为移动访问配置基于Anyconnect证书的身份验证

目录

| <u>简介</u> |
|--------------------|
| <u>先决条件</u> |
| · <u>要求</u> |
| 使用的组件 |
| <u> </u> |
| 网络图 |
| <u>向FTD添加证书</u> |
| 配置Cisco Anyconnect |
| <u>为移动用户创建证书</u> |
| 在移动设备上安装 |
| |
| <u>故障排除</u> |
| <u>调试</u> |

简介

本文档介绍在移动设备上实施基于证书的身份验证的示例。

先决条件

本指南中使用的工具和设备包括:

- 思科Firepower威胁防御(FTD)
- Firepower Management Center (FMC)
- Apple iOS设备(iPhone、iPad)
- 证书颁发机构 (CA)
- Cisco Anyconnect客户端软件

要求

Cisco 建议您了解以下主题:

- ・ 基本VPN
- SSL/TLS
- 公钥基础设施
- 使用FMC的经验
- OpenSSL
- Cisco Anyconnect

使用的组件

本文档中的信息基于以下软件和硬件版本:

- ・思科FTD
- ・思科FMC
- Microsoft CA服务器
- XCA
- Cisco Anyconnect
- Apple ipad

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

在FTD上配置Cisco Anyconnect

本节介绍通过FMC配置Anyconnect的步骤。开始之前,请务必部署所有配置。

网络图



向FTD添加证书

步骤1:在FMC设备上为FTD创建证书。导航到设备>证书,然后选择添加,如下图所示:

| Firepower Management Center Devices / Certificates | Overview An | alysis Policies | Devices Objects | AMP | Intelligence | ۹ | Deploy | \$ \$ \$ | admin 🕶 |
|---|-------------|------------------|-----------------|-----|--------------|---|--------|-----------------|---------|
| | = | | | | | - | | \langle | Add |
| Name | Domain | Enrollment Type | Status | | | | | | |
| V = FTD1 | | | | | | | | | |
| FTD | Global | Manual (CA & ID) | CA ID | | | | | ₽ 🖉 | C 🗑 |
| V Tcoutrie-FTD2 | | | | | | | | | |
| ftd2 | Global | PKCS12 file | CA (, ID) | | | | | G• 🕜 | C 🕯 |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | łow To | | | | |
| | | | | | | | | | |

第二步:选择VPN连接所需的FTD。从devices下拉列表中选择FTD设备。单击+图标可添加新的证 书注册方法,如下图所示:

| ← → C @ O & https: | //tcoutrie-fmc. tcoutrie-s | ecurity301.com/ddd/#P | KiCerificate 🏠 😇 生 lin 🖽 🖸 🕻 | 8 0 | = 🐮 = |
|------------------------------|-----------------------------------|-----------------------|--|--------------|-----------------|
| Getting Started School Work | | | | C | Other Bookmarks |
| CISCO Devices / Certificates | Overview An | alysis Policies | Devices Objects AMP Intelligence Q Deploy | \$ \$ | 🛛 admin 🕶 |
| | | | | | Add |
| | | | | | _ |
| Name | Domain | Enrollment Type | Status | | |
| V = FTD1 | | | | | |
| FTD | Global | Manual (CA & ID) | LOA L.R. | ₽ ₽ | C . |
| V Tcoutrie-FTD2 | | | | | |
| ftd2 | Global | PKCS12 file | Add New Certificate | ₽ ₽ | C T |
| | | | Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate. Tooutrier-FTD2 Cert Enrollment*: Select a certificate entrollment object + + + + + + + + + + + + + + + + + + + | | |
| | | | | | |
| | | | | | |
| | | | How To | | |

第三步:将证书添加到设备。选择在环境中获取证书的首选方法。

提示:可用选项包括:自签名证书 — 本地生成新证书、SCEP — 使用简单证书注册协议从 CA获取证书、手动 — 手动安装根和身份证书、PKCS12 — 上传包含根、身份和私钥的加密 证书捆绑包。

| Add Cert Enrollme | nt | | ? |
|---------------------------|------------------------|---|------|
| Name* ftdcert Description | | | |
| CA Information | Certificate Parameters | Key Revocation | |
| Enrollment Type: | PKCS12 File | ▼ | |
| PKCS12 File*: | Tcoutrie-ftd2.p12 | Browse PKCS12 File | |
| Passphrase: | | | |
| | Skip Check for CA fla | g in basic constraints of the CA Certif | cate |
| | | Cancel | Save |

