セキュアなクライアントVPNユーザに対するス タティックIPアドレス割り当ての設定

| 内科 | 容 |
|-------------|---------------|
| はじめ | <u>512</u> |
| <u>前提</u> 条 | |
| <u>要</u> 何 | <u>#</u> |
| 使月 | 用するコンポーネント |
| <u>背景該</u> | <u>兑明</u> |
| <u>設定</u> | |
| <u>確認</u> | |
| トラフ | <u>ブルシュート</u> |

はじめに

このドキュメントでは、LDAP属性マップを使用してリモートアクセスVPNユーザにスタティッ クIPアドレスを割り当てる方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Active Directory (AD)
- Lightweight Directory Access Protocol(LDAP)
- Cisco Secure Firewall脅威対策
- Cisco Secureファイアウォール管理センター

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Windows Server 2022
- FTDバージョン7.4.2
- FMCバージョン7.4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

背景説明

◆ 注:IPアドレス割り当てにレルムを使用し、LDAP属性マップを設定するオプションは、 firepowerバージョン6.7以降でサポートされています。先に進む前に、firepowerのバージョ ンが6.7以降であることを確認してください。

設定

ステップ 1: Devices > Remote Accessに移動し、目的のRemote Access VPN Policyを選択しま す。目的の接続プロファイルを選択します。AAAタブで、Authentication ServerとAuthorization Serverのレルムを選択します。

| Edit Connection Profile | | 0 |
|--|--|-----|
| Connection Profile:* Group Policy:* | RAVPN_PROFILE DfltGrpPolicy + Group Policy AAA Aliases | |
| Authentication | AAA Only | |
| Authentication Method: Authentication Server: | WINDOWS_2022_AD (AD) | |
| Use secondary authenticat | Fallback to LOCAL Authentication | |
| Authorization | | |
| Authorization Server: | Use same authentication server 💌 | |
| | Allow connection only if user exists in authorization database Configure LDAP Attribute Map | |
| Accounting | | - 1 |
| Accounting Server: | | - 1 |
| Advanced Settings | | |
| | Cancel Sav | /e |

ステップ 2: Devices > Remote Accessに移動し、目的のリモートアクセスVPNポリシーを選択し ます。Advanced > Address Assignment Policyの順に選択し、Use authorization server (Only for RADIUS or Realm)オプションが有効になっていることを確認します。



ステップ 3: Advanced > LDAP Attribute Mappingの順に移動し、LDAP Attribute Nameが msRADIUSFramedIPAddressに設定され、Cisco Attribute NameがIETF-Radius-Framed-IP-Addressに設定された名前マップを追加します。

| Firewall Managemen Devices / VPN / Edit Advance | nt Center Overview Analysis P | folicies Devices Objects Integration | Deploy Q ổ 🌣 🛛 admin - 📩 SECURE |
|--|--|---|---|
| RAVPN_POLICY | | | Save Cancel |
| Enter Description | | | |
| | | | Policy Assignments (1) |
| | | | Local Realm: None Dynamic Access Policy: None |
| Connection Profile Access Inte | erfaces Advanced | | |
| Secure Client Images | LDAP Attribute Mapping | | |
| Secure Client Customization | LDAP attribute mapping can be configured to enable | LDAP server to perform authorization. | |
| GUI Text and Messages | | | + |
| Icons and Images | Realm | Мар | |
| Scripts | WINDOWS_2022_AD | | / i |
| Binaries | | | |
| Custom Installer Transforms | | Configure LDAP Attribute Map | 1 |
| Address Assignment Policy | | Realm: | |
| Cartificata Mans | | WINDOWS_2022_AD (AD) + | |
| Group Policies | | | |
| LDAP Attribute Mapping | | LDAP attribute Maps: + | |
| Load Balancing | | Name Map: | |
| ✓ IPsec | | LDAP Attribute Name Cisco Attribute Name | |
| Crypto Maps | | msRADIUSFramedIPAddress v IETF-Radius-Framed-IP-Address v | |
| IKE Policy | | Value Maps: | |
| IPsec/IKEv2 Parameters | | LDAP Attribute Value Cisco Attribute Value | |
| | | Add Value Map | |
| | | | |
| | | | |
| | | Cancel OK | |
| | | | |

ステップ 4: Windows ADサーバでServer Managerを開き、Tools > Active Directory Users and Computersの順に移動します。userで右クリックして、Properties > Dial-inの順に選択し、Assign Static IP Addressesチェックボックスをオンにします。

| Jo | hn | Doe | Pro | perties |
|----|----|-----|-----|---------|
| | | | | |

| | control | Remote D | esktop Se | rvices Profile | COM+ |
|---|---|-----------------|-------------|-----------------------------------|--------------|
| General | Address | Account | Profile | Telephones | Organization |
| Member | Of | Dial-in | Envi | ronment | Sessions |
| Network Allow Deny Control | Access Pen access access ol access th | mission ——— | twork Polic | 2y | |
| Callback | Caller-ID: Options — allback v Caller (Boy | ting and Perm | Г | | |
| C Alum | in Callback | | ote Acces | s Service only) | |
| C Alway | vs Callback t | to: | | s Service only) | |
| C Alway Assign Define If Dial-in co | n Static IP A P addresses | to: ddresses | this | s Service only) Static IP Addr | esses |

