# Konfigurieren des Shrew Soft VPN-Clients für die Verbindung mit dem Router der Serie RV34X

# Ziel

Dieses Dokument soll zeigen, wie der Shrew Soft VPN-Client für die Verbindung mit einem Router der Serie RV340 verwendet wird.

Sie können die neueste Version der Shrew Soft VPN-Clientsoftware hier herunterladen:

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

Unterstützte Geräte | Softwareversion

RV340 | 1.0.3.17 (neueste Version herunterladen)

RV340 W | 1.0.3.17 (neueste Version herunterladen)

RV345 | 1.0.3.17 (neueste Version herunterladen)

RV345P | 1.0.3.17 (neueste Version herunterladen)

Einführung/Anwendungsfall

Mit IPSec VPN (Virtual Private Network) können Sie Remote-Ressourcen sicher abrufen, indem Sie einen verschlüsselten Tunnel im Internet einrichten. Die Router der Serie RV34X fungieren als IPSEC VPN-Server und unterstützen den Shrew Soft VPN-Client. Dieser Leitfaden zeigt Ihnen, wie Sie Ihren Router und den Shrew Soft Client konfigurieren, um eine Verbindung mit einem VPN zu sichern.

Dieses Dokument besteht aus zwei Teilen:

Konfigurieren des Routers der Serie RV340

Konfigurieren des Shrew Soft VPN-Clients

Konfigurieren des Routers der Serie RV34X:

Zunächst konfigurieren Sie das Client-to-Site-VPN auf dem RV34x.

Schritt 1

In VPN > Client-to-Site,



# Schritt 2

Hinzufügen eines Client-to-Site-VPN-Profils

| ٨        | Getting Started       | Client to Site               |                 |                         | Apply | Cancel |
|----------|-----------------------|------------------------------|-----------------|-------------------------|-------|--------|
| Ģ        | Status and Statistics |                              |                 |                         |       |        |
| 쓭        | Administration        | IPSec Client-to-Site Tunnels |                 |                         |       | ^      |
| ٥        | System Configuration  |                              |                 |                         |       |        |
| ۲        | WAN                   | Group/Tunnel Name 🕈          | WAN Interface 🕈 | Authentication Method 🗢 |       |        |
| 4        | LAN                   |                              |                 |                         |       | -      |
| <b>?</b> | Wireless              |                              |                 |                         |       |        |
| 8        | Routing               |                              |                 |                         |       |        |
|          | Firewall              |                              |                 |                         |       |        |
|          | I VPN                 |                              |                 |                         |       |        |
|          | VPN Status            |                              |                 |                         |       |        |
|          | IPSec Profiles        |                              |                 |                         |       |        |
|          | Site-to-Site          |                              |                 |                         |       |        |
| C        | Client-to-Site 2      |                              |                 |                         |       |        |

Schritt 3

Wählen Sie die Option Cisco VPN Client aus.



## Schritt 4

Aktivieren Sie das Kontrollkästchen Aktivieren, um das VPN-Clientprofil zu aktivieren. Außerdem konfigurieren Sie den *Gruppennamen*, wählen die WAN-Schnittstelle aus und geben einen Pre-shared Key ein.

**Hinweis:** Beachten Sie den *Gruppennamen* und den *vorinstallierten Schlüssel*, die bei der Konfiguration des Clients später verwendet werden.

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

#### Schritt 5

Lassen Sie die **Benutzergruppentabelle** jetzt leer. Dies gilt für die *Benutzergruppe* auf dem Router, wurde jedoch noch nicht konfiguriert. Stellen Sie sicher, dass der **Modus** auf **Client** eingestellt ist. Geben Sie den **Pool-Bereich für Client-LAN ein**. Wir verwenden die Nummern 172.16.10.1 bis 172.16.10.10.

**Hinweis:** Der Pool-Bereich sollte ein eindeutiges Subnetz verwenden, das an keiner anderen Stelle im Netzwerk verwendet wird.

| User Group:                                     |              |
|---|--------------|
| User Group Table                                |              |
| <ul> <li>+ mi</li> <li>□ Group Name </li> </ul> |              |
|   |              |
| Mode:   | O NEM        |
| Pool Range for Client LAN                       |              |
| Start IP:                                       | 172.16.10.1  |
| End IP:   | 172.16.10.10 |

#### Schritt 6

Hier konfigurieren Sie die Einstellungen für die **Moduskonfiguration**. Hier sind die Einstellungen, die wir verwenden werden:

**Primärer DNS-Server**: Wenn Sie einen internen DNS-Server haben oder einen externen DNS-Server verwenden möchten, können Sie diesen hier eingeben. Andernfalls wird der Standardwert auf die RV340 LAN-IP-Adresse festgelegt. In unserem Beispiel verwenden wir die Standardeinstellung.

