Grundlegende Konfiguration der Firewall-Einstellungen auf dem RV215W

Ziel

Eine Firewall ist ein Funktionssatz, der die Sicherheit des Netzwerks gewährleistet. Ein Router gilt als starke Hardware-Firewall. Dies liegt daran, dass Router den gesamten eingehenden Datenverkehr überprüfen und unerwünschte Pakete verwerfen können.

In diesem Artikel wird erläutert, wie Sie die grundlegenden Firewall-Einstellungen auf der RV215W konfigurieren.

Anwendbare Geräte

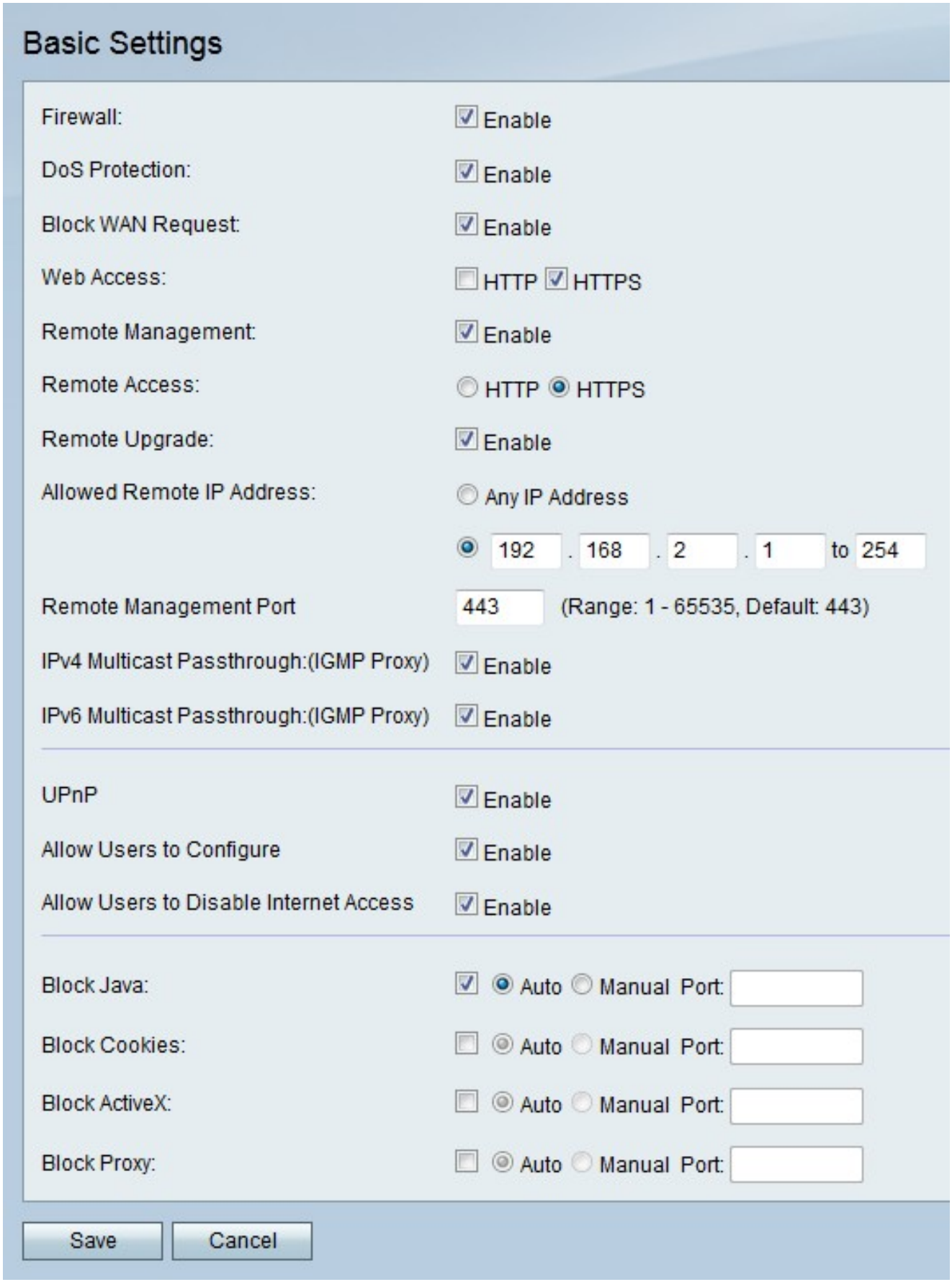
RV215W

Softwareversion

·1.1.0.5

Grundlegende Einstellungen

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Basic Settings (Firewall > Grundeinstellungen)**. Die Seite *Grundeinstellungen* wird geöffnet:



Schritt 2: Aktivieren Sie im Feld "Firewall" die **Option Aktivieren**, um die Firewall-Konfiguration auf dem RV215W zu aktivieren.

Schritt 3: Aktivieren Sie im Feld "DoS-Schutz" die Option "**Aktivieren**", um den DoS-Schutz (Denial of Service) auf dem RV215W zu aktivieren. Der DoS-Schutz dient dazu, ein Netzwerk vor DDoS-Angriffen (Distributed Denial of Service) zu schützen. DDoS-Angriffe

sollen ein Netzwerk so weit überfluten, dass die Ressourcen des Netzwerks nicht mehr verfügbar sind. Der RV215W nutzt den DoS-Schutz, um das Netzwerk durch die Beschränkung und Entfernung unerwünschter Pakete zu schützen.

