配置Shrew Soft VPN客户端以连接到RV34X系列路由器

目标

本文档的目的是展示如何使用Shrew Soft VPN客户端连接到RV340系列路由器。

您可以从以下位置下载最新版本的Shrew Soft VPN客户端软件:

https://www.shrew.net/download/vpn

适用设备 |软件版本

RV340 | 1.0.3.17<u>(下载最新)</u>

RV340W | 1.0.3.17(下载<u>最新版</u>)

RV345 | 1.0.3.17(下载<u>最新版</u>)

RV345P | 1.0.3.17(下载<u>最新版</u>)

简介/使用案例

IPSec VPN(虚拟专用网络)允许您通过在Internet上建立加密隧道来安全地获取远 程资源。RV34X系列路由器用作IPSEC VPN服务器,并支持Shrew Soft VPN客户端 。本指南将向您展示如何配置路由器和Shrew Soft Client以保护与VPN的连接。

本文档包含两部分:

配置RV340系列路由器

配置Shrew Soft VPN客户端

配置RV34X系列路由器:

首先,我们将在RV**34x上配置客**户端到站点VPN

第1步

在VPN > Client-to-Site中,



步骤 2

添加客**户端到站点VPN配**置文件

	Getting Started	Client to Site			Analy	Canal
¢	Status and Statistics				Арру	Caricer
쇱	Administration	IPSec Client-to-Site Tunnels				^
٥	System Configuration					
Ø	WAN	Group/Tunnel Name 🗢	WAN Interface \$	Authentication Method 🗢		
#	LAN					
Ş	Wireless					
æ	Routing					
	Firewall					
E	VPN 1					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
C	Client-to-Site 2					

步骤 3

选择Cisco VPN Client选项。



步骤 4

选中Enable框,使VPN客户端配置文件处于活动状态。我们还将配置*组名*称,选**择WAN接**口,并输 入预共享密钥。

注意:请注意组名和预共享密钥,它们稍后将在配置客户端时使用。

Enable:	
Group Name:	Clients
Interface:	WAN1 ~
IKE Authentication Method	b
Pre-shared Key:	
	•••••
Minimum Pre-shared Key Complexity:	•••••
Minimum Pre-shared Key Complexity: Show Pre-shared Key:	Enable Enable

暂时将**用户组表**留空。这是用于路*由器*上的用户组,但我们尚未对其进行配置。确保模**式**设置为**客** 户端。输入客户端LAN的池范围。我们将使用172.16.10.1到172.16.10.10。

注意:池范围应使用网络中其他位置未使用的唯一子网。

User Group:	
User Group Table	
 + mi □ Group Name 	
Mode:	Client O NEM
Pool Range for Client LAN	
Start IP:	172.16.10.1
End IP:	172.16.10.10

步骤 6

此处是配置模式配置设置的位置。我们将使用以下设置:

主 DNS 服务器:如果您有内部DNS服务器或想使用外部DNS服务器,可以在此处输入。否则 ,默认设置为RV340 LAN IP地址。我们将在示例中使用默认值。

分割隧道:选中以启用分割隧道。这用于指定哪些流量将通过VPN隧道。我们将在示例中使用分 割隧道。

拆分隧道表:输入VPN客户端应通过VPN访问的网络。本示例使用RV340 LAN网络。

Mode Configuration			
Primary DNS Server:	192.168.1.1		
Secondary DNS Server:			
Primary WINS Server:			
Secondary WINS Server:			
Default Domain:			
Backup Server 1:		(IP Address or Domain Name)	
Backup Server 2:		(IP Address or Domain Name)	
Backup Server 3:		(IP Address or Domain Name)	
Split Tunnel:	Ø		
Split Tunnel Table			
+ 🕜 🛍			
☑ IP Address ≑			Netmask 🗢
192.168.1.0			255.255.255.0

单击Save后,我们可以在IPSec Client-to-Site Groups列表中看到Profile。

Client to Site		
IPSec Client-to-Site Tunnels		
 + I and a second second	WAN Interface \$	Authentication Method 🗢
Clients	WAN1	Pre-shared Key

步骤 8

现在,我们将配**置用**于验证VPN客户端用户的用户组。在**系统配置 >用户组**中,单**击"+"以添**加用户 组。



输	入	组	名	称。	0
---	---	---	---	----	---

Overviev	Overview		
Group Name:	VPN		

在Services部分> EzVPN/第3方中,单击Add 将此用户组链接到之前配置的客户端到站点配置文件

S User Overv Group Na	riliation Groups /iew me: VPN	RV340W-router450	XXE2	Add Feature List	27 Add Cancel
H ¢	Jser Memt	User Name \$	Joined Gr	sups * 0	
1	0	cisco	admin		
2		guest	guest		
* Should I Servic Web Logi Site to Sit	have at lease CES In/NETCON te VPN	it one account in the "ad	min" group ed O Read Only	O Administrator	
Site to	Site VPN F	Profile Member In-use 1	able		
EzVPN/3	d Party				

