Konfigurieren der passiven Authentifizierung mit Remote Access VPN-Anmeldung im FirePOWER Device Manager

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die passive Authentifizierung auf der FirePOWER Threat Defense (FTD) über den FirePOWER Device Manager (FDM) mit Remote Access VPN-Anmeldungen (RA VPN) mit AnyConnect konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse des FirePOWER Geräte-Managers
- Kenntnisse des Remote Access VPN
- Identitätsrichtlinien

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

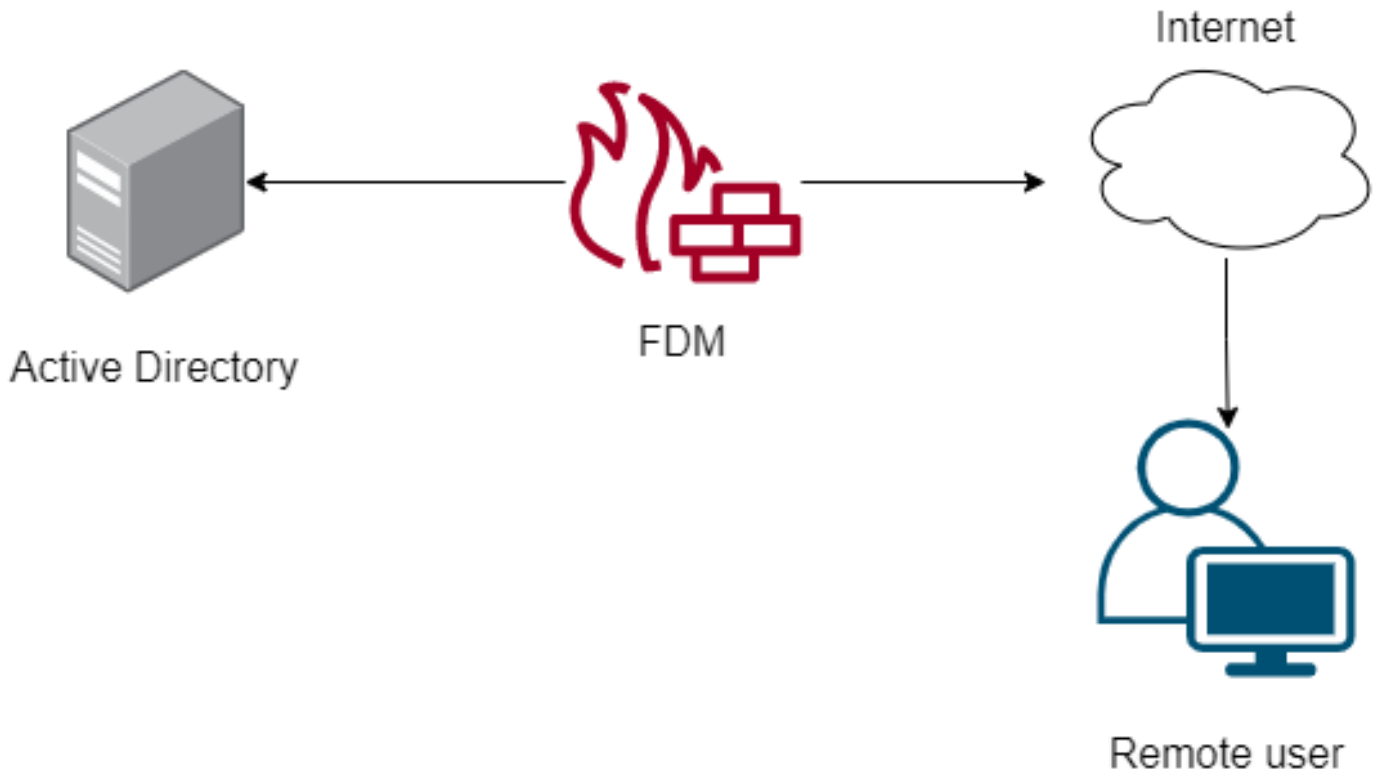
Die Identitätsrichtlinie kann Benutzer erkennen, die einer Verbindung zugeordnet sind. Die verwendete Methode ist Passive Authentication (Passive Authentifizierung), da die Benutzeridentität von anderen Authentifizierungsdiensten (LDAP) abgerufen wird.

