

在RV34x系列路由器上配置DMZ

目標

本文檔旨在向您展示如何在RV34x系列路由器上配置非軍事區(DMZ)主機和硬體DMZ。

簡介

DMZ是網路中的一個位置，它對Internet開放，同時保護防火牆後的區域網(LAN)。將主網路與單個主機、整個子網或「子網」分隔開，可確保通過DMZ訪問您的服務（如網際網路遊戲、視訊會議、Web或電子郵件伺服器）的使用者無法訪問您的LAN。思科提供兩種使用DMZ的方法，即DMZ主機和硬體DMZ。DMZ主機允許LAN上的一台主機暴露於網際網路，而硬體DMZ（子網路/範圍）是向公眾開放的子網路。

在規劃DMZ時，可以考慮使用私有或公有IP地址。私有IP地址對您來說是唯一的，只在LAN上。公共IP地址對於您的組織來說是唯一的，並且由您的Internet服務提供商(ISP)分配。要獲取公共IP地址，您需要聯絡您的ISP。

大多數使用者會使用硬體DMZ，因為它會自動設定VLAN和自己的網段。對於「硬體DMZ」，我們使用子網或範圍選項。DMZ主機的配置更簡單，因為您不必配置訪問規則，但安全性較低。

WAN-to-DMZ以及LAN-to-DMZ都是最常用的使用案例。還允許DMZ到WAN，因為DMZ電腦可能需要作業系統補丁或更新，但是DMZ到LAN應該被阻止，因為它可能是潛在的安全漏洞。例如，Internet上的駭客使用DMZ作為跳線伺服器。

在使用案例方面，DMZ主機和硬體DMZ之間的區別是：

如果您想將某些內容暴露到Internet，但您有一台多功能一體伺服器，或者您沒有備用公有IP地址，則應使用DMZ主機。將伺服器放在其中一個VLAN中，並將其設定為DMZ主機。然後，外部使用者可以通過路由器的WAN IP訪問伺服器。

如果要將某些內容暴露到Internet，並且有多個伺服器（每個伺服器都有特定的服務）和相同數量的公有IP地址，則應使用硬體DMZ。將這些伺服器連線到指定的DMZ埠（即RV340的LAN 4），並用您在路由器或子網中配置的同公用IP地址配置它們）。然後，外部使用者可以通過這些IP地址訪問每台伺服器。

DMZ	比較	對比度
主機	隔離流量	單個主機，完全開啟網際網路
子網/範圍	隔離流量	多種裝置和型別，完全開啟網際網路。

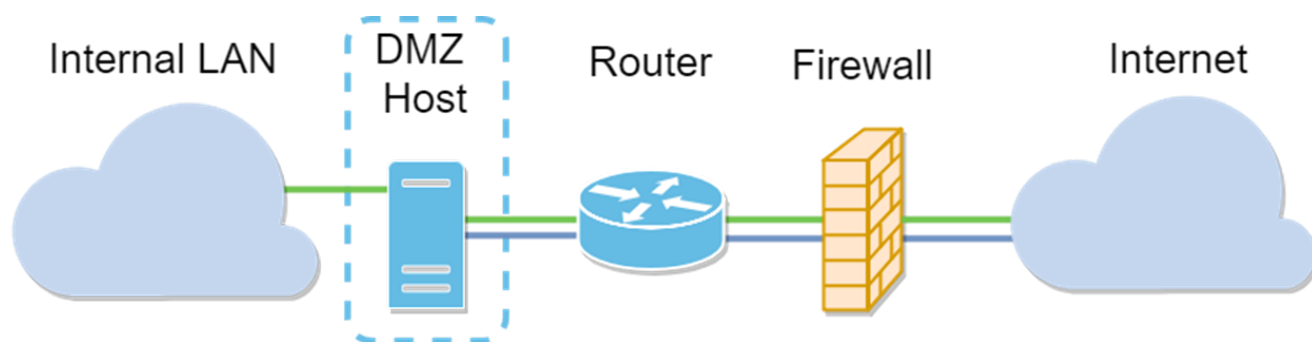
附註：在本示例中，配置DMZ子網時，我們會將交換機插入路由器的DMZ埠。

要瞭解如何在交換機上啟用SSH，請參閱以下文章：[在300/500系列託管交換機上啟用SSH服務](#)。

要瞭解如何在RV160/RV260上配置DMZ，請參閱以下文章：[適用於RV160/RV260路由器的](#)

