

# Firepower Device Manager에서 원격 액세스 VPN 로그인으로 수동 인증 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[확인](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Firepower Device Manager(FDM)를 통해 Firepower FTD(Threat Defense)에서 AnyConnect를 사용하여 RA VPN(Remote Access VPN) 로그인을 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Firepower Device Manager입니다.
- 원격 액세스 VPN.
- ID 정책.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD(Firepower Threat Defense) 버전 7.0
- Cisco AnyConnect Secure Mobility Client 버전 4.10
- AD(Active Directory)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 배경 정보

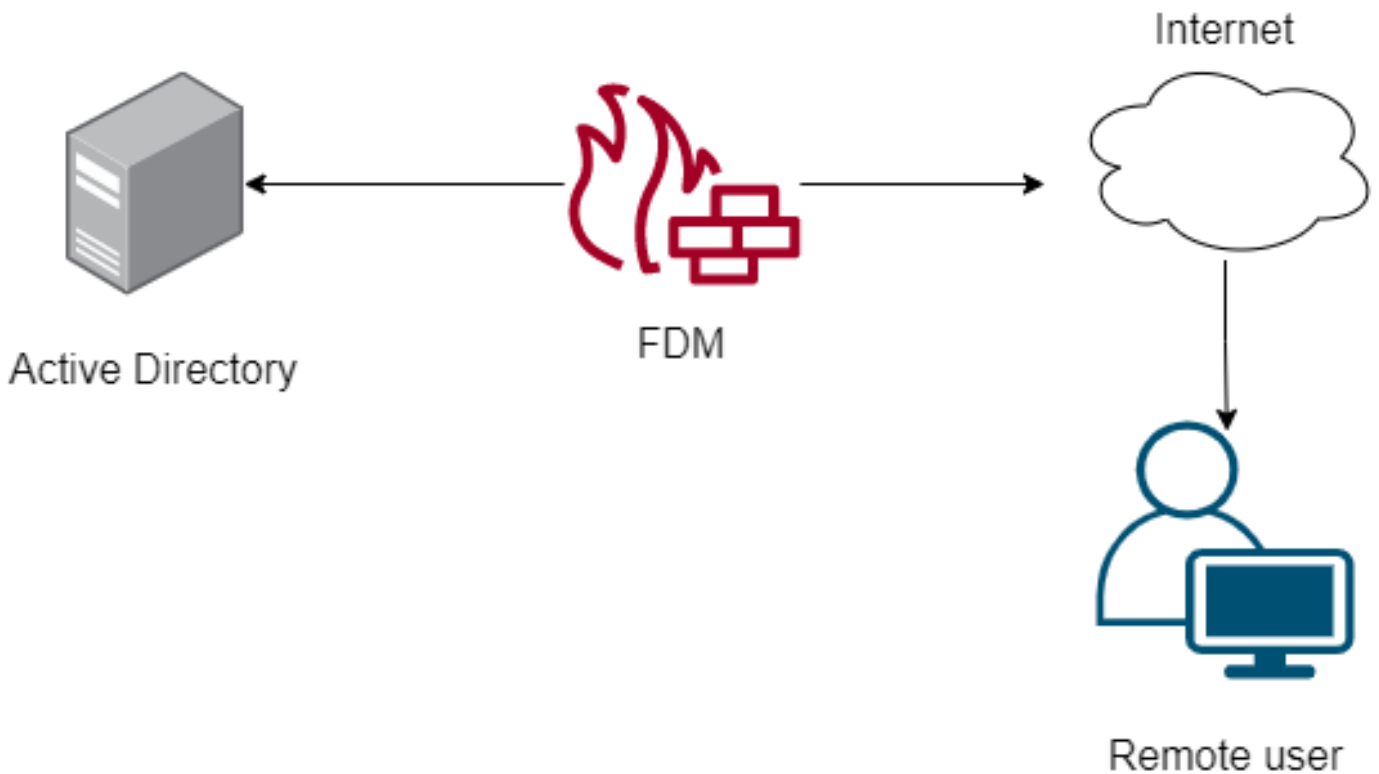
ID 정책은 연결과 연결된 사용자를 탐지할 수 있습니다. 사용자 ID가 다른 인증 서비스(LDAP)에서 가져오므로 사용되는 방법은 수동 인증입니다.

