

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

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

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

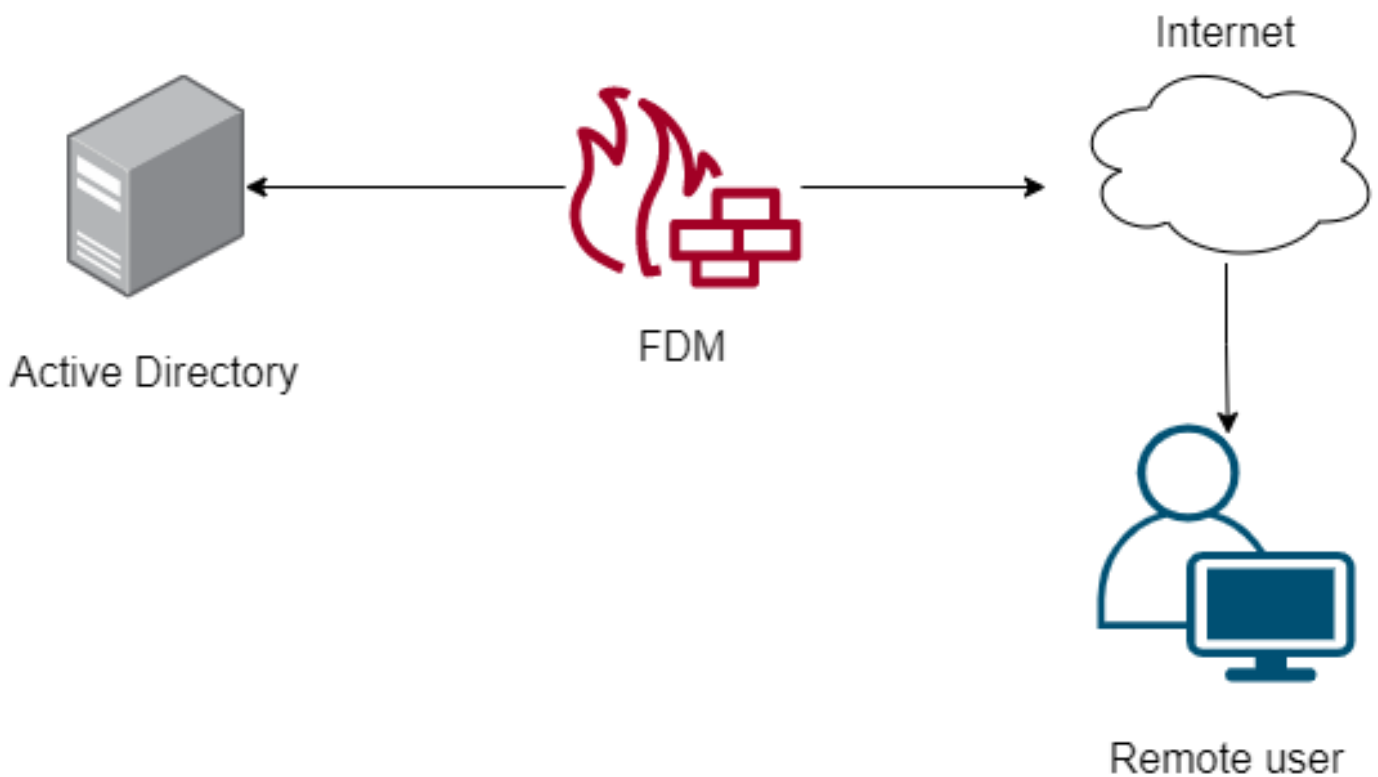
Die Identitätsrichtlinie kann Benutzer erkennen, die einer Verbindung zugeordnet sind. Die verwendete Methode ist Passive Authentication (Passive Authentifizierung), da die Benutzeridentität von anderen Authentifizierungsdiensten (LDAP) abgerufen wird.

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

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

Konfiguration

Netzwerkdigramm



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:

! 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>
Directory Server Configuration			
📡 192.168.26.202:389			Test ▼
Add another configuration			
		CANCEL	OK

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.

Primary Identity Source	
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	

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.

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

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.

Order: 1, Title: AnyConnect, AD Identity Source: AnyConnect_LDAP, Action: Passive Auth

PASSIVE AUTHENTICATION
For all types of connections, obtain user identity from other authentication services without prompting for username and password.

With Identity Sources: Anyconnect

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports
ANY	ANY	ANY	ANY	ANY	ANY

Schritt 5: Erstellen der Zugriffskontrollregel in der Zugriffskontrollrichtlinie

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

#	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	

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.

Order: 1, Title: Inside_Outside_Rule, Action: Allow

Source/Destination Applications URLs **Users** Intrusion Policy File policy Logging

AVAILABLE USERS: AnyConnect_LDAP \ administrator, **AnyConnect_LDAP \ brazil**, AnyConnect_LDAP \ calo-maintenance

CONTROLLING ACCESS FOR USERS AND USER GROUPS

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, you can apply the appropriate access controls whether the user changes 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 from one group to another.

Stellen Sie die Änderungen bereit.

Überprüfung

Überprüfen der erfolgreichen Testverbindung mit dem AD

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


TEST ✓ **Connection to realm is successful**

[Add another configuration](#)

CANCEL OK

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

Cisco AnyConnect | 192.168.27.44




Group:

Username:

Password:

OK Cancel

Cisco AnyConnect Secure Mobility Client



VPN:
Connected to 192.168.27.44.

Disconnect

00:00:58 IPv4

Settings Info Cisco

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  : 000000000001700060f81f8c
Security Grp  : none                               Tunnel Zone : 0
firepower#
```

Fehlerbehebung

Sie können das `user_map_query.pl` script 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
```