Im FDM kann die passive Authentifizierung mit zwei verschiedenen Optionen erfolgen:

- Remote Access VPN-Anmeldungen
- Cisco Identity Services Engine (ISE)

Konfiguration

Netzwerkdiagramm



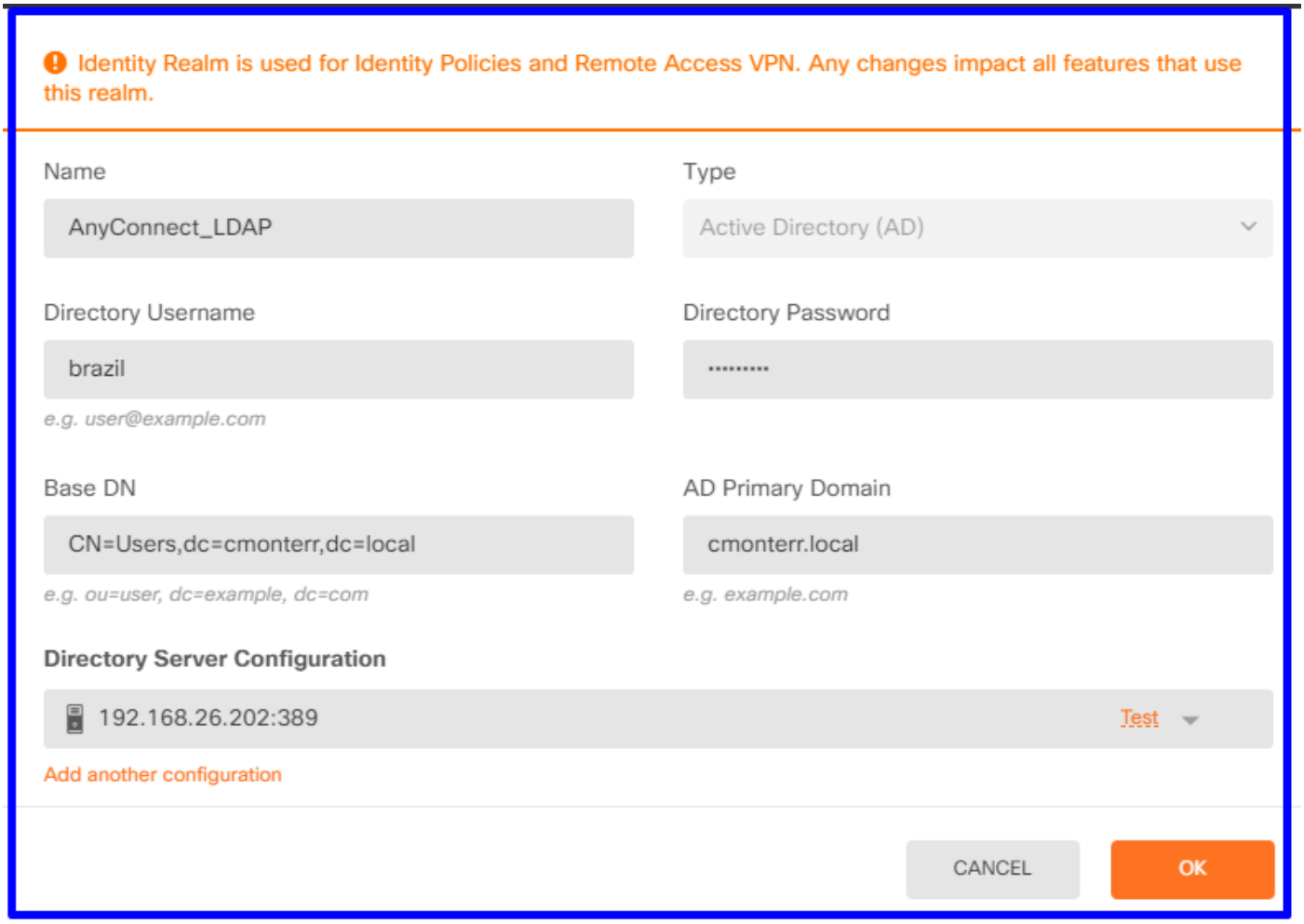
In diesem Abschnitt wird beschrieben, wie Sie die passive Authentifizierung auf FDM konfigurieren.

