# 为FlexVPN远程用户配置RADIUS属性映射

目录		
<u>简介</u>		
<u>先决条件</u>		
<u>要求</u>		
<u>使用的组件</u>		
<u>配置</u>		
<u>网络图</u>		
<u>配置</u>		
<u>路由器配置</u>		
<u>身份服务引擎(ISE)配置</u>		
客户端配置		
<u>验证</u>		
<u>故障排除</u>		
调试和日志		
<u>工作场景</u>		
<u>相关信息</u>		

# 简介

本文档介绍如何使用思科身份服务引擎(ISE)配置FlexVPN以验证身份并执行属性组映射。

# 先决条件

要求

Cisco 建议您了解以下主题:

- 通过CLI在Cisco IOS® XE路由器上配置了IKEV2/IPsec的远程访问虚拟专用网络(RAVPN)
- 思科身份服务引擎(ISE)配置
- 思科安全客户端(CSC)
- RADIUS协议

使用的组件

本文档基于以下软件和硬件版本:

- 思科CSR1000V (VXE) -版本17.03.04a
- 思科身份服务引擎(ISE) 3.1
- 思科安全客户端(CSC) 5.0.05040版
- Windows 11

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。

### 配置

#### 网络图





#### 路由器配置

步骤1:在设备上配置用于身份验证和本地授权的RADIUS服务器:

aaa new-model aaa group server radius FlexVPN-Authentication-Server server-private 192.168.30.110 key Cisco123 aaa authentication login FlexVPN-Authentication-List group FlexVPN-Authentication-Server aaa authorization network FlexVPN-Authorization-List local

aaa authentication login <list\_name>命令是指身份验证、授权和记帐(AAA)组(用于定义 RADIUS服务器)。

aaa authorization network <list\_name> local命令声明将使用本地定义的用户/组。

步骤2.配置信任点以存储路由器证书。由于路由器的本地身份验证类型为RSA,因此设备要求服务 器使用证书对自身进行身份验证:

crypto pki trustpoint FlexVPN-TP enrollment url http://192.168.50.230:80 subject-name CN=192.168.50.225 revocation-check none rsakeypair FlexVPN\_KEY

第三步:为每个不同的用户组定义一个IP本地池:

ip local pool group1 172.16.10.1 172.16.10.50 ip local pool group2 172.16.20.1 172.16.20.50

第四步: 配置本地授权策略:

crypto ikev2 authorization policy FlexVPN-Local-Policy

无需在授权策略上进行配置,因为身份验证服务器负责根据用户所属的组发送相关值(DNS、池、 受保护路由等)。但是,必须将其配置为在我们的本地授权数据库中定义用户名。

﹐第5步(可选):创建IKEv2建议和策略(如果未配置,则使用智能默认值):

crypto ikev2 proposal IKEv2-prop encryption aes-cbc-256 integrity sha256 group 14

crypto ikev2 policy IKEv2-pol proposal IKEv2-prop

第6步(可选):配置转换集(如果未配置,则使用智能默认值):

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac mode tunnel

步骤 7. 使用正确的本地和远程身份、身份验证方法(本地和远程)、信任点、AAA和用于连接的虚 拟模板接口配置IKEv2配置文件:

crypto ikev2 profile FlexVPN-IKEv2-Profile match identity remote key-id cisco.example identity local dn authentication local rsa-sig authentication remote eap query-identity pki trustpoint FlexVPN-TP aaa authentication eap FlexVPN-Authentication-List aaa authorization group eap list FlexVPN-Authorization-List FlexVPN-Local-Policy aaa authorization user eap cached virtual-template 100 aaa authorization user eap cached命令指定必须缓存EAP身份验证期间接收的属性。 此命令对配 置至关重要,因为如果没有此命令,身份验证服务器发送的数据将不被使用,从而导致连接失败。



注意:远程key-id必须与XML文件中的key-id值匹配。如果未在XML文件中对其进行修改 ,将使用默认值(\*\$AnyConnectClient\$\*),并且必须在IKEv2配置文件中进行配置。

步骤 8 配置IPsec配置文件并分配转换集和IKEv2配置文件:

crypto ipsec profile FlexVPN-IPsec-Profile
set transform-set TS
set ikev2-profile FlexVPN-IKEv2-Profile

步骤9配置一个环回接口。虚拟访问接口从其借用IP地址:

interface Loopback100
ip address 10.0.0.1 255.255.255.255

步骤 10 创建将用于创建不同虚拟访问接口的虚拟模板,并链接第8步中创建的IPSec配置文件:

interface Virtual-Template100 type tunnel ip unnumbered Loopback100 tunnel mode ipsec ipv4 tunnel protection ipsec profile FlexVPN-IPsec-Profile-1

步骤 11在路由器上禁用基于HTTP-URL的证书查找和HTTP服务器:

no crypto ikev2 http-url cert
no ip http server
no ip http secure-server

### 身份服务引擎(ISE)配置

步骤1:登录ISE服务器并导航到管理>网络资源>网络设备:

Cisco ISE	Q What page are you looking for?				
Dashboard	Context Visibility	Operations Policy	Administration	Work Centers	
Recent Pages	System	Network Resources	pxGrid Servi	ices	
Groups Groups Authorization Profiles Results Network Devices Policy Sets	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services	Summary Client Mar Diagnostic Settings Feed Service Profiler	nagement ;s e	
	Settings	Device Portal Management	Threat Centi	ric NAC	
	Identity Management	Blocked List BYOD	Third Party	y Vendors	
Shortcuts	Identities Groups External Identity Sources Identity Source Sequences Settings	Certificate Provisioning Client Provisioning Mobile Device Manageme My Devices Custom Portal Files			
esc) - Collapse menu Make a wish		Settings			

ISE常规菜单

第二步:单击Add将路由器配置为AAA客户端:

Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	More $\vee$
Network Devices	Networ	k Devices			
Device Security Settings					Selected 0 Total 1 🔗 🗔
	🖉 Edit 🕇 🕂	id 📋 Duplicate 🕁 Import	🗅 Export 🗸 👌 Generate PAC	📋 Delete 🖂	All $\sim$ $\nabla$
	Name	e 🗠 IP/Mask Profile N	lame Location	Туре	Description
		D_ROU disco	(i) All Locations	All Device Types	

添加新网络设备

输入网络设备名称和IP地址字段,然后选中RADIUS Authentication Settings框并添加共享密钥,此 值必须与创建路由器上的RADIUS服务器对象时使用的值相同。

## Network Devices



名称和IP地址



RADIUS Authentication Settings

### **RADIUS UDP Settings**

Protocol	RADIUS		
Shared Secret		 Show	
Use Second Sha	ared Secret 🥡		
networkDevices.second	SharedSecret		Show

Radius密码

Click Save.