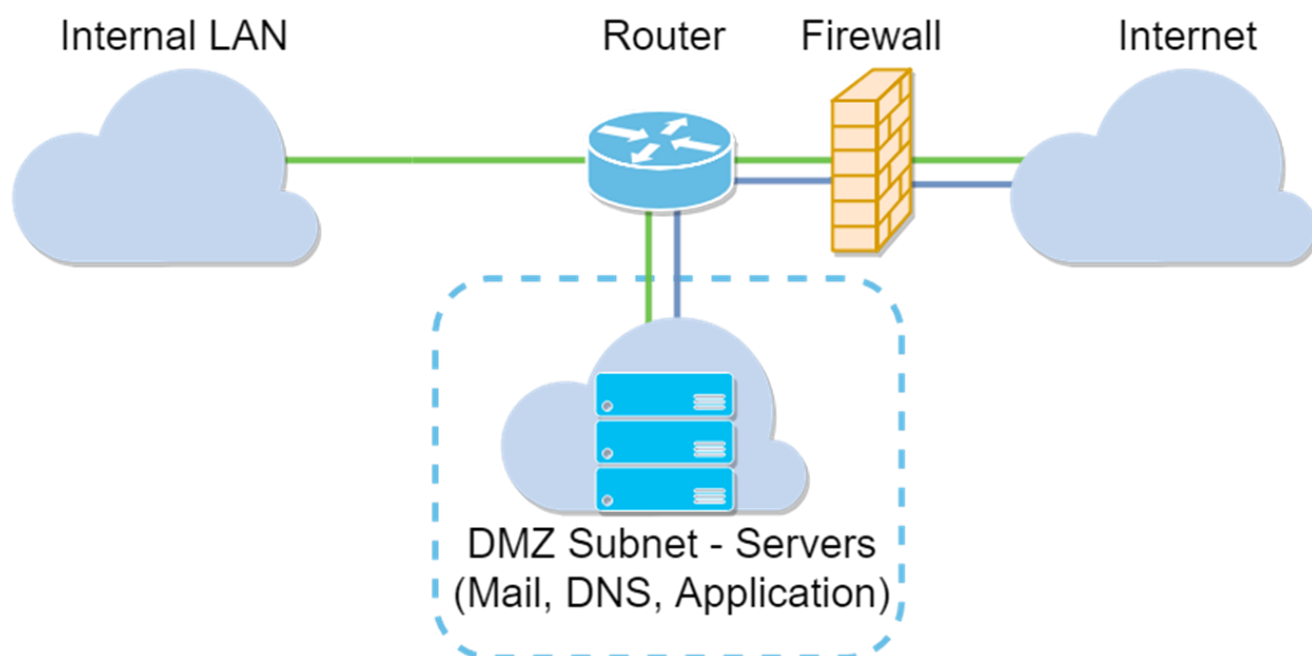
[DMZ選項。](#)

