使用预共享密钥在Windows 8 PC和ASA之间配置 L2TP over IPsec

目录

简介 <u>先决条件</u> 要求 限制 使用的组件 规则 背景信息 配置 网络图 全通道配置 使用自适应安全设备管理器(ASDM)的ASA配置 使用CLI的ASA配置 Windows 8 L2TP/IPsec客户端配置 拆分隧道配置 ASA上的配置 L2TP/IPsec客户端上的配置 验证 故障排除 相关信息

简介

本文档介绍如何使用思科自适应安全设备(ASA)和Windows 8本地客户端之间的预共享密钥在 IPsec上配置第2层隧道协议(L2TP)。

L2TP over Internet协议安全(IPsec)提供在单个平台中部署和管理L2TP虚拟专用网络(VPN)解决方案 以及IPsec VPN和防火墙服务的功能。

先决条件

要求

Cisco 建议您了解以下主题:

- •从客户端计算机到ASA的IP连接。要测试连接,请尝试从客户端终端ping ASA的IP地址,反之 亦然
- •确保UDP端口500和4500以及封装安全负载(ESP)协议在连接路径的任何位置都不会被阻止

限制

- L2TP over IPsec仅支持IKEv1。不支持IKEv2。
- ASA上带IPsec的L2TP允许LNS与集成在Windows、MAC OS X、Android和Cisco IOS等操作 系统中的本地VPN客户端进行互操作。仅支持带IPsec的L2TP,ASA不支持本地L2TP本身。
- •Windows客户端支持的最小IPsec安全关联生存期为300秒。如果ASA上的生存期设置为少于 300秒,则Windows客户端会忽略该生命期,并将其替换为300秒的生存期。
- ASA仅在本地数据库上支持点对点协议(PPP)身份验证密码身份验证协议(PAP)和Microsoft质询 握手身份验证协议(CHAP)版本1和2。可扩展身份验证协议(EAP)和CHAP由代理身份验证服务 器执行。因此,如果远程用户属于使用authentication eap-proxy或authentication chap命令配置 的隧道组,并且ASA配置为使用本地数据库,则该用户无法连接。

支持的PPP身份验证类型

ASA上的L2TP over IPsec连接仅支持表中所示的PPP身份验证类型

	AAAM	I务器支持和PPP身份验证类型
AAA服务器	器类型	支持的PPP身份验证类型
本地	;	PAP、MSCHAPv1、MSCHAPv2
RADIL	JS PAP、C	CHAP、MSCHAPv1、MSCHAPv2、EAP-Proxy
TACAC	S+	PAP、CHAP、MSCHAPv1
LDAF	0	PAP
NT		PAP
Kerber	os	PAP
SDI		SDI
PPP身份验证	正类型特征	
关键字	认证类型	特征
CHAP	CHAP	为响应服务器质询,客户端返回加密的[质询加密密码],其中包含明文用户名
EAP代理	EAP	启用EAP,该EAP允许安全设备将PPP身份验证过程代理到外部RADIUS身份
	Microsoft	
ms-chap-v1	CHAP,版本1	与CHAP类似 伯更安全的是 服务哭仅友佬和比较加宓宓码 而不是像CH
ms-chap-v2	Microsoft	今0171 天区,但史史王的定,派乃船区仔阁和比农加出出码,而平定家017
	CHAP,版本,2	
pap	PAP	在身份验证期间传递明文用户名和密码,因此不安全。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •运行软件版本9.4(1)的Cisco 5515系列ASA
- L2TP/IPSec客户端(Windows 8)

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。

相关产品

此配置也可与 Cisco ASA 5500 系列安全设备 8.3(1) 一起使用。

规则

背景信息

第2层隧道协议(L2TP)是一种VPN隧道协议,允许远程客户端使用公有IP网络与私有企业网络服务 器安全通信。L2TP使用PPP over UDP(端口1701)来隧道化数据。

L2TP协议基于客户端/服务器模型。该功能分为L2TP网络服务器(LNS)和L2TP接入集中器(LAC)。 LNS通常在网络网关(如本例中的ASA)上运行,而LAC可以是拨号网络接入服务器(NAS)或具有 捆绑的L2TP客户端(如Microsoft Windows、Apple iPhone或Android)的终端设备。

配置

本部分提供配置本文档中所述功能的信息。

注意:有关本文档所用命令的详细信息,请使用<u>命令查找工具(仅限注册用户)。</u>

注意:此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中 使用的 RFC 1918 地址。

网络图



全通道配置

使用自适应安全设备管理器(ASDM)的ASA配置

请完成以下步骤:

步骤1.登录到ASDM,然后导航到**Wizards>VPN Wizards>Ipsec(IKEv1)Remote Access VPN** Wizard。

Gisco ASDM 7.2 for ASA - 10.106.44.216						
File View Too	ols	Wizards	Window Help			
Home 🏤	Confi	Startup Wizard		Ва	Back 🔿 Forward 🦻 Help	
VPN Wizards			Site-to-site VPN Wizard			
Device List		Hig	gh Availability and Scalability Wizard		AnyConnect VPN Wizard	
Add Delete	Unified Communication Wizard			Clientless SSL VPN Wizard		
Find:	_	Pac	cket Capture Wizard		IPsec (IKEv1) Remote Access VPN Wizard	
Image:).63					

