# RV34x系列路由器上的ACL最佳實踐

#### 目標

本文的目的是描述使用RV34x系列路由器建立訪問控制清單(ACL)的最佳實踐。

### 適用裝置 | 韌體版本

- RV340 | 1.0.03.20(下載 最新版本)
- RV340W | 1.0.03.20(下載 最新版本)
- RV345 | 1.0.03.20(下載**最新版本)**
- RV345P | 1.0.03.20(下載 最新版本)

# 簡介

您想對網路進行更多控制嗎?您想採取額外措施保證網路安全嗎?如果是,則訪問控制 清單(ACL)可能正是您所需要的。

ACL由共同定義網路流量配置檔案的一個或多個訪問控制條目(ACE)組成。然後,思科 軟體功能(例如流量過濾、優先順序或自訂佇列)可參考此設定檔。每個ACL都包含操 作元素(允許或拒絕)以及基於標準(例如源地址、目標地址、協定和協定特定引數 )的過濾元素。

根據您輸入的條件,您可以控制特定流量進入和/或離開網路。路由器收到封包時,會檢 查封包,以根據存取清單判斷轉送或捨棄封包。

實施此安全級別取決於不同的使用案例,其中會考慮特定的網路場景和安全需求。

必須注意的是,路由器可能會根據路由器的配置自動建立訪問清單。在這種情況下,您 可能會看到訪問清單,除非您更改路由器配置,否則您無法清除這些清單。

## 為什麼使用存取清單

- 在大多數情況下,我們使用ACL為訪問我們的網路提供基本的安全級別。例如,如果不配置ACL,預設情況下,可以允許通過路由器的所有資料包傳送到我們網路的所有部分。
- ACL可以允許一台主機、IP地址範圍或網路,並阻止另一台主機、IP地址範圍或網路訪問 同一區域(主機或網路)。
- 通過使用ACL,您可以決定在路由器介面上轉發或阻止哪些型別的流量。例如,您可以允許安全殼層(SSH)檔案傳輸通訊協定(SFTP)流量,同時封鎖所有作業階段啟始通訊協定 (SIP)流量。

### 使用存取清單的時間

- 您應在位於內部網路和外部網路(如Internet)之間的路由器中配置ACL。
- •您可以使用ACL控制進出內部網路特定部分的流量。
- 當您需要過濾介面上的傳入流量或傳出流量,或同時過濾兩者時。
- 您應該為每個協定定義ACL以控制流量。

# 使用存取清單設定基本安全性的最佳實踐

- 實施ACL,只允許那些拒絕所有其他協定的協定、埠和IP地址。
- •阻止聲稱具有相同目的地址和來源位址的傳入封包(對路由器本身的著陸攻擊)。
- 對內部(受信任的)系統日誌主機啟用ACL日誌記錄功能。
- •如果在路由器上使用簡易網路管理通訊協定(SNMP),則必須設定SNMP ACL和複雜的 SNMP社群字串。
- 僅允許內部地址從內部介面進入路由器,並且僅允許目的地為內部地址的流量從外部(外 部介面)進入路由器。
- 如果未使用,則阻止組播。
- 封鎖某些網際網路控制訊息通訊協定(ICMP)訊息型別(重新導向、回應)。
- 請一律考慮輸入ACL的順序。例如,當路由器決定轉送還是封鎖封包時,它會根據每個 ACL陳述式,以建立ACL的順序來測試封包。

# Cisco RV34x系列路由器中的訪問清單實施

網路拓撲示例



# 範例案例

在此情境中,我們將複製此網路圖表,其中有一台RV345P路由器和兩個不同的VLAN介面。VLAN 1和VLAN2中各有一個PC,VLAN 1中也有伺服器。VLAN間路由已啟用,因此VLAN 1和VLAN 2使用者可以彼此通訊。現在,我們將應用訪問規則來限制VLAN 2使用者與VLAN 1中此伺服器之間的通訊。