FDM에서 수동 인증은 두 가지 옵션으로 작동할 수 있습니다.

- 원격 액세스 VPN 로그인
- Cisco ISE(Identity Services Engine)

## 구성

### 네트워크 다이어그램



이 섹션에서는 FDM에서 수동 인증을 구성하는 방법에 대해 설명합니다.

### 1단계. ID 소스 구성

사용자 ID를 능동적으로(사용자 인증 프롬프트) 수집하든 수동적으로 수집하든, 사용자 ID 정보가 있는 AD(Active Directory) 서버를 구성해야 합니다.

Objects(개체)>Identity Services(ID 서비스)로 이동하고 AD옵션을 선택하여 Active Directory를 추가합니다.

Active Directory 구성을 추가합니다.

❗ 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 <small>e.g. user@example.com</small>	Directory Password	.....
Base DN	CN=Users,dc=cmonterr,dc=local <small>e.g. ou=user, dc=example, dc=com</small>	AD Primary Domain	cmonterr.local <small>e.g. example.com</small>
<b>Directory Server Configuration</b>			
📡 192.168.26.202:389			Test ▼
<a href="#">Add another configuration</a>			
		CANCEL	OK

## 2단계. RA VPN 구성

이 [링크](#)에서 원격 액세스 VPN 컨피그레이션을 검토할 수 있습니다.

## 3단계. RA VPN 사용자에게 대한 인증 방법을 구성합니다.

RA VPN 컨피그레이션에서 인증 방법을 선택합니다. 사용자 인증을 위한 기본 독립 원본은 AD여야 합니다.

<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	

참고: RA VPN의 Global Settings(전역 설정)에서 Bypass Access Control Policy for decrypted

traffic (sysopt permit-vpn)(해독된 트래픽에 대한 액세스 제어 정책 우회(Bypass Access Control Policy for decrypt permit-vpn) 옵션을 선택 취소하여 Access Control Policy를 사용하여 AnyConnect 사용자로부터 오는 트래픽을 검사할 수 있습니다.

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: The interfaces through which remote access VPN users can connect to the internal networks

- inside (GigabitEthernet0/1)

Inside Networks: 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.

- FDM\_Local\_network

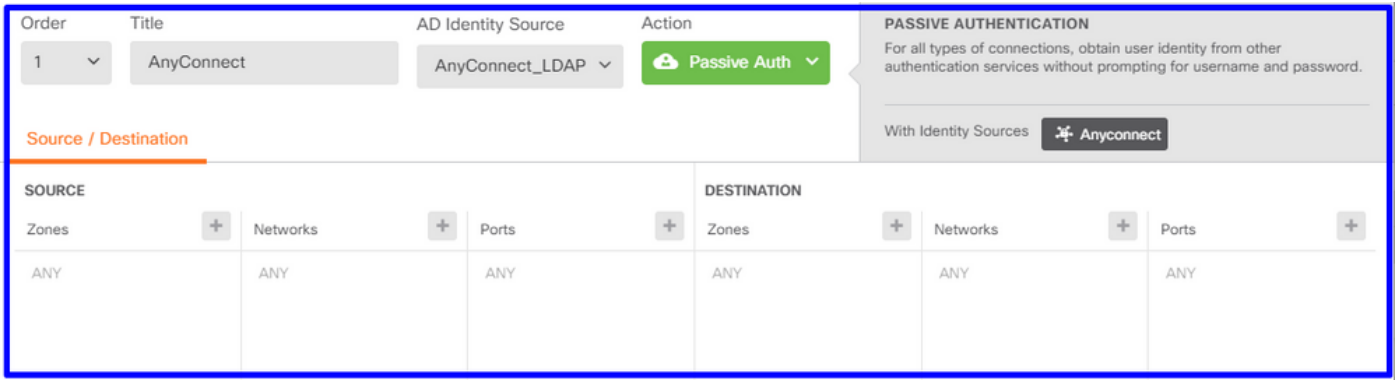
4단계. 수동 인증을 위한 ID 정책을 구성합니다.