主機DMZ拓撲



附註：使用主機DMZ時，如果主機被惡意攻擊者破壞，您的內部LAN可能會受到進一步的安全入侵。

子網DMZ拓撲



適用裝置

RV34x

軟體版本

1.0.02.16

配置DMZ主機

步驟1.登入到路由器的Web配置頁。



Router

cisco



English



Login

©2017-2019 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

步驟2.導覽至Firewall > DMZ Host。



LAN



Routing



Firewall

1

Basic Settings

Access Rules

Network Address
Translation

Static NAT

Port Forwarding

Port Triggering

Session Timeout

DMZ Host

2



VPN

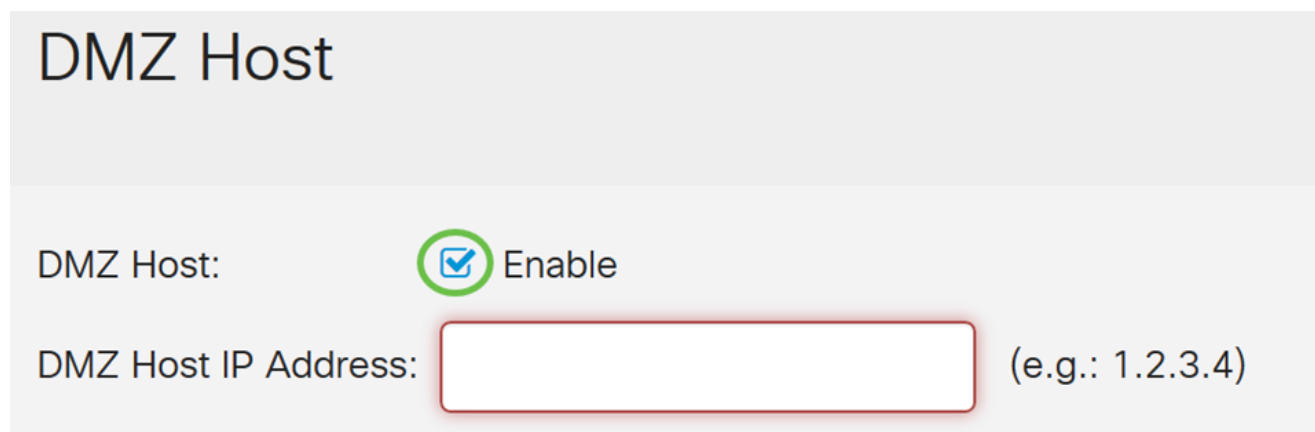


Security



QoS

步驟3. 在DMZ主機欄位中，勾選**Enable**覈取方塊以啟用DMZ主機。



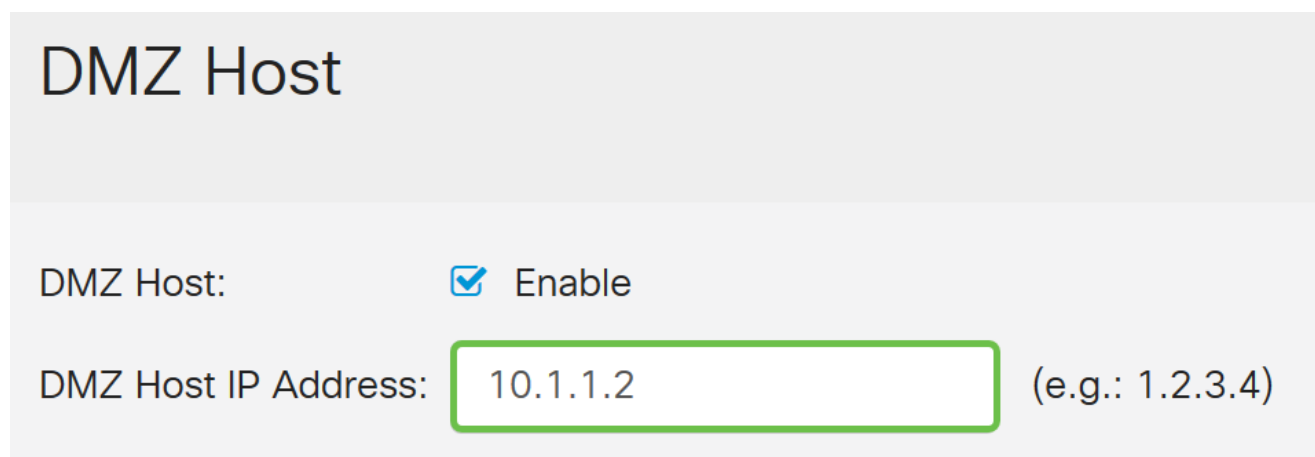
DMZ Host

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

步驟4. 在DMZ主機IP地址中輸入主機的IP地址，該IP地址將公開給Internet以使用網際網路遊戲、視訊會議、Web或電子郵件伺服器等服務。

附註：要使DMZ主機功能正常工作，需要為LAN DMZ主機提供固定或靜態IP地址。確保它與您的路由器位於同一網路中。當DMZ位於另一個VLAN中時，您也可以進行設定。



DMZ Host

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

步驟5. 按一下**Apply**，儲存組態。



DMZ Host Apply Cancel

DMZ Host: Enable

DMZ Host IP Address: (e.g.: 1.2.3.4)

您現在應該已經成功啟用DMZ主機。

步驟6. (可選) 在接下來的幾個步驟中，我們將向您展示一種驗證DMZ主機的方法。導覽至 **Firewall > Basic Settings**。



System Configuration



WAN



LAN



Routing



Firewall

1

Basic Settings

2

Access Rules

Network Address
Translation

Static NAT

Port Forwarding

Port Triggering

Session Timeout

DMZ Host



VPN

步驟7. (可選) 在此範例中，已啟用遠端Web管理並選中HTTPS。這是通過WAN IP地址遠端登入Web配置頁。在此步驟中，我們將埠號調整為6000。範圍為1025-6535。