### 第三步:导航到管理>身份管理> Groups:

Cisco ISE	Q What page are you looking	) for?			
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers
Recent Pages	System	Network	Resources	pxGrid Servi	ices
Groups Authorization Profiles Results Policy Sets	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access	Networ Networ Externa RADIU: NAC M Externa Locatio	rk Devices rk Device Groups rk Device Profiles al RADIUS Servers S Server Sequences lanagers al MDM on Services	Summary Client Mar Diagnostic Settings Feed Service Profiler	nagement :s e
Shortcuts	Identity Management Identities Groups External Identity Sources Identity Source Sequences	Device P Blocke BYOD Certific Cilient I Mobile My Det	ortal Management d List cate Provisioning Provisioning Device Manageme <i>v</i> ices	Threat Centr	<b>Hc NAC</b> y Vendors
≫ + (ℓ) - Expand menu esc - Collapse menu Make a wish	Settings	Custor Setting	n Portal Files Is		

ISE常规菜单

第四步:单击User Identity Groups,然后单击Add:

Identity Groups	User Identity Groups	
< 12 Ø		Selected 0 Total 10 🖯 🚷
> 🗅 Endpoint Identity Groups		$\nabla$ $\sim$ IIA
> 🗀 User Identity Groups	Name $\wedge$ Description	
	ALL_ACCOUNTS (default)     Default ALL_ACCOUNTS (default) User Group	
	Default Employee User Group	
	GROUP_ACCOUNTS (default)     Default GROUP_ACCOUNTS (default) User Group	

添加新组

### 输入组名称并单击Submit。

Name	Group1		
Description		 	



Cancel

组信息



注意:重复步骤3和4,根据需要创建多个组。

第五步: 导航到管理>身份管理>身份:

Cisco ISE	Q What page are you looking	g for?	
Dashboard	Context Visibility	Operations Policy	Administration Work Centers
Recent Pages	System	Network Resources	pxGrid Services
Network Devices Authorization Profiles Results Policy Sets	Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks	Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM	Summary Client Management Diagnostics Settings Feed Service
	Backup & Restore Admin Access Settings	Location Services Device Portal Management	Profiler Threat Centric NAC
	Identity Management Identities Groups	Blocked List BYOD Certificate Provisioning Client Provisioning	Third Party Vendors
Shortcuts	External Identity Sources Identity Source Sequences Settings	Mobile Device Manageme My Devices Custom Portal Files	
esc - Collapse menu Make a wish		Settings	

ISE常规菜单

第六步:单击Add,以便在服务器本地数据库中创建新用户:

Identities Groups	External Ident	tity Sources	Identity Source Sequence	s Settings					
Users Latest Manual Network Scan F	Net	twork Ac	cess Users						
							Selected 0 1	Fotal 0 📿	٥
	🖉 Edit	+ Add 🛞	) Change Status \vee 🛛 🕁 Import	🗅 Export 🗸 🛛 📋 🕻	Delete 🗸 🔲 Duj	plicate		All $\sim$	7
		Status U	sername ^ Descr	ption First Nam	e Last Name	Email Address	User Identity Grou	Admin	
				No	data available				

添加用户

输入用户名和登录密码.然后,导航到此页末尾,选择User Group:

$\sim$	Network Acc	ess User			
ſ	* Username USE	r1		_	
	Status Z	nabled V			
	Email				
$\sim$	Passwords				
	Password Type:	Internal Users V			
		Password	Re-Enter Password		
	* Login Password			Generate Password	í
	Enable Password			Generate Password	i
用户名	4和密码				

 $\sim$  Account Options

Description	
Change password on next login	User Groups
Account Disable Policy	
Disable account if date exceeds 20	ALL_ACCOUNTS (default)
	Market Employee
✓ User Groups	Group2
	GROUP_ACCOUNTS (default)
Select an item	

将正确的组分配给用户

Click Save.



注意:重复步骤5和6,创建所需的用户并将其分配到相应的组。

第7步:导航到策略>策略集:

Cisco ISE	Q What page are you looking					
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages Groups	Policy Sets	Profiling				
Network Devices Authorization Profiles	Posture	Client Prov	isioning			
Results Policy Sets	Policy Elements Dictionaries Conditions Results					
Shortcuts (#) + (/) - Expand menu (#) - Collapse menu Make a wish						

ISE常规菜单

### 通过点击屏幕右侧的箭头来选择默认授权策略:

Policy	/ Sets				Reset	Reset Policyset	Hitcour	nts	Save
٠	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Serve	er Sequence	Hits	Actions	View
0	ζ Search								
				+					
	0	Default	Default policy set		Default Network Access	$\boxtimes \vee +$	35	ŝ	>

选择授权策略

步骤 8 点击Authorization Policy旁边的下拉菜单箭头将其展开。然后,点击添加(+)图标以添加新规 则:

Authorization Policy (14)			
	Results		
Status Rule Name Conditions	Profiles	Security Groups	Hits Actions
		coounty another	

添加新的授权规则

输入规则的名称并选择Conditions列下的add (+)图标:

🕂 Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search						
0	Group1_AuthZ_Rule	+	Select from list	> + Select from list	<u>~</u> +	ŝ

添加条件

步骤 9 在"属性编辑器"(Attribute Editor)文本框中单击,然后单击身份组。选择身份组-名称属性:

