Konfiguration der Zugriffskontrolle auf dem RV315W VPN-Router

Ziel

Die Zugriffskontrollkonfiguration ermöglicht die Einschränkung des Zugriffs auf eine bestimmte IP-Adresse. Es gibt verschiedene Optionen, um die Einschränkungen anzupassen. Tageszeit, Wochentage, IP-Adressen, physischer Port und Protokolltyp sind Beispiele für Anpassungsfunktionen für die Zugriffskontrollrichtlinie.

Dieser Artikel erläutert die Verwendung und Konfiguration der Zugriffskontrollen auf dem RV315W VPN-Router.

Anwendbares Gerät

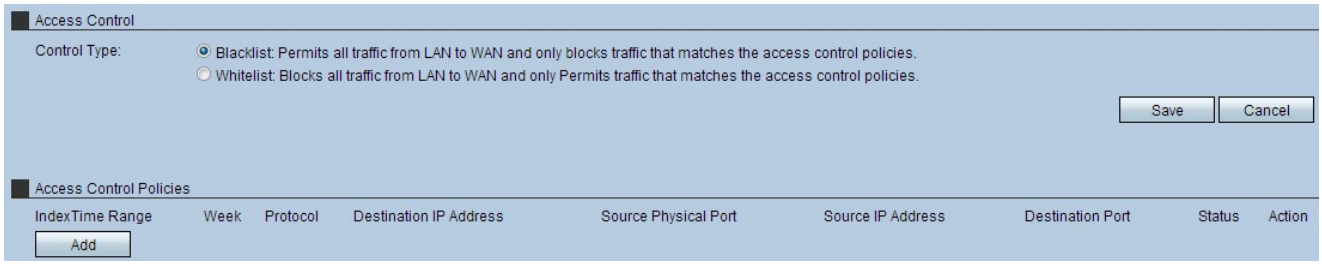
RV315W

Softwareversion

·1.01.03

Konfigurationsmanagement

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Sicherheit > Zugriffskontrolle aus**. Die Seite *Zugriffskontrolle* wird geöffnet:



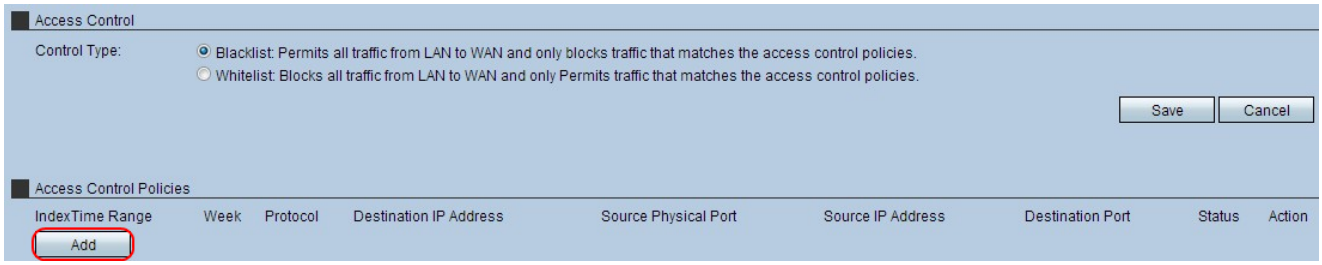
Schritt 2: Klicken Sie im Feld Systemsteuerungstyp entweder auf die Optionsschaltfläche Sperrliste oder Liste zulassen.

·Sperrliste - Diese Option lässt den gesamten Datenverkehr vom LAN zum WAN zu, mit Ausnahme des Datenverkehrs, der durch die Zugriffskontrolleinstellungen blockiert wird.