附註：如果在遠端訪問Web管理頁面時進行了此配置，則您的頁面可能會在載入螢幕上掛起。這表示連線埠已變更為您調整後的內容。

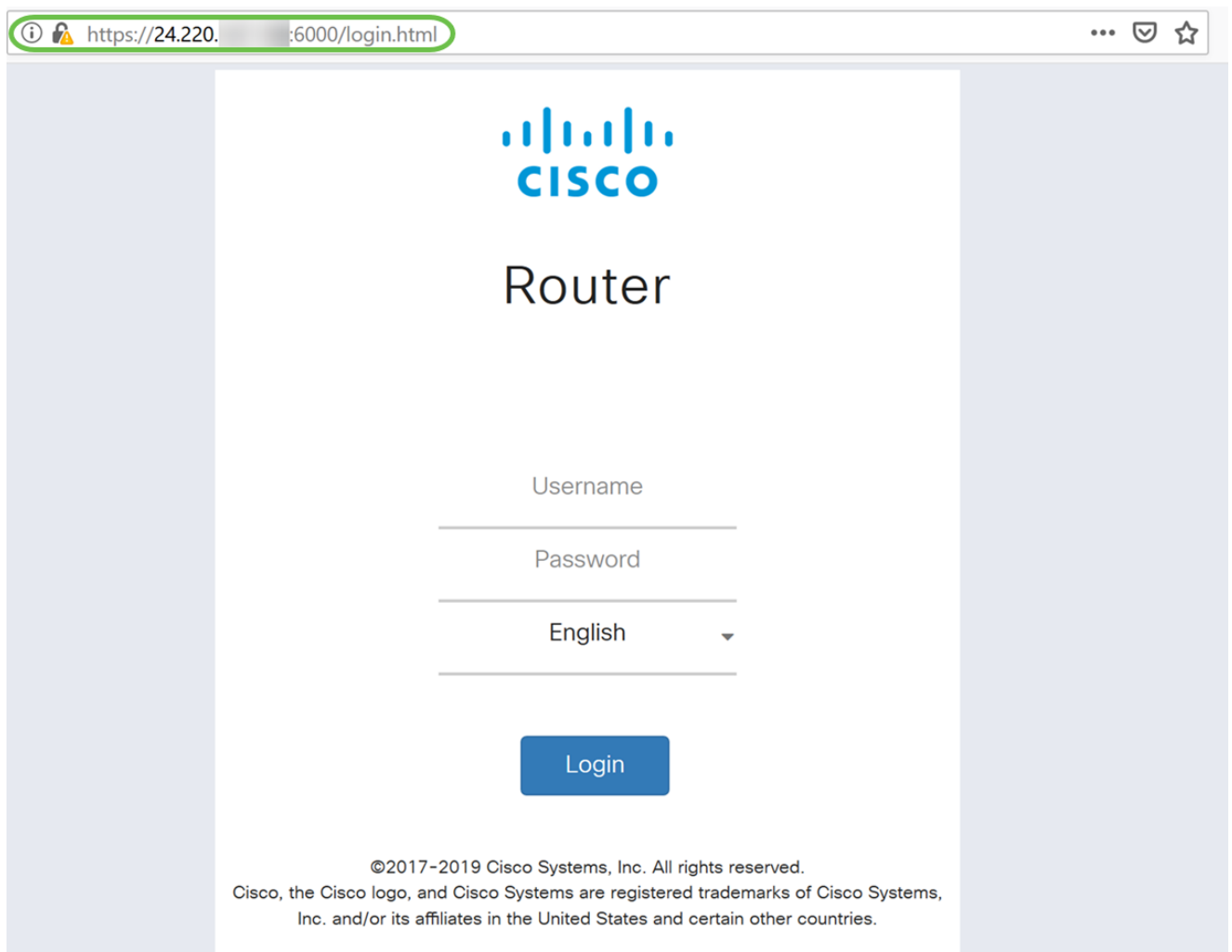
Remote Web Management: Enable

HTTP HTTPS

Port (Default: 443, Range: 1025 - 65535)

步驟8. 鍵入https://[WANIPAddress]:port (其中WAN IP地址是路由器的實際WAN IP地址)，然後輸入:port (在本節的步驟5中設定的埠號)，確認您可以訪問路由器的網路配置頁。在本例中，我們輸入了https://24.220.x.x:6000，但您要包括實際數字而不是x。x用於隱藏我們的公共WAN IP地址。