**U** ^

### **Conditions Studio**

Library	Editor
	Click to add an attribute Select attribute for condition
BYOD_is_Registered	♥ □ ▲ ● ♀ ♀ ₽ ₽ Ø Ⅰ □ ◊ ↓ ♥ ₺ ?
Catalyst_Switch_Local_Web_Aut hentication	Dictionary Attribute ID Info
: E Compliance_Unknown_Devices	All Dictionaries V Attribute ID
: E Compliant_Devices	IdentityGroup Description
EAP-MSCHAPv2	🗥 IdentityGroup Name 🕕
EAP-TLS	A InternalUser IdentityGroup
: E Guest_Flow	A PassiveID PassiveID_Groups
MAC_in_SAN ()	
Network_Access_Authentication_ Passed	
: F Non_Cisco_Profiled_Phones	

选择条件

选择与运算符相同,然后点击下拉菜单箭头显示可用选项并选择User Identity Groups:<GROUP\_NAME>。

### Editor

	IdentityGroup·Name	3	
*	Equals 🗸	Choose from list or type	
	Set to 'Is not'	User Identity Groups:GROUP_ACCOUNTS (default)	Save
		User Identity Groups:Group1	
		User Identity Groups:Group2	
		User Identity Groups:GuestType_Contractor (default)	
		User Identity Groups:GuestType_Daily (default)	

选择组

### Click Save.

### 第10步:在配置文件列中,点击添加(+)图标并选择创建新授权配置文件:

					Results			
Ð	Status	Rule Name		Conditions	Profiles	Security Groups	Hits	Actions
0	(Search	1						
	0	Group1_AuthZ_Rule	8	IdentityGroup·Name EQUALS User Identity Groups:Group1	Select from list	Select from list $\sim$ +	10	ŝ
		Wireless Black List		Uvireless_Access	Create a New Authorization Profile			-0
	•	Default	AND	R IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist		Select from list V+	0	ţĊţ

创建授权配置文件

输入配置文件名称

# Add New Standard Profile

#### Authorization Profile

* Name	Profile_group1	
Description		
* Access Type	ACCESS_ACCEPT	~
Network Device Profile	ditte Cisco 🗸 🕀	
Service Template		
Track Movement		
Agentless Posture		
Passive Identity Tracking		

配置文件信息

### 导航到此页末尾的高级属性设置,然后单击下拉菜单箭头。然后单击Cisco并选择cisco-avpair—[1]:

imes  Advanced Attributes Settings		
Select an item		
	EQ.	
	< < < < >	
$\vee$ Attributes Details	cisco-abort-cause[21]	
Access Type = ACCESS_ACCEPT	cisco-account-info[250]	
	cisco-assign-ip-pool[218]	
	cisco-av-pair[1]	
	cisco-call-filter[243]	
	cisco-call-id[141]	

添加要配置的cisco-av-pair属性,然后单击add (+)图标添加其他属性:





注意:有关属性规范(名称、语法、说明、示例等),请参阅FlexVPN RADIUS属性配置 指南:

FlexVPN和互联网密钥交换版本2配置指南,Cisco IOS XE Fuji 16.9.x -支持的RADIUS属性



注意:重复上述步骤以创建必要的属性。

Click Save.

接下来的属性已分配给每个组:

• 组1属性:

#### $\scriptstyle \lor$ Advanced Attributes Settings

H	Cisco:cisco-av-pair	~ '	ipsec:dns-servers=10.0.50.10 🗸 💻
H	Cisco:cisco-av-pair	~ '	ipsec:route-set=prefix 192.161 🗸 💻
H	Cisco:cisco-av-pair	~ -	ipsec:addr-pool=group1 🗸 🚍 🕂

-	<ul> <li>Attributes Details</li> </ul>
	Access Type = ACCESS_ACCEPT
	cisco-av-pair = ipsec:dns-servers=10.0.50.101
	cisco-av-pair = ipsec:route-set=prefix 192.168.100.0/24
	cisco-av-pair = ipsec:addr-pool=group1

#### Group1属性

### • 组2属性:

 $\scriptstyle \lor$  Advanced Attributes Settings

H	Cisco:cisco-av-pair 🗸	-	ipsec:dns-servers=10.0.50.20 🗸	-	
H	Cisco:cisco-av-pair 🗸 🗸	=	ipsec:route-set=prefix 192.16ł 🗸	-	
H	Cisco:cisco-av-pair 🗸	-	ipsec:addr-pool=group2 ~	-	+

Γ	imes Attributes Details
l	Access Type = ACCESS_ACCEPT
L	cisco-av-pair = ipsec:dns-servers=10.0.50.202
L	cisco-av-pair = ipsec:route-set=prefix 192.168.200.0/24
l	cisco-av-pair = ipsec:addr-pool=group2
1	

组2属性

第11步:点击下拉菜单箭头,然后选择在第10步中创建的授权配置文件:

🕂 Status	Rule Name		Condit	tions	Profiles	Security Groups	Hits	Actions
Q Search	n							
ø	Group1_AuthZ_Rule	8	Identii Group	tyGroup-Name EQUALS User Identity bs:Group1	Select from list	Select from list $\sim$ +	10	ŝ
ø	Wireless Black List Default	AND	F	Wireless_Access IdentityGroup-Name EQUALS Endpoint Identity Groups:Blacklist	DenyAccess NSP_Onboard Non_Cisco_IP_Phones	Select from list $\sim$ +	0	¢
0	Profiled Cisco IP Phones	28	Identii Group	tyGroup-Name EQUALS Endpoint Identity s:Profiled:Cisco-IP-Phone	PermitAccess	Select from list $\sim$ +	0	ŝ
0	Profiled Non Cisco IP Phones	=	Non_0	Cisco_Profiled_Phones	Profile_group1 Non_Cisco_IP_Phones × V	Select from list $\vee+$	0	ŝ

分配授权配置文件

#### Click Save.



注意:重复步骤8到11,为每个组创建必要的授权规则。

第 12 步(可选): 如果需要编辑授权配置文件,请导航到Policy > Results:

Cisco ISE	Q What page are you looking	ig for?				
Dashboard	Context Visibility	Operations	Policy	Administration	Work Centers	
Recent Pages	Policy Sets	Profiling				
Results Identities	Posture	Client Pro	visioning			
Groups Network Devices	Policy Elements					
	Dictionaries Conditions Results					
Shortcuts						
🗮 + 🕧 - Expand menu						
esc) - Collapse menu Make a wish						M