Schritt 1: Konfigurieren der Identitätsquelle

Unabhängig davon, ob Sie die Benutzeridentität aktiv (über die Eingabeaufforderung für die Benutzerauthentifizierung) oder passiv erfassen, müssen Sie den Active Directory (AD)-Server konfigurieren, der die Benutzeridentitätsinformationen enthält.

Navigieren Sie **zu Objects>Identity** Services, und wählen Sie die Option ADaus, um das Active Directory hinzuzufügen.

Fügen Sie die Active Directory-Konfiguration hinzu:

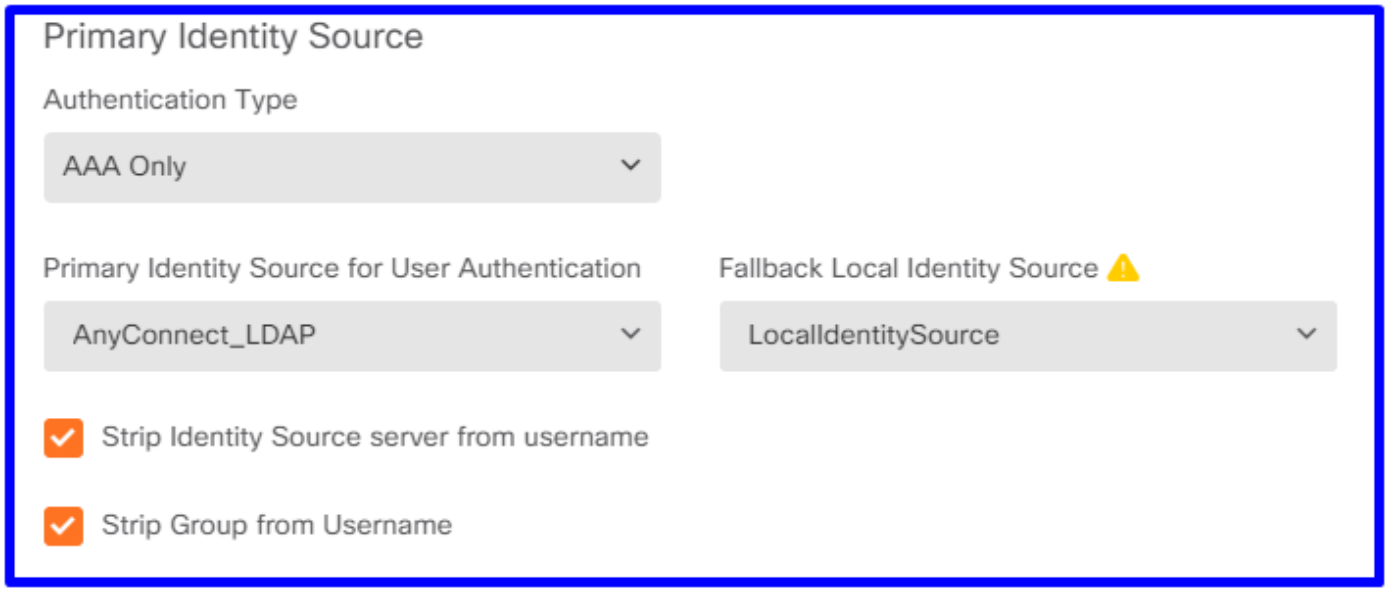


Schritt 2: Konfigurieren des RA VPN

Die Remote Access VPN-Konfiguration kann über diesen Link überprüft werden.

