Konfigurieren von Gruppenrichtlinien auf dem Router der Serie RV34x

Ziel

Eine Gruppenrichtlinie ist ein Satz benutzerorientierter Attribut- oder Wertpaare für IPSec-Verbindungen (Internet Protocol Security), die entweder intern (lokal) auf dem Gerät oder extern auf einem RADIUS (Remote Authentication Dial-In User Service)- oder LDAP-Server (Lightweight Directory Access Protocol) gespeichert werden. Eine Tunnelgruppe verwendet eine Gruppenrichtlinie, die Begriffe für VPN-Benutzerverbindungen (Virtual Private Network) festlegt, nachdem der Tunnel erstellt wurde.

Mit Gruppenrichtlinien können Sie ganze Attributsätze auf einen Benutzer oder eine Benutzergruppe anwenden, anstatt jedes Attribut einzeln für jeden Benutzer angeben zu müssen. Sie können auch die Gruppenrichtlinienattribute für einen bestimmten Benutzer ändern.

In diesem Dokument wird erläutert, wie Sie Gruppenrichtlinien für die RV34x VPN Router-Serie konfigurieren.

Anwendbare Geräte

- Serie RV34x

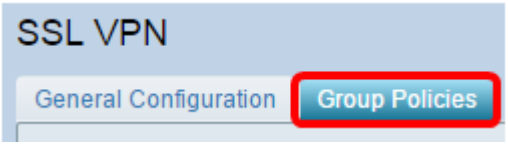
Softwareversion

- 1,0/01,16

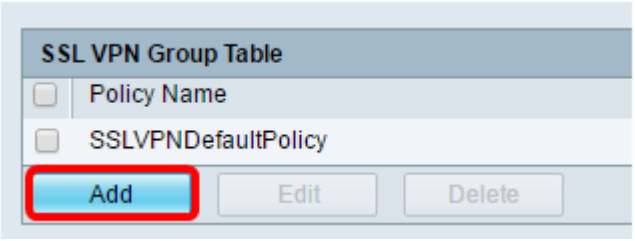
Gruppenrichtlinien konfigurieren

Schritt 1: Melden Sie sich beim webbasierten Router-Dienstprogramm an, und wählen Sie **VPN > SSL VPN aus**.

Schritt 2: Klicken Sie im Bereich SSL VPN auf die Registerkarte **Gruppenrichtlinien**.

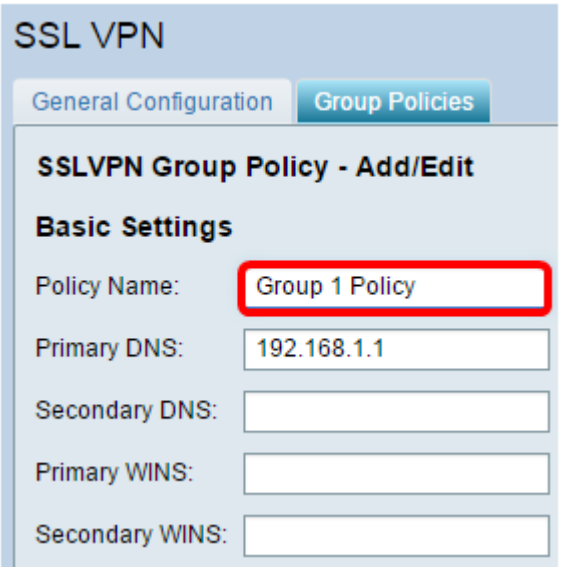


Schritt 3: Klicken Sie auf die Schaltfläche **Hinzufügen** unter der Tabelle für SSL VPN-Gruppen, um eine Gruppenrichtlinie hinzuzufügen.



