

# 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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[コンフィギュレーション](#)

[確認](#)

[トラブルシューティング](#)

[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)バージョン7.0
- Cisco AnyConnectセキュアモバイル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

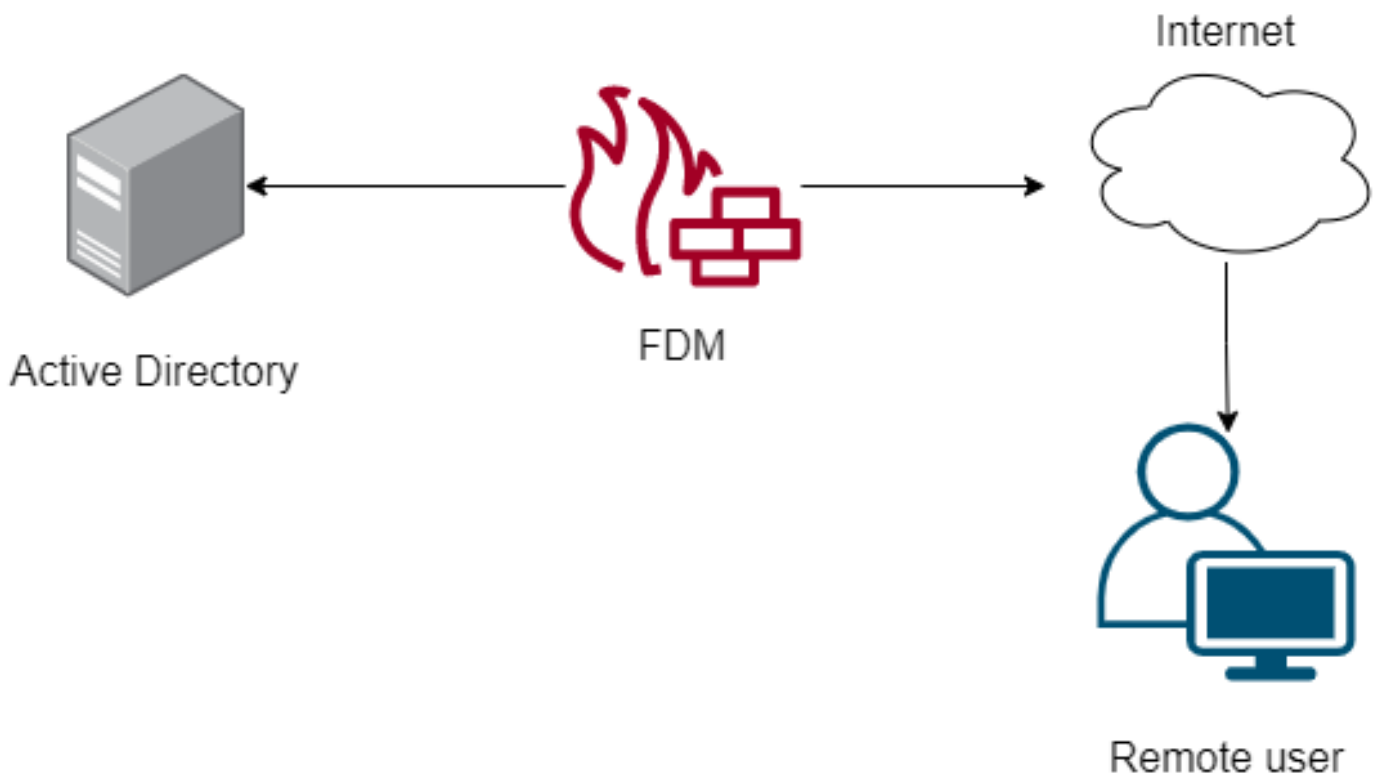
アイデンティティポリシーは、接続に関連付けられているユーザを検出できます。ユーザIDは他の認証サービス(LDAP)から取得されるため、使用される方式はパッシブ認証です。

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

### ネットワーク図



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	Type
AnyConnect_LDAP	Active Directory (AD) ▼
Directory Username	Directory Password
brazil <small>e.g. user@example.com</small>	.....
Base DN	AD Primary Domain
CN=Users,dc=cmonterr,dc=local <small>e.g. ou=user, dc=example, dc=com</small>	cmonterr.local <small>e.g. example.com</small>
<b>Directory Server Configuration</b>	
📄 192.168.26.202:389 <span style="float: right;">Test ▼</span>	
<a href="#">Add another configuration</a>	
<span>CANCEL</span> <span>OK</span>	

## 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 [ます](#)

## 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。

<b>Primary Identity Source</b>	
Authentication Type	
AAA Only ▼	
Primary Identity Source for User Authentication	Fallback Local Identity Source ⚠
AnyConnect_LDAP ▼	LocalIdentitySource ▼
<input checked="" type="checkbox"/> Strip Identity Source server from username	
<input checked="" type="checkbox"/> 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: AnyConnect\_VPN

Outside Interface: outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface: fdm.ravpn  
e.g. ravpn.example.com

Port: 443  
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)

NAT Exempt

Inside Interfaces: inside (GigabitEthernet0/1)

Inside Networks: FDM\_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一
- 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。

## 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。

#	NAME	ACTION	SOURCE			DESTINATION			APPLICATIONS	URLS	USERS	ACTIONS
			ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS				
> 1	Inside_Outside...	Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	brazil	

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。

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 Access VPN. Any changes impact all features that use this realm.