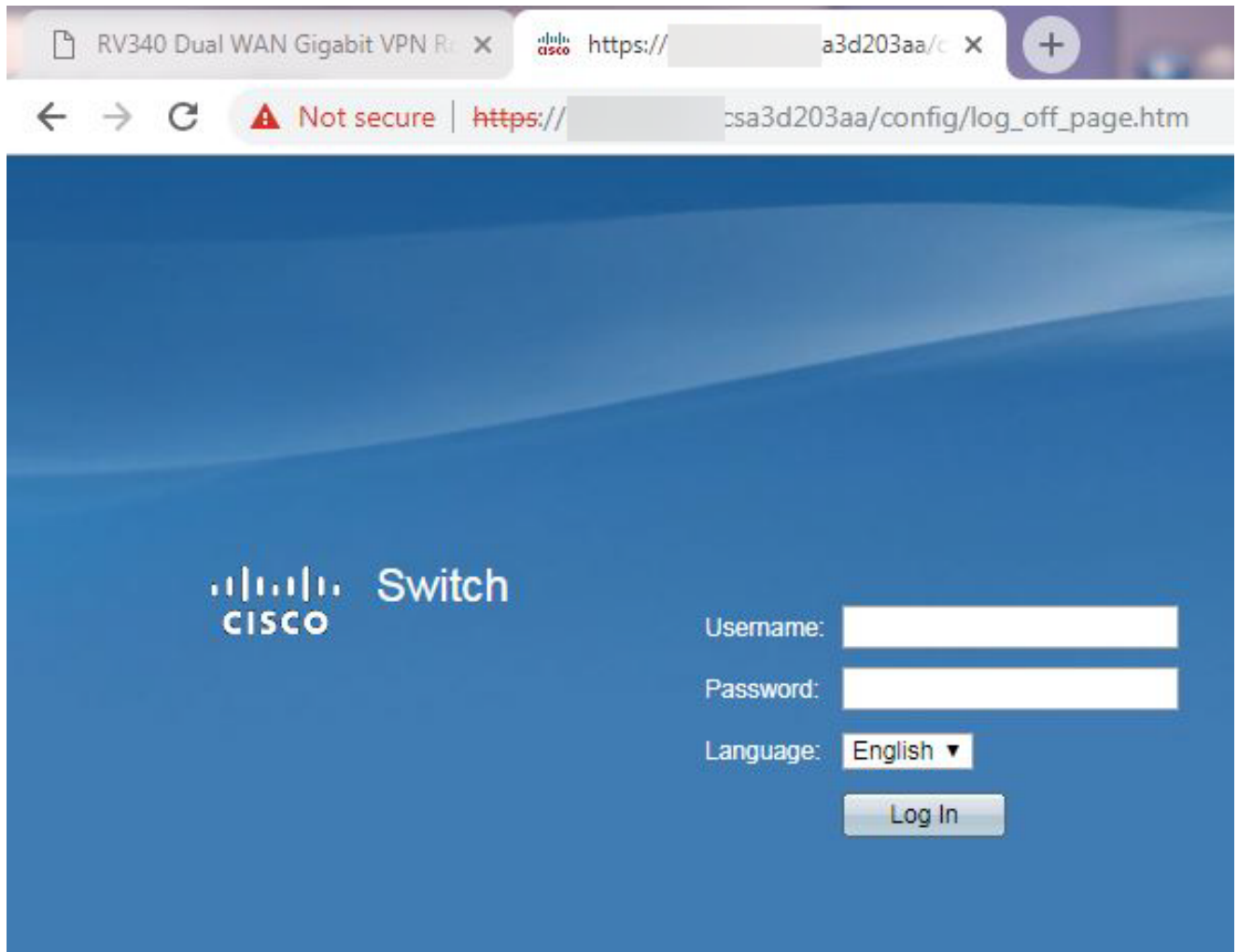
附註：確保您退出VPN，有時VPN不允許您訪問Web配置頁面。



步驟9. 您現在應該能夠使用WAN