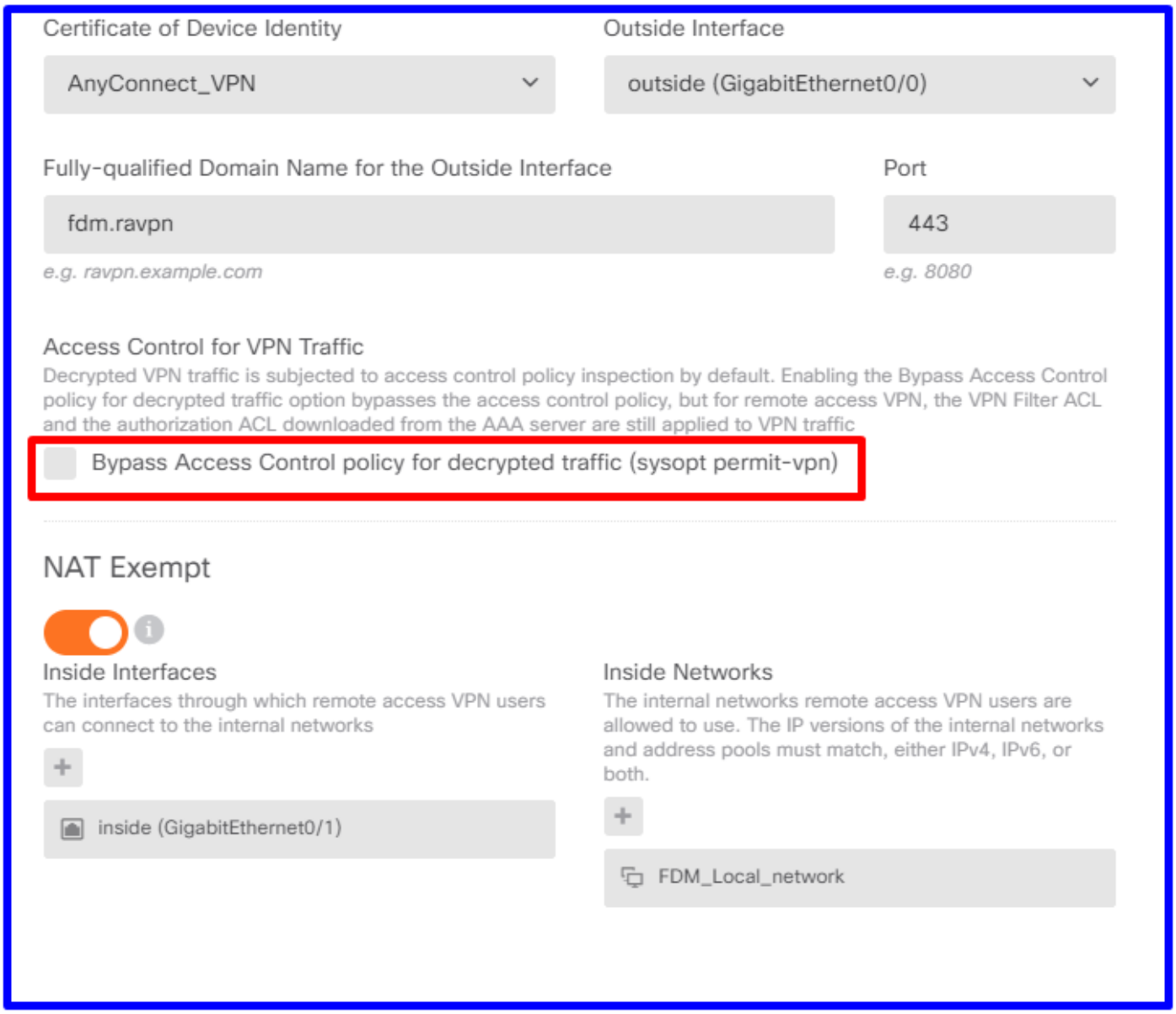
Schritt 3: Konfigurieren der Authentifizierungsmethode für RA VPN-Benutzer

Wählen Sie in der RA VPN-Konfiguration die Authentifizierungsmethode aus. Die primäre Quelle für die Benutzerauthentifizierung muss das AD sein.



Anmerkung: Deaktivieren Sie in den Globalen Einstellungen des RA VPN die Option Bypass

Access Control Policy für entschlüsselten Datenverkehr (**sysopt permit-vpn**), um die Möglichkeit zu ermöglichen, den von den AnyConnect-Benutzern stammenden Datenverkehr mithilfe einer Zugriffskontrollrichtlinie zu überprüfen.



