モバイルアクセス用のAnyconnect証明書ベース 認証の設定

| 内容 |
|---------------------------------|
| |
| 前提条件 |
| <u>要件</u> |
| <u>使用するコンポーネント</u> |
| <u>FTDでのCisco Anyconnectの設定</u> |
| <u>ネットワーク図</u> |
| <u>FTDへの証明書の追加</u> |
| <u>Cisco Anyconnectの設定</u> |
| <u>モバイルユーザ用の証明書の作成</u> |
| <u>モバイルデバイスでのインストール</u> |
| |
| <u>トラブルシュート</u> |
| <u>デバッグ</u> |
| |

概要

このドキュメントでは、モバイルデバイスに証明書ベースの認証を実装する例について説明しま す。

前提条件

このガイドで使用するツールとデバイスは次のとおりです。

- Cisco Firepower Threat Defense (FTD)
- Firepower Management Center (FMC)
- Apple iOSデバイス(iPhone、iPad)
- 認証局(CA)
- Cisco Anyconnectクライアントソフトウェア

要件

次の項目に関する知識があることが推奨されます。

- 基本的なVPN
- SSL/TLS
- 公開キーインフラストラクチャ
- FMCの使用経験

- OpenSSL
- Cisco AnyConnect

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。

- ・シスコFTD
- Cisco FMC
- Microsoft CA Server
- XCA
- Cisco AnyConnect
- Apple ipad

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。

FTDでのCisco Anyconnectの設定

ここでは、FMC経由でAnyConnectを設定する手順について説明します。開始する前に、すべての設定を必ず導入してください。

 Image: Authority
 Firepower Management

 Certificate
 Center

 Authority
 Image: Center

 Image: Image: Center
 Image: Center

 Image: Ce

ネットワーク図

ステップ1:FMCアプライアンスでFTDの証明書を作成します。次の図に示すように、Devices > Certificateの順に移動し、Addを選択します。

| Norm Double Ordinant Type Source Ordinant Type Y10 Obdet Moutle (A.4.0) Sole D | Firepower Management Center Devices / Certificates | Overview An | alysis Policies | Devices Objects A | MP Intelligence | | ٩ | Deploy 💕 | 🜣 📵 admin 🕶 |
|---|---|-------------|------------------|-------------------|-----------------|--|---|----------|-------------|
| Nome Nome <th< td=""><td></td><td>-</td><td></td><td></td><td></td><td></td><td>-</td><td></td><td>Add</td></th<> | | - | | | | | - | | Add |
| YPD 0x84 Marvai (CA & 0) 0x8 0x8 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | Name | Domain | Enrollment Type | Status | | | | | |
| PD 0x0at Mamati (0A 6 80) MA D D D C 0 No2 0x0at PXC512 84 AA D D D C 0 D | V == FTD1 | | | | | | | | |
| | FTD | Global | Manual (CA & ID) | CA LD | | | | | ₽ @ C ∎ |
| | ✓ IIII Tcoutrie-FTD2 | | | | | | | | |
| | ftd2 | Global | PKCS12 file | CA LD | | | | | B• 12 C ∎ |
| 11 111 | | | | | | | | | |
| 17 W1 | | | | | | | | | |
| 10111 | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| Now To | | | | | | | | | |
| Now To | | | | | | | | | |
| Now To | | | | | | | | | |
| How To | | | | | | | | | |
| How To | | | | | | | | | |
| How To | | | | | | | | | |
| How To | | | | | | | | | |
| How To | | | | | | | | | |
| How To | | | | | | | | | |
| | | | | | How To | | | | |

ステップ 2:VPN接続に必要なFTDを選択します。デバイスドロップダウンからFTDアプライア ンスを選択します。+アイコンをクリックして、次の図に示すように新しい証明書登録方式を追加 します。

| ← → C 	 O 	 A https:/ | //tcoutrie-fmc.tcoutrie-s | ecurity301.com/ddd/#P | KICerificate 🗘 🤝 🗄 🕼 🖽 🛈 🔒 | ิ ด | ▼ = |
|---|---------------------------|-----------------------|--|--------|---------------|
| Getting Started C School C Work | | | | 00 | her Bookmarks |
| CISCO Firepower Management Center Devices / Certificates | Overview An | alysis Policies | Devices Objects AMP Intelligence Q Deploy 💞 | ¢ 0 | admin 🕶 |
| | | | | | Add |
| Name | Domain | Enrollment Type | Status | | |
| ∨ ≕ FTD1 | | | | | |
| FTD | Global | Manual (CA & ID) | | ₿• 🖉 C | ŵ. |
| V == Tcoutrie-FTD2 | | | | | |
| ftd2 | Global | PKCS12 file | Add New Certificate | ₿• 🖉 C | ¥. |
| | | | Add a new certificate the device using cert enrollment object which is used to generate CA and identify certificate. | | |
| | | | How To | | |