ISE常规菜单

### 导航到授权>授权配置文件。单击要修改的配置文件的复选框,然后单击Edit:

■ Cisco ISE	Policy · Policy Elements	Q (7) 50 \$
Dictionaries Conditions	Results	
Authentication > Authorization V Authorization Profiles Downloadable ACLs	Standard Authorization Profiles For Policy Export go to Administration > System > Backup & Restore > Policy Export  P Edit + Add Duplicate Delete	t Page Selected 1 Total 11 📿 🔅 All ~ ▽
Profiling >	Name Profile	∧ Description
Posture >	Blackhole_Wireless_Access # Cisco ()	Default profile used to blacklist wireless devices. Ensure that you co
	Cisco_IP_Phones (1) 🗰 Cisco (1)	Default profile used for Cisco Phones.
Client Provisioning >	Cisco_Temporal_Onboard 🗰 Cisco 🕡	Onboard the device with Cisco temporal agent
	Cisco_WebAuth  Cisco (i)	Default Profile used to redirect users to the CWA portal.
	NSP_Onboard at Cisco ()	Onboard the device with Native Supplicant Provisioning
	Non_Cisco_IP_Phones 🗰 Cisco 🕧	Default Profile used for Non Cisco Phones.
	Profile_group1   Cisco (;	
	Profile_group2   Cisco ()	
	UDN 🗰 Cisco 🕧	Default profile used for UDN.
	DenyAccess	Default Profile with access type as Access-Reject
	PermitAccess	Default Profile with access type as Access-Accept

编辑授权配置文件

### 客户端配置

步骤1:使用XML配置文件编辑器创建XML配置文件。此示例是用于创建本文档的示例:

#### <#root>

<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w3.org/2001/XMLSc</pre> <ClientInitialization> <UseStartBeforeLogon UserControllable="true">true</UseStartBeforeLogon> <AutomaticCertSelection UserControllable="false">true</AutomaticCertSelection> <ShowPreConnectMessage>false</ShowPreConnectMessage> <CertificateStore>All</CertificateStore> <CertificateStoreMac>All</CertificateStoreMac> <CertificateStoreLinux>All</CertificateStoreLinux> <CertificateStoreOverride>true</CertificateStoreOverride> <ProxySettings>Native</ProxySettings> <AllowLocalProxyConnections>true</AllowLocalProxyConnections> <AuthenticationTimeout>30</AuthenticationTimeout> <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart> <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect> <LocalLanAccess UserControllable="true">false</LocalLanAccess> <DisableCaptivePortalDetection UserControllable="true">false</DisableCaptivePortalDetection> <ClearSmartcardPin UserControllable="false">true</ClearSmartcardPin> <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport> <AutoReconnect UserControllable="false"> true <AutoReconnectBehavior UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior> </AutoReconnect> <SuspendOnConnectedStandby>false</SuspendOnConnectedStandby> <AutoUpdate UserControllable="false">true</AutoUpdate> <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration> <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement> <LinuxLogonEnforcement>SingleLocalLogon</LinuxLogonEnforcement> <WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment> <LinuxVPNEstablishment>LocalUsersOnly</LinuxVPNEstablishment> <AutomaticVPNPolicy>false</AutomaticVPNPolicy> <PPPExclusion UserControllable="false"> **Disable** <PPPExclusionServerIP UserControllable="false"/> </PPPExclusion> <EnableScripting UserControllable="false">false</EnableScripting> <EnableAutomaticServerSelection UserControllable="false"> false <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement> <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime> </EnableAutomaticServerSelection> <RetainVpnOnLogoff>false </RetainVpnOnLogoff> <CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover> <AllowManualHostInput>true</AllowManualHostInput> </ClientInitialization> <ServerList> <HostEntry> <HostName> FlexVPN HUB </HostName> <HostAddress> 192.168.50.225 </HostAddress> <PrimaryProtocol>

IPsec

<StandardAuthenticationOnly> true <AuthMethodDuringIKENegotiation>

EAP-MD5

</AuthMethodDuringIKENegotiation> <IKEIdentity>

#### cisco.example

</IKEIdentity> </StandardAuthenticationOnly> </PrimaryProtocol> </HostEntry> </ServerList> </AnyConnectProfile>

- <HostName> -用于指代主机、IP地址或完全限定域名(FQDN)的别名。这在CSC框中显示。
- <HostAddress> FlexVPN集线器的IP地址或FQDN。
- <PrimaryProtocol> -必须设置为IPsec以强制客户端使用IKEv2/IPsec而不是SSL。
- <AuthMethodDuringIKENegotiation> -必须设置为在EAP中使用EAP-MD5。这是根据ISE服务 器进行身份验证所必需的。
- <IKEIdentity> -此字符串由客户端作为ID\_GROUP类型ID负载发送。这可用于将客户端与中心 上的特定IKEv2配置文件进行匹配。

## 验证

步骤1:导航到安装CSC的客户端。连接到FlexVPN中心并输入user1凭证:

🕲 Cis	sco Secure Client — 🗍 刘	<
	AnyConnect VPN: Please enter your username and password. FlexVPN HUB Connect	
	Scisco Secure Client   FlexVPN HUB > ×	
¢	Username: user1 Password: ******	
	OK Cancel	

User1凭证

第二步:建立连接后,点击齿轮图标(左下角)并导航到AnyConnectVPN>Statistics。 在地址信 息部分中确认分配的IP地址属于为组1配置的池:

S Cisco Secure Client		-		×
cisco Secure (	Client &			0
Status Overview	Virtual Private Network (VPN)			
AnyConnect VPN >	Preferences Statistics Route Details Firewall Message History			_
Secure Endpoint	Connection Information         State:       Connected         Tunnel Mode (IPv4):       Split Include         Tunnel Mode (IPv6):       Drop All Traffic         Dynamic Tunnel Exclusion:       None         Dynamic Tunnel Inclusion:       None         Duration:       00:00:22         Session Disconnect:       None         Management Connection State:       Disconnected (user tunnel active)         Address Information       Client (IPv4):         Client (IPv6):       Not Available         Server:       Bytes	Ex	A port Stats	\$