Name

AnyConnect\_LDAP

Type

Active Directory (AD)

Directory Username

brazil

*e.g. user@example.com*

Directory Password

.....

Base DN

CN=Users,dc=cmonterr,dc=local

*e.g. ou=user, dc=example, dc=com*

AD Primary Domain

cmonterr.local

*e.g. example.com*

### Directory Server Configuration

📄 192.168.26.202:389

Hostname / IP Address

192.168.26.202

*e.g. ad.example.com*

Port

389

Interface

inside (GigabitEthernet0/1)

Encryption

NONE

Trusted CA certificate

Please select a certificate

TEST

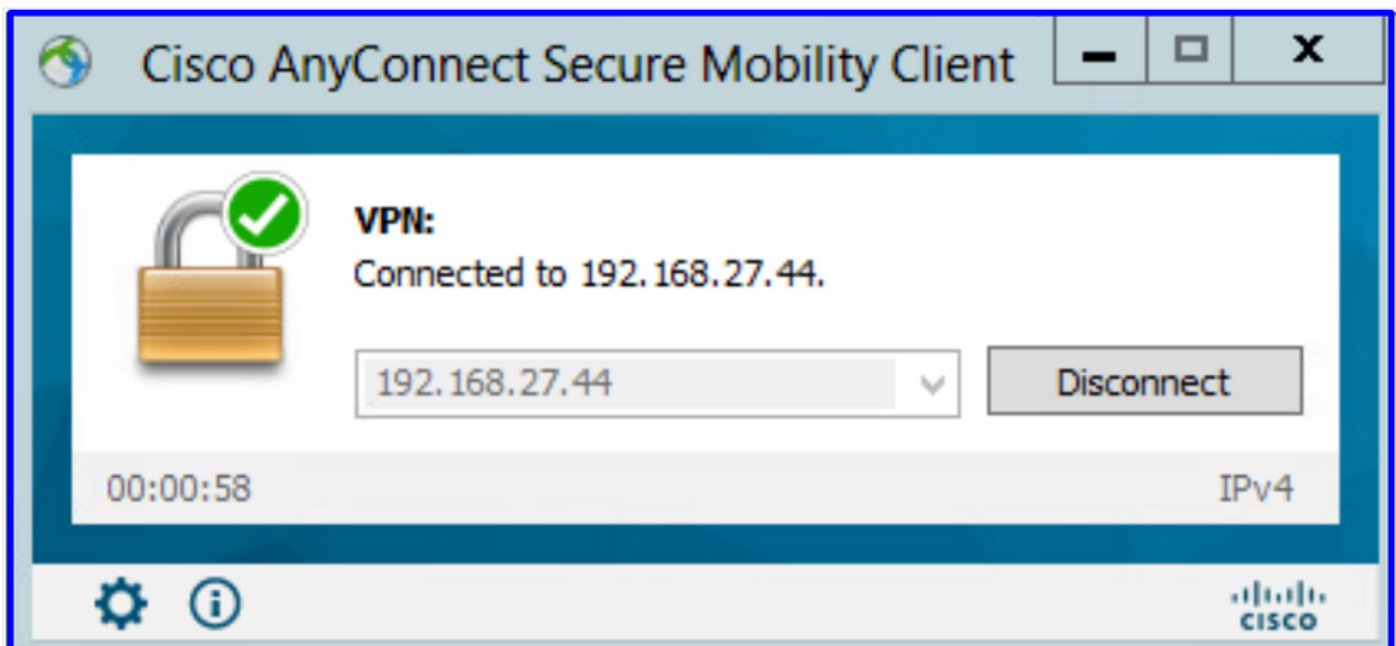
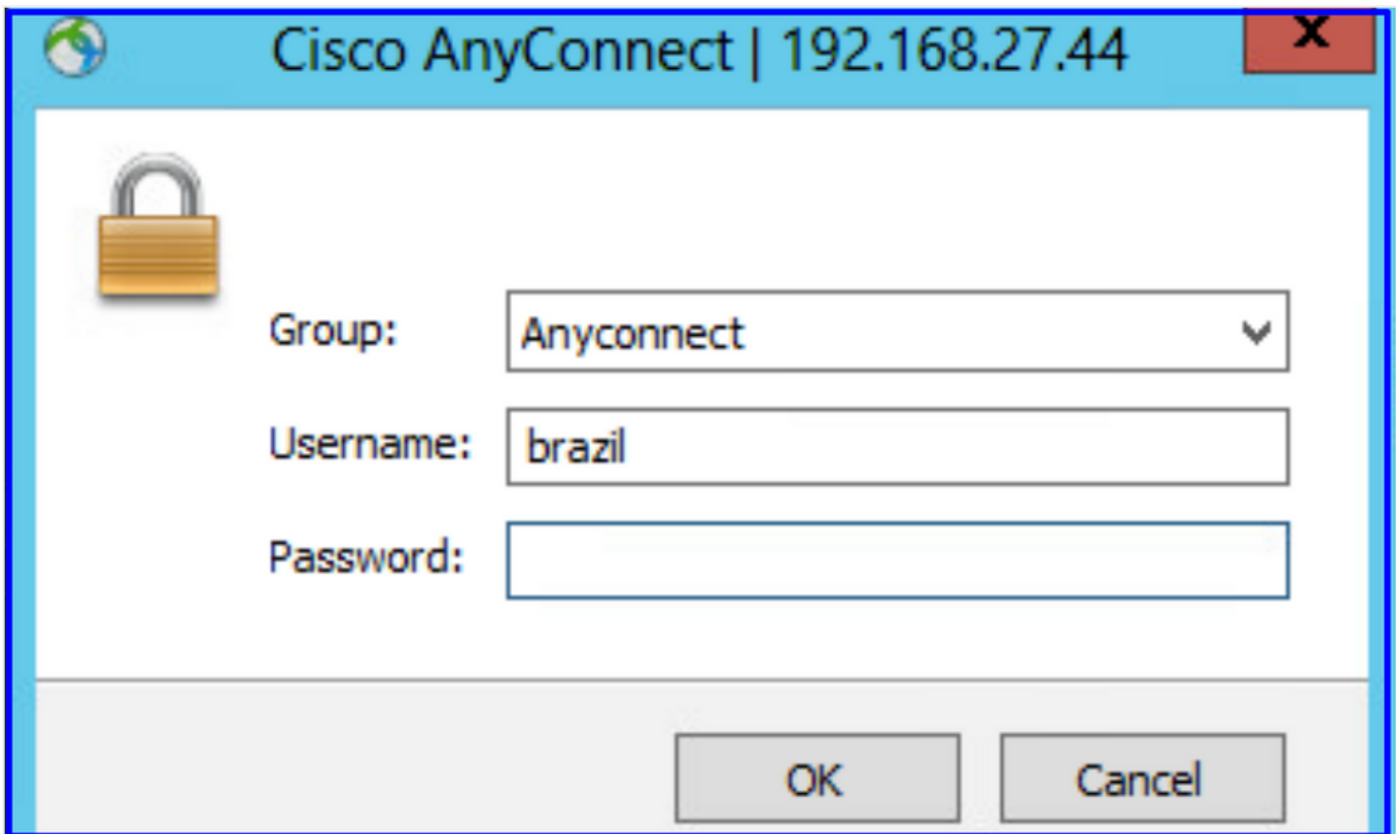
✓ Connection to realm is successful