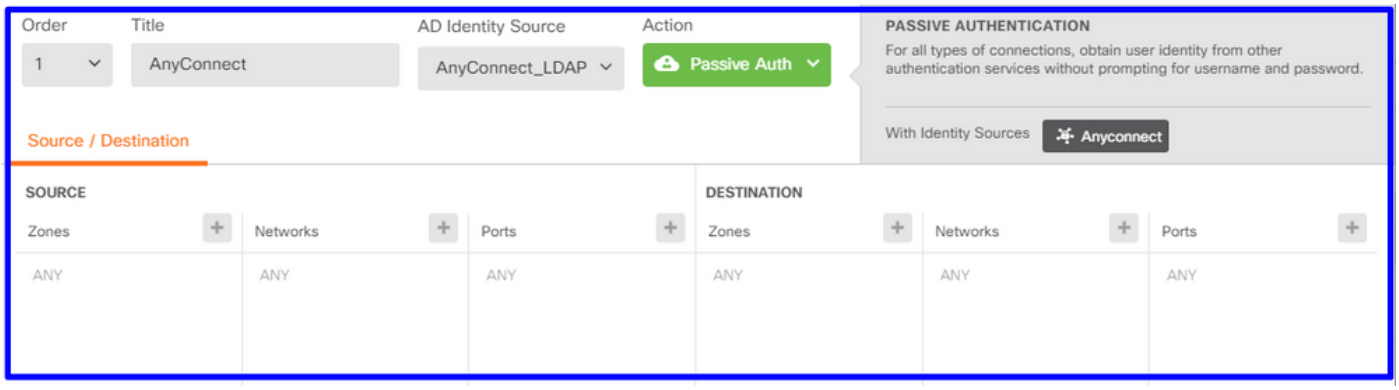
Schritt 4: Konfigurieren der Identitätsrichtlinie für die passive Authentifizierung

Sie müssen die Identitätsrichtlinie erstellen, um die passive Authentifizierung zu konfigurieren. Die Richtlinie muss die folgenden Elemente enthalten:

- AD-Identitätsquelle: Dasselbe gilt für Schritt 1
- Aktion: PASSIVE AUTO

Um die Identitätsregel zu konfigurieren, navigieren Sie **zur** Schaltfläche **Policies>Identity >** wählen Sie **[+]**, um eine neue Identitätsregel hinzuzufügen.

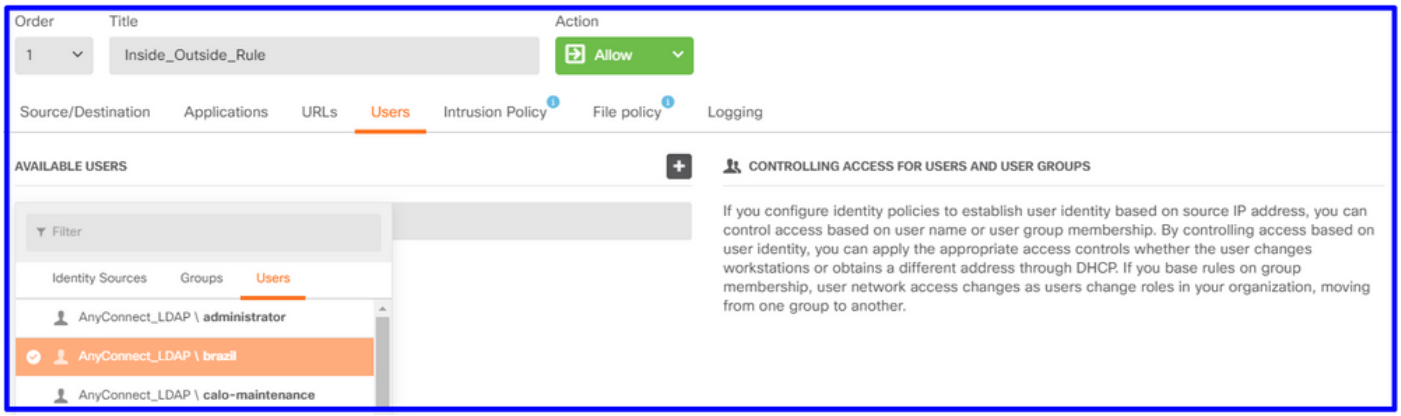
- Definieren Sie die Quell- und Zielsubnetze, in denen die passive Authentifizierung angewendet wird.