步骤2.出现Remote Access VPN设置窗口。从下拉列表中,选择必须终止VPN隧道的接口。在本示例中,外部接口连接到WAN,因此终止此接口上的VPN隧道。保留"启用入**站IPSec会话以绕过接口** 访问列表"框。组策略和每用户授权访问列表仍适用于检查的流量,因此无需在外部接口上配置新访问列表,以允许客户端访问内部资源。单击 Next。

🔁 VPN Wizard	
VPN Wizard	IPsec IKEv1 Remote Access Wizard (Step 1 of)
Branch	Use this wizard to configure new new IPsec (IKEV1) remote access VPN tunnels. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel. This wizard creates basic tunnel configurations that you can edit later using the ASDM.
ISP)	VPN Remote Access
Corporate	Remote Access
Network	
Scatter yo	VPN Tunnel Interface: iputside:
	Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.
	< Back Next > Finish Cancel Help

步骤3.如此映像所示,选择客户端类型为**Microsoft Windows客户端,使用L2TP over IPSec**和**MS-CHAP-V1**和**MS-CHAP-V2**作为PPP身份验证协议,因为PAP不安全,并且LOCAL数据库不支持其 他身份验证类型作为身份验证服务器,然后单击**Next**。



步骤4.选择**Pre-shared-key**身份验证方法,并键入在客户端必须相同的预共享密钥,然后单击 Next,如下图所示。

VPN Wizard	
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of) The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client. Authentication Method Pre-shared key Pre-Shared Key: Clsc0@123 Certificate Certificate Signing Algorithm: rsa-sig Certificate Name: Challenge/response authentication (CRACK) Tunnel Group For VPN clients using L2TP over IPsec with pre-shared key authentication, DefaultRAGroup tunnel group must be used. Tunnel Group Name: DefaultRAGroup
	< Back Next > Finish Cancel Help

步骤5.指定对尝试L2TP over IPsec连接的用户进行身份验证的方法。可以使用外部AAA身份验证服务器或其自己的本地数据库。如果**要根据ASA的本地数据库对客**户端进行身份验证,请选择 Authenticate using the local user database(使用本地用户数据库进行身份验证),然后单击 **Next(下一步)。**

注意:请参阅<u>为VPN用户配置RADIUS身份验证</u>,以使用外部AAA服务器对用户进行身份验证 。

步骤6.要向本地数据库添加新用户以进行用户身份验证,请输入用户名和密码,然后单击ADD,否则数据库中的现有用户帐户可以使用,如下图所示。单击 Next。

VPN Wizard		in the second se	×
VPN Wizard Branch Branch SP Branch Branch	User Accounts (Step 5 of 11) Add new users into the user authen or to remove them from the databas Users/AAA > User Accounts in the r	ntication database. To edit existin se, go to Configuration > Device main ASDM window.	g entries in the database Management >
Corporate Network	Username: test Password (optional): ••••• Confirm Password (optional): •••••	Add >> Delete	
		< Back Next > Fi	nish Cancel Help

步骤7.从下拉列表中,选择要用于为客户端分配IP地址的地址池。要创建新地址池,请单**击"新**建 ",如下图所示。

VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch Fr	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN dients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
THE IN	Pool Name: New
	Pool Settings
Z-HUIMM	Range Start Address:
T	Range End Address:
	Subnet Mask:
	< Back Next > Finish Cancel Help

步骤8.系统将显示Add IPv4 Pool对话框。

- 1. 输入新 IP 地址池的名称。
- 2. 输入起始和结束 IP 地址。
- 3. 输入子网掩码,然后点击确定。

is VPN Wizard		×	
VPN Wizard	Address Pool (Step	p 6 of 11)	
Branch	Enter a pool of lo dients.	ocal addresses to be used for assigning dynamic IP addresses to remote VPN	
Home	📑 Add IPv4 Pool		
Corporate Network	Name:	Address-pool	
Gentle Va	Starting IP Address:	192.168.1.1 New	
	Ending IP Address:	192.168.1.254	
L'UUIII	Subnet Mask:	255.255.255.0	
T	ОК	Cancel Help	
		JUDIICT MOSK.	
		< Back Next > Finish Cancel Help	

步骤9.验证池设置并单击"下一步"。

📴 VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Branch Franch Franch Franch Franch Horno	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN dients.
Corporate Network	Tunnel Group Name : DefaultRAGroup
The state	Pool Name: Address-pool New
	Pool Settings
THUILIN	Range Start Address: 192.168.1.1
T	Range End Address: 192.168.1.254
	Subnet Mask: 255.255.0
	< Back Next > Finish Cancel Help

步骤10.配置要推送到客户端的属性或将其留空,然后单击"下一步"。

T VPN Wizard		×
VPN Wizard	Attributes Pushed to Client (Optional)((Step 7 of 11)
Branch Frankting	Attributes you configure below are push ASA. If you do not want an attribute pus	ed to the VPN client when the client connects to the shed to the client, leave the corresponding field blank.
Corporate Network	Tunnel Group:	DefaultRAGroup
a contra	Primary DNS Server:	8.8.8
	Secondary DNS Server:	4.4.4.2
- THU	Primary WINS Server:	
-I-I-I	Secondary WINS Server:	
	Default Domain Name:	cisco.com
		<back next=""> Finish Cancel Help</back>

