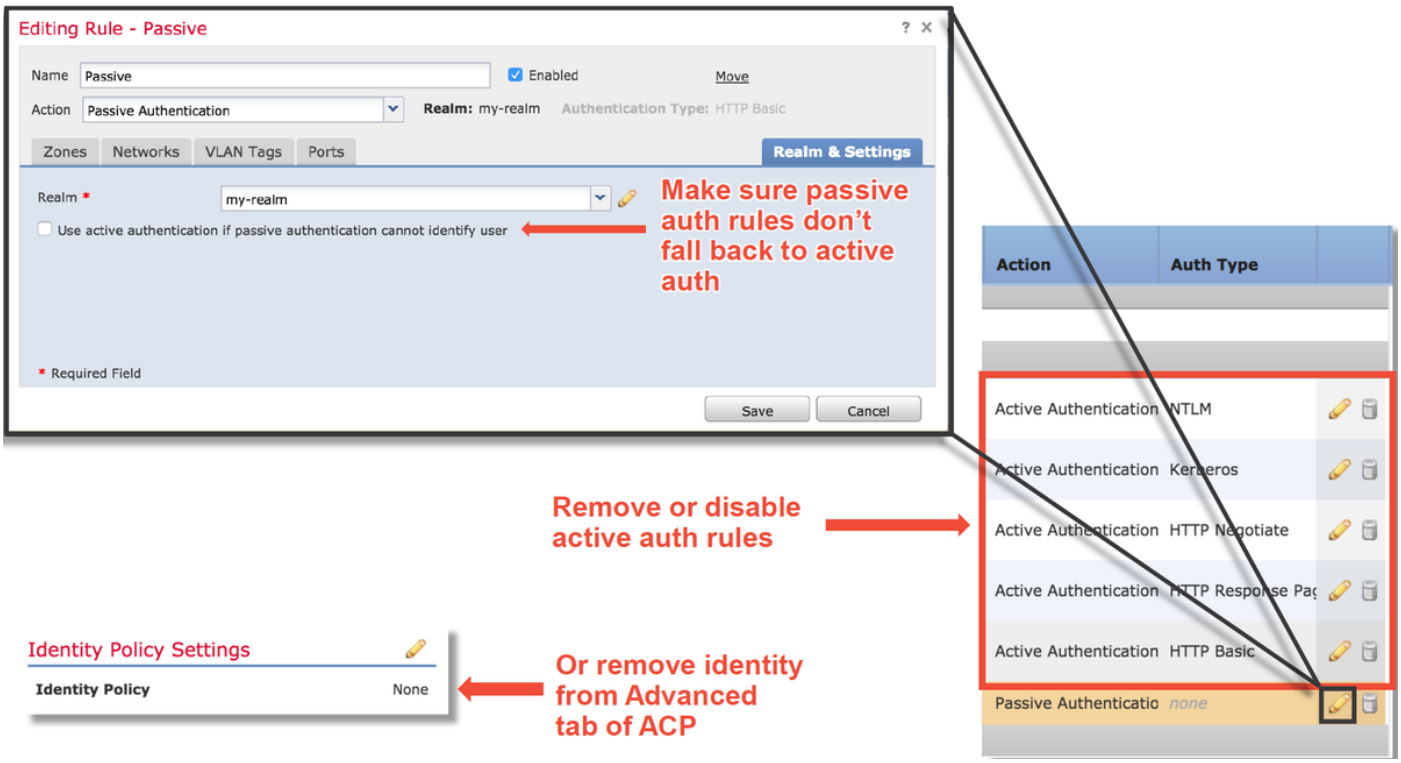
Após a autorização de NTLM, o cliente é redirecionado de volta para a sessão original, para que possa alcançar seu destino pretendido, que é http://www.cisco.com.

Etapas de mitigação

Alternar para somente autenticação passiva

Quando usada em uma política de identidade, a autenticação ativa tem a capacidade de descartar tráfego permitido (somente HTTP(s)), se algo der errado no processo de redirecionamento. Uma etapa de mitigação rápida é desativar qualquer regra na Política de identidade com a ação da **Autenticação ativa**.

Além disso, certifique-se de que todas as regras com 'Autenticação passiva' como ação não tenham a opção 'Usar autenticação ativa se a autenticação passiva não puder identificar o usuário' marcada.



Dados a fornecer ao TAC

Dados	Instruções
Solucionar problemas do Firepower Management Center (FMC)	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Solucionar problemas do dispositivo Firepower que inspeciona o tráfego	https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html
Capturas de pacote de sessão completa	Consulte este artigo para obter instruções

Próximas etapas

Se for determinado que o componente Autenticação ativa não é a causa do problema, a próxima etapa será solucionar o problema do recurso de Política de intrusão.

Clique aqui para prosseguir para o próximo artigo.