IP地址訪問DMZ埠中裝置的網路配置頁面，而無需新增埠號。

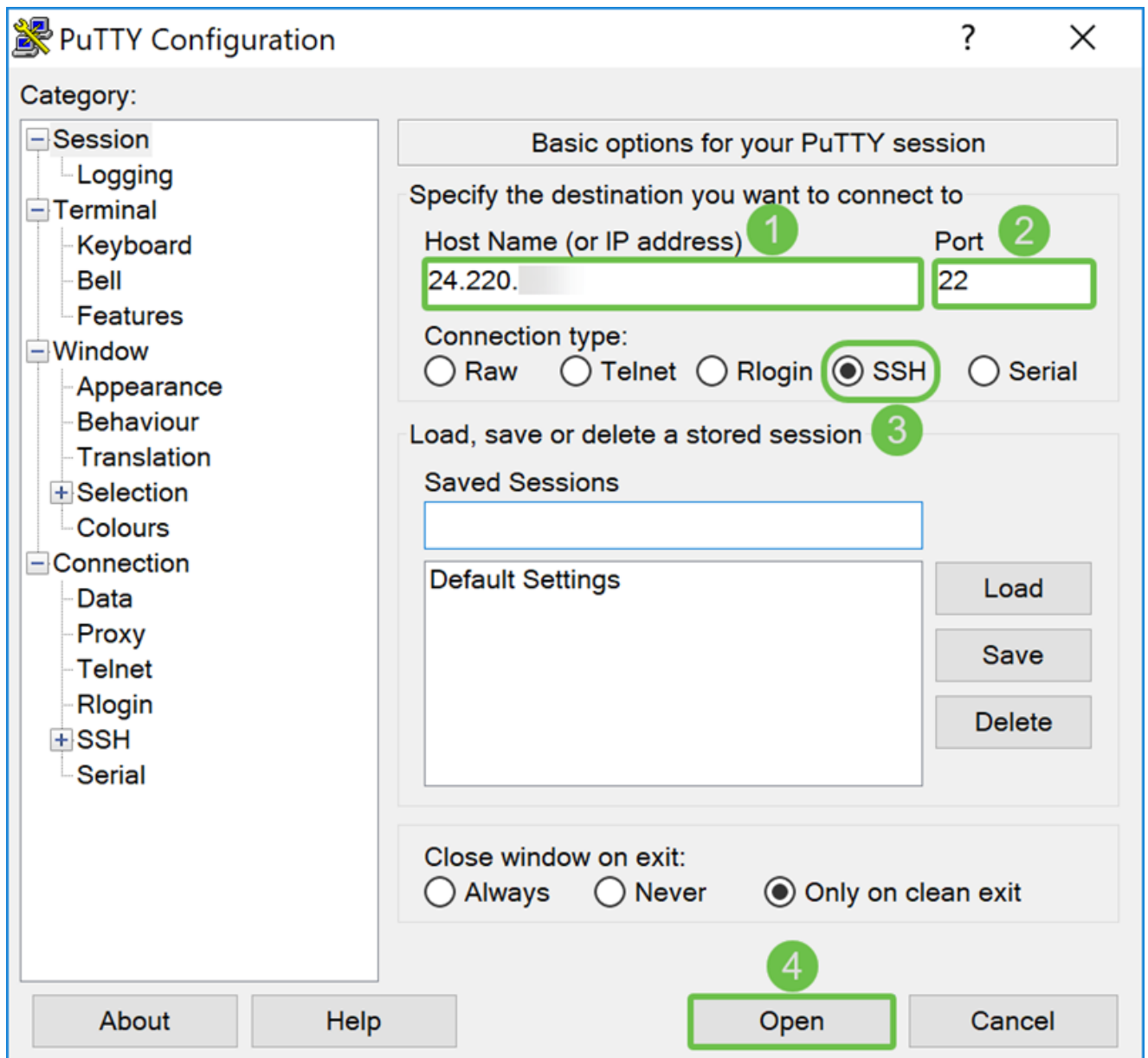
https://24.220.x.x:6000 — 將顯示路由器的web配置頁面。