步骤 11:确保未选**中启用完全转发保密(PFS)**框,因为某些客户端平台不支持此功能。**启用拆分隧 道以允许远程用户同时对上述定义的资源进行加密访问**,并且未选中对Internet框的未加密访问,这 意味着启用全隧道,其中来自客户机的所有流量(包括互联网流量)将通过VPN隧道发送到ASA。 单击 **Next**。

C VPN Wizard	
VPN Wizard	IPsec Settings (Optional) (Step 8 of 11)
Branch Frank Frank Frank Frank	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the Exempt Networks field blank.
Corporate	Interface:
	Exempt Networks:
	Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.
	Enable Perfect Forwarding Secrecy (PFS)
	Diffie-Hellman Group: 1
	< <u>Back</u> <u>Next</u> > <u>Finish</u> <u>Cancel</u> <u>H</u> elp

步骤12.查看摘要信息,然后单击"完**成"。**



使用CLI的ASA配置

步骤1.配置IKE第1阶段策略参数。

此策略用于保护对等体之间的控制流量(即保护预共享密钥和第2阶段协商)

ciscoasa(config)#crypto ikev1 policy 10 ciscoasa(config-ikev1-policy)#authentication pre-share ciscoasa(config-ikev1-policy)#encryption 3des ciscoasa(config-ikev1-policy)#hash sha ciscoasa(config-ikev1-policy)#group 2 ciscoasa(config-ikev1-policy)#lifetime 86400 ciscoasa(config-ikev1-policy)#exit 步骤2.配置转换集。

它包含用于保护数据流量的IKE第2阶段策略参数。由于Windows L2TP/IPsec客户端使用IPsec传输 模式,因此请将该模式设置为传输。默认为隧道模式

ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac ciscoasa(config)#crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport 步骤3.配置动态映射。

当Windows客户端从ISP或本地DHCP服务器(例如调制解调器)获取动态IP地址时,ASA不知道对 等体IP地址,这在ASA端的静态对等体配置中会造成问题。因此,必须进行动态加密配置,在这种 配置中,所有参数不一定都定义,而缺失的参数稍后会通过客户端的IPSec协商动态获知。 ciscoasa(config)#crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA

步骤4.将动态映射绑定到静态加密映射并应用加密映射并在外部接口上启用IKEv1

无法在接口上应用动态加密映射,因此请将其绑定到静态加密映射。动态加密集应是加密映射集中 优先级最低的加密映射(即,它们应具有最高的序列号),以便ASA首先评估其他加密映射。仅当 其他(静态)映射条目不匹配时,才会检查动态加密映射集。

ciscoasa(config)#crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map ciscoasa(config)#crypto map outside_map interface outside ciscoasa(config)#crypto ikev1 enable outside 步骤5.创建P地址池

创建一个地址池,从该地址池将IP地址动态分配给远程VPN客户端。忽略此步骤以使用ASA上的现 有池。

ciscoasa(config)#ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 **步骤6.配置组策略**

将组策略标识为内部,这表示从本地数据库提取属性。

ciscoasa(config)#group-policy L2TP-VPN internal

注意:L2TP/IPsec连接可以配置默认组策略(DfltGrpPolicy)或用户定义的组策略。无论哪种情况,必须将组策略配置为使用L2TP/IPsec隧道协议。在默认组策略的VPN协议属性上配置 I2tp-ipsec,如果未在其上配置vpn-protocol属性,则默认组策略将继承到用户定义的组策略。

配置属性,如vpn隧道协议(在本例中为l2tp-ipsec)、域名、DNS和WINS服务器IP地址以及新用户 帐户

ciscoasa(config)#group-policy L2TP-VPN attributes

ciscoasa(config-group-policy)#dns-server value 8.8.8.8 4.4.4.2

ciscoasa(config-group-policy)#vpn-tunnel-protocol l2tp-ipsec

ciscoasa(config-group-policy)#default-domain value cisco.com

除使用AAA外,还在设备上配置用户名和密码。如果用户是使用Microsoft CHAP第1版或第2版的 L2TP客户端,并且ASA配置为根据本地数据库进行身份验证,则必须包含mschap关键字。例如 , username <username> password <password> mschap。

ciscoasa(config-group-policy)# username test password test mschap 步骤7.配置隧道组

使用tunnel-group命令创建隧道组,并指定用于为客户端分配IP地址的本地地址池名称。如果身份验 证方法为预共享密钥,则隧道组名称必须为DefaultRAGroup,因为客户端上没有指定隧道组的选项 ,因此它只会降级到默认隧道组。使用default-group-policy命令将组策略绑定到隧道组

ciscoasa(config)#tunnel-group DefaultRAGroup general-attributes

ciscoasa(config-tunnel-general)#address-pool Address-pool

ciscoasa(config-tunnel-general)#default-group-policy L2TP-VPN

ciscoasa(config-tunnel-general)#exit

注意:如果执行基于预共享密钥的身份验证,则必须配置默认连接配置文件(隧道组)DefaultRAGroup。如果执行基于证书的身份验证,则可以根据证书标识符选择用户定义的 连接配置文件

使用tunnel-group ipsec-attributes命令进入ipsec属性配置模式以设置预共享密钥。

ciscoasa(config)# tunnel-group DefaultRAGroup ipsec-attributes ciscoasa(config-tunnel-ipsec)# ikev1 pre-shared-key C!sc0@123 ciscoasa(config-tunnel-ipsec)#exit

