

Configurar a autenticação passiva com o login de VPN de acesso remoto no Firepower Device Manager

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configuração](#)

[Verificação](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como configurar a Autenticação Passiva no Firepower Threat Defense (FTD) através do Firepower Device Manager (FDM) com logins de VPN de Acesso Remoto (RA VPN) com AnyConnect.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Firepower Device Manager.
- VPN de acesso remoto.
- Política de identidade.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

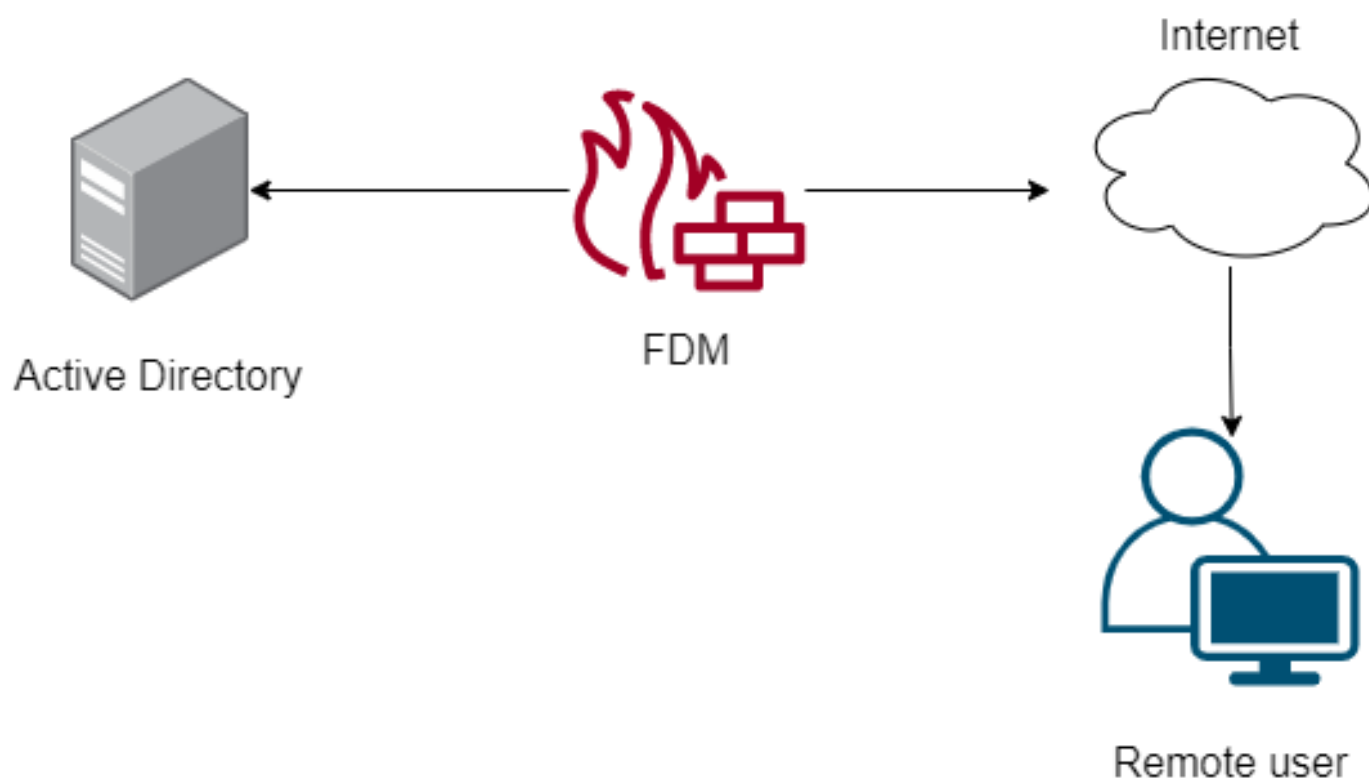
A Política de identidade pode detectar usuários associados a uma conexão. O método usado é Autenticação Passiva, pois a identidade do usuário é obtida de outros serviços de autenticação (LDAP).

No FDM, a autenticação passiva pode funcionar com duas opções diferentes:

- Logons de VPN de acesso remoto
- Cisco Identity Services Engine (ISE)

Configuração

Diagrama de Rede



Esta seção descreve como configurar a autenticação passiva no FDM.

Etapa 1. Configurar a origem da identidade

Quer você colete a identidade do usuário ativamente (pelo prompt para autenticação do usuário) ou passivamente, você precisa configurar o servidor do Active Directory (AD) que tem as informações de identidade do usuário.

Navegue **até Objetos > Serviços de identidade** e selecione a opção AD para adicionar o Active Directory.