步骤 11

您现在应该在EzVPN/第三方的列表中看到"客户端到站点组名称"

EzVPN/3rd Par	EzVPN/3rd Party					
EzVPN/3rd Party Profile Member In-use Table						
+ m	∔ ⋒					
□ # \$	Group Name 🗢					
□ 1	Clients					

步骤 12

应用用**户**组配置后,您将在**用户组**列表中看到该配置,并显示新用户组将与我们之前创建的客户端 到站点配置文件一起使用。

⊗ .∳	Getting Started Status and Statistics	User Groups			
*	Administration	User Groups Table			
Ľ.	System Conliguration	+ 🕑 🔒			
	System	Group 🗢	Web Login/NETCONF/RESTCONF \$	S2S-VPN ¢	EzVPN/3rd Party \$
	Time	O VPN	Disabled	Disabled	Clients
	Log	admin	Admin	Disabled	Disabled
	Email	guest	Disabled	Disabled	Disabled
	User Accounts				
	User Groups				

现在,我们将在"系统配置"(System Configuration)>"用**户帐户"(**User Accounts)**中配置新用**户。单击 '+'创建新用户。

ocal	User N	Membership List	
+	6	J 📥	
	# \$	User Name 🗢	Group * 🗢
0	1	cisco	admin
0	2	guest	guest

步骤 14

输入新**用户名**和新**密码**。验证组已**设**置为我们刚**配置的**新用户组。完成后单击"应用"。

User Accounts					
Add User Acco	ount				
User Name	vpnuser				
New Password		(Range: 0 - 127)			
New Password Confirm					
Group	VPN •				

步骤 15

新用**户**将显示在本地用户**列表中**。

ocal U	ser Membership List	
+ @	8 🖮 📥	
□ #	User Name \$	Group * 🗢
0 1	cisco	admin
0 2	guest	guest
03	vpnuser	VPN

RV340系列路由器的配置完成。现在,我们将配置Shrew Soft VPN客户端。

配置ShrewSoft VPN客户端

现在,我们将配置Shrew Soft VPN客户端。

第1步

打开ShrewSoft VPN Access Manager, 然后单击"添**加"**添加配置文件。在显示的VPN Site Configuration窗口中,配置General选项卡:

主机名或 IP 地址:使用WAN IP地址(或RV340的主机名)

自动配置:选择ike config pull

适配器模式:选择使用虚拟适配器和分配的地址

PN Site Configu	iration					
General Client	Name Res	olution	Authent	ication P 🔨 🕨		
Remote Hos	ł					
Host Name	or IP Address			Port		
192.168.75.	113			500		
Auto Config	uration	ike con	fig pull	•		
Local Host						
Adapter Mo	de					
Use a virtu	Use a virtual adapter and assigned address					
MTU		🗸 Obta	in Auton	natically		
1380	Address					
	Netmask					
	ſ	Sav	e	Cancel		

配置"客户**端"**选项卡。我们只使用默认设置。

VPN Site Configuration					
General Client Name Resolutio	n Authentication P				
- Firewall Options					
NAT Traversal	enable 🔻				
NAT Traversal Port	4500				
Keep-alive packet rate	15 Secs				
IKE Fragmentation	enable 🔻				
Maximum packet size	540 Bytes				
Other Options					
Enable Dead Peer Detection					
Enable ISAKMP Failure Notifications					
🔽 Enable Client Login Banner					
Save Cancel					

步骤 3

在"名称**解析"**选项卡> DNS选项卡中,选中**启用**DNS框,并保持选中**自动获取**框。

VPN Site Configuration					
General Client Name	Resolution Authentication P				
DNS WINS					
Enable DNS	V Obtain Automatically				
Server Address #1					
Server Address #2					
Server Address #3					
Server Address #4					
	🔽 Obtain Automatically				
DNS Suffix					
	Save Cancel				

步骤 4

在"名**称解析**"选项卡> WINS选项卡中,选中启用WINS框,并保持选中自动获取框。

VPN Site Configuration					
General Client Name Re	solution Authent	ication P 🔹 🕨			
DNS WINS					
C Enable WINS	📝 Obtain Automatically				
Server Address #1					
Server Address #2					
	Save	Cancel			
l	Ouve	Cuncer			

配置"身份**验证"**选项卡>"**本地身份**"选项卡:

标识类型:选择密**钥标识符**

密钥ID字符串:输入在RV34x上配置的组名

PN Site Configuration						
General Client Name Resolution Authentication P · · ·						
Authentication Method Mutual PSK + XAuth						
Local Identity Remote Identity Credentials						
Identification Type						
Key Identifier 🗸						
Key ID String						
Clients						
Save Cancel						