패시브 인증을 구성하려면 ID 정책을 생성해야 하며, 정책에는 다음 요소가 있어야 합니다.

- AD ID 소스:1단계에서 추가한 것과 동일합니다.
- 작업:수동 인증

ID 규칙을 구성하려면 Policies>Identity >select[+] 버튼으로 이동하여 새 ID 규칙을 추가합니다.

- 수동 인증이 적용되는 소스 및 대상 서브넷을 정의합니다.

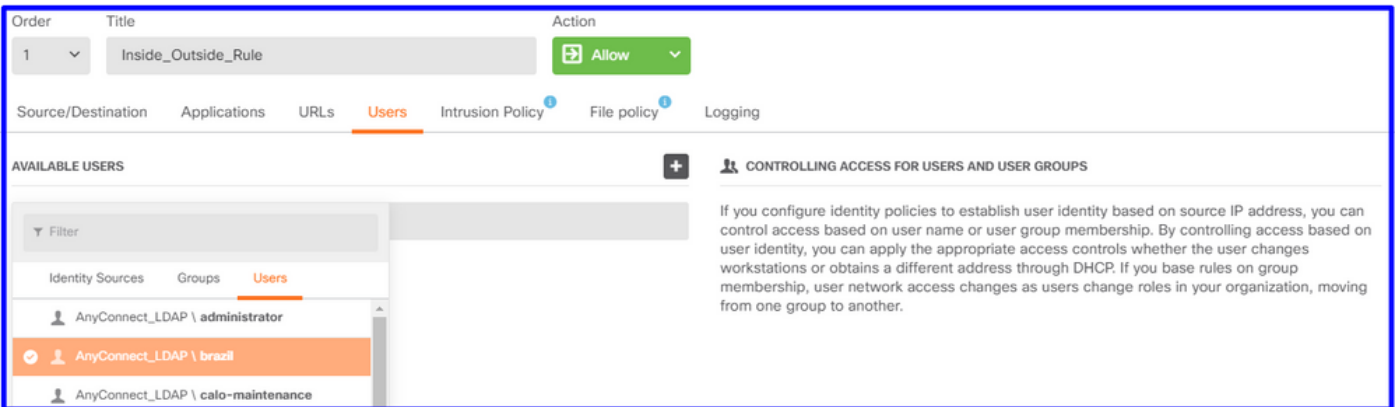


5단계. 액세스 제어 정책에 액세스 제어 규칙을 생성합니다.

사용자를 기반으로 트래픽을 허용하거나 차단하도록 Access Control 규칙을 구성합니다.

#	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	

사용자 또는 사용자 그룹이 수동 인증을 갖도록 구성하려면 Users(사용자) 탭을 선택합니다. 사용자 그룹 또는 개별 사용자를 추가할 수 있습니다.



변경 사항을 구축합니다.

## 확인

AD와의 테스트 연결이 성공했는지 확인합니다.