Schritt 5: Erstellen der Zugriffskontrollregel in der Zugriffskontrollrichtlinie

Konfigurieren Sie die Zugriffskontrollregel, um Datenverkehr basierend auf Benutzern zuzulassen oder zu blockieren.

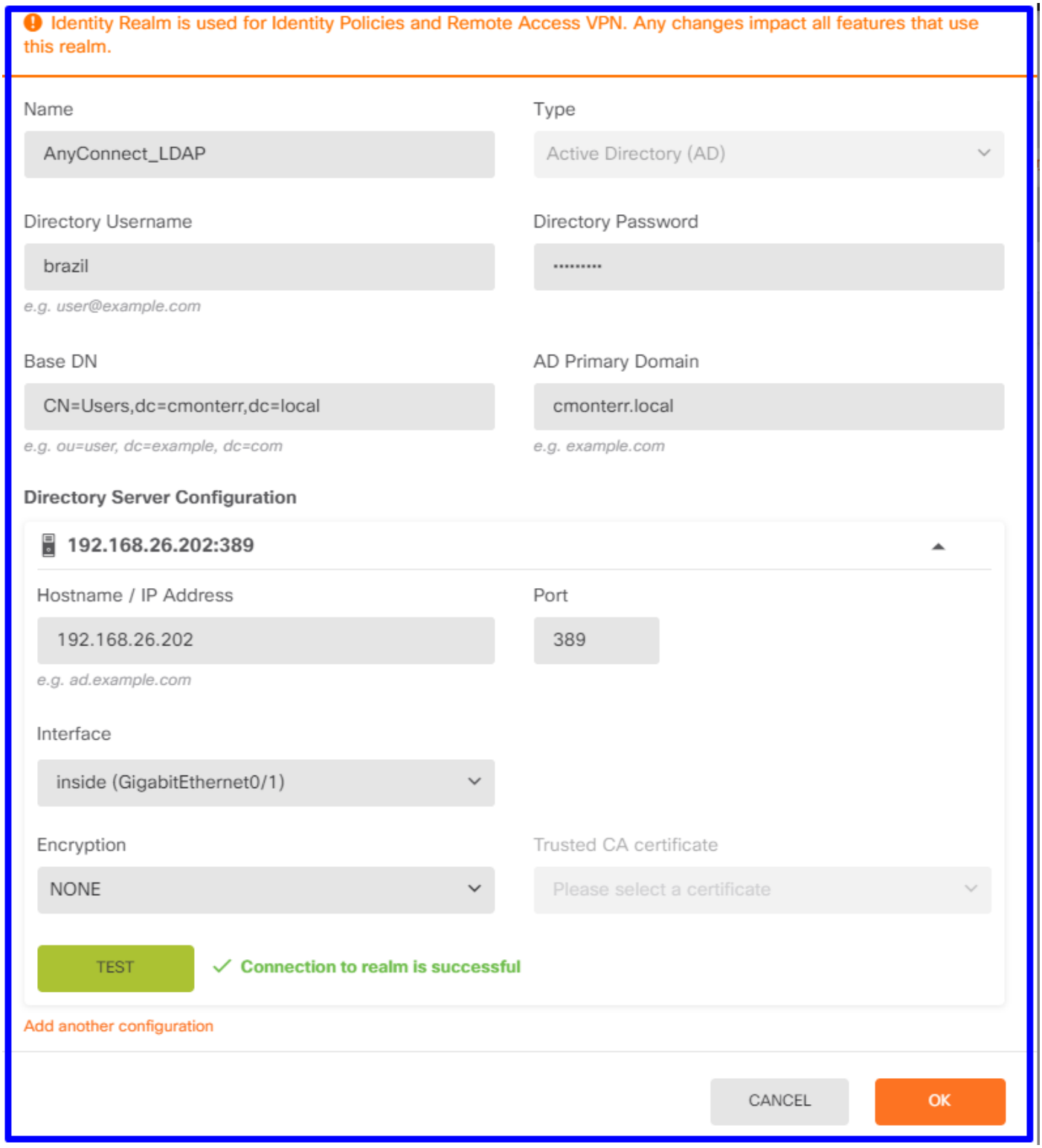
Um die Benutzer- oder Benutzergruppe für die passive Authentifizierung zu konfigurieren, wählen Sie die Registerkarte Benutzer aus. Sie können eine Benutzergruppe oder einen einzelnen Benutzer hinzufügen.



