

在RV340或RV345路由器上配置安全套接字層虛擬專用網路(SSL VPN)

特別宣告：許可結構 — 韌體版本1.0.3.15及更高版本。接下來，AnyConnect將只對客戶端許可證收取費用。

有關RV340系列路由器上的AnyConnect許可的其他資訊，請檢視[RV340系列路由器的AnyConnect許可](#)一文。

目標

安全套接字層虛擬專用網路(SSL VPN)網關允許遠端使用者使用Web瀏覽器建立安全VPN隧道。此功能可透過SSL超文字傳輸通訊協定安全(HTTPS)瀏覽器支援，使用原生超文字傳輸通訊協定(HTTP)，輕鬆存取各種Web資源和啟用Web的應用程式。

SSL VPN允許使用者通過加密網路流量使用安全且經過身份驗證的路徑遠端訪問受限網路。

RV340和RV345路由器支援Cisco AnyConnect VPN客戶端，也稱為Anyconnect安全移動客戶端。預設情況下，這些路由器支援兩個SSL VPN隧道，使用者可註冊支援最多50個隧道的許可證。安裝並啟用後，SSL VPN將建立安全的遠端訪問VPN隧道。

本文旨在展示如何在RV340或RV345路由器上配置SSL VPN。

適用裝置

- RV340
- RV345
- 思科安全行動化使用者端

軟體版本

- 1.0.03.15 — RV340、RV345
- 4.4.01054 — AnyConnect安全行動化使用者端

配置SSL VPN

步驟1.訪問路由器基於Web的實用程式並選擇VPN > SSL VPN。



步驟2.按一下On單選按鈕啟用Cisco SSL VPN伺服器。

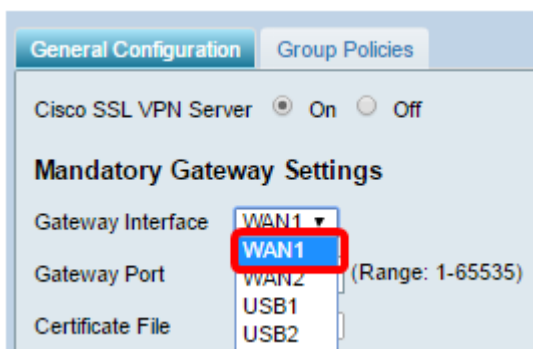


強制網關設定

必須使用以下配置設定：

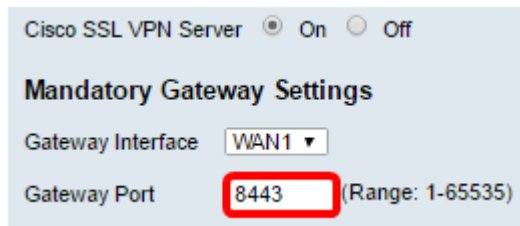
步驟3.從下拉選單中選擇Gateway Interface。此埠將用於通過SSL VPN隧道傳輸流量。選項包括：

- WAN1
- WAN2
- USB1
- USB2



附註：在本例中，選擇了WAN1。

步驟4.在Gateway Port欄位中輸入用於SSL VPN網關的埠號，範圍為1到65535。



Cisco SSL VPN Server ☒ On ☐ Off

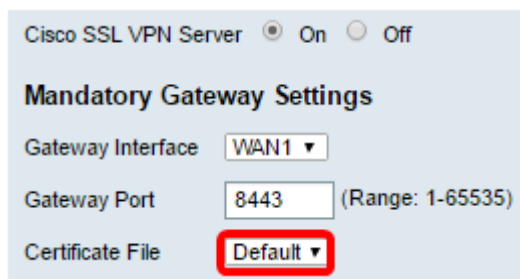
Mandatory Gateway Settings

Gateway Interface

Gateway Port (Range: 1-65535)