### 組態范例

### 步驟1

使用您配置的憑證登入到路由器的Web使用者介面(UI)。



# Router



# 要配置ACL,請導航到Firewall > Access Rules,然後點選plus圖示新增新規則。

Firewall 1	ilialia cisco	RV345P-router44	.91EF		cisco (adr	nin) English 🔻	90 🕩
Basic Settings	Access Rules	6				Apply Restore to	Default Rules
Network Address Translation	IPv4 Access Rules	Table					
Static NAT	3+2 💼						
Port Forwarding	□ Priority <b>≑</b> E	inable  Action	Services \$	Source Interface \$	Source \$	Destination Interface \$	Destination \$
Port Triggering	4001 🚯 🔄	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any
Session Timeout	4002 🕄 🔄	Z Denied	IPv4: All Traffic	WAN	Any	VLAN	Any

### 步驟3

配置訪*問規則*引數。套用ACL以限制伺服器(IPv4:192.168.1.10/24)VLAN2使用者訪問。 在此方案中,引數如下:

- 規則狀態: 啟用
- Action:拒絕
- 服務:所有流量
- 日誌:正確
- 源介面: VLAN2
- 來源位址:任何
- 目標介面: VLAN1
- 目的地位址:單個IP 192.168.1.10
- 計畫名稱: 隨時隨地

按一下「Apply」。

在本例中,我們拒絕任何裝置從VLAN2存取伺服器,然後允許存取VLAN1中的其他裝置。您 的需要可能會有所不同。

8	Routing	e alado r	RV345P-router44	5P-router4491EF cisco (admin) Englist • ?				
	Firewall	CISCO						
	Basic Settings	Access Rules	6		2 (	Apply		
	Access Rules							
	Network Address	Rule Status:	C Enable					
	Iranslation	Action:	Deny •					
	Static NAT	Services:	⊙ IPv4 O IPv6	All Traffic				
	Port Forwarding	Log:	True •					
	Port Triggering	Source Interface:	VLAN2 VLAN2					
	Session Timeout	Source Address						
	DMZ Host	Source Address.	Any •					
F	VPN	Destination Interface:	VLAN1 •					
Ţ		Destination Address:	Single IP 🔹	192.168.1.10				
T	QoS	Scheduling						
æ	Configuration Wizards							
	License	Schedule Name:	ANYTIME	Click here to configure the schedules				
步	驟4							

Access Rules清單將顯示如下:

*	Routing Firewall	₿	S vilully RV345P-router4491EF						cisco (admin) English 🔹 💡 🚺 🕩			
_	Basic Settings	Acc	ess Rul	es					A	Restore to D	Default Rules	
	Network Address Translation	IPv4	Access Ru	les Table								
	Static NAT	+	Image: Second secon	Enable 🗢	Action 🗢	Services 🗢	Source Interface 🗢	Source 🗢	Destination Interface 🗢	Destination 🗢	Schedule 🗢	
	Port Forwarding		1	ſ.	Denied	IPv4: All Traffic	VLAN2	Any	VLAN1	192.168.1.10	ANYTIME	
	Port Triggering		4001 🚯	Ø	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any	ANYTIME	
	Session Timeout		4002 🚯	œ.	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any	ANYTIME	

驗證

要驗證服務,請開啟命令提示符。在Windows平台上,可通過按一下Windows按鈕,然後在電腦左下方的搜尋框中鍵入cmd,然後從選單中選擇Command Prompt來實現。

輸入以下命令:

- 在VLAN2中的PC(192.168.3.173)上,對伺服器(IP:192.168.1.10)。 您將收到*Request timed out*通知,這意味著不允許通訊。
- 在VLAN2中的PC(192.168.3.173)上,對VLAN1中的其他PC(192.168.1.109)執行ping操作 。您將收到成功的回覆。

C:\Users\Cisco>ping 192.168.1.10
Pinging 192.168.1.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.10:
 Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Cisco>ping 192.168.1.109
Pinging 192.168.1.109 with 32 bytes of data:
Reply from 192.168.1.109: bytes=32 time=1ms TTL=127

您已看到在Cisco RV34x系列路由器上配置訪問規則的必要步驟。現在,您可以應用該 策略在網路中建立符合您需求的訪問規則!