User1统计信息

导航到AnyConnectVPN > Route details,确认显示的信息对应于为group1配置的安全路由和 DNS:

Sisco Secure Client		-	×
cisco Secure	Client &		0
Status Overview	Virtual Private Network (VPN)		
AnyConnect VPN >	Preferences Statistics Route Details Firewall Message History		
Secure Endpoint	Non-Secured Routes (IPv4)           0.0.0.0/0           Secured Routes (IPv4)           192.168.100.0/24           10.0.50.101/32		•

用户1路由详细信息

第三步:对user2凭证重复第1步和第2步,检查信息是否与此组的ISE授权策略上配置的值匹配:

🕙 Cisco Se	cure Client	-	( <b>Ú</b> )	×
	AnyConnect VPN: Please enter your username and passwo FlexVPN HUB	ord.	Connect	
	Cisco Secure Client   FlexVPN HUB Please enter your username and passw Username: user2	ord.		×
*	OK	Ca	incel	co

用户2凭证

0	Cisco	Secure	Client
---	-------	--------	--------

()

\_

# Secure Client

Status Overview	Virtual Private Network (VPN)	
AnyConnect VPN >	Preferences Statistics Route Details Firewall Message History	
Secure Endpoint	Connection Information         State:       Connected         Tunnel Mode (IPv4):       Split Include         Tunnel Mode (IPv6):       Drop All Traffic         Dynamic Tunnel Exclusion:       None         Dynamic Tunnel Inclusion:       None         Duration:       00:00:12         Session Disconnect:       None         Management Connection State:       Disconnected (user tunnel active)	
	Address Information          Client (IPv4):       172.16.20.5         Client (IPv6):       Not Available         Server:          Bytes          Reset       Export Stats	•

用户2统计信息

Sisco Secure Client		-	×
cisco Secure	Client		0
Status Overview	Virtual Private Network (VPN)		
AnyConnect VPN >	Preferences Statistics Route Details Firewall Message History		
Secure Endpoint	Non-Secured Routes (IPv4)           0.0.0.0/0           Secured Routes (IPv4)           192.168.200.0/24           10.0.50.202/32		•

用户2路由详细信息

# 故障排除

### 调试和日志

在Cisco路由器上:

1. 使用IKEv2和IPSec调试验证头端和客户端之间的协商:

debug crypto ikev2 debug crypto ikev2 packet debug crypto ikev2 error debug crypto ikev2 internal debug crypto ipsec debug crypto ipsec error

2. 使用AAA调试验证本地和/或远程属性的分配:

```
debug aaa authorization
debug aaa authentication
debug radius authentication
```

在ISE上:

• RADIUS实时日志

### 工作场景

接下来的输出是成功连接的示例:

• 用户1调试输出:

#### <#root>

```
Jan 30 02:57:21.088: AAA/BIND(000000FF): Bind i/f
Jan 30 02:57:21.088: AAA/AUTHEN/LOGIN (000000FF):
```

Pick method list 'FlexVPN-Authentication-List'

```
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.088: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-for-
Jan 30 02:57:21.088: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.088: idb is NULL
Jan 30 02:57:21.088: RADIUS(00000FF): Config NAS IPv6: ::
Jan 30 02:57:21.089: RADIUS(00000FF): acct_session_id: 4245
Jan 30 02:57:21.089: RADIUS(00000FF): sending
```

Jan 30 02:57:21.089: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1 Jan 30 02:57:21.089: RADIUS: Message Authenticator encoded Jan 30 02:57:21.089: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/85, len 229

RADIUS: authenticator C9 82 15 29 AF 4B 17 61 - 27 F4 5C 27 C2 C3 50 34 Jan 30 02:57:21.089: RADIUS: Service-Type [6] 6 Login [1] Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 26 Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 20 "service-type=Login" Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 36 Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.089: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130" Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 64 Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z Jan 30 02:57:21.089: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.089: RADIUS: Vendor, Cisco [26] 21 Jan 30 02:57:21.089: RADIUS: Cisco AVpair [1] 15 "coa-push=true" Jan 30 02:57:21.089: RADIUS: EAP-Message [79] 12 RADIUS: 02 3B 00 0A 01 75 73 65 72 31 [ ;user1] Jan 30 02:57:21.089: RADIUS: Message-Authenticato[80] 18 RADIUS: E7 22 65 E0 DC 03 3A 49 0B 01 49 2A D5 3F AD 4F [ "e:II\*?0] Jan 30 02:57:21.089: RADIUS: NAS-IP-Address [4] 6 192.168.30.100 Jan 30 02:57:21.089: RADIUS: 000000FF): Sending a IPv4 Radius Packet Jan 30 02:57:21.090: RADIUS(00000FF): Started 5 sec timeout Jan 30 02:57:21.094: RADIUS:

Received from id 1645/85 192.168.30.110:1645, Access-Challenge, len 137

RADIUS: authenticator 67 2B 9D 9C 4D 1F F3 E8 - F6 EC 9B EB 8E 49 C8 A5
Jan 30 02:57:21.094: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA]
RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;]
Jan 30 02:57:21.094: RADIUS: EAP-Message [79] 8
RADIUS: 01 52 00 06 0D 20 [ R ]
Jan 30 02:57:21.094: RADIUS: Message-Authenticato[80] 18
RADIUS: 38 8A B1 31 72 62 06 40 4F D4 58 48 E8 36 E7 80 [ 81rb@OXH6]
Jan 30 02:57:21.094: RADIUS(00000FF): Received from id 1645/85
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 02:57:21.097: AAA/AUTHEN/LOGIN (00000FF):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.097: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-forJan 30 02:57:21.097: RADIUS(000000FF): Config NAS IP: 0.0.0.0
Jan 30 02:57:21.097: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.097: idb is NULL
Jan 30 02:57:21.097: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.097: RADIUS(ENCODE(00000FF): acct\_session\_id: 4245

