

# Konfigurieren des Gruppen-Clients für das Gateway Virtual Private Network (VPN) auf den VPN-Routern der Serien RV320 und RV325

## Ziel

Ein Virtual Private Network (VPN) ist ein privates Netzwerk, das verwendet wird, um die Geräte des Remote-Benutzers virtuell über das öffentliche Netzwerk zu verbinden, um die Sicherheit zu gewährleisten. Eine der Arten von VPNs ist ein Client-to-Gateway-VPN. Mit dem Client-to-Gateway können Sie verschiedene Zweigstellen Ihres Unternehmens in verschiedenen geografischen Regionen per Fernzugriff verbinden, um die Daten sicherer zwischen den Gebieten zu übertragen und zu empfangen. Gruppen-VPN ermöglicht eine einfache Konfiguration des VPN, da die Konfiguration des VPNs für jeden Benutzer nicht mehr erforderlich ist. Die RV32x VPN Router-Serie unterstützt maximal zwei VPN-Gruppen.

In diesem Dokument wird erläutert, wie ein Gruppen-Client-zu-Gateway-VPN auf VPN-Routern der Serie RV32x konfiguriert wird.

## Anwendbare Geräte

- RV320 Dual-WAN VPN-Router
- RV325 Gigabit Dual-WAN VPN-Router

## Softwareversion

- v1.1.0.09

## Konfigurieren von Group Client zum Gateway-VPN

Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **VPN > Client to Gateway** aus. Die Seite *Client to Gateway* wird geöffnet:

## Client to Gateway

### Add a New Tunnel

Tunnel     Group VPN     Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

Enable:

### Local Group Setup

Local Security Gateway Type:

IP Only

IP Address:

0.0.0.0

Local Security Group Type:

Subnet

IP Address:

192.168.1.0

Subnet Mask:

255.255.255.0

### Remote Client Setup

Remote Security Gateway Type:

IP Only

IP Address

:

Schritt 2: Klicken Sie auf das Optionsfeld **Group VPN**, um ein Gruppen-Client-to-Gateway-VPN hinzuzufügen.

## Client to Gateway

### Add a New Group VPN

Tunnel

Group VPN

Easy VPN

Group No. 1

Tunnel Name:

Interface:

Keying Mode: IKE with Preshared key

Enable:

### Local Group Setup

Local Security Group Type:

IP Address:

Subnet Mask:

### Remote Client Setup

Remote Client:

Domain Name:

## Neuen Tunnel hinzufügen

Schritt 1: Geben Sie den Namen des Tunnels in das Feld *Tunnelname* ein.

### Client to Gateway

**Add a New Group VPN**

Tunnel     Group VPN     Easy VPN

Group No.    1

Tunnel Name:    tunnel\_1

Interface:    WAN1

Keying Mode:    IKE with Preshared key

Enable:   

---

**Local Group Setup**

Local Security Group Type:    Subnet

IP Address:    192.168.1.0

Subnet Mask:    255.255.255.0

---

**Remote Client Setup**

Remote Client:    DomainName(FQDN)

Domain Name:   

**Hinweis:** Gruppennummer: Stellt die Nummer der Gruppe dar. Es ist ein automatisch generiertes Feld.

Schritt 2: Wählen Sie aus der Dropdown-Liste *Schnittstelle* die entsprechende Schnittstelle aus, über die die VPN-Gruppe eine Verbindung mit dem Gateway herstellt.

## Client to Gateway

### Add a New Group VPN

Tunnel  Group VPN  Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1  
WAN1  
WAN2  
USB1  
USB2

Keying Mode:

Enable:

### Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

### Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

Schritt 3: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um das Gateway-to-Gateway-VPN zu aktivieren. Standardmäßig ist sie aktiviert.

### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

---

**Remote Client Setup**

Remote Client: DomainName(FQDN)

Domain Name:

**Hinweis:** Keying Mode (Aktivierungsmodus): Zeigt den verwendeten Authentifizierungsmodus an. IKE mit dem vorinstallierten Schlüssel ist die einzige Option, d. h. das IKE-Protokoll (Internet Key Exchange) wird verwendet, um automatisch einen vorinstallierten Schlüssel zu generieren und auszutauschen, um eine authentifizierte Kommunikation für den Tunnel herzustellen.

Schritt 4: Um die bisher vorhandenen Einstellungen zu speichern und den Rest als Standard beizubehalten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## Lokale Gruppeneinrichtung

Schritt 1: Wählen Sie aus der Dropdown-Liste *Local Security Group Type* (Typ der lokalen Sicherheitsgruppe) den entsprechenden lokalen LAN-Benutzer oder eine Benutzergruppe aus, die auf den VPN-Tunnel zugreifen kann. Der Standardwert ist "Subnet".

### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No.

Tunnel Name:

Interface:

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type:

IP Address:

Subnet Mask:

---

**Remote Client Setup**

Remote Client:

Domain Name:

Die verfügbaren Optionen sind wie folgt definiert:

- IP - Nur ein bestimmtes LAN-Gerät kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse des LAN-Geräts in das Feld *IP-Adresse* ein. Die Standard-IP-Adresse lautet 192.168.1.0.
- Subnetz - Alle LAN-Geräte in einem bestimmten Subnetz können auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die IP-Adresse und die Subnetzmaske der LAN-Geräte in das Feld *IP-Adresse* und *Subnetzmaske* ein. Die Standardmaske ist 255.255.255.0.
- IP Range (IP-Bereich): Eine Reihe von LAN-Geräten kann auf den Tunnel zugreifen. Wenn Sie diese Option wählen, geben Sie die erste und letzte IP-Adresse für den Bereich in den Feldern *Start IP* und *End IP (IP-Startadresse)* ein. Der Standardbereich liegt zwischen 192.168.1.0 und 192.168.1.254.

Schritt 2: Um die bisher vorgenommenen Einstellungen zu speichern und den Rest als Standard beizubehalten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## Remote-Client-Setup

Schritt 1: Wählen Sie den entsprechenden Remote-LAN-Benutzer oder die Benutzergruppe aus, die über die Dropdown-Liste *Remote Security Group Type (Typ der Remote-Sicherheitsgruppe)* auf den VPN-Tunnel zugreifen kann.

### Client to Gateway

**Add a New Group VPN**

Tunnel   
 Group VPN   
 Easy VPN

Group No. 1

Tunnel Name: tunnel\_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

---

**Local Group Setup**

Local Security Group Type: IP

IP Address: 192.168.3.0

---

**Remote Client Setup**

Remote Client: 
DomainName(FQDN)
  
DomainName(FQDN)
  
Email Address(USER FQDN)
  
Microsoft XP/2000 VPN Client

Domain Name:

Die verfügbaren Optionen sind wie folgt definiert:

- Domain Name (FQDN)-Authentifizierung - Der Zugriff auf den Tunnel ist über eine registrierte Domäne möglich. Wenn Sie diese Option wählen, geben Sie den Namen der registrierten Domäne in das Feld *Domänenname ein*.
- E-Mail-Adresse (USER FQDN) Authentifizierung - Der Zugang zum Tunnel ist über eine E-Mail-Adresse möglich. Wenn Sie diese Option wählen, geben Sie die E-Mail-Adresse in das Feld *E-Mail-Adresse ein*.
- Microsoft XP/2000 VPN Client - Der Zugriff auf den Tunnel ist über eine Client-Software möglich, die eine integrierte Microsoft XP- oder 2000 VPN Client-Software ist.

Schritt 2: Um die bisher vorgenommenen Einstellungen zu speichern und den Rest als Standard beizubehalten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## IPSec-Einrichtung

Schritt 1: Wählen Sie in der Dropdown-Liste *DH Group (Phase 1 DH Group)* die entsprechende Diffie-Hellman (DH)-Gruppe aus. Phase 1 dient zum Aufbau der Simplex, Logical Security Association (SA) zwischen den beiden Enden des Tunnels, um eine sichere authentifizierte Kommunikation zu unterstützen. Diffie-Hellman ist ein kryptografisches Schlüsselaustauschprotokoll, das in Phase 1 der Verbindung verwendet wird, um einen geheimen Schlüssel zur Authentifizierung der Kommunikation freizugeben.



**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- Group1 (768-Bit) - Berechnet den Schlüssel am schnellsten, aber am wenigsten sicher.
- Group2 (1024-Bit) - Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Group5 (1536-Bit) - Berechnet den Schlüssel am langsamsten, ist aber am sichersten.

Schritt 2: Wählen Sie in der Dropdown-Liste *Verschlüsselung der Phase 1* die geeignete Verschlüsselungsmethode zur Verschlüsselung des Schlüssels aus. AES-128 wird für hohe Sicherheit und schnelle Leistung empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption : 

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die zwar keine sehr sichere Verschlüsselungsmethode ist, aber für die Abwärtskompatibilität erforderlich sein kann.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüsselgröße, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller und sicherer als 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128 und schneller, aber weniger sicher als AES-256.
- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 3: Wählen Sie die entsprechende Authentifizierungsmethode aus der Dropdown-Liste *Phase 1 Authentication (Authentifizierung Phase 1)* aus. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication: 

- MD5
- MD5
- SHA1

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- MD5 — Message Digest Algorithm-5 (MD5) stellt eine 128-Bit-Hash-Funktion dar, die die Daten durch die Prüfsummenberechnung vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Schritt 4: Geben Sie im Feld *Phase 1 SA Life Time* (SA-Lebensdauer *Phase 1*) die Zeitdauer in Sekunden ein, die der VPN-Tunnel in Phase 1 aktiv bleibt. Die Standardzeit ist 28.800 Sekunden.

