在RV042、RV042G和RV082 VPN路由器上的非軍事區(DMZ)中配置多個公共IP

目標

非軍事區(DMZ)是一個組織的內部網路，它可用於不可信網路。根據安全性，DMZ位於可信網路與不可信網路之間。維護DMZ有助於提高組織內部網路的安全性。當存取控制清單(ACL)繫結到介面時，其存取控制元素(ACE)規則會套用於到達該介面的封包。與「訪問控制清單」中的任何ACE都不匹配的資料包將與其操作是丟棄不匹配的資料包的預設規則相匹配。

本文的目的是向您展示如何配置DMZ埠以允許多個公共IP地址，並為路由器裝置上的IP定義訪問控制清單(ACL)。

適用裝置

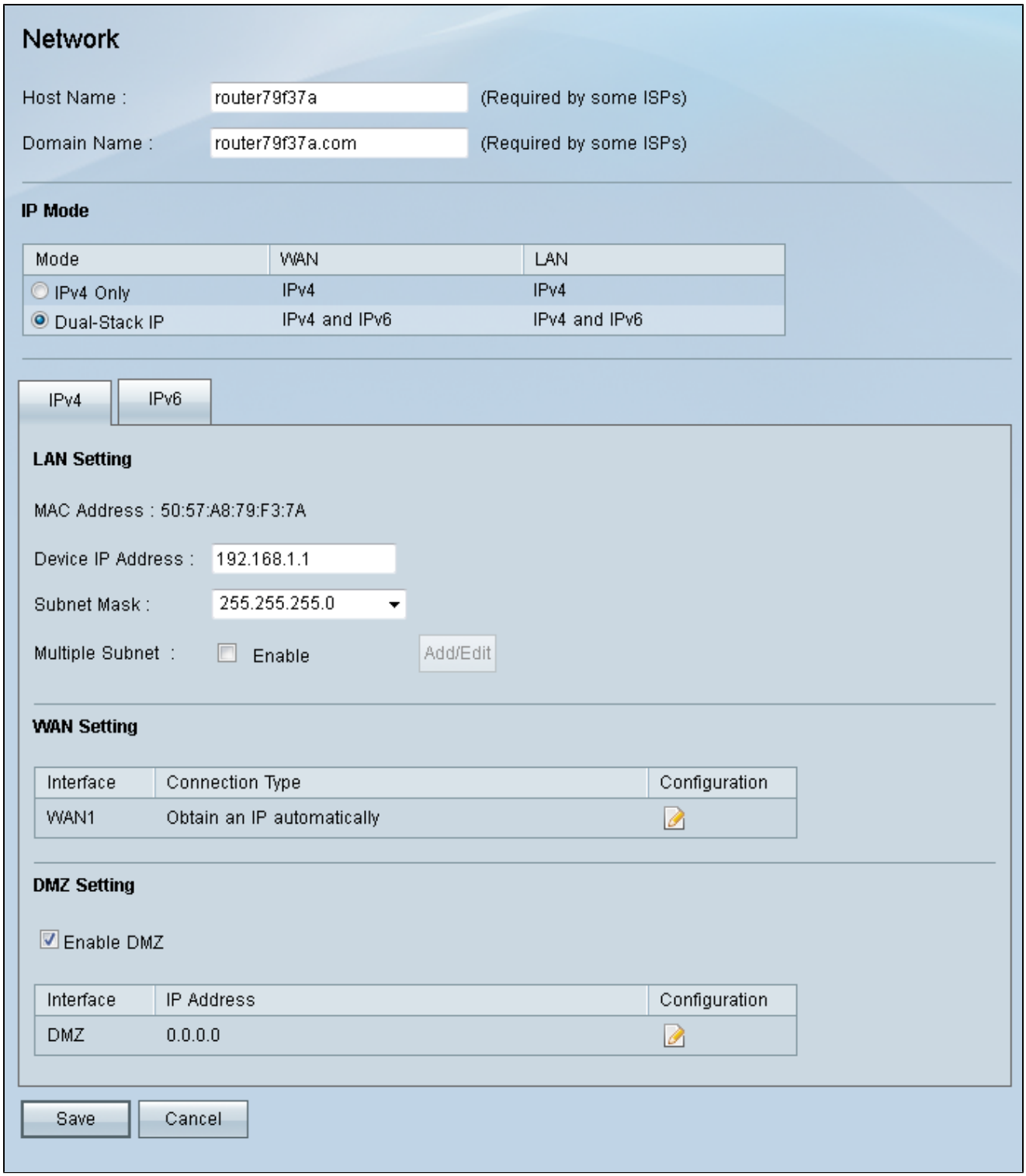
· RV042
· RV042G
· RV082

軟體版本

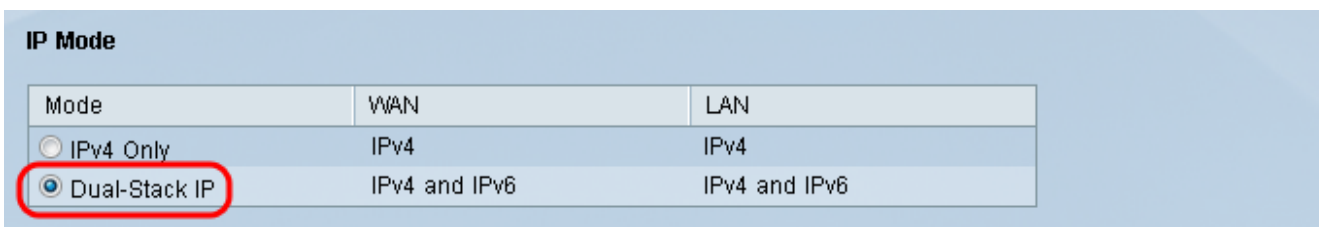
· v4.2.2.08

DMZ配置

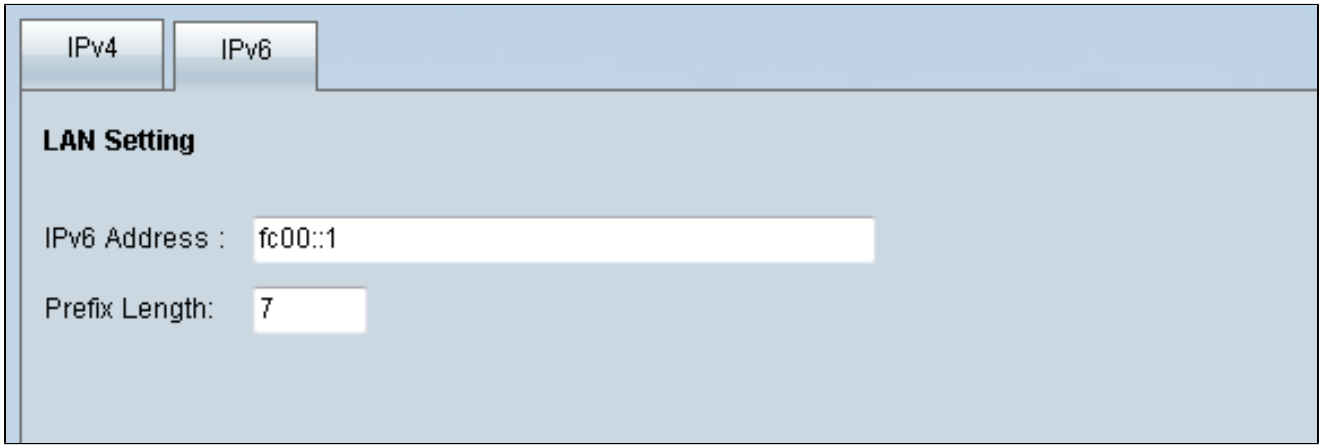
步驟 1.登入到Web Configuration Utility頁面，然後選擇Setup > Network。Network 頁面隨即開啟：