Adicione a configuração do Active Directory:

! 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

Etapa 2. Configurar a VPN do RA

A configuração da VPN de acesso remoto pode ser revisada neste [link](#)

Etapa 3. Configurar o método de autenticação para usuários de VPN RA

Na configuração da VPN RA, selecione o método de autenticação. A Origem Principal da Independência para Autenticação de Usuário deve ser o AD.

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	

Note: Nas Configurações globais da VPN RA, desmarque a opção Ignorar política de

controle de acesso para tráfego descriptografado (**sysopt permit-vpn**) para permitir a possibilidade de usar a política de controle de acesso para inspecionar o tráfego proveniente dos usuários do AnyConnect.

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

Etapa 4. Configurar a política de identidade para autenticação passiva

Você precisa criar a política de identidade para configurar a autenticação passiva, a política deve ter os seguintes elementos:

- Fonte de identidade do AD: O mesmo que você adicionou na etapa número 1
- Ação: AUTONOMIA PASSIVA

Para configurar a regra de Identidade, navegue até **Políticas > Identidade** > selecione o botão **[+]** para adicionar uma nova regra de Identidade.

- Defina as sub-redes de origem e de destino onde a autenticação passiva se aplica.

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

Etapa 5. Crie a regra de controle de acesso na política de controle de acesso

Configure a regra de controle de acesso para permitir ou bloquear o tráfego com base nos usuários.

#	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	

Para configurar o grupo de usuários ou usuários para ter autenticação passiva, selecione a guia Usuários. Você pode adicionar um grupo de usuários ou um usuário individual.

AVAILABLE USERS

Filter

Identity Sources Groups **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.

Implante as alterações.