Jan 30 02:57:21.097: RADIUS(000000FF): sending
Jan 30 02:57:21.097: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.097: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.097: RADIUS(000000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/86, len 316

RADIUS: authenticator 93 07 42 CC D1 90 31 68 - 56 D0 D0 5A 35 C3 67 BC Jan 30 02:57:21.097: RADIUS: Service-Type [6] 6 Login [1] Jan 30 02:57:21.097: RADIUS: Vendor, Cisco [26] 26 Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 20 "service-type=Login" Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 36 Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 30

#### "isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.098: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130" Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 64 Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z Jan 30 02:57:21.098: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.098: RADIUS: Vendor, Cisco [26] 21 Jan 30 02:57:21.098: RADIUS: Cisco AVpair [1] 15 "coa-push=true" Jan 30 02:57:21.098: RADIUS: EAP-Message [79] 8 RADIUS: 02 52 00 06 03 04 [ R] Jan 30 02:57:21.098: RADIUS: Message-Authenticato[80] 18 RADIUS: E0 67 24 D3 BB CF D9 E0 EE 44 98 8A 26 64 AC C9 [ g\$D&d] Jan 30 02:57:21.098: RADIUS: State [24] 91 RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L] RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4] RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA] RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session] RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930] RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;] Jan 30 02:57:21.098: RADIUS: NAS-IP-Address [4] 6 192.168.30.100 Jan 30 02:57:21.098: RADIUS(000000FF): Sending a IPv4 Radius Packet Jan 30 02:57:21.099: RADIUS(000000FF): Started 5 sec timeout Jan 30 02:57:21.101: RADIUS: Received from id 1645/86 192.168.30.110:1645, Access-Challenge, len 161 RADIUS: authenticator 42 A3 5F E0 92 13 51 13 - B2 80 56 A3 91 36 BD A1 Jan 30 02:57:21.101: RADIUS: State [24] 91 RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L] RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4] RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA] RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session] RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930] RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;] Jan 30 02:57:21.101: RADIUS: EAP-Message [79] 32 RADIUS: 01 53 00 1E 04 10 D7 61 AE 69 3B 88 A1 83 E4 EC 0F B6 EF 68 58 16 49 53 45 2D 44 49 41 4E [ Sai Jan 30 02:57:21.101: RADIUS: Message-Authenticato[80] 18 RADIUS: 3E C9 C1 E1 F2 3B 4E 4C DF CF AC 21 AA E9 C3 F0 [ >;NL!] Jan 30 02:57:21.101: RADIUS(000000FF): Received from id 1645/86

RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes Jan 30 02:57:21.103: AAA/AUTHEN/LOGIN (000000FF):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF):Orig. component type = VPN IPSEC
Jan 30 02:57:21.103: RADIUS/ENCODE(000000FF): dropping service type, "radius-server attribute 6 on-forJan 30 02:57:21.103: vrfid: [65535] ipv6 tableid : [0]
Jan 30 02:57:21.104: idb is NULL
Jan 30 02:57:21.104: RADIUS(000000FF): Config NAS IPv6: ::
Jan 30 02:57:21.104: RADIUS(000000FF): acct\_session\_id: 4245
Jan 30 02:57:21.104: RADIUS(000000FF): sending
Jan 30 02:57:21.104: RADIUS(00000FF): sending
Jan 30 02:57:21.104: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 02:57:21.104: RADIUS: Message Authenticator encoded
Jan 30 02:57:21.104: RADIUS(00000FF):

Send Access-Request to 192.168.30.110:1645 id 1645/87, len 332

RADIUS: authenticator 89 35 9C C5 06 FB 04 B7 - 4E A3 B2 5F 2B 15 4F 46 Jan 30 02:57:21.104: RADIUS: Service-Type [6] 6 Login [1] Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 26 Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 20 "service-type=Login" Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 36 Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 30

"isakmp-phase1-id=cisco.example"

Jan 30 02:57:21.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130" Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 64 Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194CAE2Z Jan 30 02:57:21.104: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.104: RADIUS: Vendor, Cisco [26] 21 Jan 30 02:57:21.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true" Jan 30 02:57:21.104: RADIUS: EAP-Message [79] 24 RADIUS: 02 53 00 16 04 10 B0 BB 3E D5 B1 D6 01 FC 9A B7 4A DB AB F7 2F B6 [ S>J/] Jan 30 02:57:21.104: RADIUS: Message-Authenticato[80] 18 RADIUS: 79 43 97 A7 26 17 3E 3B 54 B4 90 D4 76 0F E0 14 [ yC&>;Tv] Jan 30 02:57:21.104: RADIUS: State [24] 91 RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L] RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4] RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 43 41 [2F2F016FZH1194CA] RADIUS: 45 32 5A 4E 31 46 3B 33 31 53 65 73 73 69 6F 6E [E2ZN1F;31Session] RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930] RADIUS: 38 30 30 31 38 2F 32 39 3B [ 80018/29;] Jan 30 02:57:21.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100 Jan 30 02:57:21.105: RADIUS(000000FF): Sending a IPv4 Radius Packet Jan 30 02:57:21.105: RADIUS(000000FF): Started 5 sec timeout Jan 30 02:57:21.170: RADIUS:

Received from id 1645/87 192.168.30.110:1645, Access-Accept, len 233

RADIUS: authenticator 75 F6 05 85 1D A0 C3 EE - F8 81 F9 02 38 AC C1 B6 Jan 30 02:57:21.170: RADIUS: User-Name [1] 7

"user1"

Jan 30 02:57:21.170: RADIUS: Class [25] 68 RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011] RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH] RADIUS: 31 31 39 34 43 41 45 32 5A 4E 31 46 3A 49 53 45 [1194CAE2ZN1F:ISE] RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/]
RADIUS: 32 39 [ 29]
Jan 30 02:57:21.170: RADIUS: EAP-Message [79] 6
RADIUS: 03 53 00 04 [ S]
Jan 30 02:57:21.170: RADIUS: Message-Authenticato[80] 18
RADIUS: 8A A9 CC 07 61 A2 6D BA E4 EB B5 B7 73 0E EC 28 [ ams(]
Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 37
Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.101"

Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 47 Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.100.0/24"