步驟 2.在IP Mode欄位中，按一下Dual-Stack IP單選按鈕以啟用IPv6地址配置。

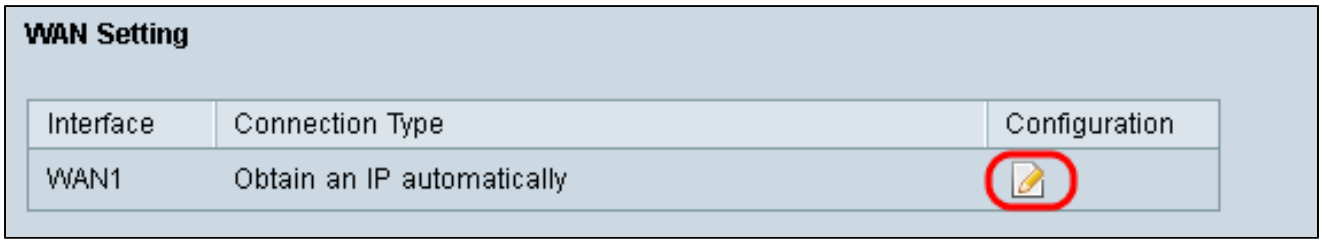


步驟 3.按一下LAN Setting欄位中的IPv6頁籤，以便在IPv6地址上配置DMZ。

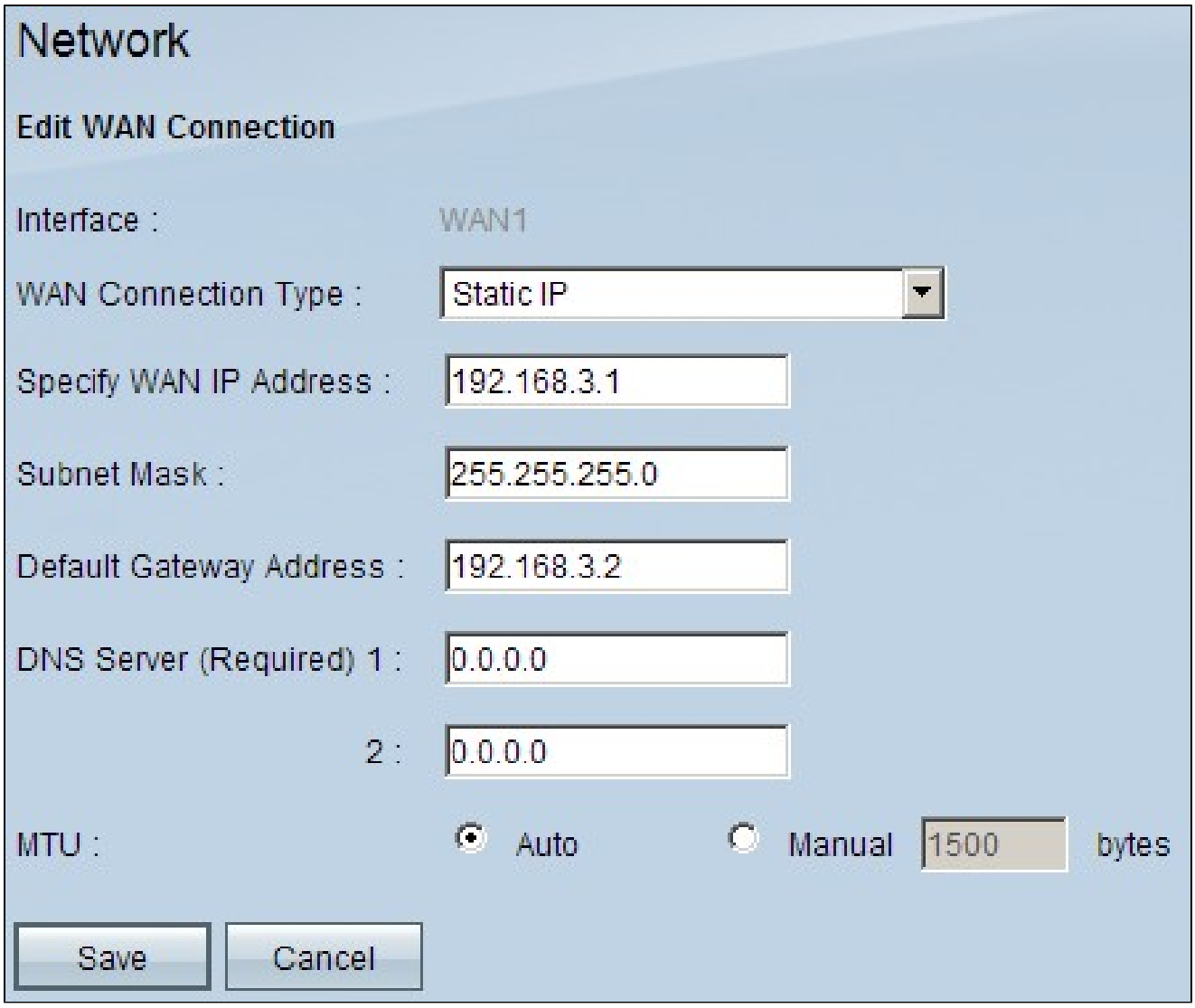


步驟4.向下滾動到DMZ設定區域，然後點選DMZ覈取方塊以啟用DMZ

步驟 5.在WAN Setting欄位中，點選Edit按鈕以編輯WAN1設定的IP Static。



Network頁面隨即開啟：



步驟 6.從WAN Connection Type下拉選單中選擇Static IP。

步驟 7.在指定WAN IP地址欄位中輸入顯示在系統摘要頁面上的WAN IP地址。

步驟 8.在Subnet Mask欄位中輸入子網掩碼地址。

步驟 9.在Default Gateway Address欄位中輸入預設網關地址。

步驟 10.在DNS Server(Required)1欄位中輸入在System Summary頁上顯示的DNS伺服器地址。