ステップ3:デバイスに証明書を追加します。環境内で証明書を取得するための推奨される方法

ステップ 4:証明書をFTDデバイスにアップロードします。パスコード(PKCS12のみ)を入力 し、次の図に示すようにSaveをクリックします。

| Add Cert Enrollme | nt | | | • |
|--|---|----------------|--------------------|-------|
| Name* ftdcert Description | | | | |
| CA Information | Certificate Parameters | Key Rev | rocation | |
| Enrollment Type: PKCS12 File*: Passphrase: | PKCS12 File Tcoutrie-ftd2.p12 Skip Check for CA flag | ag in basic co | Browse PKCS12 File | ncate |
| | | | Cancel | Save |

◇ 注:ファイルを保存すると、証明書の展開がただちに行われます。証明書の詳細を表示する には、IDを選択します。

Cisco Anyconnectの設定

リモートアクセスウィザードを使用して、FMC経由でAnyConnectを設定します。

ステップ1:リモートアクセスVPNポリシーウィザードを起動して、Anyconnectを設定します。

Devices > Remote Accessの順に移動し、Addを選択します。

| diada cisco | Firepower Management Center Devices / VPN / Remote Access | Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | | | Q | Deploy | ¢ 🗘 | admin • |
|----------------|--|----------|----------|----------|---------------------------------|-----------------------------|--------|--------------|---|---|---|--------|-----|---------|
| | | | | | | | | | | | | | | Add |
| Name | | | | | Status | | | | Last Modified | | | | | |
| RAVP | | | | | Targeting 1 de Up-to-date or | rvices n all targeted de | evices | | 2021-07-09 17:10:3 Modified by "admin" | 1 | | / 1 | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | |
| | | | | | | | | How To | | | | | | |

ステップ2:ポリシーの割り当て

ポリシーの割り当てを完了します。 a.ポリシーに名前を付けます。

b.必要なVPNプロトコルを選択します。

c.設定を適用するターゲットデバイスを選択します。

| Remote Access VPN Policy Wizard Policy Assignment 2 Connection Profile 3 Arr | yConnect ④ Access & Certificate ⑤ Summary | | |
|---|--|---|------------------|
| | Arageted Devices and Protocols Sine: FTD2 Description: Description: Image: Sile: Orageted Devices: | Before You Start Before you start, ensure the following configuration elements to be in place to complete Remote Access Markentication Server Configure Realm or RADUS Server Group or SSO to automicate VPH clients. AryConnect Client Package Mais usery ou have the relevant Clico client downloaded or you have the relevant Clico client downloaded or you have the relevant Clico client downloaded be already Configured on targeted dorder group to exable VPH access. | |
| | How To | | Cancel Back Next |

ステップ3:接続プロファイル。

a.接続プロファイルに名前を付けます。 b.認証方式をClient Certificate Onlyに設定します。

c. IPアドレスプールを割り当て、必要に応じて新しいグループポリシーを作成します。

d. Nextをクリックします。

| Remote Access VPN Policy Wizard | • |
|--|---|
| 1 Policy Assignment Oconnection Profile | AngConnect 4 Access & Destitute Summary |
| | |
| | |
| | Connection Profile Same* |
| | This same is confected as a connection allow, it can be used to connect to the VHI gameay |
| | Authentication, Authorization & Accounting (AAA): |
| | Specify the method of authentication (AAA, confluence or both), and the AAA servers that will be used for VPN convertions. |
| | Authentication Method: Client Centificate Doly • |
| | Dummer form a Map specific field 🗌 One entre RN (Distinguished Nanc) as usernane |
| | Primey Field: CN (Common Name) + |
| | Secondary Field: None • |
| | Authorization Server: Peaks or NOUCO |
| | Accounting Server: (NAUS) |
| | Client Address Assignment: |
| | Cliert IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the other of AAA server, CHCP server and IP address pool. |
| | Use DHCP Servers |
| | C Use 87 Address Pools |
| | Ilyuk Addeess Pools; SAVAPN |
| | Pyl Address Pools |
| | Group Palay: |
| | A proce policy is a collection of near-invested as each which are assigned to clear when a VMI convectors a established. Select or unare all coope Policy edges. |
| | Group Policy* (Stidlaybility *) + |
| | Edt Grup Palcy |
| | |

◆ 注:認証セッションのユーザ名の入力に使用するプライマリフィールドを選択します。この ガイドでは、証明書のCNを使用します。

ステップ4: AnyConnect.