**Remote Client Setup**

Remote Client:

---

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Schritt 5: (Optional) Um den Schlüssel besser zu schützen, aktivieren Sie das Kontrollkästchen **Perfect Forward Secrecy (Perfect Forward-Geheimhaltungsgrad perfekt umleiten)**. Mit dieser Option können Sie einen neuen Schlüssel generieren, wenn ein Schlüssel beschädigt ist. Dies ist eine empfohlene Maßnahme, da sie mehr Sicherheit bietet.

**Hinweis:** Wenn Sie in Schritt 5 die Option **Perfect Forward Secrecy (Perfekte Weiterleitungsgeheimnis)** deaktivieren, müssen Sie die DH-Gruppe für Phase 2 nicht konfigurieren.

Schritt 6: Wählen Sie die entsprechende DH-Gruppe aus der Dropdown-Liste *Phase 2 DH Group* aus.

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- Group1 (768-Bit) - Berechnet den Schlüssel am schnellsten, aber am wenigsten sicher.
- Group2 (1024-Bit) - Berechnet den Schlüssel langsamer, ist aber sicherer als Group1.
- Group5 (1536-Bit) - Berechnet den Schlüssel am langsamsten, ist aber am sichersten.

Schritt 2: Wählen Sie in der Dropdown-Liste *Verschlüsselung* der *Phase 1* die geeignete Verschlüsselungsmethode zur Verschlüsselung des Schlüssels aus. AES-128 wird für hohe Sicherheit und schnelle Leistung empfohlen. Der VPN-Tunnel muss für beide Enden dieselbe Verschlüsselungsmethode verwenden.

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption: 

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- DES - Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode, die zwar keine sehr sichere Verschlüsselungsmethode ist, aber für die Abwärtskompatibilität erforderlich sein kann.
- 3DES - Triple Data Encryption Standard (3DES) ist eine einfache 168-Bit-Verschlüsselungsmethode zur Erhöhung der Schlüsselgröße, da sie die Daten dreimal verschlüsselt. Dies bietet mehr Sicherheit als DES, aber weniger Sicherheit als AES.
- AES-128 - Advanced Encryption Standard mit 128-Bit-Schlüssel (AES-128) verwendet einen 128-Bit-Schlüssel für AES-Verschlüsselung. AES ist schneller und sicherer als DES. Im Allgemeinen ist AES auch schneller und sicherer als 3DES. AES-128 ist schneller, aber weniger sicher als AES-192 und AES-256.
- AES-192 - AES-192 verwendet einen 192-Bit-Schlüssel für die AES-Verschlüsselung. AES-192 ist langsamer, aber sicherer als AES-128 und schneller, aber weniger sicher als AES-256.
- AES-256 - AES-256 verwendet einen 256-Bit-Schlüssel für die AES-Verschlüsselung. AES-256 ist langsamer, aber sicherer als AES-128 und AES-192.

Schritt 8: Wählen Sie die entsprechende Authentifizierungsmethode aus der Dropdown-Liste *Phase-2-Authentifizierung* aus. Der VPN-Tunnel muss für beide Enden dieselbe Authentifizierungsmethode verwenden.

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Die verfügbaren Optionen sind wie folgt definiert:

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 128-Bit-Hash-Funktion dar, die die Daten durch die Berechnung der Prüfsumme vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Schritt 9: Geben Sie im Feld *Phase 2 SA Lifetime (SA-Lebensdauer)* die Zeitdauer in Sekunden ein, die der VPN-Tunnel in Phase 2 aktiv bleibt. Die Standardzeit ist 3600 Sekunden.

**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter: 

Schritt 10: (Optional) Wenn Sie die Kraftanzeige für den vorinstallierten Schlüssel aktivieren möchten, aktivieren Sie das Kontrollkästchen **Minimale Komplexität des vorinstallierten Schlüssels**.

**Hinweis:** Wenn Sie das Kontrollkästchen **Minimale Komplexität des vorinstallierten Schlüssels** aktivieren, wird im *Preshared Key Strength Meter* die Stärke des vorinstallierten Schlüssels durch farbige Balken angezeigt. Rot zeigt eine schwache Stärke, Gelb ist eine akzeptable Stärke, Grün zeigt eine starke Stärke an.

