Configuration de l'authentification passive avec connexion VPN d'accès à distance sur Firepower Device Manager

Contenu

Introduction Conditions préalables Conditions requises Components Used Informations générales Configuration Vérification Dépannage Informations connexes

Introduction

Ce document décrit comment configurer l'authentification passive sur le pare-feu FTD (Firepower Threat Defense) via le Firepower Device Manager (FDM) avec des connexions VPN d'accès distant (RA VPN) avec AnyConnect.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Device Manager.
- VPN d'accès à distance.
- Stratégie d'identité.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Threat Defense (FTD) version 7.0
- Cisco AnyConnect Secure Mobility Client version 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La stratégie d'identité peut détecter les utilisateurs associés à une connexion. La méthode utilisée est l'authentification passive, car l'identité de l'utilisateur est obtenue à partir d'autres services d'authentification (LDAP).

Dans FDM, l'authentification passive peut fonctionner avec deux options différentes :

- Connexions VPN d'accès à distance
- Cisco Identity Services Engine (ISE)

Configuration

Diagramme du réseau



Remote user

Cette section décrit comment configurer l'authentification passive sur FDM.

Étape 1. Configurer la source d'identité

Que vous collectiez l'identité de l'utilisateur activement (par l'invite d'authentification de l'utilisateur) ou passivement, vous devez configurer le serveur Active Directory (AD) qui possède les informations d'identité de l'utilisateur.

Naviguez vers Objets >Services d'identité et sélectionnez l'optionADpour ajouter Active Directory.

Ajouter la configuration Active Directory :

Identity Realm is used for Identity Policies and Remote Access VPN. Any changes impact all features that use this realm.

Name	Туре	
AnyConnect_LDAP	Active Directory (AD)	~
Directory Username	Directory Password	
brazil		
e.g. user@example.com		
Base DN	AD Primary Domain	
CN=Users,dc=cmonterr,dc=local	cmonterr.local	
e.g. ou=user, dc=example, dc=com	e.g. example.com	
Directory Server Configuration		
192.168.26.202:389		<u>Test</u> 👻
Add another configuration		
	CANCEL	ок

Étape 2. Configurer le VPN RA

La configuration du VPN d'accès à distance peut être examinée dans cette liaison

Étape 3. Configurez la méthode d'authentification pour les utilisateurs VPN RA

Dans la configuration du VPN RA, sélectionnez la méthode d'authentification. La source d'indeité principale pour l'authentification de l'utilisateur doit être AD.

Primary Identity Source	
Authentication Type	
AAA Only 🗸	
Primary Identity Source for User Authentication	Fallback Local Identity Source 🔔
AnyConnect_LDAP ~	LocalIdentitySource ~
Strip Identity Source server from username	
Strip Group from Username	

Note: Dans les paramètres globaux du VPN RA, décochez l'option Bypass Access Control

Policy pour le trafic déchiffré (**sysopt permit-vpn**) afin de permettre la possibilité d'utiliser la politique de contrôle d'accès pour inspecter le trafic provenant des utilisateurs AnyConnect.

On stiffing to a fill be deep to be stifted		
Certificate of Device Identity	Outside Interface	
AnyConnect_VPN ~	outside (GigabitEther	met0/0) ~
Fully-qualified Domain Name for the Outside Interf	ace	Port
fdm.ravpn		443
e.g. ravpn.example.com		e.g. 8080
Bypass Access Control policy for decrypted to NAT Exempt	raffic (sysopt permit-vpn)]
Inside Interfaces	Inside Networks	
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks +	Inside Networks The internal networks remo allowed to use. The IP vers and address pools must ma both.	ote access VPN users are ions of the internal networks atch, either IPv4, IPv6, or
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks	Inside Networks The internal networks remo allowed to use. The IP vers and address pools must ma both.	ote access VPN users are ions of the internal networks atch, either IPv4, IPv6, or
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks inside (GigabitEthernet0/1)	Inside Networks The internal networks remo allowed to use. The IP vers and address pools must ma both. FDM_Local_network	ote access VPN users are ions of the internal networks atch, either IPv4, IPv6, or
Inside Interfaces The interfaces through which remote access VPN users can connect to the internal networks inside (GigabitEthernet0/1)	Inside Networks The internal networks remo allowed to use. The IP vers and address pools must ma both. FDM_Local_network	ote access VPN users are ions of the internal networks atch, either IPv4, IPv6, or

Étape 4. Configurer la stratégie d'identité pour l'authentification passive

Vous devez créer la stratégie d'identité afin de configurer l'authentification passive, la stratégie doit comporter les éléments suivants :

- Source de l'identité AD : Identique à l'étape 1
- Action : AUTH PASSIVE

Afin de configurer la règle d'identité, naviguez **versPolicies>Identity >**select **[+]** pour ajouter une nouvelle règle d'identité.