Anyconnectイメージをアプライアンスに追加します。Anyconnectの推奨バージョンをアップロードし、Nextをクリックします。

💊 注:Cisco Anyconnectパッケージは、Software.Cisco.comからダウンロードできます。

ステップ5:アクセスおよび証明書。

次の図に示すように、証明書をインターフェイスに適用し、インターフェイスレベルで Anyconnectを有効にして、Nextをクリックします。

| 🔹 Firefox File Edit View History Bookmarks Tools Window Help | | | | 8 Fri Jul 30 10:40 AM |
|--|--|---|----------------|-----------------------|
| Cisco Firepower Management C × + | | | | |
| ← → C @ O A https://tcoutrie-fmc.tcoutrie-security301.co | m/ddd/#RAVpnSetupWizard | | \$ S \$ 10 0 0 | 0 e T = |
| Getting Started C School Work | | | | C Other Bookmarks |
| strutte Firepower Management Center Overview Analysis Process / VPN / Setup Wizard | olicies Devices Objects AMP Intelligence | | Q, Deploy | 👂 🌣 🔕 admin 🕶 |
| = | | | | |
| Remote Access VPN Policy Wizard | | | | |
| Policy Assignment (2) Connection Profile (3) AnyConnect | Access & Certificate 5 Summary | | | |
| Remote User | AnyConnect Client Internet Cutside | VPN Inside Corporate Resources | | |
| | Network Interface for Incoming VPN Access Select or create an interface Group or a Security Zone that conta | AAA | | |
| | Interface group/Security Zone:* outside | • + | | |
| | Enable DTLS on member | interfaces | | |
| | All the devices must have interfaces as part of the Interface | Group/Security Zone selected. | | |
| | Device Certificates | | | |
| | Device certificate (also called Identity certificate) identifies the VI clients. Select a certificate which is used to authenticate the VPM | PN gateway to the remote access I gateway. | | |
| | Certificate Enrollment:* ftd2 | • + | | |
| | Enroll the selected certifi | cate object on the target devices | | |
| | Access Control for VPN Traffic | | | |
| | All decrypted traffic in the VPN tunnel is subjected to the Access this option to bypass decrypted traffic from the Access Control P | Control Policy by default. Select olicy. | | |
| | | | | |
| | | | New Tol | |
| | | | Cancel | |

手順6:要約.

設定を確認します。すべてチェックアウトしたら、finishをクリックしてからdeployをクリックし ます。

モバイルユーザ用の証明書の作成

接続に使用するモバイルデバイスに追加する証明書を作成します。

ステップ1:XCAです。

a. XCAを開きます

- b.新しいデータベースの起動
- ステップ2:CSRを作成します。
- a. Certificate Signing Request(CSR)を選択します

c.証明書に必要なすべての情報とともに値を入力します

d.新しいキーを生成する

e.終了したら、OKをクリックします。

| | 🛷 X Certificate | and Key management | | |
|-----------------------------------|-----------------|------------------------|--------------|-------------------|
| Create Certificate signing reques | t | | | a) Formations 74. |
| Source | Extensions | Key usage Netscape | Advanced | |
| Distinguished name | | | | |
| Internal name | | organizationName | | |
| countryName | | organizationalUnitName | | |
| stateOrProvinceName | | commonName | Cisco_Test | |
| localityName | | emailAddress | | |
| | | | | |
| Туре | | Content | | Add |
| | | | | Delete |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| Private kev | | | | |
| Cieco Test 1 (DCA:2048 | .:=\ | | | to a new loss |
| CISCO_Test_T (RSA-2048 | ort) | Used key | s too Genera | ite a new key |
| | | | | |
| | | | C | ancel OK |
| | | | | |