💊 注意:保存文件后,立即部署证书。要查看证书详细信息,请选择ID。

配置Cisco Anyconnect

使用远程访问向导通过FMC配置Anyconnect。

步骤1:启动远程访问VPN策略向导以配置Anyconnect。

导航到设备>远程访问,然后选择添加。

| diada cisco | Firepower Management Center Devices / VPN / Remote Access | Overview | Analysis | Policies | Devices | Objects | AMP | Intelligence | | Q | Deploy | 6 ¢ | admin • |
|----------------|--|----------|----------|----------|----------------------------------|--------------------------|-------|--------------|--|---|--------|------------|---------|
| | | | | | | | | | | | | → | Add |
| Name | | | | | Status | | | | Last Modified | | | | |
| RAVP | 4 | | | | Targeting 1 dev Up-to-date on | ices all targeted dev | lices | | 2021-07-09 17:10:31 Modified by "admin" | | / 1 | | |
| | | | | | | | | | | | | | |

第二步:策略分配。

完成策略分配: a.命名策略。

b.选择所需的VPN协议。

c.选择要应用配置的目标设备。

| Remote Access VPN Policy Wizard | | | | | | | | | | |
|--|---|--|--|--|--|--|--|--|--|--|
| 🕒 Policy Assignment 2 Connection Profile 3 AnyConnect 6 Access & Certificate 6 Summary | | | | | | | | | | |
| Targeted Devices and Protocols Trip Trip Description: Description: <td>Carbona Construction Constru</td> | Carbona Construction Constru | | | | | | | | | |
| How To | Cancel Back Next | | | | | | | | | |

第三步:连接配置文件。

a.命名连接配置文件。

b.将身份验证方法设置为Client Certificate Only。

c.分配IP地址池,如果需要,创建新的组策略。

d.单击下一步。

| | - | |
|-------------------------------------|---|--|
| a Access VPN Policy Wittard | = | |
| Access VPN Policy Wizard | | |
| icy Assignment 🚺 Connection Profile | 3 AnyConnect 4 Access & Certificate 5 Summary | |
| | | |
| | Connection Profile: | |
| | Connection Pudies seecily the sumal group publices for a VMR connection. These policies pertains to oreating the sumal task: how AAA is accompliable and how addresses are assigned. They also include user artificates, which are difficult in provide difficult. | |
| | Covaction Puttiniania & WARPET | |
| | Authentication, Authorization & Accounting (AAA): | |
| | Server's his method of authentication (AAA, certification or locit), and the AAA assess that will be used for VPN certestration. | |
| | Autoentication Methods Cenet Certificate Only | |
| | Control A Log search faith C and C Control A Log search faith C Control A | |
| | 1 mmg ya ku kuman ku | |
| | Authorization Server: Press or InCOD | |
| | Accounting Server: Account v + | |
| | Clent Address Assignment: | |
| | Client P address care to assigned from AAA server, and P address pools. Them multiple options are statistical, P address assignment for all the solutier AAA servers. (DEM server and P address pool). | |
| | backAA.Seere Jaanse HARDS on g | |
| | S Use IP Address Pods | |
| | Diva Address Pool: BAUTN / | |
| | Pr/ Advans Note | |
| | A group policy is a collection of user-inverted associated antibiotes which are assigned to cleart when a VM | |
| | Group Mary* DMGyrlaicy + + | |
| | Edit Group Palicy | |

✤ 注意:选择要用于输入身份验证会话的用户名的主字段。本指南中使用了证书的CN。

第四步:AnyConnect.

将Anyconnect映像添加到设备。上传Anyconnect的首选版本,然后单击Next。

注意:Cisco Anyconnect软件包可以从Software.Cisco.com下载。

第五步:访问和证书。

将证书应用到接口并在接口级别启用Anyconnect(如图所示),然后单击Next。



第六步:摘要.

检查配置。如果所有签出,请单击finish,然后单击deploy。

为移动用户创建证书

创建要添加到连接中使用的移动设备的证书。

步骤1:XCA。

a.打开XCA

b.启动新数据库

第二步:创建CSR

a.选择证书签名请求(CSR)

b.选择New Request

c.输入包含证书所需全部信息的值

d.生成新密钥

e.完成后,单击OK

| eate Certificate signing request | | () Formings |
|---|--|--------------------------|
| Source | Extensions Key usage Netscape | Advanced |
| Internal name countryName stateOrProvinceName localityName | organizationName organizationalUnitName commonName emailAddress | Cisco_Test |
| Туре | Content | Add Delete |
| Private key Cisco_Test_1 (RSA:2048 bit) | 😮 🗌 Used keys | s too Generate a new key |
| | | Cancel |

╲ 注:本文档使用证书的CN。

第三步:提交企业社会责任。

a.导出CSR

b.向CA提交CSR以获取新证书

| | | I | X Certificate and Key management | |
|---|------------------------------------|--------------|---|----------------------------|
| | | Private Keys | Certificates Templates Revocation lists | |
| | Internal name A commonName Signed | | | New Pequet |
| | Cisco_Test Cisco_Test Unhandled | | | New Request |
| | | | | Export |
| | | | | Import |
| | | | | Show Details |
| | | | | Delete |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | Jarminecta Dingroof Tim |
| | | | | - Jame |
| | | | | |
| | | | | |
| D | atabase: /Users/tcoutrie/cisco.xdb | | Search | |