在隧道组ppp-attributes模式下使用**authentication type命令**配置PPP身份验证协议。禁用默认启用的 CHAP,因为如果AAA服务器配置为本地数据库,则不支持它。

ciscoasa(config)#tunnel-group DefaultRAGroup ppp-attributes ciscoasa(config-ppp)#no authentication chap ciscoasa(config-ppp)#authentication ms-chap-v2 ciscoasa(config-ppp)#exit 步骤8.配置NAT-Exemption

配置NAT-Exemption,以便客户端可以访问连接到内部接口的内部资源(在本例中,内部资源连接 到内部接口)。

ciscoasa(config)#object network L2TP-Pool ciscoasa(config-network-object)#subnet 192.168.1.0 255.255.255.0 ciscoasa(config-network-object)#exit ciscoasa(config)# nat (inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp route-lookup 完成示例配置

crypto ikev1 policy 10 authentication pre-share encryption 3des hash sha group 2 lifetime 86400 exit crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA esp-3des esp-sha-hmac crypto ipsec ikev1 transform-set TRANS-ESP-3DES-SHA mode transport crypto dynamic-map outside dyn map 10 set ikev1 transform-set TRANS-ESP-3DES-SHA crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map crypto map outside_map interface outside crypto ikev1 enable outside ip local pool Address-pool 192.168.1.1-192.168.1.254 mask 255.255.255.0 group-policy L2TP-VPN internal group-policy L2TP-VPN attributes vpn-tunnel-protocol l2tp-ipsec default-domain value cisco.com username test password test mschap exit tunnel-group DefaultRAGroup general-attributes

```
address-pool Address-pool
```

default-group-policy L2TP-VPN
exit

tunnel-group DefaultRAGroup ipsec-attributes
ikev1 pre-shared-key C!sc0@123
exit

tunnel-group DefaultRAGroup ppp-attributes
no authentication chap
authentication ms-chap-v2
exit

object network L2TP-Pool
subnet 192.168.1.0 255.255.0
exit

nat(inside,outside) source static any any destination static L2TP-Pool L2TP-Pool no-proxy-arp
route-lookup

Windows 8 L2TP/IPsec客户端配置



1.打开"控制面板"并选择"网络和共享中心"。

2.选择"**设置新连接或网络"**选项。

¥	Network and Sharing Center		×
🛞 🌛 👻 🕈 騹 « All Control P	anel Items	✓ C Search Control Panel	Q
Control Panel Home	View your basic network information and	l set up connections	
Change adapter settings	View your active networks		
Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections:	
	Change your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection Troubleshoot problems Diagnose and repair network problems, or g	ction; or set up a router or access point. net troubleshooting information.	
See also			
HomeGroup Internet Options Windows Firewall			

3.选择"连**接到工作区"选**项,然后单击"下**一步"。**

		×
📀 🔮 Set Up a Connection or Network		
Choose a connection option		
Connect to the Internet Set up a broadband or dial-up connection to the Internet.		
Set up a new network Set up a new router or access point.		
Connect to a workplace Set up a dial-up or VPN connection to your workplace.		
Net		
<u>N</u> ext	Ca	ncel

4.单击"**使用我的互联网连接(VPN)"**选项。



×

5.输入ASA的WAN接口或FQDN的IP地址以及本地有效的VPN适配器的任何名称,然后单击"创**建**"。

€	🖫 Connect to a Workpl	ace	
	Type the Internet addre	ess to connect to	
	Your network administrator c	an give you this address.	
	Internet address:	172.16.1.2	
	Destination name:	L2TP VPN	
	Use a smart card		
	Remember my creder	ntials	
	Allow other people to This option allows any	use this connection yone with access to this computer to use this connection.	
		Crea	te Cancel

6.在"网络和共享中心"上,选择**窗口左**窗格中的"更改适配器设置"选项。

¥	Network and Sharing Cent	er – 🗆 🗙			
🛞 🌛 👻 🕈 🚆 « All Cont	trol Panel Items 🔸 Network and Sharing Center	✓ ♂ Search Control Panel			
Control Panel Home View your basic network information and set up connections					
Change adapter settings	View your active networks				
Change advanced sharing settings	Network 2 Public network	Access type: No Internet access Connections: I Ethernet			
	Change your networking settings				
Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point.					
Troubleshoot problems Diagnose and repair network problems, or get troubleshooting information.					

7.右键单击最近为L2TP VPN创建的适配器,然后选择"属**性"。**



8.导航至**Security**选项卡,选择Type of VPN as Layer 2 Tunneling Protocol with IPsec(L2TP/IPsec),然后单**击Advanced settings(高级设置)。**

L2TP VPN Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
Advanced settings
Require encryption (disconnect if server declines)
Authentication
O Use Extensible Authentication Protocol (EAP)
✓
Properties
O Allow these protocols
Unencrypted password (PAP)
Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
Automatically use my Windows logon name and password (and domain, if any)
OK Cancel

9.输入与隧道组DefaultRAGroup中所述相同的预共享密钥,**然后**单击**OK**。在本例中 ,C!sc0@123用作预共享密钥。

Advanced Properties
L2TP
 Use preshared key for authentication Key: C!sc0@123
Use certificate for authentication
verify the Name and Usage attributes of the server's certificate
OK Cancel