https://24.220.x.x — 將顯示交換機的web配置頁面。

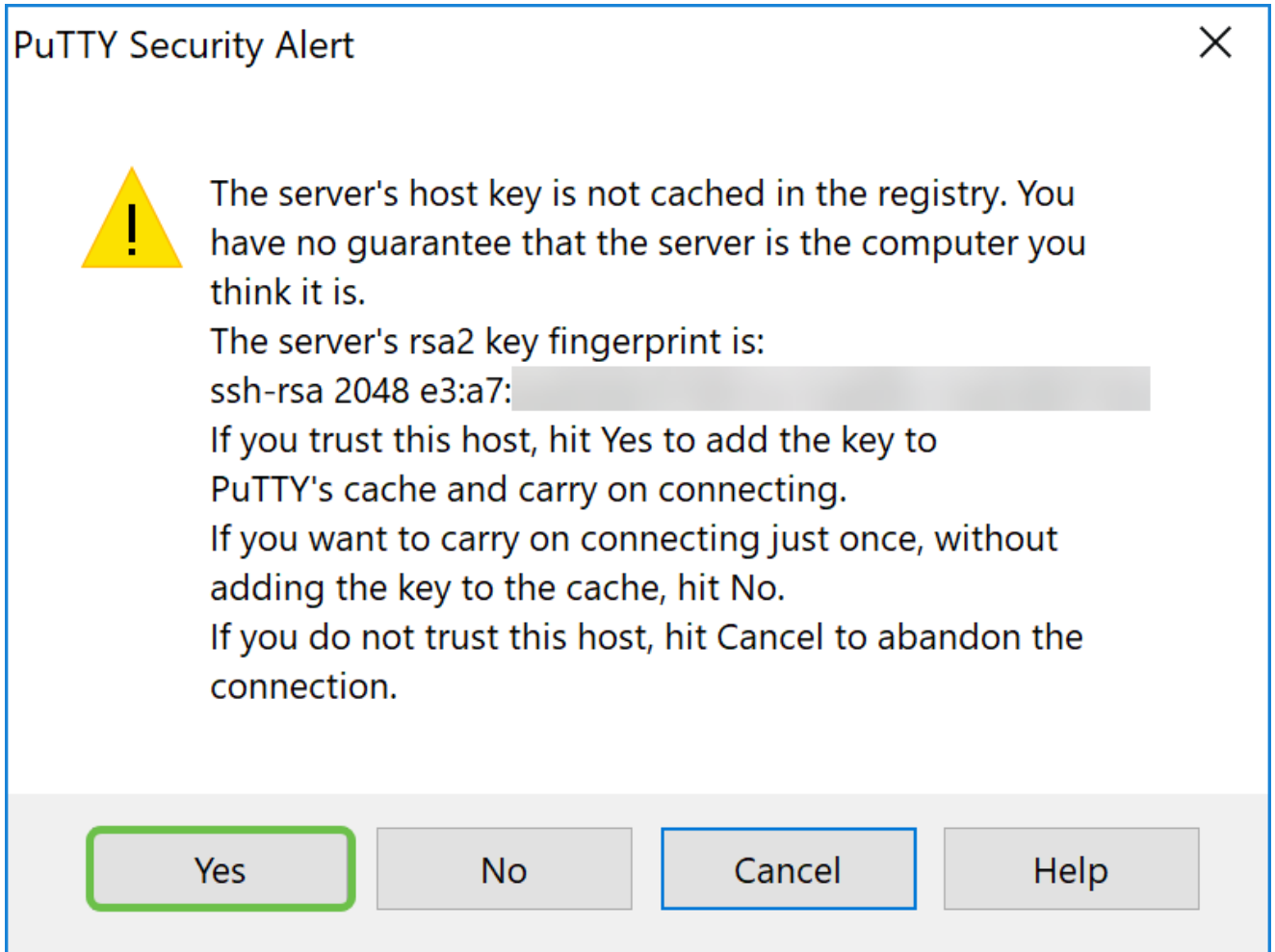


步驟10.我們將使用PuTTY通過SSH連線到交換機。在 *Host Name(或IP address)* 欄位中輸入裝置的公用IP地址。確保輸入了埠22並選擇了SSH。按一下Open開始連線。

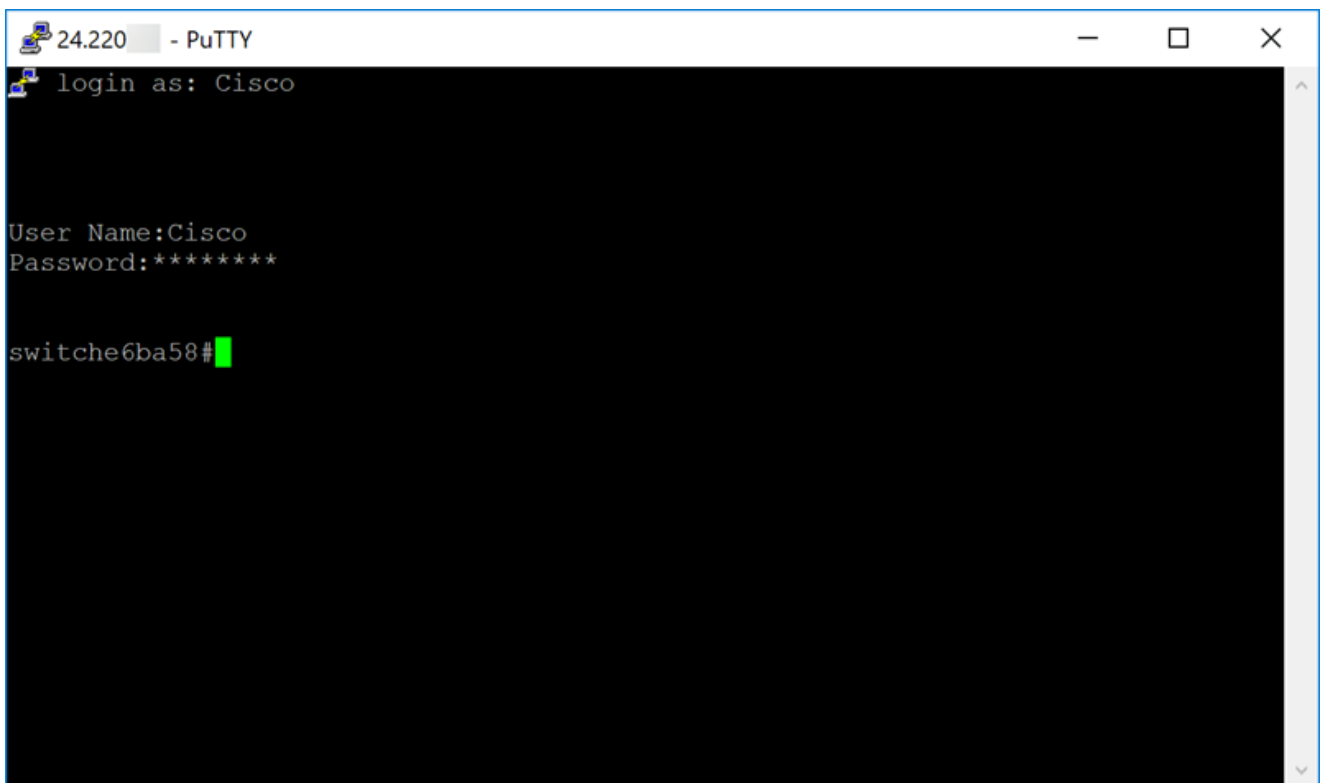
附註：如果您想通過SSH連線到交換機，請記得首先在交換機上啟用SSH。在大多數交換機中，可以導航到**安全 > TCP/UDP服務**以啟用**SSH服務**。要使用Windows進行SSH，您可以下載PuTTY。有關以下專案的詳細資訊，請參閱以下檔案：[如何使用SSH或Telnet訪問SMB交換機CLI](#)。建議使用SSH，但Telnet不是SSH，因為SSH更安全。



