# Firepower Device Managerでのリモートアクセ スVPNログインによるパッシブ認証の設定

# 内容

```
概要
<u>前提条件</u>
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>コンフィギュレーション</u>
<u>確認</u>
トラブルシュート</u>
関連情報
```

## 概要

このドキュメントでは、AnyConnectを使用したリモートアクセスVPNログイン(RA VPN)を使用 して、Firepower Device Manager(FDM)を介してFirepower Threat Defense(FTD)でパッシブ認証 を設定する方法について説明します。

# 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Device Manager。
- リモート アクセス VPN.
- •アイデンティティポリシー。

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Threat Defense(FTD)/ $(-\dot{\nu} = 27.0)$
- Cisco AnyConnectセキュアモビリティクライアントバージョン4.10
- Active Directory ( AD )

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

## 背景説明

アイデンティティポリシーは、接続に関連付けられているユーザを検出できます。ユーザIDは他の認証サービス(LDAP)から取得されるため、使用される方式はパッシブ認証です。

FDMでは、パッシブ認証は次の2つの異なるオプションで動作できます:

- リモートアクセスVPNログイン
- Cisco Identity Services Engine ( ISE )

# コンフィギュレーション





Remote user

この項では、FDMでのパッシブ認証の設定方法について説明します。

ステップ1:IDソースの設定

ユーザIDをアクティブに(ユーザ認証のプロンプトで)収集するか、パッシブに収集するかにか かわらず、ユーザID情報を持つActive Directory(AD)サーバを設定する必要があります。

[Objects] > [Identity Services] に移動し、オプション[AD]を選択してActive Directoryを追加します 。

Active Directory設定を追加します。

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре	
AnyConnect_LDAP	Active Directory (AD)	~
Directory Username	Directory Password	
brazil		
e.g. user@example.com		
Base DN	AD Primary Domain	
CN=Users,dc=cmonterr,dc=local	cmonterr.local	
e.g. ou=user, dc=example, dc=com	e.g. example.com	
Directory Server Configuration		
192.168.26.202:389	Test	~
Add another configuration		
	CANCEL	ок

#### **ステップ2:** RA VPNの設定

リモートアクセスVPNの設定は、このリンクで確認でき<u>ます</u>

ステップ3:RA VPNユーザの認証方式の設定

RA VPN設定で、認証方式を選択します。ユーザ認証のプライマリインデックスソースはADであ る必要があります。

Primary Identity Source			
Authentication Type			
AAA Only	~		
Primary Identity Source for User Authenticat	ion	Fallback Local Identity Source 🔔	
AnyConnect_LDAP	~	LocalldentitySource	~
Strip Identity Source server from userna	ame		
Strip Group from Username			