10.选择身份验证方法作为"允许这些协议",并确保仅选中"**Microsoft CHAP版本2(MS-CHAP v2)"复 选框,**然后单击"确**定"**。

L2TP VPN Properties
General Options Security Networking Sharing
Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)
Advanced settings
Require encryption (disconnect if server declines)
Authentication O Use Extensible Authentication Protocol (EAP)
Properties
 Allow these protocols Unencrypted password (PAP) Challenge Handshake Authentication Protocol (CHAP)
Microsoft CHAP Version 2 (MS-CHAP v2)
 Automatically use my Windows logon name and password (and domain, if any)
OK Cancel

11.在网络连接下,右键单击L2TP VPN适配器,然后选择"连接/断**开"。**



12.网络图标将弹出并单击L2TP VPN连接上的连接。



13.输入用户凭据,然后单击"确**定"**。

Networks	
Connecting to 172.16.1.2	
Network Authentication	
User name	
Password	
Domain:	
OK Cancel	

如果两端的参数匹配,将建立L2TP/IPsec连接。



拆分隧道配置

分割隧道功能可用于定义必须加密的子网或主机的流量。这包括配置与此功能关联的访问控制列表 (ACL)。此ACL上定义的子网或主机的流量通过隧道从客户端加密,这些子网的路由安装在PC路由 表中。ASA会拦截来自客户端的DHCPINFORM消息,并使用子网掩码、域名和无类静态路由做出 响应。

ASA上的配置

ciscoasa(config)# access-list SPLIT standard permit 10.1.1.0 255.255.255.0 ciscoasa(config)# group-policy DefaultRAGroup attributes ciscoasa(config-group-policy)# split-tunnel-policy tunnelspecified ciscoasa(config-group-policy)# split-tunnel-network-list value SPLIT ciscoasa(config-group-policy)# intercept-dhcp 255.255.255.255 enable L2TP/IPsec客户端上的配置

1.右键单击L2TP VPN适配器并选择"属性"。



2.导航至"网络"选项卡,选择"Internet协议版本4(TCP/IPv4)",然后单击"属性"。

L2TP VPN Properties	×
General Options Security Networking Sharing	
This connection uses the following items:	
 Internet Protocol Version 4 (TCP/IPv4) File and Printer Sharing for Microsoft Networks 	
Install 🛞 Uninstall Properties	ונ
Description	
wide area network protocol that provides communication across diverse interconnected networks.	
UK Cance	

3.单击"高**级"**选项。

Internet Protocol Version 4 (TCP/IPv4) Properties ? ×
General	
You can get IP settings assigned au supports this capability. Otherwise, y administrator for the appropriate IP se	tomatically if your network ou need to ask your network ettings.
Obtain an IP address automatic	ally
Use the following IP address:	
IP address:	· · ·
Obtain DNS server address aut Use the following DNS server a	addresses:
Preferred DNS server:	
Alternate DNS server:	
	Advanced
	OK Cancel

4.取消选中"**在远程网络上使用默认网关"选**项,然后单击"**确定"**。

Advanced TCP/IP Settings ? ×
IP Settings DNS WINS
This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.
Use default gateway on remote network Disable class based route addition
Automatic metric
Interface metric:
OK Cancel

验证

使用本部分可确认配置能否正常运行。

注意:<u>命令输出解释程序工具(仅限注册用户)支持某些 show</u> 命令。使用输出解释器工具来 查看 show 命令输出的分析。

• show crypto ikev1 sa — 显示对等体上的所有当前IKE SA。

ciscoasa# show crypto ikev1 sa

IKEv1 SAs:

```
Active SA: 1
Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1
```

1 IKE Peer:

10.1.1.2

Type : user Role : responder Rekey : no

State : MM_ACTIVE

● show crypto ipsec sa - 显示对等体上的所有当前 IPsec SA。

ciscoasa# show crypto ipsec sa interface: outside Crypto map tag:

outside_dyn_map

```
, seq num: 10, local addr: 172.16.1.2
```

local ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/

17/1701

```
) remote ident (addr/mask/prot/port): (10.1.1.2/255.255.255.255/
```

17/1701

```
)
```

current_peer: 10.1.1.2, username: test

dynamic allocated peer ip: 192.168.1.1

dynamic allocated peer ip(ipv6): 0.0.0.0

#pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29

#pkts decaps: 118, #pkts decrypt: 118, #pkts verify: 118

#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 29, #pkts comp failed: 0, #pkts decomp failed: 0
#post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0

#send errors: 0, #recv errors: 0 local crypto endpt.: 172.16.1.2/0, remote crypto endpt.: 10.1.1.2/0 path mtu 1500, ipsec overhead 58(36), media mtu 1500 PMTU time remaining (sec): 0, DF policy: copy-df ICMP error validation: disabled, TFC packets: disabled current outbound spi: E8AF927A current inbound spi : 71F346AB inbound esp sas: spi: 0x71F346AB (1911768747) transform: esp-3des esp-sha-hmac no compression in use settings ={RA, Transport, IKEv1, } slot: 0, conn_id: 4096, crypto-map: outside_dyn_map sa timing: remaining key lifetime (kB/sec): (237303/3541) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000003 outbound esp sas: spi: 0xE8AF927A (3903820410) transform: esp-3des esp-sha-hmac no compression in use settings ={RA, Transport, IKEv1, } slot: 0, conn_id: 4096, crypto-map: outside_dyn_map sa timing: remaining key lifetime (kB/sec): (237303/3541) IV size: 8 bytes replay detection support: Y Anti replay bitmap: 0x0000000 0x0000001