**!** 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	Directory Password	.....
<i>e.g. user@example.com</i>			
Base DN	CN=Users,dc=cmonterr,dc=local	AD Primary Domain	cmonterr.local
<i>e.g. ou=user, dc=example, dc=com</i>		<i>e.g. example.com</i>	

### Directory Server Configuration

**192.168.26.202:389**

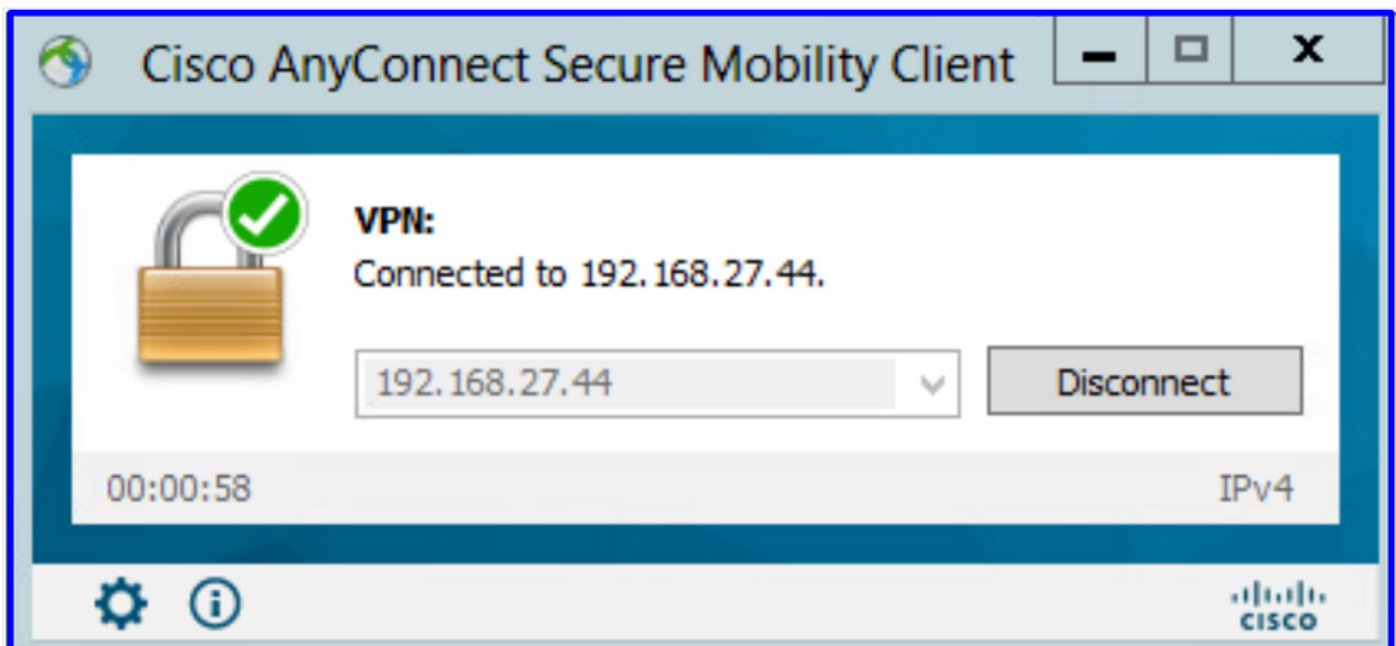
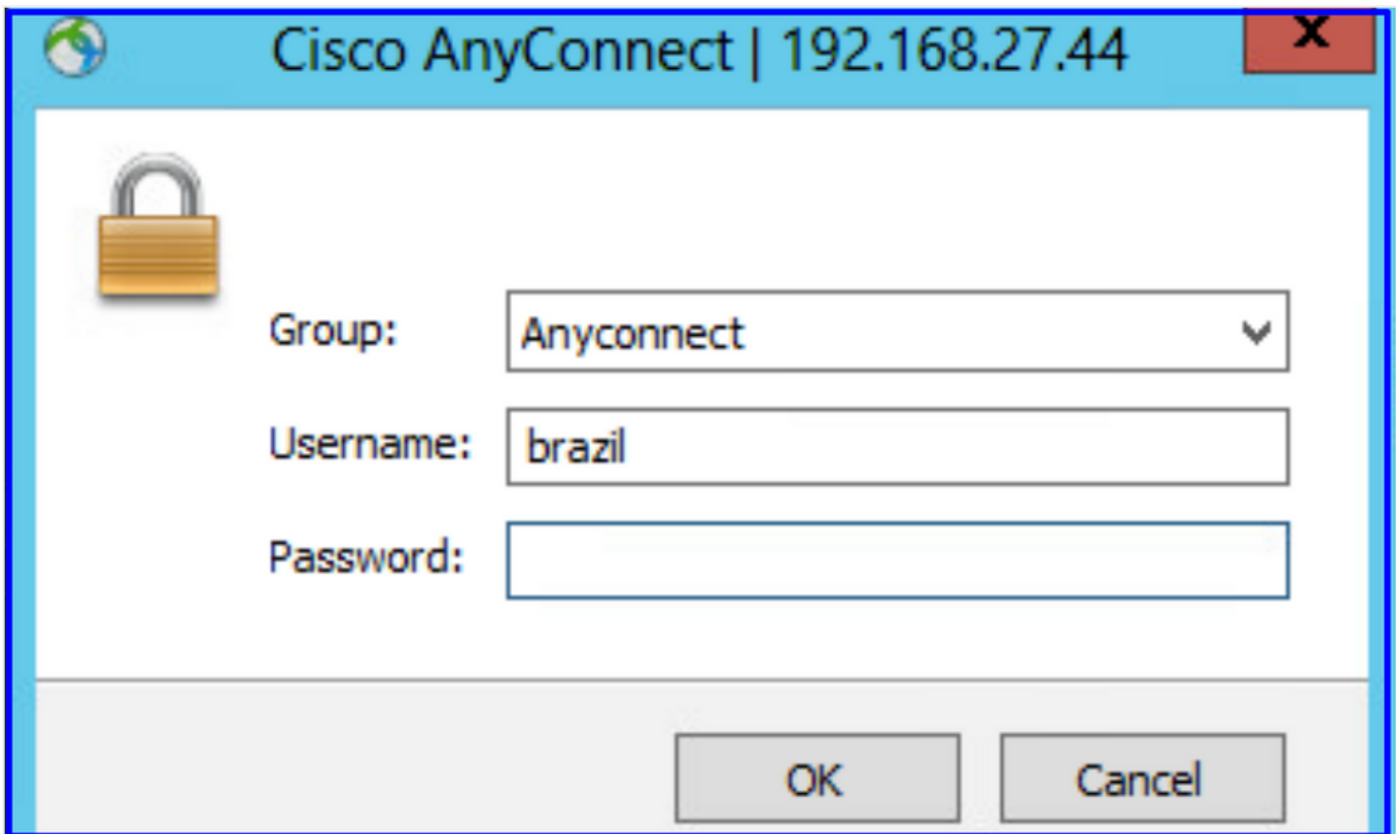
Hostname / IP Address	192.168.26.202	Port	389
<i>e.g. ad.example.com</i>			
Interface	inside (GigabitEthernet0/1)		
Encryption	NONE	Trusted CA certificate	Please select a certificate

**TEST** ✓ **Connection to realm is successful**

[Add another configuration](#)

CANCEL OK

원격 사용자가 AD 자격 증명을 사용하여 AnyConnect 클라이언트로 로그인할 수 있는지 확인합니다.



사용자가 VPN 풀의 IP 주소를 가져왔는지 확인합니다.

```
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#
```

## 문제 해결

user\_map\_query.plscript를 사용하여 FDM에 사용자 IP 매핑이 있는지 확인할 수 있습니다.

```
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:~#
```

통화 모드에서는 다음을 구성할 수 있습니다.



## 시스템은 id-debugger를 지원하여 리디렉션이 성공했는지 확인합니다.

```
> 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
```

## 관련 정보

### FDM에서 관리되는 FTD에서 원격 액세스 VPN 구성

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