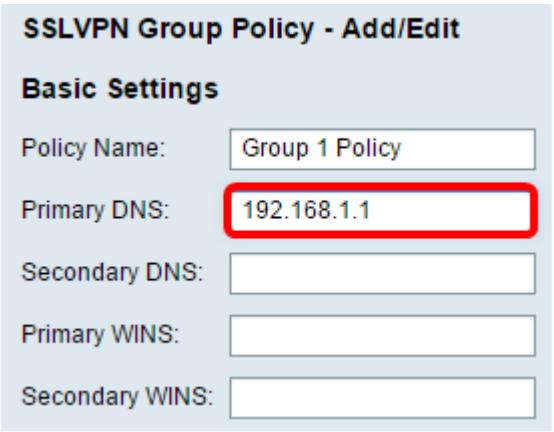
Hinweis: Die Tabelle der SSL VPN-Gruppen zeigt die Liste der Gruppenrichtlinien auf dem Gerät. Sie können auch die erste Gruppenrichtlinie in der Liste bearbeiten, die SSLVPNDefaultPolicy heißt. Dies ist die vom Gerät bereitgestellte Standardrichtlinie.

Schritt 4: Geben Sie den bevorzugten Richtliniennamen in das Feld *Policy Name (Richtlinienname*) ein.



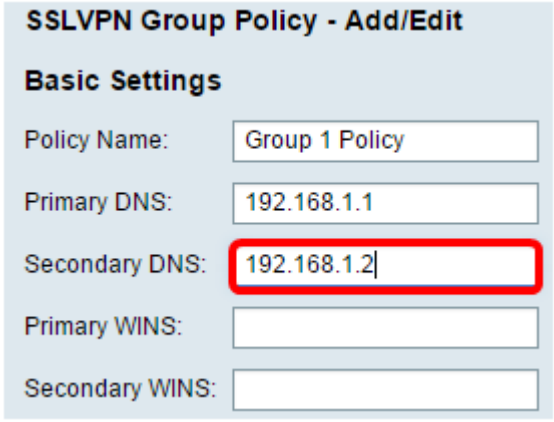
Hinweis: In diesem Beispiel wird die Richtlinie für Gruppe 1 verwendet.

Schritt 5: Geben Sie die IP-Adresse des primären DNS in das angegebene Feld ein. Standardmäßig wird diese IP-Adresse bereits angegeben.



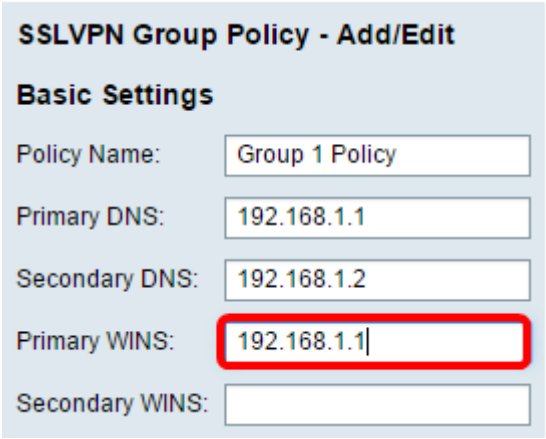
Hinweis: In diesem Beispiel wird 192.168.1.1 verwendet.

Schritt 6: (Optional) Geben Sie die IP-Adresse des sekundären DNS in das angegebene Feld ein. Dies dient als Backup für den Fall, dass der primäre DNS ausfällt.



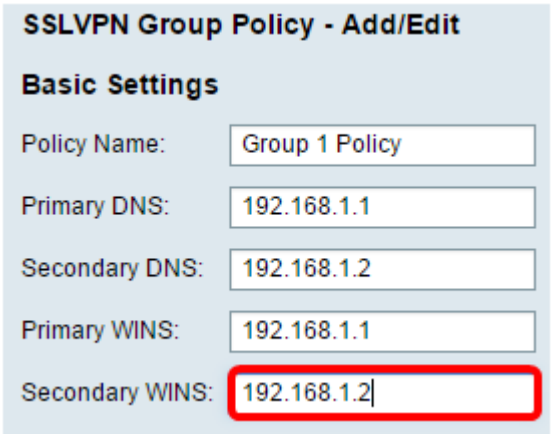
Hinweis: In diesem Beispiel wird 192.168.1.2 verwendet.