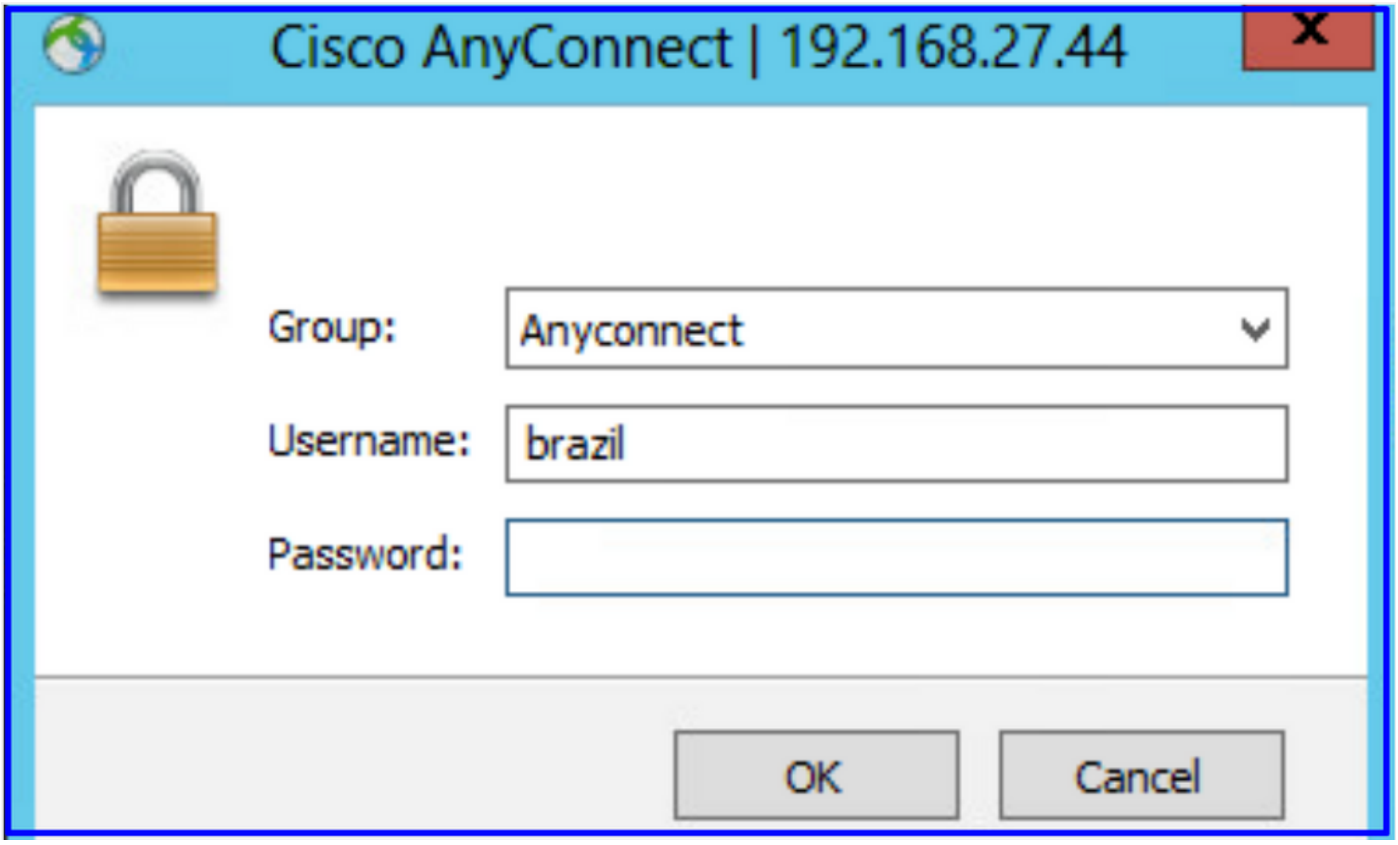
Stellen Sie die Änderungen bereit.