Split-Tunnel: Aktivieren Sie Split Tunneling. Mit diesem Parameter wird festgelegt, welcher

Datenverkehr über den VPN-Tunnel geleitet wird. In unserem Beispiel wird Split Tunnel verwendet.

**Tunneltabelle aufteilen:** Geben Sie die Netzwerke ein, auf die der VPN-Client über das VPN zugreifen soll. In diesem Beispiel wird das LAN-Netzwerk RV340 verwendet.

| 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:          | 8           |                             |               |
| Split Tunnel Table     |             |                             |               |
| + 🕜 🏛                  |             |                             |               |
| ☑ IP Address \$        |             |                             | Netmask 🗢     |
| ☑ 192.168.1.0          |             |                             | 255.255.255.0 |

#### Schritt 7

Wenn Sie auf **Speichern** klicken, wird das Profil in der Liste **IPSec-Client-to-Site-Gruppen** angezeigt.

| Client to Site               |                            |                         |  |  |  |
|------------------------------|----------------------------|-------------------------|--|--|--|
| IPSec Client-to-Site Tunnels | iec Client-to-Site Tunnels |                         |  |  |  |
| <ul> <li></li></ul>          | WAN Interface 🗢            | Authentication Method 🗢 |  |  |  |
| Clients                      | WAN1                       | Pre-shared Key          |  |  |  |

#### Schritt 8

Wir konfigurieren nun eine **Benutzergruppe** für die Authentifizierung von VPN-Client-Benutzern. Klicken Sie unter **Systemkonfiguration > Benutzergruppen** auf ", um eine Benutzergruppe hinzuzufügen.



Geben Sie einen Gruppennamen ein.

| Overview    | V   |  |
|-------------|-----|--|
| Group Name: | VPN |  |

### Schritt 10

Klicken Sie im **Services**-Abschnitt > **EzVPN/Drittanbieter** auf **Hinzufügen**, um diese Benutzergruppe mit dem **Client-to-Site-**Profil zu verknüpfen, das Sie zuvor konfiguriert haben.

| Ð           | ululu<br>cisco | RV340W-router           | 4500E2            |                            | ×      |  |  |
|-------------|----------------|-------------------------|-------------------|----------------------------|--------|--|--|
| User Groups |                |                         |                   | Add Feature List           |        |  |  |
|             |                |                         |                   | Select a Profile Clients • |        |  |  |
| Over        | viou           |                         |                   |                            |        |  |  |
| Oven        | view           |                         |                   | Add                        | Cancel |  |  |
| Group Na    | ame: VPN       | 4                       |                   |                            |        |  |  |
| Local       | User Mem       | bership List            |                   |                            |        |  |  |
| н о         | Join ¢         | User Name ¢             | Joined Gr         | oups * •                   |        |  |  |
| 1           |                | cisco                   | admin             |                            |        |  |  |
| 2           |                | guest                   | guest             |                            |        |  |  |
| * Should    | have at lea    | st one account in the ' | admin" group      |                            |        |  |  |
| Servi       | ces            |                         |                   |                            |        |  |  |
| Web Log     | in/NETCON      | IF/RESTCONF O Di        | abled O Read Only | O Administrator            |        |  |  |
| Site to Si  | ite VPN        |                         |                   |                            |        |  |  |
| Site to     | Site VPN       | Profile Member In-us    | se Table          |                            |        |  |  |
| +           |                |                         |                   |                            |        |  |  |
|             | ∎ ≎ Con        | nection Name ©          |                   |                            |        |  |  |
| EzVPN/3     | rd Party       |                         |                   |                            |        |  |  |
| EzVPN       | I/3rd Party    | Profile Member In-u     | se Table          |                            |        |  |  |
| +           |                |                         |                   |                            |        |  |  |
| 0           | II © Gro       | up Name 🌣               |                   |                            |        |  |  |
|             |                |                         |                   |                            |        |  |  |

Sie sollten nun den Client-to-Site-Gruppennamen in der Liste für EzVPN/Drittanbieter sehen.