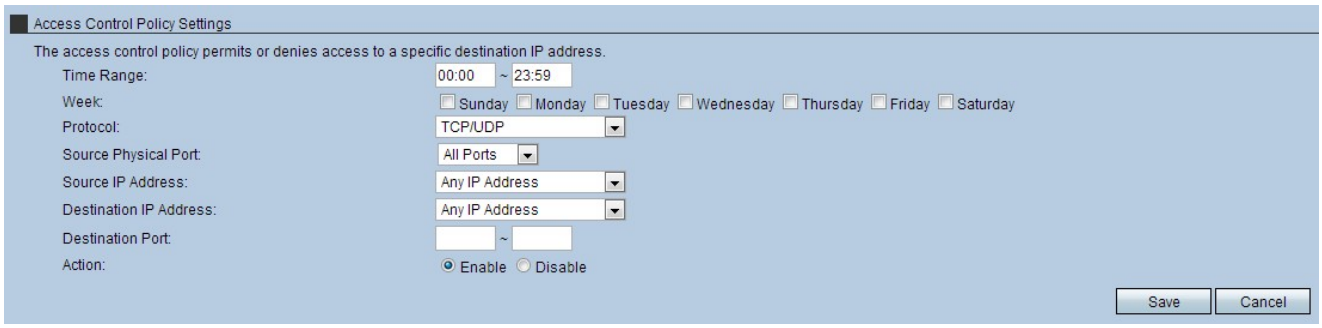
·Liste zulassen - Diese Option blockiert den gesamten Datenverkehr vom LAN zum WAN, mit Ausnahme des Datenverkehrs, der durch die Zugriffskontrolleinstellungen zugelassen ist.

Weitere Informationen finden Sie im Glossar.

Schritt 3: Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.



Schritt 4: Klicken Sie auf **Hinzufügen**, um eine neue Zugriffskontrollrichtlinie hinzuzufügen. Die Seite *Zugriffskontrollrichtlinieneinstellungen* wird geöffnet:



Schritt 5: Geben Sie im Feld "Time Range" einen Bereich ein. Diese Option ist die Zeit, zu der die Zugriffskontrollrichtlinie wirksam ist.

Schritt 6: Wählen Sie Wochentage aus, um den Zugriff zuzulassen oder zu beschränken. Diese Option ist der Wochentag, an dem die Zugriffskontrollrichtlinie wirksam ist.

Schritt 7: Wählen Sie aus der Dropdown-Liste Protocol (Protokoll) das Protokoll aus, für das die Zugriffskontrolle gilt.

·TCP - Dieses Protokoll wird verwendet, um Daten von einer Anwendung an das Netzwerk zu übertragen. TCP wird in der Regel für Anwendungen verwendet, bei denen die Datenübertragung abgeschlossen und Pakete nicht verworfen werden müssen.

·UDP - Dieses Protokoll ist für Client-/Server-Netzwerkanwendungen bestimmt, die auf dem Internetprotokoll (IP) basieren. Der Hauptzweck dieses Protokolls ist die Verwendung von Live-Anwendungen. (VOIP, Spiele usw.)

·TCP/UDP - Wählen Sie dieses Protokoll aus, um TCP und UDP zu verwenden. Dies ist das Standardprotokoll.

·ICMP - Dieses Protokoll sendet Fehlermeldungen und ist für die Fehlerbehandlung im Netzwerk verantwortlich. Verwenden Sie dieses Protokoll, um eine Benachrichtigung zu erhalten, wenn im Netzwerk Probleme mit der Paketübermittlung auftreten.

·HTTP - Dieses Protokoll ermöglicht die sichere Kommunikation zwischen einem Webserver und einem Browser. Verwenden Sie dieses Protokoll, wenn Pakete sicher zwischen Server und Browser übertragen werden müssen.

·FTP - Dieses Protokoll überträgt die Dateien zwischen Computern. Wählen Sie dieses Protokoll aus, wenn Dateien zwischen mehreren Geräten ausgetauscht werden.

·SMTP - Dieses Protokoll behandelt die Übertragung von E-Mails. Wählen Sie dieses Protokoll beim Austausch von E-Mails aus.

·POP3 — Dieses Protokoll wird mit SMTP in Bezug auf E-Mails kombiniert. POP3 lädt E-

Mails von einem E-Mail-Server auf einen PC herunter. Wählen Sie dieses Protokoll beim Herunterladen von E-Mails aus.

Schritt 8: Wählen Sie in der Dropdown-Liste Source Physical Port (Physischer Quellport) den Port aus, für den die Zugriffskontrolle gilt.