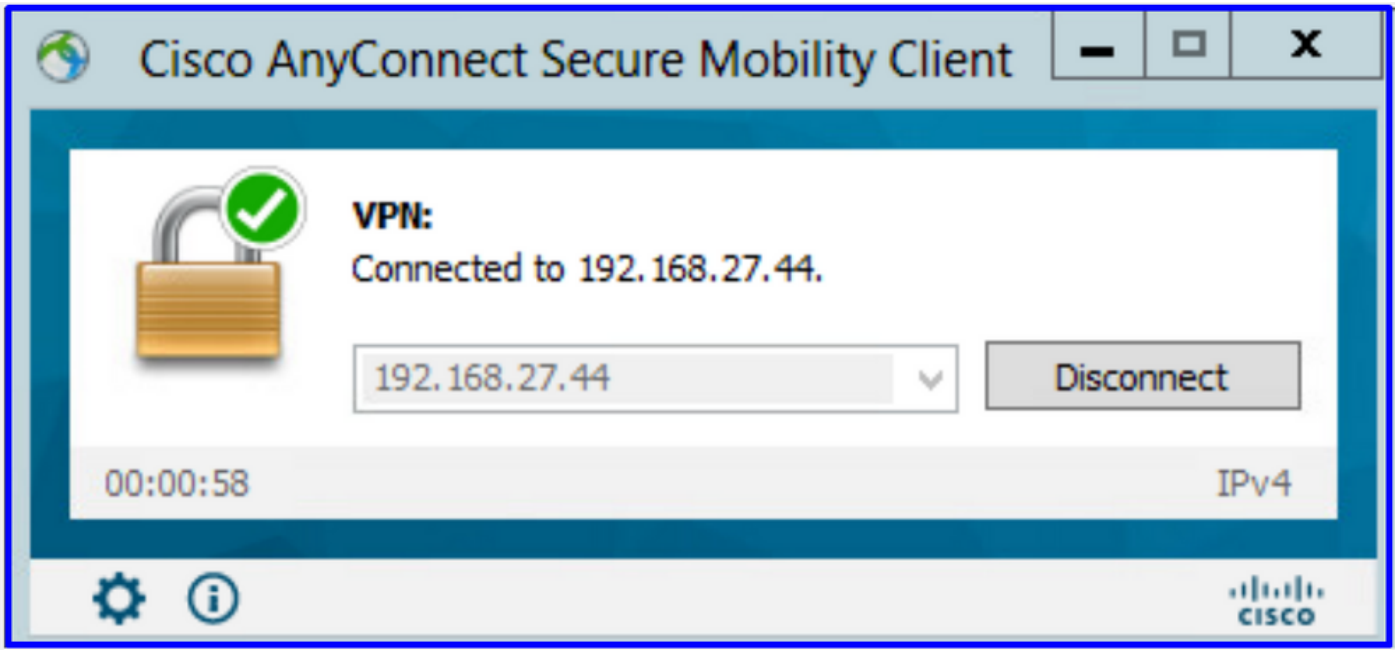
Überprüfung

Überprüfen der erfolgreichen Testverbindung mit dem AD



Überprüfen Sie, ob sich der Remote-Benutzer mit dem AnyConnect-Client mit ihren AD-Anmeldeinformationen anmelden kann.





Überprüfen, ob der Benutzer eine IP-Adresse des VPN-Pools erhält

```
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 : 0000000000001700060f81f8c
Security Grp : none                      Tunnel Zone  : 0

firepower#
```

Fehlerbehebung

Sie können das **user_map_query.**plscript verwenden, um zu überprüfen, ob der FDM über die Benutzer-IP-Zuordnung verfügt.

```
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:~#
```

Im Klickmodus können Sie Folgendes konfigurieren:

Identitätsdebuggen der Systemunterstützung, um zu überprüfen, ob die Umleitung erfolgreich ist.

```
> 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
```