ステップ 5:Static IP Addressesを選択して、static IP addressをユーザに割り当てます。

| Static IP Addresses | × |
|-------------------------------|--------------------|
| Assign a static IPv4 address: | 172 . 16 . 20 . 73 |
| Assign a static IPv6 address: | |
| Prefix: | |
| Interface ID: | |
| OK | Cancel |

手順 6:VPNゲートウェイに接続し、Cisco Secure Clientを使用してログインします。設定した 固定IPアドレスがユーザに割り当てられます。

| S Cisco Secure Client | - | × |
|--|--|--------------|
| cisco Secure (| Client | 0 |
| General | Virtual Private Network (VPN) | |
| Status Overview | Preferences Statistics Route Details Firewall Message History | |
| AnyConnect VPN > | Connection Information | - ^ Î |
| Zero Trust Access | Tunnel Mode (IPv4): Tunnel All Traffic | - 11 |
| Network | Dynamic Tunnel Exclusion: None Dynamic Tunnel Inclusion: None | |
| ISE Posture | Duration: 00:00:26 Session Disconnect: None | |
| Umbreila | Management Connection State: Disconnected (user tunnel active) Address Information | _ |
| | Client (IPv4): 172.16.20.73 Client (IPv6): Not Available Server: 10.0.0.1 | |
| Collect diagnostic information for all installed components. | Bytes Reset E | xport Stats |

確認

debug Idap 255を有効にして、msRADIUSFramedIPAddress LDAP属性が取得されることを確認 します。

```
[13] Session Start
[13] New request Session, context 0x000015371bf7a628, reqType = Authentication
[13] Fiber started
[13] Creating LDAP context with uri=ldap://192.168.2.101:389
[13] Connection to LDAP server: ldap://192.168.2.101:389, status = Successful
[13] supportedLDAPVersion: value = 3
[13] supportedLDAPVersion: value = 2
[13] Binding as (Administrator@test.example) [Administrator@test.example]
[13] Performing Simple authentication for Administrator@test.example to 192.168.2.101
[13] LDAP Search:
Base DN = [CN=Users,DC=test,DC=example]
Filter = [sAMAccountName=jdoe]
Scope = [SUBTREE]
[13] User DN = [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Talking to Active Directory server 192.168.2.101
[13] Reading password policy for jdoe, dn:CN=John Doe,CN=Users,DC=test,DC=example
[13] Read bad password count 0
[13] Binding as (jdoe) [CN=John Doe, CN=Users, DC=test, DC=example]
[13] Performing Simple authentication for jdoe to 192.168.2.101
[13] Processing LDAP response for user jdoe
[13] Message (jdoe):
[13] Authentication successful for jdoe to 192.168.2.101
[13] Retrieved User Attributes:
[13] objectClass: value = top
[13] objectClass: value = person
[13] objectClass: value = organizationalPerson
[13] objectClass: value = user
[13] cn: value = John Doe
[13] sn: value = Doe
[13] givenName: value = John
[13] distinguishedName: value = CN=John Doe,CN=Users,DC=test,DC=example
[13] instanceType: value = 4
[13] whenCreated: value = 20240928142334.0Z
[13] whenChanged: value = 20240928152553.0Z
[13] displayName: value = John Doe
[13] uSNCreated: value = 12801
[13] uSNChanged: value = 12826
[13] name: value = John Doe
[13] objectGUID: value = .....fA.f...;.,
[13] userAccountControl: value = 66048
[13] badPwdCount: value = 0
[13] codePage: value = 0
[13] countryCode: value = 0
[13] badPasswordTime: value = 0
[13] lastLogoff: value = 0
[13] lastLogon: value = 0
[13] pwdLastSet: value = 133720070153887755
[13] primaryGroupID: value = 513
[13] userParameters: value = m: d.
[13] objectSid: value = .....Q=.S....=...Q...
[13] accountExpires: value = 9223372036854775807
[13] logonCount: value = 0
[13] sAMAccountName: value = jdoe
```

[13] sAMAccountType: value = 805306368 [13] userPrincipalName: value = jdoe@test.example [13] objectCategory: value = CN=Person,CN=Schema,CN=Configuration,DC=test,DC=example [13] msRADIUSFramedIPAddress: value = -1408232375 [13] mapped to IETF-Radius-Framed-IP-Address: value = -1408232375 [13] msRASSavedFramedIPAddress: value = -1408232375 [13] dSCorePropagationData: value = 16010101000000.0Z [13] lastLogonTimestamp: value = 133720093118057231 [13] Fiber exit Tx=522 bytes Rx=2492 bytes, status=1 [13] Session End

トラブルシュート

debug コマンド:

debug webvpn 255

LDAPのデバッグ

目的のRA VPNユーザに割り当てられたスタティックIPアドレスを検証するコマンド:

show vpn-sessiondb anyconnect filter name <ユーザ名>

<#root>

firepower#

show vpn-sessiondb anyconnect filter name jdoe

Session Type: AnyConnect

Username : jdoe Index : 7 Assigned IP : 172.16.20.73 Public IP : 10.0.0.10 Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel License : AnyConnect Premium Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256 Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384 Bytes Tx : 14664 Bytes Rx : 26949 Group Policy : DfltGrpPolicy Tunnel Group : RAVPN_PROFILE Login Time : 11:45:48 UTC Sun Sep 29 2024 Duration : Oh:38m:59s Inactivity : Oh:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : cb0071820000700066f93dec Security Grp : none Tunnel Zone : 0 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。