#### Schritt 12

Nachdem Sie die Benutzergruppenkonfiguration **angewendet** haben, wird diese in der Liste **Benutzergruppen** angezeigt. Die neue Benutzergruppe wird mit dem zuvor erstellten Client-to-Site-Profil verwendet.

| 8 | Getting Started       | User Groups       |                               |            |                    |
|---|-----------------------|-------------------|-------------------------------|------------|--------------------|
| ¢ | Status and Statistics | ocor areapo       |                               |            |                    |
| 쓭 | Administration        | User Groups Table |                               |            |                    |
| ۰ | System Configuration  | + 7 *             |                               |            |                    |
|   | 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           |                   |                               |            |                    |

#### Schritt 13

Jetzt konfigurieren Sie einen neuen Benutzer in **Systemkonfiguration > Benutzerkonten**. Klicken Sie auf "+", um einen neuen Benutzer zu erstellen.



Geben Sie den neuen **Benutzernamen** zusammen mit dem **neuen Kennwort ein**. Überprüfen Sie, ob die **Gruppe** auf die neue soeben konfigurierte **Benutzergruppe** eingestellt ist. Klicken Sie abschließend auf **Übernehmen**.

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

## Schritt 15

Der neue Benutzer wird in der Liste der lokalen Benutzer angezeigt.

| Local User Membership List   |         |           |  |
|------------------------------|---------|-----------|--|
| 🕂 🗭 前 📩<br>□ # ¢ User Name ≎ |         | Group * 🗢 |  |
| ) 1                          | cisco   | admin     |  |
| 2                            | guest   | guest     |  |
| 3                            | vpnuser | VPN       |  |

Damit ist die Konfiguration des Routers der Serie RV340 abgeschlossen. Jetzt wird der Shrew Soft VPN-Client konfiguriert.

# Konfigurieren des ShrewSoft VPN-Clients

Jetzt wird der Shrew Soft VPN-Client konfiguriert.

#### Schritt 1

Öffnen Sie den ShrewSoft *VPN Access Manager*, und klicken Sie auf **Hinzufügen**, um ein Profil hinzuzufügen. Im sich öffnenden Fenster *VPN Site Configuration* konfigurieren Sie die Registerkarte **General**:

Hostname oder IP-Adresse: Verwenden Sie die WAN-IP-Adresse (oder den Hostnamen des RV340).

Automatische Konfiguration: Wählen Sie die Option Konfigurationsanfrage aus.

Adaptermodus: Wählen Sie Einen virtuellen Adapter und zugewiesene Adresse verwenden.

| VPN Site Configuration    |                           |  |  |  |  |  |  |
|---------------------------|---------------------------|--|--|--|--|--|--|
| General Client Name Re    | solution Authentication P |  |  |  |  |  |  |
| Remote Host               |                           |  |  |  |  |  |  |
| Host Name or IP Address   | Port                      |  |  |  |  |  |  |
| 192.168.75.113            | 500                       |  |  |  |  |  |  |
| Auto Configuration        | ike config pull 🗸         |  |  |  |  |  |  |
| Local Host                |                           |  |  |  |  |  |  |
| Adapter Mode              |                           |  |  |  |  |  |  |
|                           |                           |  |  |  |  |  |  |
| Use a virtual adapter and | assigned address          |  |  |  |  |  |  |
| мти                       | Obtain Automatically      |  |  |  |  |  |  |
| 1380 Address              | · · · · ·                 |  |  |  |  |  |  |
| Netmask                   |                           |  |  |  |  |  |  |
|                           |                           |  |  |  |  |  |  |
|                           |                           |  |  |  |  |  |  |
| (                         | Save Cancel               |  |  |  |  |  |  |

#### Schritt 2

Konfigurieren Sie die Registerkarte Client. Wir verwenden nur die Standardeinstellungen.

| VPN Site Configuration         |                    |     |  |  |  |  |
|--------------------------------|--------------------|-----|--|--|--|--|
| General Client Name Resolution | 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                  |                    | 51  |  |  |  |  |
| 🛛 📝 Enable Dead Peer Detectio  | n                  |     |  |  |  |  |
| 🛛 📝 Enable ISAKMP Failure Noti | fications          |     |  |  |  |  |
| 🔽 Enable Client Login Banner   |                    |     |  |  |  |  |
|                                |                    |     |  |  |  |  |
| Save Cancel                    |                    |     |  |  |  |  |