Verificação

Verifique se a conexão de teste com o AD foi bem-sucedida

! 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

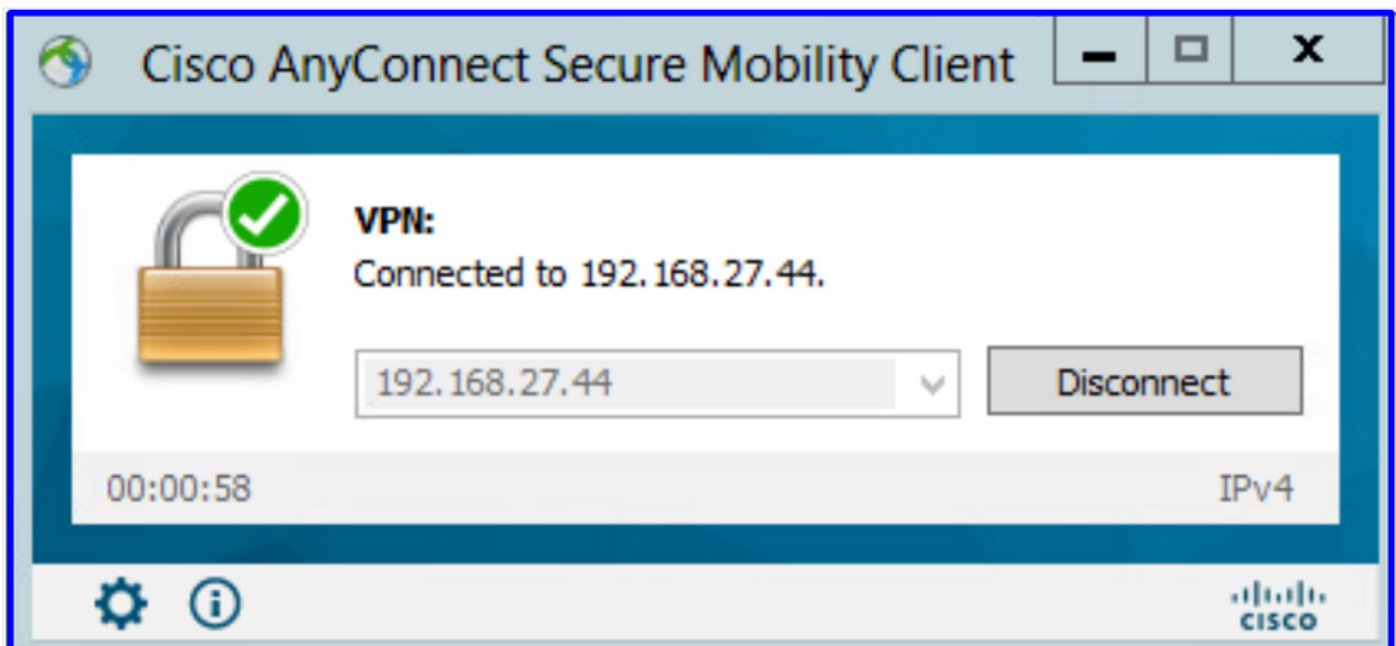
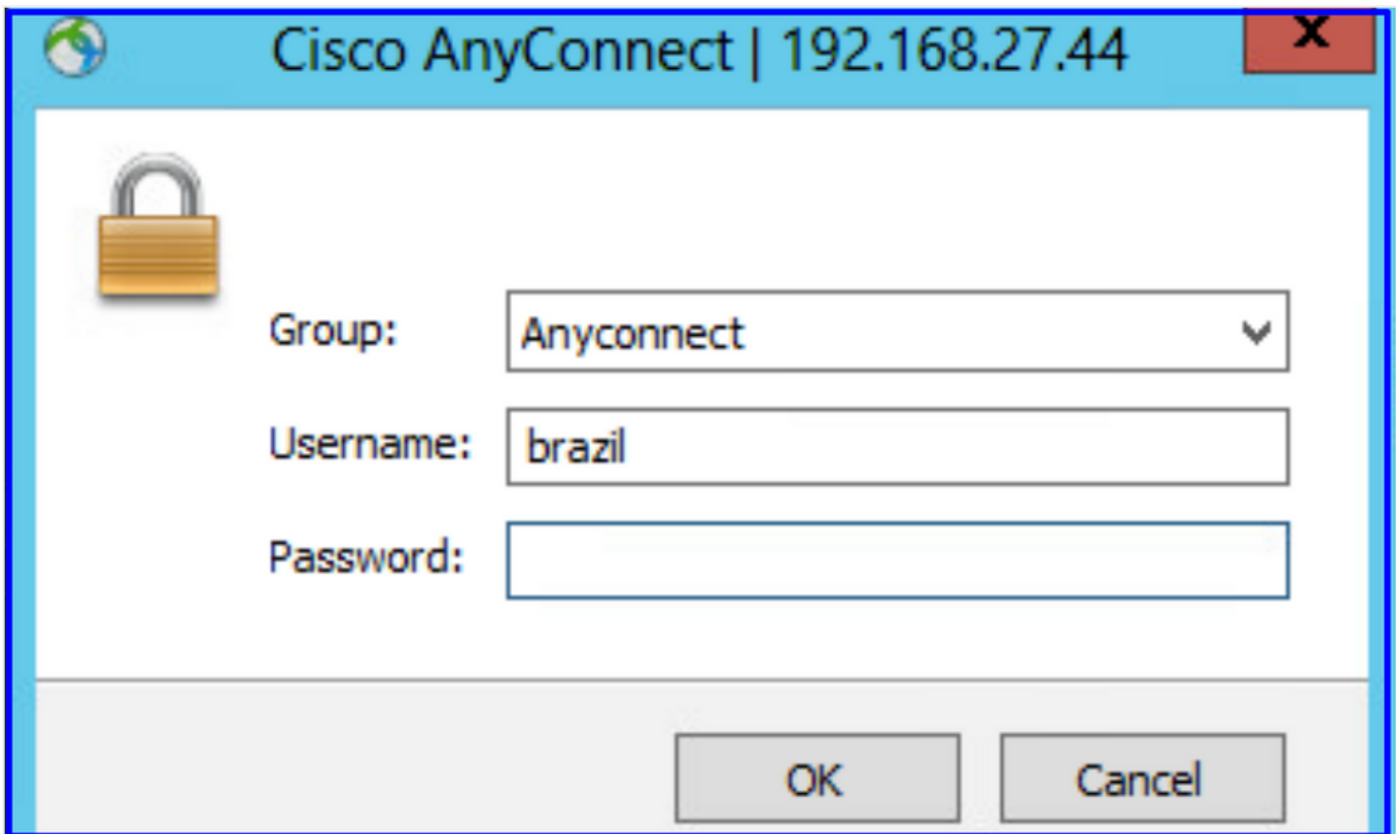
Hostname / IP Address	192.168.26.202	Port	389
<i>e.g. ad.example.com</i>			
Interface	inside (GigabitEthernet0/1)		
Encryption	NONE	Trusted CA certificate	Please select a certificate

TEST ✓ **Connection to realm is successful**

[Add another configuration](#)

CANCEL OK

Verifique se o usuário remoto pode fazer login com o cliente AnyConnect com suas credenciais do AD.



Verifique se o usuário obtém um endereço IP do pool VPN

```
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#
```

Troubleshoot

Você pode usar o `user_map_query.pl` script para validar se o FDM tem o mapeamento ip do usuário

```
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:~# █
```


No modo de silêncio, você pode configurar:

o sistema oferece suporte à depuração de identidade para verificar se o redirecionamento foi bem-sucedido.

```
> 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
```

Informações Relacionadas

Configurar VPN de acesso remoto no FTD gerenciado pelo FDM

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