注: RA VPNの[Global Settings]で、[Bypass Access Control Policy for decrypted traffic

# (**sysopt permit-vpn**)]オプションのチェックマークを外し、AnyConnectユーザからのトラフィックを検査するためにアクセスコントロールポリシーを使用できるようにします。

Certificate of Device Identity       Outside Interface         AnyConnect_VPN       outside (GigabitEthernet0/0)         Fully-qualified Domain Name for the Outside Interface       Port         fdm.ravpn       443         e.g. ravpn.example.com       443         Access Control for VPN Traffic       Bypass Access Control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       Inside Interfaces         NAT Exempt       Inside Interfaces       The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.         Image: Inside (GigabitEthernet0/1)       Image: FDM_Local_network			
AnyConnect_VPN       ✓       outside (GigabitEthernet0/0)       ✓         Fully-qualified Domain Name for the Outside Interface       Port         fdm.ravpn       443         e.g. ravpn.example.com       e.g. 8080         Access Control for VPN Traffic       Bypass Access Control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter AcC and the authorization ACL downloaded from the AAA server are still applied to VPN traffic         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       NAT Exempt         Imiterfaces through which remote access VPN users are and address pools must match, either IPv4, IPv6, or both.       The internal networks and address pools must match, either IPv4, IPv6, or both.         Imite (GigabitEthernet0/1)       Imite (GigabitEthernet0/1)       Imiterfacel_network	Certificate of Device Identity	Outside Interface	
Fully-qualified Domain Name for the Outside Interface       Port         fdm.ravpn       443         e.g. ravpn.example.com       e.g. 8080         Access Control for VPN Traffic         Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       Name VPN Filter ACL downloaded from the AAA server are still applied to VPN traffic         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       Name VPN Filter ACL downloaded from the AAA server are still applied to VPN traffic         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       Name VPN Filter ACL downloaded from the AAA server are still applied to VPN traffic         Mathematical Interfaces       Inside Networks       Inside Networks         Inside Interfaces       Name VPN server are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.         Image: Inside (GigabitEthermet0/1)       Image: Image: Image Im	AnyConnect_VPN ~	outside (GigabitEthernet0/0)	~
Fully-qualified Domain Name for the Outside Interface Port   fdm.ravpn 443   e.g. ravpn.example.com e.g. 8080   Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic Bypass Access Control policy for decrypted traffic (sysopt permit-vpn) NATE Exempt The interfaces Inside Interfaces The interfaces through which remote access VPN users can connect to the intermal networks an and address pools must match, either IPv4, IPv6, or both. imiside (GigabitEthernet0/1) Imiside (GigabitEthernet0/1)			
fdm.ravpn       443         e.g. ravpn.example.com       e.g. 8080         Access Control for VPN Traffic       Bypass Access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter AcL         Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)       Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)         MATE Exempt       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Material Interfaces       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Material Interfaces       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted traffic (sysopt permit-vpn)         Image: Control policy for decrypted traffic (sysopt permit-vpn)       Image: Control policy for decrypted tra	Fully-qualified Domain Name for the Outside Interf	ace Port	
e.g. ravpn.example.com e.g. ravpn.example.com e.g. 8080  Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL ad the authorization ACL downloaded from the AAA server are still applied to VPN traffic Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)  NAT Exempt  The interfaces The interface The interf	fdm.ravpn	443	
Access Control for VPN Traffic Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)	e.g. ravpn.example.com	e.g. 8080	
<ul> <li>Inside Interfaces</li> <li>The interfaces through which remote access VPN users can connect to the internal networks</li> <li>★</li> <li>Inside (GigabitEthernet0/1)</li> </ul> Inside (GigabitEthernet0/1) Inside (GigabitEthernet0/1) Inside (GigabitEthernet0/1)	Bypass Access Control policy for decrypted tr NAT Exempt	affic (sysopt permit-vpn)	
FDM_Local_network	Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks	Inside Networks The internal networks remote access VPN users are allowed to use. The IP versions of the internal network and address pools must match, either IPv4, IPv6, or both.	ks
°□ FDM_Local_network		E EDM Legel actual	
		·L PDM_Local_network	

ステップ4:パッシブ認証のためのアイデンティティポリシーの設定

パッシブ認証を設定するには、アイデンティティポリシーを作成する必要があります。ポリシー には次の要素が必要です。

• AD IDソース:手順1で追加したものと同じ

• Action:パッシブ認証

アイデンティティルールを設定するには、[Policies] > [Identity] > [select [+] ボタンに移動し、新 しいアイデンティティルールを追加します。

•パッシブ認証が適用される送信元サブネットと宛先サブネットを定義します。

Order Title 1 ~ AnyConne	AD Ic	AD Identity Source Action AnyConnect_LDAP   AnyConnect_LDAP		PASSIVE AUTHENTICATION For all types of connections, obtain user identity from other authentication services without prompting for username and password.			
Source / Destination	ource / Destination			With Identity Sources			
SOURCE			DESTINATION				
Zones +	Networks +	Ports	+ Zones	+	Networks	Ports +	
ANY	ANY	ANY	ANY		ANY	ANY	

### ステップ5:アクセスコントロールポリシーへのアクセスコントロールルールの作成

ユーザに基づいてトラフィックを許可またはブロックするように、アクセスコントロールルール を設定します。

			SOURCE	JRCE DESTINATION		DESTINATION							
н	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS		ACTIONS
>	Inside_Outside	Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	brazil	<b>G</b> C.	

