# RV34X Series Router에 연결하도록 Shrew Soft VPN 클라이언트 구성

### 목표

이 문서의 목적은 Shrew Soft VPN 클라이언트를 사용하여 RV340 Series 라우터에 연결하는 방법 을 보여 주는 것입니다.

shrew Soft VPN 클라이언트 소프트웨어의 최신 버전을 여기에서 다운로드할 수 있습니다.

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

### 적용 가능한 디바이스 | 소프트웨어 버전

RV340 | 1.0.3.17 <u>(최신 다운로드)</u>

RV340W | 1.0.3.17(<u>최신 다운로드</u>)

RV345 | 1.0.3.17(<u>최신 다운로드</u>)

RV345P | 1.0.3.17(<u>최신 다운로드</u>)

#### 소개/활용 사례

IPSec VPN(Virtual Private Network)을 사용하면 인터넷을 통해 암호화된 터널을 설 정하여 원격 리소스를 안전하게 확보할 수 있습니다.RV34X 시리즈 라우터는 IPSEC VPN 서버로 작동하며 Shrew Soft VPN Client를 지원합니다.이 가이드에서는 라우터 와 Shrew Soft Client를 구성하여 VPN에 대한 연결을 보호하는 방법을 보여줍니다.

이 문서는 두 부분으로 구성됩니다.

RV340 Series 라우터 구성

shrew Soft VPN 클라이언트 구성

## RV34X Series 라우터를 구성합니다.

먼저 RV34x에서 Client-to-Site VPN을 구성합니다.

VPN > Client-to-Site에서



#### 2단계

#### 클라이언트 **대 사이트** VPN 프로파일 추가

	Getting Started	Client to Site			Apply	Cancel
G	Status and Statistics				Арру	Caricer
앹	Administration	IPSec Client-to-Site Tunnels				^
٥	System Configuration					
0	WAN	Group/Tunnel Name 🕈	WAN Interface 🗢	Authentication Method \$		
4	LAN					-
\$	Wireless					
8	) Routing					
	Firewall					
	J VPN					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
Г	Client-to-Site					

#### 3단계

Cisco VPN Client 옵션을 선택합니다.



#### 4단계

Enable(활성화) 확인란을 선택하여 VPN 클라이언트 프로파일을 활성화합니다.또한 *그룹 이름*을 구성하고 WAN 인터페이스를 선택한 다음 **사전 공유 키를 입력하겠습니다**.

**참고:**그룹 이름 및 사전 공유 키는 나중에 클라이언트를 구성할 때 사용되므로 주의하십시오.

Enable:	
Group Name:	Clients
Interface:	WAN1 ~
IKE Authentication Metho	d
<ul> <li>IKE Authentication Method</li> <li>Pre-shared Key:</li> </ul>	d •••••
<ul> <li>IKE Authentication Method</li> <li>Pre-shared Key: Minimum Pre-shared Key Complexity:</li> </ul>	d ••••• □ Enable
<ul> <li>IKE Authentication Method</li> <li>Pre-shared Key:</li> <li>Minimum Pre-shared Key Complexity: Show Pre-shared Key:</li> </ul>	d ••••• Enable Enable

사용자 **그룹 테이블**을 비워둡니다.라우터의 *사용자 그룹*에 대한 것이지만 아직 구성하지 않았습니 다.Mode(**모드)**가 Client(클라이언트)로 **설정되었는지 확인합니다**.클라이언트 LAN 풀 범위를 입력 합니다.172.16.10.1~172.16.10.10을 사용하겠습니다

참고:풀 범위는 네트워크의 다른 곳에서 사용되지 않는 고유한 서브넷을 사용해야 합니다.

Client O NEM
172.16.10.1
172.16.10.10

#### 6단계

여기서 모드 컨피그레이션 설정을 구성합니다.사용할 설정은 다음과 같습니다.

**기본 DNS 서버**:내부 DNS 서버가 있거나 외부 DNS 서버를 사용하려는 경우 여기에 입력할 수 있습니다.그렇지 않으면 기본값은 RV340 LAN IP 주소로 설정됩니다.여기서는 기본값을 사용 합니다.

**스플릿 터널:**스플릿 터널링을 활성화하려면 선택합니다.VPN 터널을 통해 이동할 트래픽을 지 정하는 데 사용됩니다.여기서는 스플릿 터널을 사용합니다.

분할 터널 테이블:VPN 클라이언트가 VPN을 통해 액세스할 수 있는 네트워크를 입력합니다.이 예에서는 RV340 LAN 네트워크를 사용합니다.

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:	ß		
Split Tunnel Table			
+ 🕜 🏛			
IP Address ≑			Netmask 🗢
☑ 192.168.1.0			255.255.255.0

Save(저장)를 클릭한 후 IPSec Client-to-Site Groups(IPSec 클라이언트-사이트 그룹) 목록에서 Profile(프로필)을 볼 수 있습니다.