步骤 6

在"身份**验证"**选项卡> **"远程身份**"选项卡中,我们将保留默认设置。

标识类型:IP Address

使用已发现的远程主机地址框:已选中

VPN Site Configuration					
General Client Name Resolution Authentication					
Authentication Method Mutual PSK + XAuth					
Local Identity Remote Identity Credentials					
Identification Type					
IP Address 🗸					
Address String					
Use a discovered remote host address					
Save Cancel					

步骤 7

在"身份验证"选项卡> "凭证"选项卡中, 配置以下内容:

认证方法:选择Mutual PSK +扩展验证

预共享密钥:输入在RV340客户端配置文件中配置的预共享密钥

PN Site Configuration
General Client Name Resolution Authentication P · · ·
Authentication Method Mutual PSK + XAuth
Local Identity Remote Identity Credentials
Server Certificate Autority File
Client Certificate File
Client Private Key File
Pre Shared Key
•••••
Save Cancel

步骤 8

对于"**第1阶**段"(Phase 1)选项卡,我们将保留默认设置:

交换类型: 攻击性

DH交换:第2组

密码算法:自动

散列算法:自动

VPN Site Configuration					
Client Name Resolutio	n Authentication Phase 1 P				
- Proposal Parameters -					
Exchange Type	aggressive 💌				
DH Exchange	group 2 💌				
Cipher Algorithm	auto 💌				
Cipher Key Length	The Bits				
Hash Algorithm	auto 💌				
Key Life Time limit	86400 Secs				
Key Life Data limit	0 Kbytes				
Enable Check Point Compatible Vendor ID					
Save Cancel					

步骤 9

我们还将使用"第2阶段"(Phase 2)选**项卡的默**认值:

转换算法:自动

HMAC算法:自动

PFS**交换:**禁用

压缩算法:禁用

Name Resolution Authentic	cation Phase 1 Phase 2 🔹 🕨			
Proposal Parameters				
Transform Algorithm	auto 🗸			
Transform Key Length	The Bits			
HMAC Algorithm	auto 🔻			
PFS Exchange	disabled 🔹			
Compress Algorithm	disabled 🔹			
Key Life Time limit	3600 Secs			
Key Life Data limit	0 Kbytes			
	Sava Cancol			

对于**Policy**选项卡,我们将使用以下设置:

策略生成级别:自动

维护持续安全关联:已选中

自动获取拓扑或全部隧道:已选中

由于我们在RV340上配置了分割隧道,因此我们无需在此处进行配置。

IPSEC Policy Configuration Policy Generation Level Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource Add Modify Delete	Site Configuration	х ())
IPSEC Policy Configuration Policy Generation Level Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource Add Modify Delete	Intentication Phase I Phase 2 Policy	.1.
Policy Generation Level auto Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource Add Modify	IPSEC Policy Configuration	
Maintain Persistent Security Associations Obtain Topology Automatically or Tunnel All Remote Network Resource Add Modify Delete	Policy Generation Level auto	
Colored Point Colored All Remote Network Resource Add Modify Delete	Maintain Persistent Security Associations	
Remote Network Resource Add Modify Delete	Obtain Topology Automatically or Tunnel All	
Add Modify Delete	Remote Network Resource	
Add Modify Delete		
Add Modily Delete	Add Madity Dalata	
	Add Modify Delete	

完成后,单击 Save(保存)。

现在,我们已准备好测试连接。在"VPN Access Manager(VPN访问管理器)"中,突出显示连接配置 文件并单击"**Connect(连**接)"按钮。

(3) VPN Access Manager					
File Edit	View	Help			
8	•	2	0		
Connect	Add	Modify	Delete		
Connectio	n Name	/ Hos	st Name	Authenticat	
🔁 192.168	.75.113	192	.168.75.113	8 mutual-psk	

步骤 12

在出现**的VPN Connect**窗口中,使用我们在RV340上创建的**用户帐户**的凭证输入**用户名**和**密码**(步骤13和14)。

VPN Connect	t - 192.168.75.113		
Connect Netwo	rk		
config log do d	(ar aita 1100 100 7E 110		
coning loaded for site 192.166.75.113			
Condentiale			
Credentials			
Username	vpnuser		
Password	•••••		
	Connect	Evit	
	Connect	EAR	

完成后,单击Connect。

步骤 13

验证隧道是否已连接。您应该看到隧道已启用。

S VPN Connect - 192.168.75.113	X
Connect Network	
local id configured remote id configured pre-shared key configured bringing up tunnel network device configured tunnel enabled	4
Credentials	
Username vpnuser	
Password	
Disconnect Cance	I

结论

现在,您已设置通过VPN连接到网络。