Jan 30 02:57:21.170: RADIUS: Vendor, Cisco [26] 30 Jan 30 02:57:21.170: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group1"

Jan 30 02:57:21.171: RADIUS(000000FF): Received from id 1645/87 RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes Jan 30 02:57:21.175: AAA/BIND(00000100): Bind i/f Jan 30 02:57:21.175: AAA/AUTHOR (0x100):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 02:57:21.176: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to Jan 30 02:57:21.192: %SYS-5-CONFIG\_P: Configured programmatically by process Crypto INT from console as Jan 30 02:57:21.376: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access1, changed state to up

用户2调试输出:

#### <#root>

Jan 30 03:28:58.102: AAA/BIND(00000103): Bind i/f Jan 30 03:28:58.102: AAA/AUTHEN/LOGIN (00000103):

Pick method list 'FlexVPN-Authentication-List'

Jan 30 03:28:58.103: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.103: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-forJan 30 03:28:58.103: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.103: idb is NULL
Jan 30 03:28:58.103: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.103: RADIUS(00000103): acct\_session\_id: 4249
Jan 30 03:28:58.103: RADIUS(0000103): sending
Jan 30 03:28:58.103: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.103: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.103: RADIUS(0000103):

Send Access-Request to 192.168.30.110:1645 id 1645/88, len 229

```
RADIUS: authenticator 71 99 09 63 19 F7 D7 0B - 1D A9 4E 64 28 6F A5 64
Jan 30 03:28:58.103: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.103: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.103: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 30
"isakmp-phase1-id=cisco.example"
Jan 30 03:28:58.104: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z
Jan 30 03:28:58.104: RADIUS: User-Name [1] 7
"user2"
Jan 30 03:28:58.104: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.104: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.104: RADIUS: EAP-Message [79] 12
RADIUS: 02 3B 00 0A 01 75 73 65 72 32 [ ;user2]
Jan 30 03:28:58.104: RADIUS: Message-Authenticato[80] 18
RADIUS: 12 62 2F 51 12 FC F7 EC F0 87 E0 34 1E F1 AD E5 [ b/Q4]
Jan 30 03:28:58.104: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.104: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.105: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.109: RADIUS:
Received from id 1645/88 192.168.30.110:1645, Access-Challenge, len 137
RADIUS: authenticator 98 04 01 EA CD 9B 1E A9 - DC 6F 2F 17 1F 2A 5F 43
Jan 30 03:28:58.109: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.110: RADIUS: EAP-Message [79] 8
RADIUS: 01 35 00 06 0D 20 [ 5 ]
Jan 30 03:28:58.110: RADIUS: Message-Authenticato[80] 18
RADIUS: E3 A6 88 B1 B6 3D 93 1F 39 B3 AE 9E EA 1D BB 15 [ =9]
Jan 30 03:28:58.110: RADIUS(00000103): Received from id 1645/88
RADIUS/DECODE: EAP-Message fragments, 6, total 6 bytes
Jan 30 03:28:58.112: AAA/AUTHEN/LOGIN (00000103):
Pick method list 'FlexVPN-Authentication-List'
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC
Jan 30 03:28:58.112: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-
Jan 30 03:28:58.112: RADIUS(00000103): Config NAS IP: 0.0.0.0
Jan 30 03:28:58.112: vrfid: [65535] ipv6 tableid : [0]
Jan 30 03:28:58.113: idb is NULL
Jan 30 03:28:58.113: RADIUS(00000103): Config NAS IPv6: ::
Jan 30 03:28:58.113: RADIUS/ENCODE(00000103): acct_session_id: 4249
Jan 30 03:28:58.113: RADIUS(00000103): sending
Jan 30 03:28:58.113: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1
Jan 30 03:28:58.113: RADIUS: Message Authenticator encoded
Jan 30 03:28:58.113: RADIUS(00000103):
```

Send Access-Request to 192.168.30.110:1645 id 1645/89, len 316

```
RADIUS: authenticator 56 BD F0 9A 4B 16 5C 6C - 4E 41 00 56 8D C0 3A 8C
Jan 30 03:28:58.113: RADIUS: Service-Type [6] 6 Login [1]
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 26
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 20 "service-type=Login"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 36
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 30
"isakmp-phase1-id=cisco.example"
Jan 30 03:28:58.113: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 64
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z
Jan 30 03:28:58.113: RADIUS: User-Name [1] 7
"user2"
Jan 30 03:28:58.113: RADIUS: Vendor, Cisco [26] 21
Jan 30 03:28:58.113: RADIUS: Cisco AVpair [1] 15 "coa-push=true"
Jan 30 03:28:58.113: RADIUS: EAP-Message [79] 8
RADIUS: 02 35 00 06 03 04 [ 5]
Jan 30 03:28:58.113: RADIUS: Message-Authenticato[80] 18
RADIUS: 47 1F 36 A7 C3 9B 90 6E 03 2C B8 D7 FE A7 13 44 [ G6n,D]
Jan 30 03:28:58.113: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.114: RADIUS: NAS-IP-Address [4] 6 192.168.30.100
Jan 30 03:28:58.114: RADIUS(00000103): Sending a IPv4 Radius Packet
Jan 30 03:28:58.114: RADIUS(00000103): Started 5 sec timeout
Jan 30 03:28:58.116: RADIUS:
Received from id 1645/89 192.168.30.110:1645, Access-Challenge, len 161
RADIUS: authenticator 84 A3 30 3D 80 BC 71 42 - 1B 9B 49 EF 0B 1B 02 02
Jan 30 03:28:58.116: RADIUS: State [24] 91
RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L]
RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4]
RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4]
RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session]
RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930]
RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;]
Jan 30 03:28:58.116: RADIUS: EAP-Message [79] 32
RADIUS: 01 36 00 1E 04 10 EB 9F A5 AC 70 1F 4D D6 48 05 9D EC 1F 29 67 AE 49 53 45 2D 44 49 41 4E [ 6pM
Jan 30 03:28:58.116: RADIUS: Message-Authenticato[80] 18
RADIUS: 08 5E BC EF E5 38 50 CD FB 3C B3 E9 99 0A 51 B3 [ ^8P<Q]
Jan 30 03:28:58.116: RADIUS(00000103): Received from id 1645/89
RADIUS/DECODE: EAP-Message fragments, 30, total 30 bytes
Jan 30 03:28:58.118: AAA/AUTHEN/LOGIN (00000103):
Pick method list 'FlexVPN-Authentication-List'
```