附註：在本例中，8443用作埠號。

步驟5.從下拉式清單中選擇Certificate File。此證書對嘗試通過SSL VPN隧道訪問網路資源的使用者進行身份驗證。下拉選單包含預設證書和匯入的證書。



Cisco SSL VPN Server ☒ On ☐ Off

Mandatory Gateway Settings

Gateway Interface

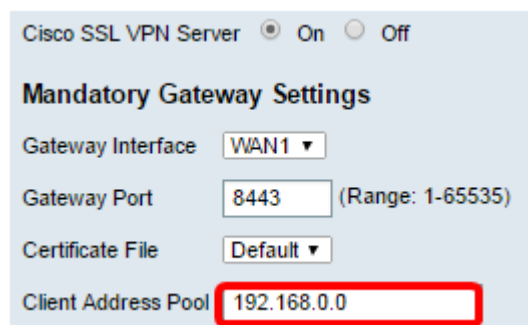
Gateway Port (Range: 1-65535)

Certificate File

附註：在本例中，選擇了Default。

步驟6.在Client Address Pool欄位中輸入客戶端地址池的IP地址。此池將是分配給遠端VPN客戶端的IP地址範圍。

附註：確保IP地址範圍不與本地網路上的任何IP地址重疊。



Cisco SSL VPN Server ☒ On ☐ Off

Mandatory Gateway Settings

Gateway Interface

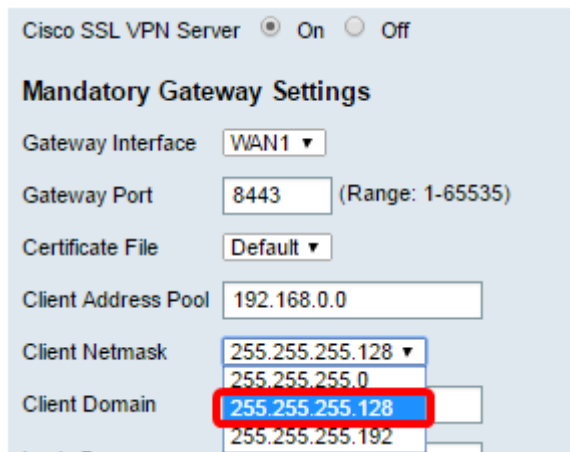
Gateway Port (Range: 1-65535)

Certificate File

Client Address Pool

附註：本示例使用192.168.0.0。

步驟7.從下拉選單中選擇Client Netmask。



Cisco SSL VPN Server ☒ On ☐ Off

Mandatory Gateway Settings

Gateway Interface

Gateway Port (Range: 1-65535)

Certificate File

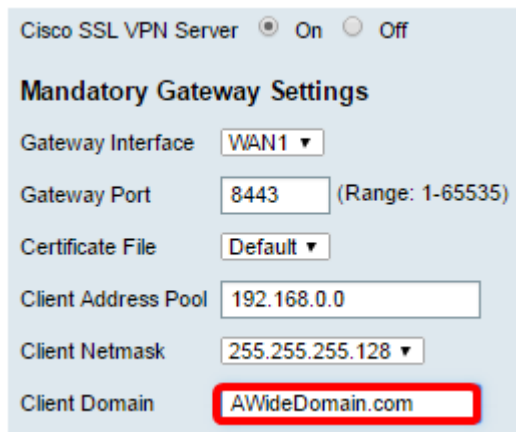
Client Address Pool

Client Netmask

Client Domain

附註：在此範例中，選擇255.255.255.128。

步驟8.在Client Domain（客戶端域）欄位中輸入客戶端域名。這是應推送到SSL VPN客戶端的域名。



Cisco SSL VPN Server ☒ On ☐ Off

Mandatory Gateway Settings

Gateway Interface

Gateway Port (Range: 1-65535)