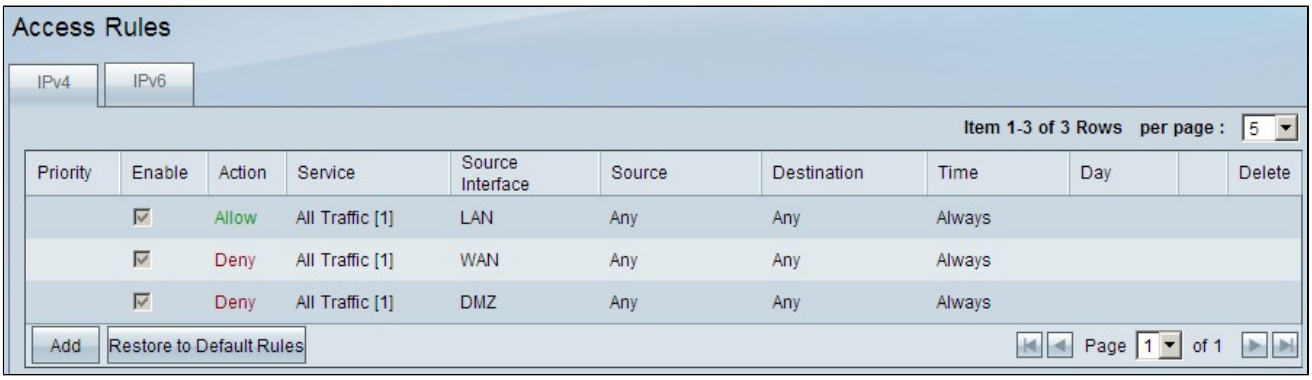
注意：DNS伺服器地址2是可選的。

步驟 11.選擇最大傳輸單位(MTU)為自動或手動。如果選擇手動，請為手動MTU輸入位元組。

步驟 12.按一下Save頁籤以儲存設定。

ACL定義

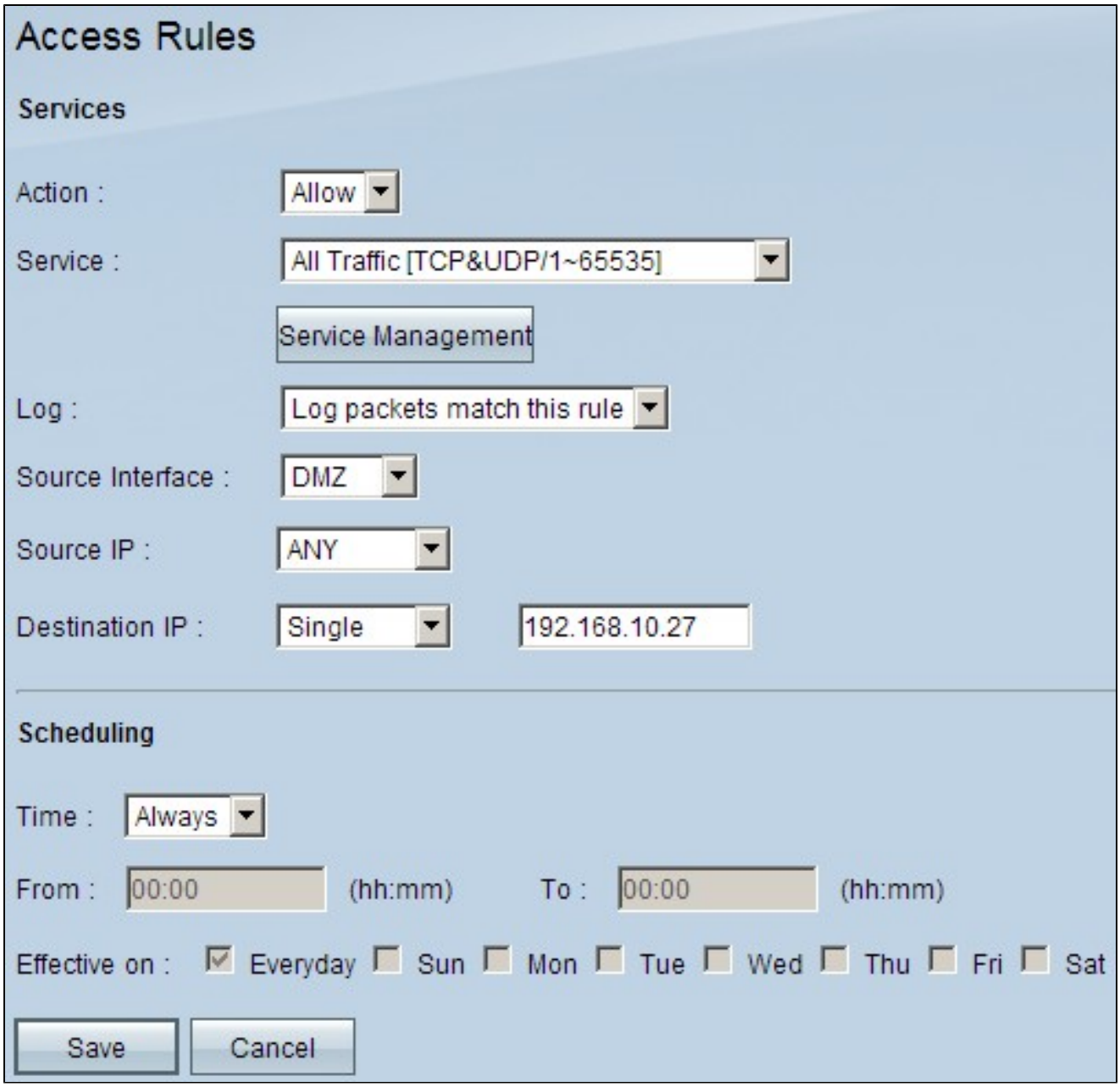
步驟 1.登入到Web配置實用程式頁面，然後選擇Firewall > Access Rules。Access Rules頁面隨即開啟：



注意：輸入「訪問規則」頁面時，無法編輯預設訪問規則。

步驟 2.按一下Add按鈕新增新訪問規則。

Access Rules頁面現在將顯示Service和Scheduling區域的選項。



步驟 3.從Action下拉選單中選擇Allow以允許該服務。

步驟 4.從Service下拉選單中選擇All Traffic [TCP&UDP/1~65535] 以啟用DMZ的所有服務。

步驟 5.從Log下拉選單中選擇Log packets match this rule，以僅選擇與訪問規則匹配的日誌。

步驟 6.從Source Interface下拉式清單中選擇DMZ。這是訪問規則的源。

步驟 7.從Source IP下拉選單中選擇Any。

步驟 8.從Destination IP下拉選單中選擇Single。

步驟 9.在Destination IP欄位中輸入允許訪問規則的目的地的IP地址。

步驟 10.在Scheduling區域中，從Time下拉選單中選擇Always，以使訪問規則始終處於活動狀態。

註：如果從Time下拉選單中選擇Always，則訪問規則將預設設定為Everyday on欄位中的Everyday。

注意：通過從「時間」下拉選單中選擇「時間間隔」，可以選擇特定時間間隔(訪問規則對其是活動的)。然後，您可以從Effective on覈取方塊中選擇希望訪問規則處於活動狀態的天。

步驟 11.按一下Save儲存設定。

注意：如果出現彈出視窗，請按「確定」新增另一個訪問規則，或者按「取消」返回到「訪問規則」頁面。

此時將顯示在上一步中建立的訪問規則

步驟 12.按一下Edit圖示編輯建立的訪問規則。

步驟 13.按一下Delete圖示可刪除建立的訪問規則。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。