Schritt 7: (Optional) Geben Sie in das Feld die IP-Adresse des primären WINS ein.



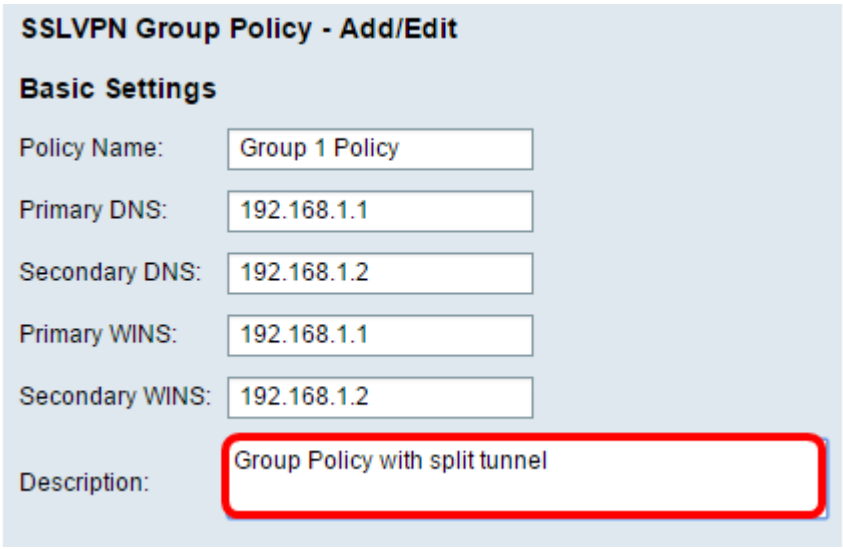
Hinweis: In diesem Beispiel wird 192.168.1.1 verwendet.

Schritt 8: (Optional) Geben Sie die IP-Adresse des sekundären WINS in das angegebene Feld ein.



Hinweis: In diesem Beispiel wird 192.168.1.2 verwendet.

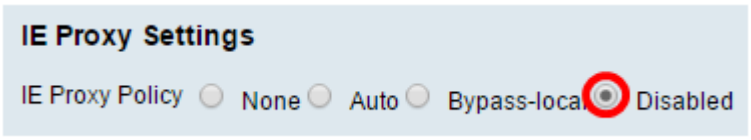
Schritt 9: (Optional) Geben Sie im Feld *Beschreibung* eine Beschreibung der Richtlinie ein.



Hinweis: In diesem Beispiel wird Gruppenrichtlinie mit Split-Tunnel verwendet.

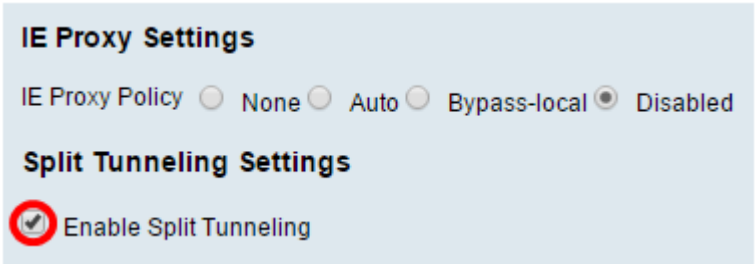
Schritt 10: (Optional) Klicken Sie auf ein Optionsfeld, um die IE-Proxy-Richtlinie auszuwählen, um die Microsoft Internet Explorer (MSIE)-Proxyeinstellungen zum Einrichten des VPN-Tunnels zu aktivieren. Folgende Optionen stehen zur Verfügung:

- None (Keine): Der Browser kann keine Proxy-Einstellungen verwenden.
- Auto (Automatisch): Ermöglicht dem Browser, die Proxy-Einstellungen automatisch zu erkennen.
- Bypass-local (Lokal umgehen): Ermöglicht dem Browser, die Proxyeinstellungen zu umgehen, die auf dem Remote-Benutzer konfiguriert sind.
- Disabled (Deaktiviert): Deaktiviert die MSIE-Proxyeinstellungen.