● show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec — 显示有关L2TP over IPsec连接的详细信息。

ciscoasa# show vpn-sessiondb detail ra-ikev1-ipsec filter protocol l2tpOverIpSec

Session Type: IKEv1 IPsec Detailed

Username : test

Index : 1

Assigned IP : 192.168.1.1 Public IP : 10.1.1.2

Protocol: IKEv1 IPsec L2TPOverIPsecLicense: Other VPNEncryption: IKEv1: (1)3DES IPsec: (1)3DES L2TPOverIPsec: (1)noneHashing: IKEv1: (1)SHA1 IPsec: (1)SHA1 L2TPOverIPsec: (1)noneBytes Tx: 1574Pkts Tx: 29Pkts Tx Drop: 0Pkts Rx Drop<: 0</td>

Group Policy : L2TP-VPN

Tunnel Group : DefaultRAGroup

Login Time : 23:32:48 UTC Sat May 16 2015 Duration : 0h:04m:05s Inactivity : 0h:00m:00s VLAN Mapping : N/A VLAN : none Audt Sess ID : 0a6a2577000010005557d3a0 Security Grp : none IKEv1 Tunnels: 1 IPsec Tunnels: 1

IKEv1:

Tunnel ID : 1.1 UDP Src Port : 500 IKE Neg Mode : Main Encryption : 3DES Rekey Int (T): 28800 Seconds D/H Group : 2 Filter Name :

L2TPOverIPsec Tunnels: 1

UDP Dst Port : 500 Auth Mode : preSharedKeys Hashing : SHA1 Rekey Left(T): 28555 Seconds

IPsec:

Tunnel ID	:	1.2			
Local Addr	:	172.16.1.2/255.255.255	255/17/1701		
Remote Addr	:	10.1.1.2/255.255.255.25	55/17/1701		
Encryption	:	3des	Hashing	:	SHA1
Encapsulation	:	Transport			
Rekey Int (T)	:	3600 Seconds	Rekey Left(T)	:	3576 Seconds
Rekey Int (D)	:	250000 K-Bytes	Rekey Left(D)	:	250000 K-Bytes
Idle Time Out	:	30 Minutes	Idle TO Left	:	29 Minutes
Bytes Tx	:	1574	Bytes Rx	:	12752
Pkts Tx	:	29	Pkts Rx	:	118

L2TPOverIPsec:

Tunnel ID : 1.3

Username : test

Assigned IP : 192.168.1.1

Public IP : 10.1.1.2

```
Encryption : none
```

Idle Time	Out:	30 Minutes	Idle TO Left	:	27 Minutes
Client OS	:	Microsoft			
Client OS	Ver:	6.2			
Bytes Tx	:	475	Bytes Rx	:	9093
Pkts Tx	:	18	Pkts Rx	:	105

在ASDM上,在**Monitoring > VPN > VPN Statistics > Sessions**下,可以看到有关VPN会话的一般 信息。L2TP over IPsec会话可以按IPsec(IKEv1)Remote Access > Protocol > L2TP Over IPsec进 **行过滤**。

File View Tools Wizards Windo	File View Tools Wizards Window Help 60												
🚯 hone 🖏 Configuration 🔽 Monterrey 🕞 Save 🗞 Refersh 💿 Rack 💿 Formard 🤰 Hole													cisco
Device List 🗗 🕂 🗙	Monitoring > VPN > V	Monitoring > VPN > VPN Statistics > Sessions											
🗣 Add 📋 Delete 🚿 Connect													
Find: Go	Type		Active			Cumulative			Peak Concurrent		Inactive		
10.105.130.63 A	IKEv1 IPsec/L2TP IPse	c			1				15		1		
- 10.105.130.98 II.105.130.102													
📇 10.105.130.153 📑 10.105.130.211													
■ 10.105.130.214 ■ 10.105.130.225 ▼	Filter By: IPper(IKE y	1) Remote Access	atocal	- I ZTP Over IPper	Filter								
VPN 🗗 🕀	The off a second i	a) tempte necessi v) (n	0.000	• Jean order bee									
VPN Statistics	Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption	Login Time Duration		Client(Peer) Type Version	Bytes Tx Bytes Rx	NAC Result Posture Token				Details
VPN Cluster Loads	test	DefaultRAGroup DefaultRAGroup	192.168.1.1 64.103.236.179	IKEv1 IPsec L2TPOverIPse IKEv1: (1)3DES IPsec: (1.	05:45:13 UTC Sat May 9 : .0h:03m:23s		Microsoft 6.1	1422 24688	Unknown				Logout
Compression Statistics													Ping
Global IKE/IPsec Statistics													
Protocol Statistics													
Clentless SSL VPN													
WSA Sessions													

故障排除

本部分提供了可用于对配置进行故障排除的信息。

注意:使用 debug 命令之前,请参阅有关 Debug 命令的重要信息。

警告:在ASA上,可以设置各种调试级别;默认情况下,使用1级。如果更改调试级别,调试 的详细程度可能会增加。请谨慎执行此操作,特别是在生产环境中!

