Standardrichtlinie für die Zugriffskontrolle auf dem CVR100W VPN-Router

Ziel

Die Zugriffskontrollrichtlinie gibt dem Benutzer die Kontrolle darüber, ob Informationen vom Gerät freigegeben werden oder nicht. Diese Funktion kann die Kommunikation vom sicheren LAN zum unsicheren WAN deaktivieren. Ein Benutzer möchte den Zugriff durch diese Richtlinie einschränken, wenn er der Meinung ist, dass die über das WAN weitergeleiteten Informationen nicht sicher sind.

In diesem Artikel wird erläutert, wie die Standard-Zugriffskontrollrichtlinie auf dem CVR100W VPN-Router konfiguriert wird.

Anwendbares Gerät

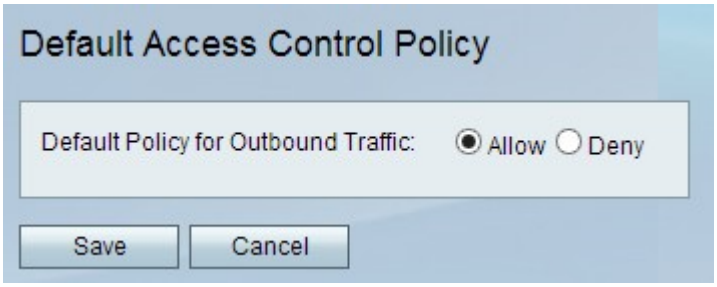
CVR100W

Softwareversion

·1.0.1.19

Standard-Zugriffskontrollrichtlinie

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Control > Default Access Control Policy (Firewall > Zugriffskontrolle > Standardzugriffskontrollrichtlinie) aus**. Die Seite *"Default Access Control Policy*" (Standardzugriffssteuerungsrichtlinie) wird geöffnet:



Schritt 2: Wählen Sie im Feld *"Default Policy for Outbound Traffic*" (Standardrichtlinie für ausgehenden Datenverkehr) eine der folgenden Optionen aus:

·Zulassen: Auf diese Weise können alle Informationen das WAN passieren und das System verlassen, falls erforderlich. Um die Sicherheit der Informationen zu erhöhen, aber den Zugriff zu vereinfachen, klicken Sie auf das Optionsfeld **Zulassen**.

·Verweigern: Dadurch werden Informationen verweigert, die über den WAN-Port übertragen werden, und das System lässt sich so konfigurieren, dass die Informationen so sicher wie möglich bleiben. Hosts vom LAN-Port können auch dann noch kommunizieren, wenn der WAN-Port deaktiviert ist. Wenn Zweifel an der Sicherheit ausgehender Informationen bestehen, klicken Sie auf das Optionsfeld **Verweigern**.

Schritt 4: Klicken Sie auf **Speichern**.