#### Schritt 3

Aktivieren Sie auf der Registerkarte **Namensauflösung > DNS** das **Kontrollkästchen DNS aktivieren**, und lassen Sie die **Kontrollkästchen Automatisch beziehen** aktiviert.

| VPN Site Configuration  | X                         |
|-------------------------|---------------------------|
| General Client Name Res | colution Authentication P |
| DNS WINS                |                           |
| Enable DNS              | ✓ Obtain Automatically    |
| Server Address #1       |                           |
| Server Address #2       |                           |
| Server Address #3       |                           |
| Server Address #4       |                           |
| DNS Suffix              | Obtain Automatically      |
|                         |                           |
|                         | Save Cancel               |

Aktivieren Sie auf der Registerkarte Namensauflösung > WINS das Kontrollkästchen WINS aktivieren, und lassen Sie das Kontrollkästchen Automatisch beziehen aktiviert.

| VPN Site Configuration                        |      |
|---|------|
| General Client Name Resolution Authentication | P    |
| DNS WINS                                      | _    |
| Enable WINS     Obtain Automatically          |      |
| Server Address #1                             |      |
| Server Address #2                             |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
|   |      |
| Save Car                                      | ncel |

#### Schritt 5

Konfigurieren Sie die Registerkarte Authentifizierung > Lokale Identität:

Identifizierungstyp: Schlüsselkennung auswählen

Schlüssel-ID-Zeichenfolge: Geben Sie den Gruppennamen ein, der auf dem RV34x

#### konfiguriert wurde.

| General Client Name Resolution Authentication P   | PN Site Configuration                         |
|---|---|
| Authentication Method Mutual PSK + XAuth  Local Identity Remote Identity Credentials  Identification Type Key Identifier  Key ID String Clients | General Client Name Resolution Authentication |
| Local Identity Remote Identity Credentials  | Authentication Method Mutual PSK + XAuth      |
| Identification Type<br>Key Identifier<br>Key ID String<br>Clients   | Local Identity Remote Identity Credentials    |
| Key ID String<br>Clients  | Identification Type                           |
| Clients   | Key Identifier                                |
|   | Clients                                       |
|   |   |
|   |   |
|   |   |
|   |   |
| Serve Cancel  | Serie Cancel                                  |

#### Schritt 6

Im Register Authentifizierung > Remote Identity bleiben die Standardeinstellungen unverändert.

Identifizierungstyp: IP-Adresse

Adresszeichenfolge: <leer>

Verwenden Sie ein erkanntes Adressfeld des Remotehosts: Aktiviert

| PN Site Configuration                             |   |  |  |  |
|---|---|--|--|--|
| General Client Name Resolution Authentication P 4 | 1 |  |  |  |
| Authentication Method Mutual PSK + XAuth          |   |  |  |  |
| Local Identity Remote Identity Credentials        |   |  |  |  |
| Identification Type                               |   |  |  |  |
| IP Address 🔹                                      |   |  |  |  |
| Address String                                    |   |  |  |  |
| Use a discovered remote host address              |   |  |  |  |
| Save Cancel                                       | ן |  |  |  |

#### Schritt 7

Konfigurieren Sie auf der Registerkarte Authentifizierung > Anmeldeinformationen Folgendes:

Authentifizierungsmethode: Wählen Sie Mutual PSK + XAuth aus

Vorinstallierter Schlüssel: Geben Sie den im RV340-Clientprofil konfigurierten Preshared Key ein.

| VPN 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                                     |

#### Schritt 8

Für die Registerkarte Phase 1 bleiben die Standardeinstellungen unverändert:

Exchange-Typ: aggressiv

DH Exchange: Gruppe 2

Verschlüsselungsalgorithmus: Automatisch

Hash-Algorithmus: Automatisch

| Client                                  | Name Resolution   | Authentication Phase 1 P 1 |  |  |
|---|-------------------|----------------------------|--|--|
| Proposal Parameters                     |                   |                            |  |  |
| Exchange Type aggressive                |                   |                            |  |  |
| DH Exchange group 2 💌                   |                   |                            |  |  |
| Cipher Algorithm auto 🗸                 |                   |                            |  |  |
| Cipher Key Length 🗾 Bits                |                   |                            |  |  |
| Has                                     | sh Algorithm      | auto 💌                     |  |  |
| Key Life Time limit 86400 Secs          |                   |                            |  |  |
| Кеу                                     | / Life Data limit | 0 Kbytes                   |  |  |
| Enable Check Point Compatible Vendor ID |                   |                            |  |  |
|   |                   | Save Cancel                |  |  |