请谨慎使用以下debug命令以排除VPN隧道的问题

• debug crypto ikev1 — 显示有关IKE的调试信息

• debug crypto ipsec — 显示有关IPsec的调试信息

以下是成功的L2TP over IPSec连接的调试输出:

```
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ SA (1) + VENDOR (13) + VENDOR (13)
```

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Received NAT-Traversal ver 02 VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing IKE SA payload
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1]Phase 1 failure: Mismatched attribute types for class Group
Description: Rcv'd: Unknown Cfg'd: Group 2
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2,
```

IKE SA Proposal # 1, Transform # 5 acceptable Matches global IKE entry # 2

```
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ISAKMP SA payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Traversal VID ver RFC payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Fragmentation VID + extended
capabilities payload
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
SA (1) + VENDOR (13) + VENDOR (13) + NONE (0) total length : 124
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + NAT-D (20) + NAT-D (20) + NONE (0) total length : 260
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing ISA_KE payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, processing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing ke payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing nonce payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing Cisco Unity VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing xauth V6 VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send IOS VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Constructing ASA spoofing IOS Vendor ID payload
(version: 1.0.0, capabilities: 2000001)
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing VID payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, Send Altiga/Cisco VPN3000/Cisco ASA GW VID
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, constructing NAT-Discovery payload
May 18 04:17:18 [IKEv1 DEBUG]IP = 10.1.1.2, computing NAT Discovery hash
May 18 04:17:18 [IKEv1]IP = 10.1.1.2,
```

Connection landed on tunnel_group DefaultRAGroup

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating keys for
Responder...
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR +
KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (20) + NAT-D
(20) + NONE (0) total length : 304
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=0) with payloads : HDR
+ ID (5) + HASH (8) + NONE (0) total length : 64
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received
10.1.1.2
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
```

Automatic NAT Detection Status: Remote end is NOT behind a NAT device This end is NOT behind a NAT device

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Connection landed on tunnel_group DefaultRAGroup May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing ID payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Computing hash for ISAKMP May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing dpd vid payload May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=0) with payloads : HDR + ID (5) + HASH (8) + VENDOR (13) + NONE (0) total length : 84 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

PHASE 1 COMPLETED

May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alive type for this connection: None May 18 04:17:18 [IKEv1]IP = 10.1.1.2, Keep-alives configured on but peer does not support keepalives (type = None) May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P1 rekey timer: 21600 seconds. May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500 May 18 04:17:18 [IKEv1 DECODE]IP = 10.1.1.2, IKE Responder starting QM: msg id = 00000001 May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 300 May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing nonce payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 10.1.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received remote Proxy Host data in ID Payload: Address 10.1.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing ID payload May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, ID_IPV4_ADDR ID received 172.16.1.2 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Received local Proxy Host data in ID Payload: Address 172.16.1.2, Protocol 17, Port 1701

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

L2TP/IPSec session detected.

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, QM IsRekeyed old sa not found by addr May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,

Static Crypto Map check, map outside_dyn_map, seq = 10 is a successful match

May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Remote Peer configured for crypto map: outside_dyn_map May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing IPSec SA payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, I

PSec SA Proposal # 2, Transform # 1 acceptable

Matches global IPSec SA entry # 10 May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, IKE: requesting SPI! IPSEC: New embryonic SA created @ 0x00007fffe13ab260, SCB: 0xE1C00540, Direction: inbound SPI : 0x7AD72E0D Session ID: 0x00001000 VPIF num : 0x0000002 Tunnel type: ra Protocol : esp Lifetime : 240 seconds May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got SPI from key engine: SPI = 0x7ad72e0dMay 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, oakley constucting quick mode May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing blank hash payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec SA pavload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing IPSec nonce payload May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing proxy ID May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2,

Transmitting Proxy Id:

Remote host: 10.1.1.2 Protocol 17 Port 1701

Local host: 172.16.1.2 Protocol 17 Port 1701

```
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, constructing qm hash payload
May 18 04:17:18 [IKEv1 DECODE]Group = DefaultRAGroup, IP = 10.1.1.2, IKE Responder sending 2nd
QM pkt: msg id = 00000001
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE SENDING Message (msgid=1) with payloads : HDR +
HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5) + NONE (0) total length : 160
May 18 04:17:18 [IKEv1]IKE Receiver: Packet received on 172.16.1.2:500 from 10.1.1.2:500
May 18 04:17:18 [IKEv1]IP = 10.1.1.2, IKE_DECODE RECEIVED Message (msgid=1) with payloads : HDR
+ HASH (8) + NONE (0) total length : 52
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, processing hash payload
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, loading all IPSEC SAs
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Generating Quick Mode Key!
IPSEC: New embryonic SA created @ 0x00007fffe1c75c00,
  SCB: 0xE13ABD20,
  Direction: outbound
   SPI
         : 0x8C14FD70
   Session ID: 0x00001000
  VPIF num : 0x0000002
```

Tunnel type: ra Protocol : esp Lifetime : 240 seconds IPSEC: Completed host OBSA update, SPI 0x8C14FD70 IPSEC: Creating outbound VPN context, SPI 0x8C14FD70 Flags: 0x00000205 SA : 0x00007fffe1c75c00 SPI : 0x8C14FD70 MTU : 1500 bytes VCID : 0x0000000 Peer : 0x0000000 SCB : 0x0AC609F9 Channel: 0x00007fffed817200 IPSEC: Completed outbound VPN context, SPI 0x8C14FD70 VPN handle: 0x000000000028d4 IPSEC: New outbound encrypt rule, SPI 0x8C14FD70 Src addr: 172.16.1.2 Src mask: 255.255.255.255 Dst addr: 10.1.1.2 Dst mask: 255.255.255.255