パッシブ認証を使用するようにユーザまたはユーザグループを設定するには、[Users]タブを選択 します。ユーザグループまたは個々のユーザを追加できます。

Order Title	Action	
1 Y Inside_Outside_Rule	Allow Y	
Source/Destination Applications URLs	Users Intrusion Policy File policy	Logging
AVAILABLE USERS	-	1 CONTROLLING ACCESS FOR USERS AND USER GROUPS
▼ Filter		If you configure identity policies to establish user identity based on source IP address, you can control access based on user name or user group membership. By controlling access based on user identity user each the consecutive consecutive whether the user characteristics.
Identity Sources Groups Users		workstations or obtains a different address through DHCP. If you base rules on group membership, user network access changes as users change roles in your organization, moving
AnyConnect_LDAP \ administrator	A	from one group to another.
AnyConnect_LDAP \ brazil		
AnyConnect_LDAP \ calo-maintenance		

変更を導入します。

# 確認

ADとのテスト接続が成功したことを確認します

Identity Realm is used for Identity Policies and Remote this realm.	Access VPN. Any changes impact all features that use
Name	Туре
AnyConnect_LDAP	Active Directory (AD)
Directory Username	Directory Password
brazil	
e.g. user@example.com	
Base DN	AD Primary Domain
CN=Users,dc=cmonterr,dc=local	cmonterr.local
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
192.168.26.202:389	*
Hostname / IP Address	Port
192.168.26.202	389
e.g. ad.example.com	
Interface	
inside (GigabitEthernet0/1)	
Encryption	Trusted CA certificate
NONE ~	Please select a certificate
TEST	1
	CANCEL OK

リモートユーザがADクレデンシャルでAnyConnectクライアントにログインできることを確認し ます。

1	Cisco AnyConnect   192.168.27.44			
	Group: Username: Password:	Anyconnect V brazil		
		OK Cancel		
🚳 Cisco	AnvConne	ct Secure Mobility Client 🗕 🗖 🗙		

<u> </u>	,,,,,,,,,	
	VPN: Connected to 192.168.27.44.	
_	192.168.27.44 🗸	Disconnect
00:00:58		IPv4
<b>\$</b> (i)		uluiu cisco

ユーザがVPNプールのIPアドレスを取得していることを確認します

firepower# show vpn-sessiondb anyconnect filter name brazil						
Session Type: A	nyConnect					
Username : Assigned IP : Protocol : License :	brazil 192.168.19.1 AnyConnect-Parent SS AnyConnect Premium	Index Public IP SL-Tunnel	: 23 : 192.168.27.40			
Encryption : Hashing : Bytes Tx : Group Policy :	AnyConnect-Parent: ( AnyConnect-Parent: ( 15818 DfltGrpPolicy	(1)none SSL-Tunr (1)none SSL-Tunr Bytes Rx Tunnel Group	nel: (1)AES-GCM-256 nel: (1)SHA384 : 2494 : Anyconnect			
Duration : Inactivity :	0h:00m:13s 0h:00m:00s	1 21 2021				
VLAN Mapping : Audt Sess ID :	N/A 000000000001700060f8	VLAN 31f8c	: none			
Security Grp :	none	Tunnel Zone	: 0			
firenower#						