💊 注:このドキュメントでは、証明書のCNを使用します。

ステップ3:CSRを送信します。

a. CSRのエクスポート

b. CSRをCAに送信して新しい証明書を取得する

| ••• | d' X (| Certificate and Key management | | |
|-------------------------------------|--------------|--------------------------------|-------------------------|---------------------|
| | Private Keys | Certificates Tem | plates Revocation lists | |
| Internal name A commonName Signed | | | | New Request |
| | | | | Export |
| | | | | Import |
| | | | | Show Details |
| | | | | Delete |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | Jazminecta DN: 0 |
| | | | | Time Time |
| | | | | |
| Database: /Users/tcoutrie/cisco.xdb | | Search | | |

注:CSRのPEM形式を使用してください。

モバイルデバイスでのインストール

ステップ1:モバイルデバイスにデバイス証明書を追加します。 ステップ2:Anyconnectアプリケーションと証明書を共有して、新しい証明書アプリケーション を追加します。

▲ 注意:手動インストールでは、ユーザは証明書をアプリケーションと共有する必要があります。これは、MDM経由でプッシュされた証明書には適用されません。

| C Documents | | certs | Ē | 9 🔡 Select |
|--------------------|-------------|---|---|---|
| Q Search | | | | Ŷ |
| Cisco_Test.p1 | DMChain.p7b | DMS | Certificate Personal Noblesse_An | Certificate Perend Noblesse_An |
| Copy Duplicate | ڻ آ | 4/25/21, 1:50 1 KB | driod.p12 5/13/21, 7:04 4 KB | driod_1.p12 5/13/21, 7:05 4 KB |
| Move Delete | | Certificate Perional | Certificate Perional | Certificate Perional |
| Info Quick Look | () () | Noblesse_IPA D_2.p12 4/25/21, 11:18 4 KB | Noblesse_IPh one.p12 4/25/21, 10:31 3 KB | Noblesse_IPh one_1.p12 4/25/21, 11:01 4 KB |
| Tags | 0 | Part P | (And A | |
| Rename Share | / ① | Noblesse_MA | Noblesse_Wi | Noblesse_Wi |
| Compress | | C_2.p12 4/25/21, 11:19 4 КВ | ndows.p12 4/25/21, 12:56 3 KB | ndowsIKE.p12 5/12/21, 12:42 4 KB |
| | | | | |

ステップ 3:PKCS12ファイルの証明書パスワードを入力します。

ステップ4:Anyconnectで新しい接続を作成します。

ステップ 5:新しい接続に移動します。Connections > Add VPN Connection。

| AnyConnect | VPN Connections | |
|---------------------------------|---------------------------|----|
| PRIMARY VIRTUAL PRIVATE NETWORK | | |
| AnyConnect VPN | CALO Cabled | i |
| Connections CALO > | НОМЕІКЕ | i) |
| Details Disconnected > | HOMEIKE-IN | i) |
| GENERAL | HOMESSL-IN | i) |
| Settings > | HomeIPEC-IN | i) |
| Diagnostics > | HomeIPSEC | Ð |
| About > | HomeSSL | Ð |
| | rtp-vpn-cluster.cisco.com | Ð |
| | Add VPN Connection | |
| | | |
| | | |
| cisco | | |

手順6:新しい接続の情報を入力します。

説明:接続に名前を付けます。

サーバアドレス:FTDのIPアドレスまたはFQDN

Advanced:その他の設定

手順7: [Advanced] を選択します。

ステップ8: Certificateを選択し、新しく追加した証明書を選択します。

| Any | Connect | | VPN Connections | | |
|----------------|------------------|---------------------------------|---|-------------|------------|
| PRIMARY VIRTUA | L PRIVATE NETWOR | к | | | |
| AnyConnect VPN | | Advance | d Select Certificate | | (j) |
| Connections | FT | | | | (i) |
| Details | Disconnecte | Disabled Selecting thi | is option will disable certificate author | tication | <u>()</u> |
| | | | | | U |
| GENERAL | | Automatic | omatically select a certificate for auth | entication. | i |
| Settings | | Noblesse | _IPAD | | i |
| Diagnostics | | Issuer: DMs | sliders-TCOUTRIE-SRV-CA | (i) > | i |
| | | Cisco Tes | Date: Apr 25, 2022 11:00:36 | | |
| About | | Issuer: DMs | sliders-TCOUTRIE-SRV-CA | (i) > | U |
| | | Expiration [| Date: Aug 02, 2022 08:12:47 | | í |
| | | Noblesse | _IPAD sliders-TCOUTRIE-SRV-CA | (i) > | <u>(</u>) |
| | | Expiration D Noblesse | Date: Apr 25, 2022 11:04:38 _IPAD | 0 | |
| Is | | Issuer: DMs | er: DMsliders-TCOUTRIE-SRV-CA | | |
| | | Expiration D | Date: Apr 25, 2022 00:42:05 | | |
| cisco | | | | | |
| | | | | | |