Client to Site		
IPSec Client-to-Site Tunnels		
+ 🕼 🎰		
□ Group/Tunnel Name ≑	WAN Interface 🗢	Authentication Method \$

#### 8단계

이제 VPN 클라이언트 사용자 인증에 사용할 **사용자 그룹**을 구성합니다.System **Configuration(시스 템 컨피그레이션**) > **User Groups(사용자 그룹)에서** '+'를 클릭하여 사용자 그룹을 추가합니다.



### **그룹 이름**을 입력합니다.

Overviev	v	
Group Name:	VPN	

#### 10단계

Services(**서비스**) 섹션 > **EzVPN/3rd Party(EzVPN/서드파티)에서 Add(추가)를** 클릭하여 이 사용자 그룹을 이전에 구성한 **Client-to-Site** Profile(클라이언트-사이트 간 프로필)에 연결합니다.

B	altalta	RV340W-router45	500E2		
	enseo			Add Feature List	×
User	Groups	S			
				Select a Profile Clients •	
Over	view				Count
Group Na	ame: VPN				Cancer
Local	Liner Memi	hambio List			
LOCA	User Merri	oersnip List			
# 0	Join ¢	User Name \$	Joined Gr	oups * 0	
1		cisco	admin		
2		guest	guest		
Servi Web Log Site to Si	CES jin/NETCON ite VPN	F/RESTCONF 💿 Disa	bled O Read Only	© Administrator	
Site to	Site VPN	Profile Member In-use	Table		
+					
	∎ ≎ Con	nection Name			
EzVPN/3	rd Party				
EzVPN	1/3rd Party	Profile Member In-us	e Table		
+					
0	∎ ¢ Gro	up Name 🌣			

### 11단계

이제 EzVPN/**타사**의 목록에 Client-to-Site Group Name이 표시되어야 합니다.

EzVPN/3rd Par	ty
EzVPN/3rd	Party Profile Member In-use Table
+ 📾	
□ # ≑	Group Name 🗢
□ 1	Clients
0 1	Ollents

#### 12단계

사용자 그룹 컨피그레이션을 적용한 후 **사용자 그룹** 목록에 해당 컨피그레이션이 표시되고 새 사용 자 그룹이 이전에 생성한 클라이언트-사이트 프로필과 함께 사용됨을 표시합니다.

⊗	Getting Started Status and Statistics	User Groups			
*	Administration	User Groups Table			
۰.	System Configuration	+ 12 0			
	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				

이제 System Configuration(시스템 컨피그레이션) > User Accounts(**사용자 계정)**에서 새 사용자를 **구성합니다**.'**+'를 클릭하여** 새 사용자를 생성합니다.

ocal U	ser Membership List		
+ 🥑	🐔 💼 📩 🗢 User Name 🗢	Group * 🗢	
□ 1	cisco	admin	
□ 2	guest	guest	

#### 14단계

새 **사용자 이름**과 **새 비밀번호를 입력합니다.그룹**이 방금 구성한 새 **사용자 그룹**으로 설정되어 있 는지 확인합니다.완료되면 Apply를 클릭합니다.

User Accounts	3	
Add User Acco	ount	
User Name	vpnuser	
New Password		( Range: 0 - 127 )
New Password Confirm		
Group	VPN •	

#### 15단계

새 사용자가 로컬 사용자 목록에 표시됩니다.

ocal User Membership List		
+ 🗷	ŵ 🕹	
□ #≎	User Name 🗢	Group * 🗢
0 1	cisco	admin
0 2	guest	guest
	vpnuser	VPN

이렇게 하면 RV340 Series 라우터의 컨피그레이션이 완료됩니다.이제 Shrew Soft VPN 클라이언 트를 구성합니다.

## 뒤쥐Soft VPN 클라이언트 구성

이제 Shrew Soft VPN 클라이언트를 구성합니다.

#### 1단계

뒤쥐Soft *VPN Access Manager를* 열고 Add를 클릭하여 프로필을 추가합니다.나타나는 *VPN Site Configuration(VPN 사이트 컨피그레이션*) 창에서 General(일반) 탭을 구성합니다.

호스트 이름 또는 IP 주소: WAN ip 주소(또는 RV340의 호스트 이름)를 사용합니다.

자동 구성:ike config pull 선택

어댑터 모드:가상 어댑터 및 할당된 주소 사용을 선택합니다.

PN Site Config	uration		X	
General Clien	t Name Resolut	ion Authenti	cation P · ·	
Remote Host Host Name or IP Address Port 192.168.75.113 500				
Auto Config	juration ike	config pull	-	
Local Host Adapter Mode Use a virtual adapter and assigned address				
MTU 1380	Address Netmask	Obtain Autom	atically	
		Save	Cancel	

Client(클라이언트) 탭을 구성합니다.기본 설정만 사용합니다.