Search Search

在移动设备上安装

步骤1:将设备证书添加到移动设备。 第二步:与Anyconnect应用共享证书以添加新的证书应用。

⚠ 注意:手动安装需要用户与应用程序共享证书。这不适用于通过MDM推送的证书。

| C Documents | | certs | Ē | Select |
|--------------------|-------------|-------------------------|---|---|
| Q Search | | | | Ŷ |
| Cisco_Test.p1 | DMChain.p7b | DMS 4/25/21, 1:50 | Certificate Certificate | Certificate Present Desse_An driod_1.p12 5/13/21_7:05 |
| Duplicate | Ē | T KD | 4 KB | 4 KB |
| Move Delete | | Certificate Personal | Certificate Personal | Certificate Personal |
| h Info | ٩ | Noblesse_IPA D_2.p12 | Noblesse_IPh one.p12 | Noblesse_IPh one_1.p12 |
| Quick Look | ۲ | 4/25/21, 11:18 4 KB | 4/25/21, 10:31 3 KB | 4/25/21, 11:01 4 KB |
| Tags | 0 | | | |
| Rename | 1 | Certificate Personal | Certificate Perional | Certificate Perional |
| Share | Û | Noblesse_MA C_2.p12 | Noblesse_Wi ndows.p12 | Noblesse_Wi ndowsIKE.p12 |
| Compress | | 4/25/21, 11:19 4 KB | 4/25/21, 12:56 3 KB | 5/12/21, 12:42 4 KB |

第三步:输入PKCS12文件的证书密码。

第四步:在Anyconnect上创建新连接。

第五步:导航到新连接;Connections > Add VPN Connection。

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

第六步:输入新连接的信息。

Description:为连接命名

服务器地址:IP地址或FQDN FTD

高级:其他配置

步骤 7.选择Advanced。

步骤 8选择Certificate,然后选择新添加的证书。

| AnyConnect | | | | VPN Connections | |
|-----------------------------|-------------|--|--|-----------------|-----|
| PRIMARY VIRTUAL PRIVATE NET | WORK | | | | |
| AnyConnect VPN | < < A | dvanced | Select Certifica | te | j |
| Connections | FT | | | | (j) |
| Details Disconne | cte s | electing this option | will disable certificate aut | hentication. | (j) |
| GENERAL | A TI | utomatic his will automatical | lly select a certificate for au | Ithentication. | (Ì) |
| Settings | | Noblesse_IPAD | COUTDIE ODV CA | (i) > | (j) |
| Diagnostics | E | Expiration Date: Apr | r 25. 2022 11:00:36 | | (i) |
| About | ~ | Cisco_Test Issuer: DMsliders-T | COUTRIE-SRV-CA | (i) > | (j) |
| | | Expiration Date: Au | a 02, 2022 08:12:47 | | i |
| | P P | Noblesse_IPAD Issuer: DMsliders-T | COUTRIE-SRV-CA | (i) > | í |
| | E P E | Expiration Date: Api Noblesse_IPAD Issuer: DMsliders-T Expiration Date: Api | r 25, 2022 11:04:38 COUTRIE-SRV-CA r 25, 2022 00:42:05 | (j) > | |
| cisco | H | | | | |

步骤 9返回Connections并测试。

一旦成功,切换将保持打开状态,详细信息将显示为已连接(connected)。



验证

命令show vpn-sessiondb detail Anyconnect显示有关所连接主机的所有信息。

₽ 提示:进一步过滤此命令的选项是添加到命令中的"filter"或"sort"关键字。

例如:

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

故障排除

调试

解决此问题所需的调试如下:

Debug crypto ca 14

Debug webvpn 255

Debug webvpn Anyconnect 255

如果连接是IPSEC而不是SSL:

Debug crypto ikev2 platform 255 Debug crypto ikev2 protocol 255 debug crypto CA 14

Anyconnect移动应用的日志:

导航到诊断> VPN调试日志>共享日志。

| 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 | |

输入以下信息:

- 问题
- 复制步骤

然后导航到发送>共享对象。

| 3:49 PM Wed Sep 29 | •••• २ 47 | | | 奈 47% ■ |
|---------------------|--|--|--|---------|
| AnyConnect | | | Diagnostics | |
| | RK | | | |
| AnyConnect VPN | Cancel | Share Logs | Send | |
| Connections Asa | Please de following | scribe the problem and steps to r fields. | Email logs to | > |
| Details Disconnecte | PROBLEM | | Administrator | > |
| GENERAL | Test | | Cisco | |
| Settings | STEPS TO | REPRODUCE | Share with | > |
| Diagnostics | Test | | | > |
| About | | | | > |
| | | | | > |
| ahaha | The data su about conf addresses, address yo purposes. | ent is for diagnostic purposes only and igured connections, as well as server a and username. This data will appear t u specify and will not be used for mark | I may contain information and endpoint identities, IP o come from the email keting or advertising | |
| CISCO | | | | |

此选项可用于使用电子邮件客户端发送日志。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。