Außerdem werden die Standardwerte für die Registerkarte Phase 2 verwendet:

Transform Algorithm: Automatisch

HMAC-Algorithmus: Automatisch

PFS Exchange: Deaktiviert

Komprimierungsalgorithmus: Deaktiviert

| Proposal Parameters  |          |        |
|----------------------|----------|--------|
| Transform Algorithm  | auto     | •      |
| Transform Key Length | •        | Bits   |
| HMAC Algorithm       | auto     | •      |
| PFS Exchange         | disabled | •      |
| Compress Algorithm   | disabled | •      |
| Key Life Time limit  | 3600     | Secs   |
| Key Life Data limit  | 0        | Kbytes |
|                      |          |        |
|                      |          |        |

Für die Registerkarte Richtlinien verwenden wir die folgenden Einstellungen:

Ebene der Richtliniengenerierung: Automatisch

Beibehalten von permanenten Sicherheitszuordnungen: Aktiviert

Topologie automatisch abrufen oder Alle tunneln: Aktiviert

Da Split-Tunneling auf dem RV340 konfiguriert wurde, muss er hier nicht konfiguriert werden.

| /PN Site Configuration                      | X  |
|---|----|
| Authentication Phase 1 Phase 2 Policy       | •• |
| IPSEC Policy Configuration                  |    |
| Policy Generation Level auto                |    |
| Maintain Persistent Security Associations   |    |
| Obtain Topology Automatically or Tunnel All |    |
| Remote Network Resource                     |    |
|   |    |
|   |    |
|   |    |
|   |    |
|   |    |
| Add Modify Delete                           |    |
|   |    |
| Save Can                                    | el |
|   |    |

Klicken Sie abschließend auf Speichern.

#### Schritt 11

Jetzt können wir die Verbindung testen. Markieren Sie im *VPN Access Manager* das Verbindungsprofil, und klicken Sie auf die Schaltfläche **Connect**.

|   | (B) VPN Access Manager |          |          |          |             |  |
|---|------------------------|----------|----------|----------|-------------|--|
| ļ | File Edit              | View He  | р        |          |             |  |
|   | 8                      | •        | 2        | 9        |             |  |
|   | Connect                | Add N    | lodify D | elete    |             |  |
|   | Connectio              | n Name 🏒 | Host N   | ame      | Authenticat |  |
|   | 192.168                | .75.113  | 192.16   | 8.75.113 | mutual-psk  |  |

#### Schritt 12

Geben Sie im VPN Connect-Fenster, das angezeigt wird, den Benutzernamen und das Kennwort mit den Anmeldeinformationen für das Benutzerkonto ein, das wir auf dem RV340 erstellt haben (Schritte 13 und 14).

| VPN Connect   | t - 192.168.75.113        |      |
|---------------|---------------------------|------|
| Connect Netwo | rk                        |      |
| config loaded | for site '192.168.75.113' |      |
| Credentials   |                           |      |
| Username      | vpnuser                   |      |
| Password      | •••••                     |      |
|               |                           |      |
|               | Connect                   | Exit |

Wenn Sie fertig sind, klicken Sie auf Verbinden.

#### Schritt 13

Überprüfen Sie, ob der Tunnel angeschlossen ist. Der Tunnel sollte aktiviert sein.

| VPN Connect   | t - 192.168.75.113                                    |        | X       |
|---|---|--------|---------|
| Connect Netwo   | rk  |        |         |
| local id configu<br>remote id configu<br>pre-shared ke<br>bringing up tun<br>network device<br>tunnel enabled | ured<br>igured<br>y configured<br>nel<br>e configured |        | 4 III > |
| Credentials   |   |        |         |
| Username  | vpnuser   |        |         |
| Password  |   |        |         |
|   | Disconnect  | Cancel |         |

# Fazit

Sie sind nun für die VPN-Verbindung mit Ihrem Netzwerk eingerichtet.