Schritt 11: Geben Sie den gewünschten Schlüssel in das Feld *Vorinstallierter Schlüssel ein*. Bis zu 30 Hexadezimalstellen können als vorinstallierter Schlüssel verwendet werden. Der VPN-Tunnel muss für beide Enden denselben vorinstallierten Schlüssel verwenden.

**Hinweis:** Es wird dringend empfohlen, den vorinstallierten Schlüssel zwischen den IKE-Peers häufig zu ändern, damit das VPN gesichert bleibt.

Schritt 12: Um die bisher vorgenommenen Einstellungen zu speichern und den Rest als Standard beizubehalten, scrollen Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

## Erweiterte Einrichtung

Schritt 1: Klicken Sie auf **Erweitert**, um die erweiterten Einstellungen zu konfigurieren.



**IPSec Setup**

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime:  sec ( Range: 120-86400, Default: 28800 )

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter:

**Advanced +**

Der Bereich *Erweitert* wird angezeigt, und es sind neue Felder verfügbar.

Phase 2 Authentication:

Phase 2 SA Lifetime:  sec ( Range: 120-28800, Default: 3600 )

Minimum Preshared Key Complexity:  Enable

Preshared Key:

Preshared Key Strength Meter:

**Advanced -**

**Advanced**

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

Schritt 2: (Optional) Aktivieren Sie das Kontrollkästchen **Aggressive Mode** (Aggressiver Modus), wenn die Netzwerkgeschwindigkeit niedrig ist. Aggressive Mode (Aggressiver Modus) tauscht die IDs der Endpunkte des Tunnels während der SA-Verbindung in Klartext

aus, was weniger Zeit für den Austausch erfordert, aber weniger sicher ist.

Schritt 3: (Optional) Aktivieren Sie das Kontrollkästchen **Compress (Support IP Payload Compression Protocol (IPComp))**, wenn Sie die Größe von IP-Datagrammen komprimieren möchten. IPComp ist ein IP-Komprimierungsprotokoll, das verwendet wird, um die Größe von IP-Datagrammen zu komprimieren, wenn die Netzwerkgeschwindigkeit niedrig ist und der Benutzer die Daten ohne Verlust schnell übertragen möchte.

Schritt 4: (Optional) Aktivieren Sie das Kontrollkästchen **Keep-Alive**, wenn die Verbindung des VPN-Tunnels immer aktiv bleiben soll. Keep-Alive hilft, die Verbindungen sofort wieder herzustellen, wenn eine Verbindung inaktiv wird.

Schritt 5: (Optional) Aktivieren Sie das Kontrollkästchen **AH Hash Algorithm (AH Hash-Algorithmus)**, wenn die Authentifizierung auf der Datenursache erfolgen soll, die Datenintegrität durch Prüfsumme erreicht werden soll und der Schutz auf den IP-Header ausgedehnt werden soll. Wählen Sie dann die entsprechende Authentifizierungsmethode aus der Dropdown-Liste aus. Der Tunnel sollte für beide Seiten denselben Algorithmus haben.

Die verfügbaren Optionen sind wie folgt definiert:

- MD5 - Message Digest Algorithm-5 (MD5) stellt eine 128-Bit-Hash-Funktion dar, die die Daten durch die Berechnung der Prüfsumme vor böswilligen Angriffen schützt.
- SHA1 - Secure Hash Algorithm Version 1 (SHA1) ist eine 160-Bit-Hash-Funktion, die sicherer ist als MD5.

Schritt 6: Aktivieren Sie das Kontrollkästchen **NetBIOS-Broadcast**, wenn nicht routbarer Datenverkehr durch den VPN-Tunnel zugelassen werden soll. Die Standardeinstellung ist deaktiviert. NetBIOS wird verwendet, um Netzwerkressourcen wie Drucker, Computer usw. im Netzwerk mithilfe von Softwareanwendungen und Windows-Funktionen wie Network Neighborhood (Netzwerkumgebung) zu erkennen.

Schritt 7: (Optional) Aktivieren Sie das Kontrollkästchen **NAT Traversal**, wenn Sie über eine öffentliche IP-Adresse aus Ihrem privaten LAN auf das Internet zugreifen möchten. NAT-Traversal wird verwendet, um die privaten IP-Adressen von internen Systemen als öffentliche IP-Adressen darzustellen, um die privaten IP-Adressen vor böswilligen Angriffen oder Entdeckungen zu schützen.

Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.