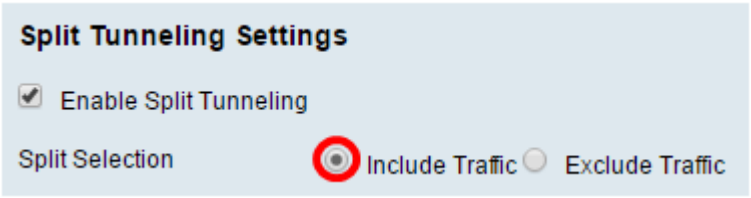


Hinweis: In diesem Beispiel wird Disabled (Deaktiviert) ausgewählt. Dies ist die Standardeinstellung.

Schritt 11: (Optional) Aktivieren Sie im Bereich Getrennte Tunneling-Einstellungen das Kontrollkästchen **Enable Split Tunneling**, um das unverschlüsselte Senden von Internetdatenverkehr an das Internet zuzulassen. Full Tunneling sendet den gesamten Datenverkehr an das Endgerät, wo er dann an die Ziel-Ressourcen weitergeleitet wird, sodass das Unternehmensnetzwerk nicht mehr über den Pfad für den Internetzugriff verfügt.

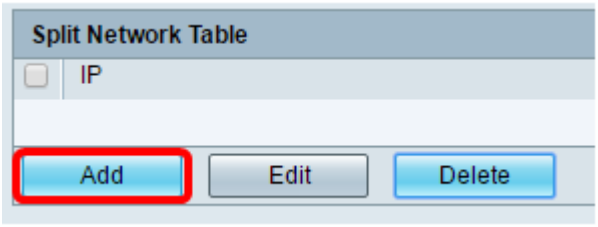


Schritt 12: (Optional) Klicken Sie auf eine Optionsschaltfläche, um festzulegen, ob beim Anwenden des Split-Tunneling Verkehr einbezogen oder ausgeschlossen werden soll.

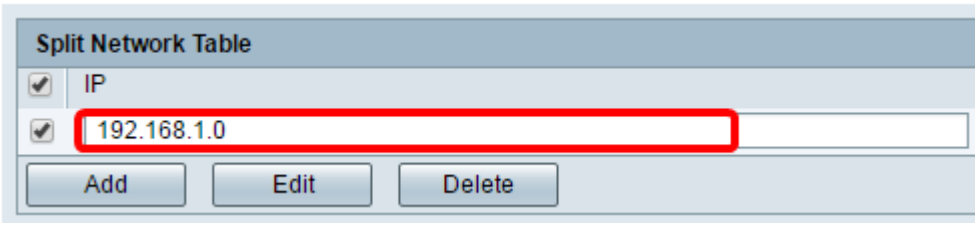


Hinweis: In diesem Beispiel wird Datenverkehr einschließen ausgewählt.

Schritt 13: Klicken Sie in der Tabelle Split Network (Netzwerk teilen) auf die Schaltfläche **Add** (Hinzufügen), um eine geteilte Netzwerkausnahme hinzuzufügen.

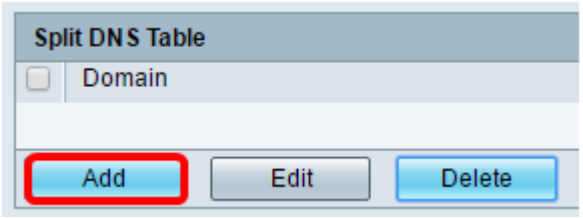


Schritt 14: Geben Sie die IP-Adresse des Netzwerks in das angegebene Feld ein.