Jan 30 03:28:58.118: RADIUS/ENCODE(00000103):Orig. component type = VPN IPSEC Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): dropping service type, "radius-server attribute 6 on-for-Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IP: 0.0.0.0 Jan 30 03:28:58.118: vrfid: [65535] ipv6 tableid : [0] Jan 30 03:28:58.118: idb is NULL Jan 30 03:28:58.118: RADIUS(00000103): Config NAS IPv6: :: Jan 30 03:28:58.118: RADIUS/ENCODE(00000103): acct\_session\_id: 4249 Jan 30 03:28:58.118: RADIUS(00000103): sending Jan 30 03:28:58.118: RADIUS/ENCODE: Best Local IP-Address 192.168.30.100 for Radius-Server 192.168.30.1 Jan 30 03:28:58.119: RADIUS: Message Authenticator encoded Jan 30 03:28:58.119: RADIUS(00000103): Send Access-Request to 192.168.30.110:1645 id 1645/90, len 332 RADIUS: authenticator A1 62 1A FB 18 58 7B 47 - 5C 8A 64 FA B7 23 9B BE Jan 30 03:28:58.119: RADIUS: Service-Type [6] 6 Login [1] Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 26 Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 20 "service-type=Login" Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 36 Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 30 "isakmp-phase1-id=cisco.example" Jan 30 03:28:58.119: RADIUS: Calling-Station-Id [31] 13 "192.168.50.130" Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 64 Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 58 "audit-session-id=L2L42F2F0116Z02L42F2F016FZH1194E444Z Jan 30 03:28:58.119: RADIUS: User-Name [1] 7 "user2" Jan 30 03:28:58.119: RADIUS: Vendor, Cisco [26] 21 Jan 30 03:28:58.119: RADIUS: Cisco AVpair [1] 15 "coa-push=true" Jan 30 03:28:58.119: RADIUS: EAP-Message [79] 24 RADIUS: 02 36 00 16 04 10 73 B7 F2 42 09 5B AB 21 D8 77 96 A2 F7 C7 83 AD [ 6sB[!w] Jan 30 03:28:58.119: RADIUS: Message-Authenticato[80] 18 RADIUS: B1 68 3C 25 9E FE 52 13 10 69 E6 BB 17 67 6F 18 [ h<?Rigo] Jan 30 03:28:58.119: RADIUS: State [24] 91 RADIUS: 35 32 43 50 4D 53 65 73 73 69 6F 6E 49 44 3D 4C [52CPMSessionID=L] RADIUS: 32 4C 34 32 46 32 46 30 31 31 36 5A 4F 32 4C 34 [2L42F2F0116Z02L4] RADIUS: 32 46 32 46 30 31 36 46 5A 48 31 31 39 34 45 34 [2F2F016FZH1194E4] RADIUS: 34 34 5A 4E 32 30 3B 33 31 53 65 73 73 69 6F 6E [44ZN20;31Session] RADIUS: 49 44 3D 49 53 45 2D 44 49 41 4E 2F 34 39 33 30 [ID=ISE-SERVER/4930] RADIUS: 38 30 30 31 38 2F 33 30 3B [ 80018/30;] Jan 30 03:28:58.119: RADIUS: NAS-IP-Address [4] 6 192.168.30.100 Jan 30 03:28:58.119: RADIUS(00000103): Sending a IPv4 Radius Packet Jan 30 03:28:58.119: RADIUS(00000103): Started 5 sec timeout Jan 30 03:28:58.186: RADIUS: Received from id 1645/90 192.168.30.110:1645, Access-Accept, len 233 RADIUS: authenticator 48 A5 A0 11 ED B8 C2 87 - 35 30 17 D5 6D D7 B4 FD Jan 30 03:28:58.186: RADIUS: User-Name [1] 7 "user2" Jan 30 03:28:58.186: RADIUS: Class [25] 68

RADIUS: 43 41 43 53 3A 4C 32 4C 34 32 46 32 46 30 31 31 [CACS:L2L42F2F011] RADIUS: 36 5A 4F 32 4C 34 32 46 32 46 30 31 36 46 5A 48 [6Z02L42F2F016FZH] RADIUS: 31 31 39 34 45 34 34 34 5A 4E 32 30 3A 49 53 45 [1194E444ZN20:ISE] RADIUS: 2D 44 49 41 4E 2F 34 39 33 30 38 30 30 31 38 2F [-DIAN/493080018/] RADIUS: 33 30 [ 30] Jan 30 03:28:58.186: RADIUS: EAP-Message [79] 6 RADIUS: 03 36 00 04 [ 6] Jan 30 03:28:58.186: RADIUS: Message-Authenticato[80] 18 RADIUS: 9E A6 D9 56 40 C8 EB 08 69 8C E1 35 35 53 18 83 [ V@i55S] Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 37 Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 31

"ipsec:dns-servers=10.0.50.202"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 47 Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 41

"ipsec:route-set=prefix 192.168.200.0/24"

Jan 30 03:28:58.187: RADIUS: Vendor, Cisco [26] 30 Jan 30 03:28:58.187: RADIUS: Cisco AVpair [1] 24

"ipsec:addr-pool=group2"

Jan 30 03:28:58.187: RADIUS(00000103): Received from id 1645/90
RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
Jan 30 03:28:58.190: AAA/BIND(00000104): Bind i/f
Jan 30 03:28:58.190: AAA/AUTHOR (0x104):

Pick method list 'FlexVPN-Authorization-List'

Jan 30 03:28:58.192: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access2, changed state to Jan 30 03:28:58.209: %SYS-5-CONFIG\_P: Configured programmatically by process Crypto INT from console as Jan 30 03:28:58.398: %LINEPROTO-5-UPDOWN:

Line protocol on Interface Virtual-Access2, changed state to up

# 相关信息

• <u>思科技术支持和下载</u>

#### 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)。