Définissez les sous-réseaux source et de destination auxquels s'applique l'authentification passive.

Order Title		AD Identity Source	Action		PAS	SIVE AUTHENTICATIO	DN	- Identify from other	
1 ∨ AnyCon	nect	AnyConnect_LDAP	~ 🗠 F	Passive Auth		if all types of connections, obtain user identity from other ithentication services without prompting for username and password.			
Source / Destination					With	Identity Sources	Anyconne	ect	
SOURCE				DESTINATION					
Zones	+ Networks	+ Ports	+	Zones	+	Networks	+	Ports	+
ANY	ANY	ANY		ANY		ANY		ANY	

Étape 5. Créer la règle de contrôle d'accès dans la stratégie de contrôle d'accès

Configurez la règle de contrôle d'accès pour autoriser ou bloquer le trafic en fonction des utilisateurs.

Г				SOURCE			DESTINATION							
L	н	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS		ACTIONS
>	1	Inside_Outside	Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	brazil	S. C.	

Afin de configurer les utilisateurs ou le groupe d'utilisateurs pour qu'ils disposent d'une authentification passive, sélectionnez l'onglet Utilisateurs. Vous pouvez ajouter un groupe d'utilisateurs ou un utilisateur individuel.

Order Title	A	ction	
1 ~ Inside_Outside_Rule		Allow ✓	
Source/Destination Applications URLs	Users Intrusion Policy	File policy	Logging
AVAILABLE USERS		+	1 CONTROLLING ACCESS FOR USERS AND USER GROUPS
¥ Filter			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
Identity Sources Groups Users			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
AnyConnect_LDAP \ administrator	A		from one group to another.
San AnyConnect_LDAP \ brazil			
AnyConnect_LDAP \ calo-maintenance			

Déployez les modifications.

Vérification

Vérifiez que la connexion de test avec AD a réussi

Identity Realm is used for Identity Policies and Remote this realm.	Access VPN. Any changes impact all features that use
Name	Туре
AnyConnect_LDAP	Active Directory (AD)
Directory Username	Directory Password
brazil	
e.g. user@example.com	
Base DN	AD Primary Domain
CN=Users,dc=cmonterr,dc=local	cmonterr.local
e.g. ou=user, dc=example, dc=com	e.g. example.com
Directory Server Configuration	
192.168.26.202:389	*
Hostname / IP Address	Port
192.168.26.202	389
e.g. ad.example.com	
Interface	
inside (GigabitEthernet0/1)	
Encryption	Trusted CA certificate
NONE 🗸	Please select a certificate
TEST Connection to realm is successful Add another configuration	1
	CANCEL

Vérifiez que l'utilisateur distant peut se connecter avec le client AnyConnect avec ses informations d'identification Active Directory.

3	Cisco Ang	yConnect 192.168.27.44
	Group: Username: Password:	Anyconnect V brazil
		OK Cancel
🕙 Cisco	o AnyConneo	ct Secure Mobility Client 🗕 🗖 🗙

	VPN: Connected to 192.168.27.44. 192.168.27.44	V	Disconnect
00:00:58			IPv4
¢ ()			uluiu cisco

Vérifier que l'utilisateur obtient une adresse IP du pool VPN

firepower# show vpn-s	essiondb anyco	onnect filter na	me	brazil
Session Type: AnyConn	lect			
Username : brazil Assigned IP : 192.16 Protocol : AnyCon License : AnyCon Encryption : AnyCon Hashing : AnyCon	8.19.1 nect-Parent S nect Premium nect-Parent:	Index Public IP SL-Tunnel (1)none SSL-Tun (1)none SSL-Tun	: : nel	23 192.168.27.40 : (1)AES-GCM-256
Bytes Tx : 15818 Group Policy : DfltGr Login Time : 13:22: Duration : Oh:00m Inactivity : Oh:00m	pPolicy 20 UTC Wed Ju 1:13s 1:00s	Bytes Rx Tunnel Group 1 21 2021	:	2494 Anyconnect
VLAN Mapping : N/A Audt Sess ID : 000000	000001700060 f 8	VLAN 31f8c		none
Security Grp : none		Tunnel Zone		0

Dépannage

Vous pouvez utiliser **user_map_query.**plscript pour valider que le FDM possède le mappage ip utilisateur

En mode clish, vous pouvez configurer :

prise en charge du système identity-debugpour vérifier si la redirection a réussi.

```
> 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 > 8.8.8-53 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 > 8.8.8-53 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 > 8.8.8-53 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 O 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 > 8.8.8-53 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 > 8.8.8-53 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 > 8.8.8-53 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 > 8.8.8-53 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
```

Informations connexes

Configuration du VPN d'accès à distance sur FTD géré par FDM

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