Schritt 9: Wählen Sie in der Dropdown-Liste Source IP Address (Quell-IP-Adresse) die IP-Adresse(n) aus, auf die die Zugriffskontrolle angewendet wird(en).

·Beliebige IP-Adresse: Wählen Sie diese Option, um alle IP-Adressen zuzulassen oder zu verweigern. Wählen Sie das Optionsfeld Aktivieren oder Deaktivieren für diese Option aus.

·Single IP Address (Eine IP-Adresse): Wählen Sie diese Option, um einzelne IP-Adressen zuzulassen oder zu verweigern. Geben Sie die entsprechende IP-Adresse in das Feld Quell-IP-Adresse ein.

·IP Address Range (IP-Adressbereich): Wählen Sie diese Option, um IP-Adressen basierend auf einem ausgewählten Bereich zuzulassen oder zu verweigern. Geben Sie den entsprechenden IP-Adressbereich im ersten und zweiten Feld Quell-IP-Adresse ein.

Schritt 10: Wählen Sie in der Dropdown-Liste Destination IP Address (Ziel-IP-Adresse) die IP-Adresse(n) aus, für die die Zugriffskontrolle gilt.

·Beliebige IP-Adresse: Wählen Sie diese Option, um alle IP-Adressen zuzulassen oder zu verweigern. Klicken Sie für diese Option auf das Optionsfeld Aktivieren oder Deaktivieren.

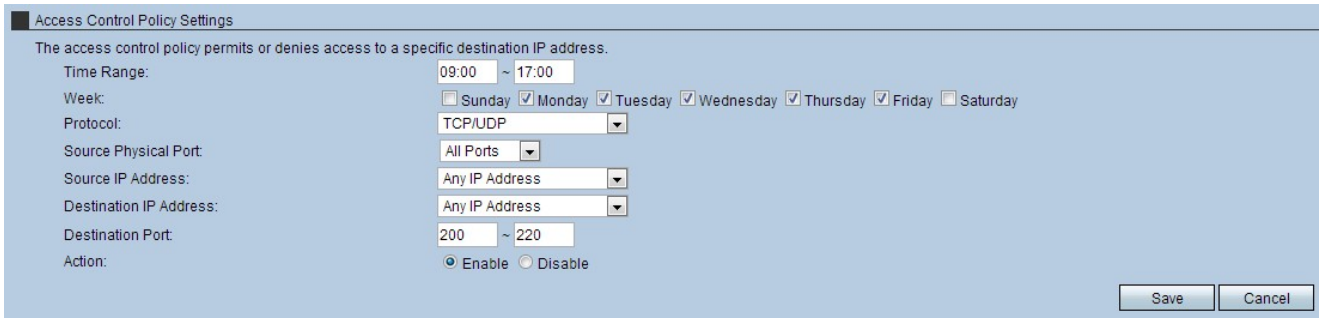
·Eine einzelne IP-Adresse - Wählen Sie diese Option, um eine einzelne IP-Adresse zuzulassen oder zu verweigern. Geben Sie die entsprechende IP-Adresse im Feld Ziel-IP-Adresse ein.

·IP Address Range (IP-Adressbereich): Wählen Sie diese Option, um IP-Adressen basierend auf einem ausgewählten Bereich zuzulassen oder zu verweigern. Geben Sie im ersten und zweiten Feld "Ziel-IP-Adresse" den entsprechenden IP-Adressbereich ein.

Schritt 11: Geben Sie in den Feldern Ziel-Port den Port-Bereich eines Protokolls oder einer Anwendung ein, auf das bzw. die die Zugriffskontrolle angewendet wird.

Schritt 12: Klicken Sie auf das Optionsfeld **Aktivieren**, um die Zugriffskontrollrichtlinie zu aktivieren.

Schritt 13: Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.



Schritt 14: (Optional) Um eine Zugriffskontrollrichtlinie zu löschen, klicken Sie unter der Überschrift Aktion auf das Abfalleimer-Symbol.

Schritt 15: (Optional) Um eine Zugriffskontrollrichtlinie zu bearbeiten, klicken Sie unter der

Überschrift Aktion auf das Umschlagsymbol.