VPN Site Configuration				
General Client Name Resolution 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				

#### 3단계

Name Resolution(**이름 확인**) 탭 **> DNS** 탭에서 Enable DNS(**DNS 활성화**) 확인란을 선택하고 Obtain Automatically(자동 **가져오기**) 확인란을 선택한 상태로 둡니다.

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

#### 4단계

Name Resolution(**이름 확인**) 탭 **> WINS** 탭**에서 Enable WINS(WINS 활성화)** 상자를 선택하고 Obtain Automatically(**자동 가져오기**) 확인란을 선택한 상태로 둡니다.

General       Client       Name Resolution       Authentication       P · · ·         DNS       WINS         Image: Client       Name Resolution       Authentication       P · · ·         DNS       WINS       Obtain Automatically         Server Address #1
DNS       WINS         Image: Constraint of the state of
Image: Enable WINS       Image: Obtain Automatically         Server Address #1       Image: Obtain Automatically         Server Address #2       Image: Obtain Automatically
Server Address #1
Server Address #2
Save Cancel

Authentication(**인증**) 탭 > Local Identity(**로컬 ID**) 탭을 구성합니다.

#### 식별 유형:키 식별자 선택

**키 ID 문자열**:RV34x에 구성된 **그룹 이름**을 입력합니다.

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

#### 6단계

Authentication(**인증**) 탭 > Remote Identity(원격 ID) 탭에서 기본 설정을 그대로 둡니다.

**식별 유형**:IP 주소

검색된 원격 호스트 주소 상자 사용:선택

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				

#### 7단계

Authentication(**인증**) 탭 > Credentials(자격 증명) 탭에서 다음을 구성합니다.

인증 방법:상호 PSK + XAuth 선택

사전 공유 키:RV340 Client Profile에 구성된 사전 공유 키를 입력합니다.

General Client	Name Resolution	Authentication P · ·	
Authentication M	fethod Mutual PS	SK + XAuth 🔹	
Local Identity	Remote Identity Cr	redentials	
Server Certifi	icate Autority File		
Client Certificate File			
Client Private Kay File			
	, noy i no		
Pre Shared I	(ev		
•••••			

#### 8단계

1단계 탭의 경우 기본 설정은 그대로 둡니다.

Exchange 유형:공격적

#### **DH 교환:**그룹 2

#### **암호 알고리즘**:자동

#### **해시 알고리즘**:자동

VPN Site Configuration				
Client	Name Resolution	Authentication Pha	se 1 F 🔸 🕨	
- Prop	osal Parameters			
Exchange Type		aggressive	aggressive 🔹	
DH	Exchange	group 2	-	
Cipher Algorithm		auto	•	
Cipl	her Key Length	•	Bits	
Has	sh Algorithm	auto	-	
Key Life Time limit		86400	Secs	
Key Life Data limit		0	Kbytes	
Enable Check Point Compatible Vendor ID				
Save Cancel				

#### 9단계

2단계 탭의 기본값도 사용합니다.

**변환 알고리즘**:자동

**HMAC 알고리즘**:자동

**PFS 교환**:비활성화됨

**압축 알고리즘:**비활성화됨

Name Resolution Authentic	ation 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	
	Save	

Policy 탭의 경우 다음 설정을 사용합니다.

정책 생성 레벨:자동

**영구 보안 연결 유지**:선택

**토폴로지 자동 가져오기 또는 모두 터널**:선택

RV340에서 **스플릿 터널링**을 구성했으므로 여기서 구성할 필요가 없습니다.

Authe	tication Phase 1 Phase 2 Policy
IPS	EC Policy Configuration
P	licy Generation Level auto
	Maintain Persistent Security Associations
	Obtain Topology Automatically or Tunnel All
	Remote Network Resource
	Add Modify Delete
	Add Modify Delete

완료되면 **저장**을 클릭합니다.

이제 연결을 테스트할 준비가 되었습니다. VPN Access Manager에서 연결 프로파일을 강조 표시하고 Connect(연결) 버튼을 클릭합니다.

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

#### 12단계

표시되는 VPN Connect 창에서 RV340에서 생성한 User Account의 자격 증명을 사용하여 Username 및 Password(13 및 14단계)를 입력합니다.

VPN Connect	t - 192.168.75.113					
Connect Netwo	rk					
config loaded	ior eite 102 168 75 113					
coning to acred for site 132.160.75.115						
Condentiale						
Credentials						
Username	vpnuser					
Password	•••••					
	Connect	Evit				
	Connect	EAR				

완료되면 **연결**을 클릭합니다.

13단계

터널이 연결되어 있는지 확인합니다.**터널**이 활성화되었음을 확인해야 합니다.

S VPN Con	nect - 192.168.75.113	X
Connect Ne	etwork	
local id co remote id pre-shared bringing up network de tunnel ena	nfigured configured d key configured o tunnel avice configured bled	4 III +
Credentia	als	
Userna	me vpnuser	
Passw	ord	
	Disconnect Cance	1

## 결론

그렇습니다. 이제 VPN을 통해 네트워크에 연결하도록 설정됩니다.