# トラブルシュート

user\_map\_query.plscriptを使用して、FDMにユーザーIPマッピングがあることを確認できます

clishモードでは、次のように設定できます。

```
> system support identity-debug
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol:
Please specify a client IP address: 192.168.19.1
Please specify a client port:
Please specify a server IP address:
Please specify a server port:
Monitoring identity and firewall debug messages
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 62757 -> 53, geo 14467064 -> 14467082
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 abp src
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 abp dst
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 new firewall session
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-62757 > 72.163.47.11-53 17 AS 1-1 I 0 allow action
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules params)
with zones 2 -> 2, port 62757 -> 53, geo 14467064 -> 14467082
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 Retrieved ABP info:
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 abp src
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 abp dst
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-62757 > 8.8.8-53 17 AS 1-1 I 1 new firewall session
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 HitCount data sent for rule id: 268435458,
192.168.19.1-62757 > 8.8.8.8-53 17 AS 1-1 I 1 allow action
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 53015 -> 443, geo 14467064 -> 14467082
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 abp src
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 abp dst
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 new firewall session
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-53015 > 20.42.0.16-443 6 AS 1-1 I 0 allow action
192.168.19.1-52166 > 20.42.0.16-443 6 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x102, session->logFlags = 010001
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 65207 -> 53, geo 14467064 -> 14467082
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 Retrieved ABP info:
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 abp src
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 abp dst
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 268435458,
192.168.19.1-65207 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 Starting authentication (sfAuthCheckRules params)
```

```
with zones 2 -> 2, port 65207 -> 53, geo 14467064 -> 14467082
192.168.19.1-65207 > 8.8.8-53 17 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 abp src
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 abp dst
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-65207 > 8.8.8-53 17 AS 1-1 I 0 new firewall session
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-65207 > 8.8.8.8-53 17 AS 1-1 I 0 allow action
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 Starting authentication (sfAuthCheckRules params)
with zones 2 -> 2, port 65209 -> 53, geo 14467064 -> 14467082
192.168.19.1-65209 > 8.8.8-53 17 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 abp src
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 abp dst
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-65209 > 8.8.8-53 17 AS 1-1 I 0 new firewall session
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-65209 > 8.8.8.8-53 17 AS 1-1 I 0 allow action
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 65211 -> 53, geo 14467064 -> 14467082
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 Retrieved ABP info:
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 abp src
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 abp dst
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 268435458,
192.168.19.1-65211 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 61823 -> 53, geo 14467064 -> 14467082
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 Retrieved ABP info:
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 abp src
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 abp dst
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 new firewall session
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 HitCount data sent for rule id: 268435458,
192.168.19.1-61823 > 72.163.47.11-53 17 AS 1-1 I 1 allow action
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 Starting authentication (sfAuthCheckRules params)
with zones 2 -> 2, port 61823 -> 53, geo 14467064 -> 14467082
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 abp src
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 abp dst
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 new firewall session
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-61823 > 8.8.8.8-53 17 AS 1-1 I 0 allow action
192.168.19.1-57747 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x102, session->logFlags = 010001
192.168.19.1-57747 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 268435458 ruleAction = 2 ruleReason = 0
192.168.19.1-57747 > 8.8.8.8-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001, fwFlags
```

```
= 0x102, session->logFlags = 010001
192.168.19.1-57747 > 8.8.8.8-53 17 AS 1-1 I 0 Logging EOF as part of session delete with rule_id
= 268435458 ruleAction = 2 ruleReason = 0
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 Starting authentication (sfAuthCheckRules
params) with zones 2 -> 2, port 53038 -> 443, geo 14467064 -> 14467082
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 abp src
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 abp dst
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm id = 3
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 new firewall session
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-53038 > 20.42.0.16-443 6 AS 1-1 I 0 allow action
192.168.19.1-57841 > 72.163.47.11-53 17 AS 1-1 I 1 deleting firewall session flags = 0x10001,
fwFlags = 0x102, session->logFlags = 010001
192.168.19.1-57841 > 72.163.47.11-53 17 AS 1-1 I 1 Logging EOF as part of session delete with
rule_id = 268435458 ruleAction = 2 ruleReason = 0
192.168.19.1-57841 > 8.8.8.8-53 17 AS 1-1 I 0 deleting firewall session flags = 0x10001, fwFlags
= 0x102, session->logFlags = 010001
192.168.19.1-57841 > 8.8.8.8-53 17 AS 1-1 I 0 Logging EOF as part of session delete with rule_id
= 268435458 ruleAction = 2 ruleReason = 0
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 Starting authentication (sfAuthCheckRules params)
with zones 2 -> 2, port 64773 -> 53, geo 14467064 -> 14467082
192.168.19.1-64773 > 8.8.8-53 17 AS 1-1 I 0 Retrieved ABP info:
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 abp src
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 abp dst
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 matched auth rule id = 130027046 user_id = 5
realm_id = 3
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 new firewall session
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 using HW or preset rule order 2,
'Inside_Outside_Rule', action Allow and prefilter rule 0
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 HitCount data sent for rule id: 268435458,
192.168.19.1-64773 > 8.8.8.8-53 17 AS 1-1 I 0 allow action
```

## 関連情報

#### FDMによって管理されるFTDでのリモートアクセスVPNの設定

https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215532configure-remote-access-vpn-on-ftd-manag.html