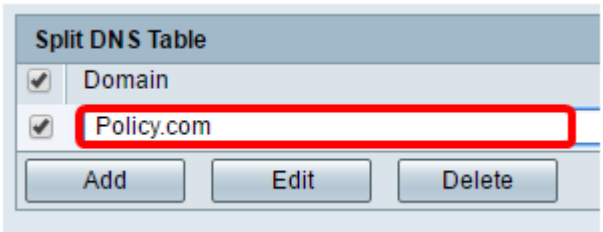


Hinweis: In diesem Beispiel wird 192.168.1.0 verwendet.

Schritt 15: Klicken Sie in der Split DNS Table (DNS-Tabelle aufteilen) auf die Schaltfläche **Hinzufügen**, um eine geteilte DNS-Ausnahme hinzuzufügen.

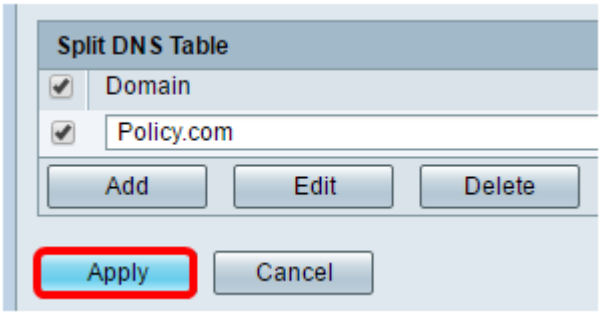


Schritt 16: Geben Sie den Domänennamen in das angegebene Feld ein.

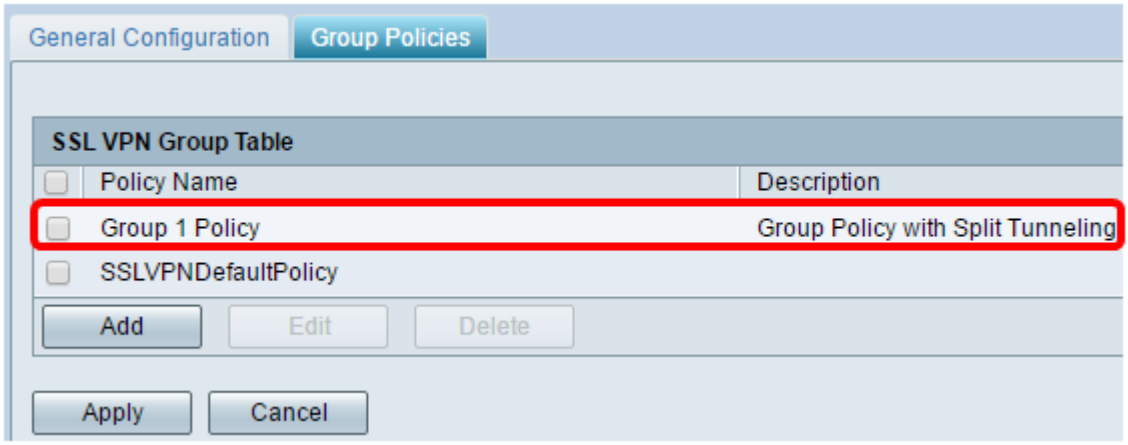


Hinweis: In diesem Beispiel wird Policy.com verwendet.

Schritt 17: Klicken Sie auf **Übernehmen**.



Nachdem die Einstellungen erfolgreich gespeichert wurden, werden Sie zur Tabelle für SSL VPN-Gruppen umgeleitet, in der die neu hinzugefügte Gruppenrichtlinie angezeigt wird.



Sie sollten nun erfolgreich Gruppenrichtlinien auf dem Router der Serie RV34x konfiguriert haben.

Wenn Sie den Easy Setup Guide für den RV340 anzeigen möchten. Klicken Sie hier.

Wenn Sie den Administrationsleitfaden für den RV340 anzeigen möchten. Klicken Sie hier. Informationen zu Gruppenrichtlinien finden Sie auf Seite 93.