ステップ9: Connectionsに戻り、テストします。

正常に完了すると、切り替えはオンのままになり、ステータスに詳細がconnectedと表示されま す。



確認

show vpn-sessiondb detail Anyconnectコマンドは、接続されているホストに関するすべての情報 を表示します。

Lント:このコマンドをさらにフィルタリングするオプションは、コマンドに追加された「 filter」キーワードまたは「sort」キーワードです。

例:

Tcoutrie-FTD3# show vpn-sessiondb detail Anyconnect

Username : Cisco_Test Index : 23 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Protocol : Anyconnect-Parent SSL-Tunnel DTLS-Tunnel License : Anyconnect Premium, Anyconnect for Mobile Encryption : Anyconnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256 Hash : Anyconnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384 Bytes Tx : 8627 Bytes Rx : 220 Pkts Tx : 4 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : SSL Tunnel Group : SSL Login Time : 13:03:28 UTC Mon Aug 2 2021 Duration : 0h:01m:49s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a7aa95d000170006107ed20 Security Grp : none Tunnel Zone : 0 Anyconnect-Parent Tunnels: 1 SSL-Tunnel Tunnels: 1 DTLS-Tunnel Tunnels: 1 Anyconnect-Parent: Tunnel ID : 23.1 Public IP : 10.118.18.168 Encryption : none Hashing : none TCP Src Port : 64983 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : apple-ios Client OS Ver: 14.6 Client Type : Anyconnect Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 6299 Bytes Rx : 220 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 SSL-Tunnel: Tunnel ID : 23.2 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 64985 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : SSL VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 2328 Bytes Rx : 0 Pkts Tx : 2 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0 DTLS-Tunnel: Tunnel ID : 23.3 Assigned IP : 10.71.1.2 Public IP : 10.118.18.168 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384 Encapsulation: DTLSv1.2 UDP Src Port : 51003 UDP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes Client OS : Apple iOS Client Type : DTLS VPN Client Client Ver : Cisco Anyconnect VPN Agent for Apple iPad 4.10.01099 Bytes Tx : 0 Bytes Rx : 0 Pkts Tx : 0 Pkts Rx : 0 Pkts Tx Drop : 0 Pkts Rx Drop : 0

トラブルシュート

デバッグ

この問題のトラブルシューティングに必要なデバッグは次のとおりです。

Debug crypto ca 14

Debug web∨pn 255

Debug webvpn Anyconnect 255

接続がSSLではなくIPSECの場合:

Debug crypto ikev2 platform 255

Debug crypto ikev2 protocol 255

debug crypto CA 14

Anyconnectモバイルアプリケーションからのログ:

Diagnostic > VPN Debug Logs > Share logsの順に移動します。

| AnyConnect | Diagnostics |
|---------------------------------|----------------------|
| PRIMARY VIRTUAL PRIVATE NETWORK | |
| AnyConnect VPN | VPN Debug Logs |
| Connections Asa1 > | Logs |
| Details Disconnected > | System Information > |
| | Share Logs |
| GENERAL | Customize Debug Logs |
| Settings > | |
| Diagnostics | Certificates |
| About > | Profile |
| | Localization |
| | |
| | |
| | |
| | |
| cisco | |
| | |

次の情報を入力します。

- 問題
- 再現手順

次に、Send > Share withの順に移動します。

| 3:49 PM Wed Sep 29 | | ••• | २ 47% 🔳 | | |
|---------------------|---|--|----------------|---|--|
| AnyConnect | | Diagnostics | | | |
| | RK | | | | |
| AnyConnect VPN | Cance | I Share Logs | Send | | |
| Connections Asa | Please of following | describe the problem and steps to r g fields. | Email logs to | > | |
| Details Disconnecte | PROBLEM | И | Administrator | > | |
| GENERAL | Test | | Cisco | | |
| Settings | STEPS TO | O REPRODUCE | Share with | > | |
| Diagnostics | Test | | | > | |
| About | | | | > | |
| | | | | > | |
| | The data sent is for diagnostic purposes only and may contain information about configured connections, as well as server and endpoint identities, IP addresses, and username. This data will appear to come from the email address you specify and will not be used for marketing or advertising purposes. | | | | |
| CISCO | | | | | |

これは、電子メールクライアントを使用してログを送信するオプションを提供します。

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。