Schritt 4: Aktivieren Sie **Aktivieren** im Feld "Block WAN Request" (WAN-Anfrage blockieren), um alle Ping-Anfragen an den RV215W vom WAN zu blockieren.

Schritt 5: Aktivieren Sie das Kontrollkästchen für den gewünschten Web-Zugriffstyp, der für die Verbindung mit der Firewall im Feld Web Access (Webzugriff) verwendet werden kann.

Schritt 6: Aktivieren Sie **Aktivieren** im Feld Remote Management (Remote-Verwaltung). Die Remote-Verwaltung ermöglicht den Zugriff auf den RV215W über ein Remote-WAN-Netzwerk.

Schritt 7: Klicken Sie auf das Optionsfeld für den gewünschten Web-Zugriffstyp, der für die Verbindung mit der Firewall vom Remote-WAN im Feld Remote Access (Remote-Zugriff) verwendet werden kann.

Schritt 8: Aktivieren Sie **Remote Upgrade**, um Remote-Benutzern die Aktualisierung der RV215W zu ermöglichen.

Schritt 9: Klicken Sie im Feld Zulässige Remote-IP-Adresse auf das Optionsfeld für die gewünschten IP-Adressen, die für den Remote-Zugriff auf den RV215W zugelassen sind.

·Beliebige IP-Adresse - Alle IP-Adressen sind zulässig.

·IP-Adresse - Geben Sie einen Bereich von zulässigen IP-Adressen ein.

Schritt 10: Geben Sie im Feld Remote Management Port (Remote-Verwaltungsport) einen Port ein, auf dem Remote-Zugriff möglich ist. Ein Remote-Benutzer muss den Remote-Port verwenden, um auf das Gerät zuzugreifen.

Hinweis: Das Format für den Remote-Zugriff ist https://<*remote-ip*>:<*remote-port*>

Schritt 11: Aktivieren Sie im Feld "IPv4 Multicast Passthrough" die **Option Enable (Aktivieren)**, damit IPv4-Multicast-Datenverkehr vom Internet über die RV215W übertragen wird. IP-Multicast ist eine Methode, mit der IP-Datagramme an eine bestimmte Gruppe von Empfängern in einer einzigen Übertragung gesendet werden.

Schritt 12: Aktivieren Sie im Feld "IPv6 Multicast Passthrough" die **Option Enable (Aktivieren)**, damit IPv6-Multicast-Datenverkehr vom Internet über die RV215W übertragen wird.

Schritt 13: Aktivieren Sie im Feld UPnP **Aktivieren**, um Universal Plug and Play (UPnP) zu aktivieren. UPnP ermöglicht die automatische Erkennung von Geräten, die mit der RV215W kommunizieren können.

Schritt 14: Aktivieren Sie im Feld "Gestattet Benutzern die Konfiguration" die Option **Aktivieren**, um Benutzern mit UPnP-fähigen Geräten die Konfiguration von UPnP-Port-Zuordnungsregeln zu ermöglichen. Port-Mapping oder Port-Forwarding wird verwendet, um die Kommunikation zwischen externen Hosts und Diensten in einem privaten LAN zu ermöglichen.

Schritt 15: Aktivieren Sie **Aktivieren** im Feld "Benutzer zum Deaktivieren des Internetzugangs zulassen", um Benutzern zu ermöglichen, den Internetzugriff auf das Gerät zu deaktivieren.

Schritt 16: Aktivieren Sie **Java blockieren**, um das Herunterladen von Java-Applets zu

verhindern. Java-Applets, die für böswillige Absichten erstellt werden, können eine Sicherheitsbedrohung für ein Netzwerk darstellen. Nach dem Herunterladen kann ein feindseliges Java-Applet Netzwerkressourcen ausnutzen. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): Blockiert automatisch Java.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Java blockiert werden soll.

Schritt 17: Aktivieren Sie **Blockieren von Cookies**, um Cookies von der Erstellung durch eine Website auszuschließen. Cookies werden von Websites erstellt, um Informationen dieser Benutzer zu speichern. Cookies können die Web-Geschichte des Benutzers verfolgen, was zu einer Verletzung der Privatsphäre führen kann. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): Cookies automatisch blockieren.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Cookies blockiert werden sollen.

Schritt 18: Aktivieren Sie **ActiveX blockieren**, um das Herunterladen von ActiveX-Applets zu verhindern. ActiveX ist ein Applet-Typ, dem es an Sicherheit fehlt. Wenn ein ActiveX-Applet auf einem Computer installiert ist, kann es alles tun, was ein Benutzer kann. Es kann schädlichen Code in das Betriebssystem einfügen, ein sicheres Intranet durchsuchen, ein Kennwort ändern oder Dokumente abrufen und senden. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): ActiveX wird automatisch blockiert.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem ActiveX blockiert werden soll.

Schritt 19: Aktivieren Sie **Proxy blockieren**, um Proxyserver zu blockieren. Proxyserver sind Server, die eine Verbindung zwischen zwei separaten Netzwerken bereitstellen. Bösartige Proxy-Server können alle unverschlüsselten Daten aufzeichnen, die an sie gesendet werden, z. B. Anmeldungen oder Kennwörter. Klicken Sie auf das Optionsfeld für die gewünschte Blockmethode.

·Auto (Automatisch): Proxy-Server werden automatisch blockiert.

·Manual Port (Manueller Port) - Geben Sie einen bestimmten Port ein, an dem Proxy-Server blockiert werden sollen.

Schritt 20: Klicken Sie auf **Speichern**.