[Add another configuration](#)

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。



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: AnyConnect
Username      : brazil                               Index      : 23
Assigned IP   : 192.168.19.1                         Public IP   : 192.168.27.40
Protocol      : AnyConnect-Parent SSL-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384
Bytes Tx      : 15818                               Bytes Rx    : 2494
Group Policy  : DfltGrpPolicy                       Tunnel Group: Anyconnect
Login Time    : 13:22:20 UTC Wed Jul 21 2021
Duration      : 0h:00m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                                VLAN        : none
Audt Sess ID  : 000000000001700060f81f8c
Security Grp  : none                               Tunnel Zone : 0
firepower#
```

## トラブルシューティング

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

```
root@firepower:~# user_map_query.pl -u brazil
WARNING: This script was not tested on this major version (7.0.0)! The results may be unexpected.
Current Time: 07/21/2021 13:23:38 UTC
Getting information on username(s)...

User #1: brazil
---
ID: 5
Last Seen: 07/21/2021 13:22:20 UTC
for_policy: 1

=====
| Database |
=====

##) IP Address
1) ::ffff:192.168.19.1

##) Group Name (ID)
1) Domain Users (11)
root@firepower:~# user_map_query.pl -i 192.168.19.1
WARNING: This script was not tested on this major version (7.0.0)! The results may be unexpected.
Current Time: 07/21/2021 13:23:50 UTC
Getting information on IP Address(es)...

IP #1: 192.168.19.1
---

=====
| Database |
=====

##) Username (ID)
1) brazil (5)
   for_policy: 1
   Last Seen: 07/21/2021 13:22:20 UTC
root@firepower:~#
```

clishモードでは、次のように設定できます。



## system support identity-debugtoリダイレクトが成功したかどうかを確認します。

```
> 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 > 8.8.8.8-53 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 > 8.8.8.8-53 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 > 8.8.8.8-53 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 > 8.8.8.8-53 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 > 8.8.8.8-53 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 > 8.8.8.8-53 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/215532-configure-remote-access-vpn-on-ftd-manag.html>