Certificate File

Client Address Pool

Client Netmask

Client Domain

附註：在此示例中，AWideDomain用作客戶端域名。

步驟9.在Login Banner欄位中輸入顯示為登入標語的文本。這將是在每次客戶端登入時顯示的標語。

Cisco SSL VPN Server ☒ On ☐ Off

Mandatory Gateway Settings

Gateway Interface

Gateway Port (Range: 1-65535)

Certificate File

Client Address Pool

Client Netmask

Client Domain

Login Banner

附註：在本例中，歡迎使用我的域！用作登入標語。

可選網關設定

以下配置設定是可選的：

步驟1.輸入介於60到86400之間的空閒超時值（以秒為單位）。這是SSL VPN會話可以保持空閒的持續時間。

Optional Gateway Settings

Idle Timeout seconds (Range: 60-86400)

附註：本例中使用的是3000。

步驟2.在Session Timeout欄位中輸入一個值(以秒為單位)。這是傳輸控制通訊協定(TCP)或使用使用者資料包通訊協定(UDP)作業階段在指定的閒置時間之後逾時的時間。範圍為60到1209600。

Optional Gateway Settings

Idle Timeout seconds (Range: 60-86400)

Session Timeout seconds (Range: 0,60-1209600)

附註：在此示例中，使用60。

步驟3.在ClientDPD Timeout欄位中輸入一個值（以秒為單位），範圍為0到3600。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。

附註：必須在VPN隧道的兩端啟用此功能。

Optional Gateway Settings		
Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)

附註：在此示例中，使用350。

步驟4.在GatewayDPD Timeout欄位中輸入一個0到3600之間的值（以秒為單位）。此值指定定期傳送HELLO/ACK消息以檢查VPN隧道的狀態。

附註：必須在VPN隧道的兩端啟用此功能。

Optional Gateway Settings		
Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)

附註：在此示例中，使用360。

步驟5.在Keep Alive欄位中輸入一個值（以秒為單位），範圍為0到600。此功能可確保您的路由器始終連線到Internet。如果斷開，它將嘗試重新建立VPN連線。

Optional Gateway Settings		
Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)
Keep Alive	40	seconds (Range: 0-600)

附註：在此示例中，使用40。

步驟6.在Lease Duration欄位中輸入要連線的隧道的持續時間值（以秒為單位）。範圍為

600到1209600。

Optional Gateway Settings		
Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)
Keep Alive	40	seconds (Range: 0-600)
Lease Duration	43500	seconds (Range: 600-1209600)

附註： 在本例中，使43500了SPAN。

步驟7.輸入可通過網路傳送的資料包大小（以位元組為單位）。範圍是從576到1406。

Optional Gateway Settings		
Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)
Keep Alive	40	seconds (Range: 0-600)
Lease Duration	43500	seconds (Range: 600-1209600)
Max MTU	1406	byte (Range: 576-1406)

附註： 在此示例中，使用1406。

步驟8.在Rekey Interval欄位中輸入中繼間隔時間。Rekey功能允許SSL金鑰在會話建立後重新協商。範圍是從0到43200。

Optional Gateway Settings

Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)
Keep Alive	40	seconds (Range: 0-600)
Lease Duration	43500	seconds (Range: 600-1209600)
Max MTU	1406	byte (Range: 576-1406)
Rekey Interval	3600	seconds (Range: 0-43200)

附註：在此範例中，使用3600。

步驟9.按一下Apply。

Optional Gateway Settings

Idle Timeout	3000	seconds (Range: 60-86400)
Session Timeout	60	seconds (Range: 0,60-1209600)
Client DPD Timeout	350	seconds (Range: 0-3600)
Gateway DPD Timeout	360	seconds (Range: 0-3600)
Keep Alive	40	seconds (Range: 0-600)
Lease Duration	43500	seconds (Range: 600-1209600)
Max MTU	1406	byte (Range: 576-1406)
Rekey Interval	3600	seconds (Range: 0-43200)

步驟10。（可選）若要永久儲存配置，請按一下閃爍的圖  標。

現在，您應該已經在RV34x路由器上成功配置了SSL VPN。

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）。