RV315W VPN路由器上的訪問控制配置

目標

訪問控制配置允許限制對特定IP地址的訪問。有多種選項可以自定義限制。一天中的時間、一 週中的天數、IP地址、物理埠和協定型別都是訪問控制策略的一些自定義功能的示例。

本文有助於解釋如何在RV315W VPN路由器上利用和配置訪問控制。

適用的裝置

·RV315W

軟體版本

•1.01.03

組態管理

步驟1.登入到Web配置實用程式並選擇Security > Access Control。Access Control頁面隨即開 啟:

Access Control							
Control Type:	Blacklist: Permit: O Whitelist: Blocks	s all traffic from LAN to WAN and or all traffic from LAN to WAN and onl	ly blocks traffic that matches the ac y Permits traffic that matches the ac	cess control policies. ccess control policies.	Sa	ve C	ancel
Access Control Polici	ies Week Protocol	Destination IP Address	Source Physical Port	Source IP Address	Destination Port	Status	Action
Add							

步驟2.按一下Control Type欄位中的Block list或Allow list單選按鈕。

·阻止清單 — 此選項允許從LAN到WAN的所有流量,但通過訪問控制設定被阻止的流量除外 。

·允許清單 — 此選項阻止從LAN到WAN的所有流量,但允許通過訪問控制設定的流量除外。

請參閱辭彙表以瞭解其他資訊。

步驟3.按一下Save以套用設定。

Access Control								
Control Type:	 Blacklist: Permits all traffic from LAN to WAN and only blocks traffic that matches the access control policies. Whitelist: Blocks all traffic from LAN to WAN and only Permits traffic that matches the access control policies. 							
						Sav	e C	Cancel
Access Control Policies	1							
IndexTime Range	Week	Protocol	Destination IP Address	Source Physical Port	Source IP Address	Destination Port	Status	Action

步驟4.按一下Add新增新的訪問控制策略。將開啟訪問控制策略設定頁面:

Access Control Policy Settings	
The access control policy permits or denies access to a sp	ecific destination IP address.
Time Range:	00:00 ~ 23:59
Week:	🗖 Sunday 🗖 Monday 🗖 Tuesday 🗖 Wednesday 🗖 Thursday 🗖 Friday 🗖 Saturday
Protocol:	TCP/UDP
Source Physical Port:	All Ports 🗨
Source IP Address:	Any IP Address
Destination IP Address:	Any IP Address
Destination Port:	~
Action:	enable O Disable
	Save Cancel

步驟5.在「時間範圍」欄位中輸入範圍。此選項是訪問控制策略生效的時間。

步驟6.選擇一週中的哪些天以允許或限制訪問。此選項表示訪問控制策略在一週中的哪些天有 效。

步驟7.從Protocol下拉選單中,選擇訪問控制適用的協定。

·TCP — 此協定用於將資料從應用程式傳輸到網路。TCP通常用於資訊傳輸必須完成且資料 包不能丟棄的應用程式。

·UDP — 此協定適用於基於網際網路協定(IP)的客戶端/伺服器網路應用。 此協定的主要用途 是即時應用。(VOIP、遊戲等)

·TCP/UDP — 選擇此協定以同時使用TCP和UDP。這是預設通訊協定。

·ICMP — 此協定傳送錯誤消息並負責網路中的錯誤處理。使用此協定可以在網路出現資料包 傳送問題時獲取通知。

·HTTP — 此協定在Web伺服器和瀏覽器之間提供安全通訊。當需要在伺服器和瀏覽器之間 安全傳輸資料包時,使用此協定。

·FTP — 此通訊協定在電腦之間傳輸檔案。在多個裝置之間交換檔案時選擇此協定。

·SMTP — 此協定處理電子郵件的傳輸。交換電子郵件時選擇此協定。

·POP3 — 此協定與SMTP在電子郵件方面結合在一起。POP3將電子郵件從電子郵件伺服器 下載到個人電腦。下載電子郵件時選擇此協定。

步驟8.從Source Physical Port下拉選單中,選擇訪問控制適用的埠。

步驟9.從Source IP Address下拉選單中,選擇訪問控制所應用的IP地址。

·任何IP地址 — 選擇此選項可允許或拒絕所有IP地址。選擇此選項的啟用或禁用單選按鈕。

·單個IP地址 — 選擇此選項可允許或拒絕單個IP地址。在Source IP Address欄位中輸入適用 的IP地址。

·IP地址範圍 — 選擇此選項可基於所選範圍允許或拒絕IP地址。在第一和第二個Source IP Address欄位中輸入適用的IP地址範圍。

步驟10.從Destination IP Address下拉選單中,選擇訪問控制所應用的IP地址。

·任何IP地址 — 選擇此選項可允許或拒絕所有IP地址。點選此選項的啟用或禁用單選按鈕。

·單個IP地址 — 選擇此選項可允許或拒絕單個IP地址。在Destination IP Address欄位中輸入 適用的IP地址。 ·IP地址範圍 — 選擇此選項可基於所選範圍允許或拒絕IP地址。在第一和第二個Destination IP Address欄位中輸入適用的IP地址範圍。

步驟11.在Destination Port欄位中, 輸入訪問控制適用的協定或應用的埠範圍。

步驟12.按一下Enable 單選按鈕以啟用訪問控制策略。

步驟13.按一下「Save」以套用設定。

Access Control Policy Settings	
The access control policy permits or denies access to a sp	ecific destination IP address.
Time Range:	09:00 ~ 17:00
Week:	🗖 Sunday 🗹 Monday 🔽 Tuesday 🗹 Wednesday 🔽 Thursday 🔽 Friday 🗖 Saturday
Protocol:	TCP/UDP
Source Physical Port:	All Ports 🗨
Source IP Address:	Any IP Address
Destination IP Address:	Any IP Address
Destination Port:	200 ~ 220
Action:	enable O Disable
	Save Cancel

步驟14.(可選)若要刪除訪問控制策略,請按一下「操作」標題下的垃圾桶圖示。

步驟15。(可選)若要編輯訪問控制策略,請按一下「操作」標題下的信封圖示。