Src ports

Upper: 1701

Lower: 1701

Op : equal

Dst ports

Upper: 1701

Lower: 1701

Op : equal

Protocol: 17

Use protocol: true SPI: 0x0000000 Use SPI: false

```
IPSEC: Completed outbound encrypt rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: New outbound permit rule, SPI 0x8C14FD70
  Src addr: 172.16.1.2
  Src mask: 255.255.255.255
  Dst addr: 10.1.1.2
   Dst mask: 255.255.255.255
   Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
   Use protocol: true
  SPI: 0x8C14FD70
  Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c76a00
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, NP encrypt rule look up for
crypto map outside_dyn_map 10 matching ACL Unknown: returned cs_id=e148a8b0;
encrypt_rule=00000000; tunnelFlow_rule=00000000
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2, Security negotiation complete for
User () Responder, Inbound SPI = 0x7ad72e0d, Outbound SPI = 0x8c14fd70
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, IKE got a KEY_ADD msg for
SA: SPI = 0x8c14fd70
IPSEC: New embryonic SA created @ 0x00007fffe13ab260,
  SCB: 0xE1C00540,
  Direction: inbound
       : 0x7AD72E0D
  SPT
  Session ID: 0x00001000
  VPIF num : 0x0000002
  Tunnel type: ra
  Protocol : esp
            : 240 seconds
  Lifetime
IPSEC: Completed host IBSA update, SPI 0x7AD72E0D
IPSEC: Creating inbound VPN context, SPI 0x7AD72E0D
  Flags: 0x00000206
  SA : 0x00007fffe13ab260
  SPI : 0x7AD72E0D
  MTU : 0 bytes
  VCID : 0x0000000
  Peer : 0x000028D4
  SCB : 0x0AC5BD5B
  Channel: 0x00007fffed817200
IPSEC: Completed inbound VPN context, SPI 0x7AD72E0D
  VPN handle: 0x000000000004174
IPSEC: Updating outbound VPN context 0x000028D4, SPI 0x8C14FD70
   Flags: 0x0000205
   SA : 0x00007fffe1c75c00
  SPI : 0x8C14FD70
  MTU : 1500 bytes
  VCID : 0x0000000
  Peer : 0x00004174
  SCB : 0x0AC609F9
   Channel: 0x00007fffed817200
IPSEC: Completed outbound VPN context, SPI 0x8C14FD70
  VPN handle: 0x000000000028d4
IPSEC: Completed outbound inner rule, SPI 0x8C14FD70
  Rule ID: 0x00007fffe1c763d0
IPSEC: Completed outbound outer SPD rule, SPI 0x8C14FD70
   Rule ID: 0x00007fffe1c76a00
```

```
IPSEC: New inbound tunnel flow rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 1701
    Lower: 1701
    Op : equal
   Dst ports
    Upper: 1701
    Lower: 1701
    Op : equal
   Protocol: 17
   Use protocol: true
   SPI: 0x0000000
  Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe13aba90
IPSEC: New inbound decrypt rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
  Use protocol: true
  SPI: 0x7AD72E0D
  Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe1c77420
IPSEC: New inbound permit rule, SPI 0x7AD72E0D
  Src addr: 10.1.1.2
  Src mask: 255.255.255.255
  Dst addr: 172.16.1.2
  Dst mask: 255.255.255.255
  Src ports
    Upper: 0
    Lower: 0
    Op : ignore
  Dst ports
    Upper: 0
    Lower: 0
    Op : ignore
   Protocol: 50
  Use protocol: true
  SPI: 0x7AD72E0D
  Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x7AD72E0D
  Rule ID: 0x00007fffe13abb80
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Pitcher: received
KEY_UPDATE, spi 0x7ad72e0d
May 18 04:17:18 [IKEv1 DEBUG]Group = DefaultRAGroup, IP = 10.1.1.2, Starting P2 rekey timer:
3420 seconds.
May 18 04:17:18 [IKEv1]Group = DefaultRAGroup, IP = 10.1.1.2,
```

PHASE 2 COMPLETED

(msgid=00000001)
May 18 04:17:18 [IKEv1]IKEQM_Active() Add L2TP classification rules: ip <10.1.1.2> mask
<0xFFFFFFF> port <1701>
May 18 04:17:21 [IKEv1]Group = DefaultRAGroup,

Username = test, IP = 10.1.1.2, Adding static route for client address: 192.168.1.1 下表显示了Windows客户端上常见的一些VPN相关错误

错误代码 可能的解决方案

691 确保输入的用户名和密码正确

789,835 确保在客户端上配置的预共享密钥与在ASA上配置相同

800 1.确保VPN类型设置为"第2层隧道协议(L2TP)"

000 2.确保已正确配置预共享密钥

809 确保UDP端口500、4500(在客户端或服务器位于NAT设备后面的情况下)和ESP流量未被阻止

相关信息

- Cisco ASA 5500 系列自适应安全设备
- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- <u>技术支持和文档 Cisco Systems</u>