步驟11.可能出現PuTTY安全警報。按一下Yes繼續連線。



步驟12.如果連線成功，系統將提示您使用憑證登入。



配置硬體DMZ

步驟1。如果要設定硬體DMZ而不是DMZ主機，請導覽至WAN > Hardware DMZ。



Getting Started



Status and Statistics



Administration



System Configuration



WAN

1

WAN Settings

Multi-WAN

Mobile Network

Dynamic DNS

Hardware DMZ

2

IPv6 Transition



LAN



Routing



Firewall

步驟2.勾選**Enable**覈取方塊以將LAN4變更為DMZ連線埠。

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

步驟3.將出現警告消息。按一下**Yes**以接受路由器對DMZ連線埠(LAN4)所做的變更，或按一下**No**以拒絕變更。

當啟用時設定DMZ時，DMZ連線埠(LAN4)組態將會自動變更，如下所示：

從LAG埠刪除 (「LAN > 埠設定」部分)

如果Port Mirror Destination是DMZ Port (LAN > Port Settings一節)，將禁用埠映象功能

從埠映象的監視埠刪除 (「LAN > 埠設定」一節)

管理狀態變為「強制授權」 (「LAN > 802.1X」一節)

「VLANs to Port Table」表中的DMZ埠值將更改為「Exclude」 (「LAN > VLAN Membership」部分)

在本例中，我們將按一下**Yes**。

Warning Message



When DMZ is enable, the DMZ Port(LAN4) configuration will be changed automatically as follows:

- Remove from LAG port (Section "LAN > Port Settings")
- Will disable Port Mirror function, if Port Mirror Destination is DMZ Port (Section "LAN > Port Settings")
- Remove from Monitoring Port of Port Mirror (Section "LAN > Port Settings")
- Administrative Status to "Force Authorized" (Section "LAN > 802.1X")
- Value of DMZ port in table "VLANs to Port Table" will change to "Exclude" (Section "LAN > VLAN Membership")

Yes

No

步驟4.選擇子網或範圍 (同一子網中的DMZ和WAN)。 在本例中，我們將選擇Subnet。

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

步驟5.輸入DMZ IP Address和Subnet Mask。插入LAN4網段的任何裝置都必須位於此網路中。

附註：確保連線到DMZ埠的裝置具有該靜態IP地址。此IP地址可能需要位於您的WAN子網之外。

在本例中，我們將為DMZ使用公共IP地址。

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address: 1

Subnet Mask: 2

Range (DMZ & WAN within same subnet)

IP Range: to

附註：如果您打算使用Range方法，則需要按一下Range單選按鈕，然後輸入ISP分配的IP地址範圍。當您擁有來自ISP的多個公有IP地址用於DMZ網路中的多個裝置時，通常使用此方法。

如果您只有一個公有IP地址，但子網不起作用，請在IP範圍欄位下的兩個欄位中輸入一個公有IP地址。IP地址需要與WAN IP子網不同的可用IP，它不能使用WAN IP地址。例如，如果為您提供的單個公有IP地址為24.100.50.1，與您的WAN IP地址位於同一子網內，則在「IP範圍」欄位中輸入24.100.50.1到24.100.50.1。

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

1 Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: 2 to

步驟6.按一下右上角的**Apply**接受DMZ設定。

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

您應該已經成功啟用硬體DMZ。

步驟7. (可選) 若要驗證這一點，請在您的PC上開啟命令提示符，方法是導航到左下方的搜尋欄並輸入**命令提示**。當出現**command prompt**應用程式時，按一下該應用程式。

附註：本示例使用Windows 10。



Filters



Best match

2



Command Prompt

App



1

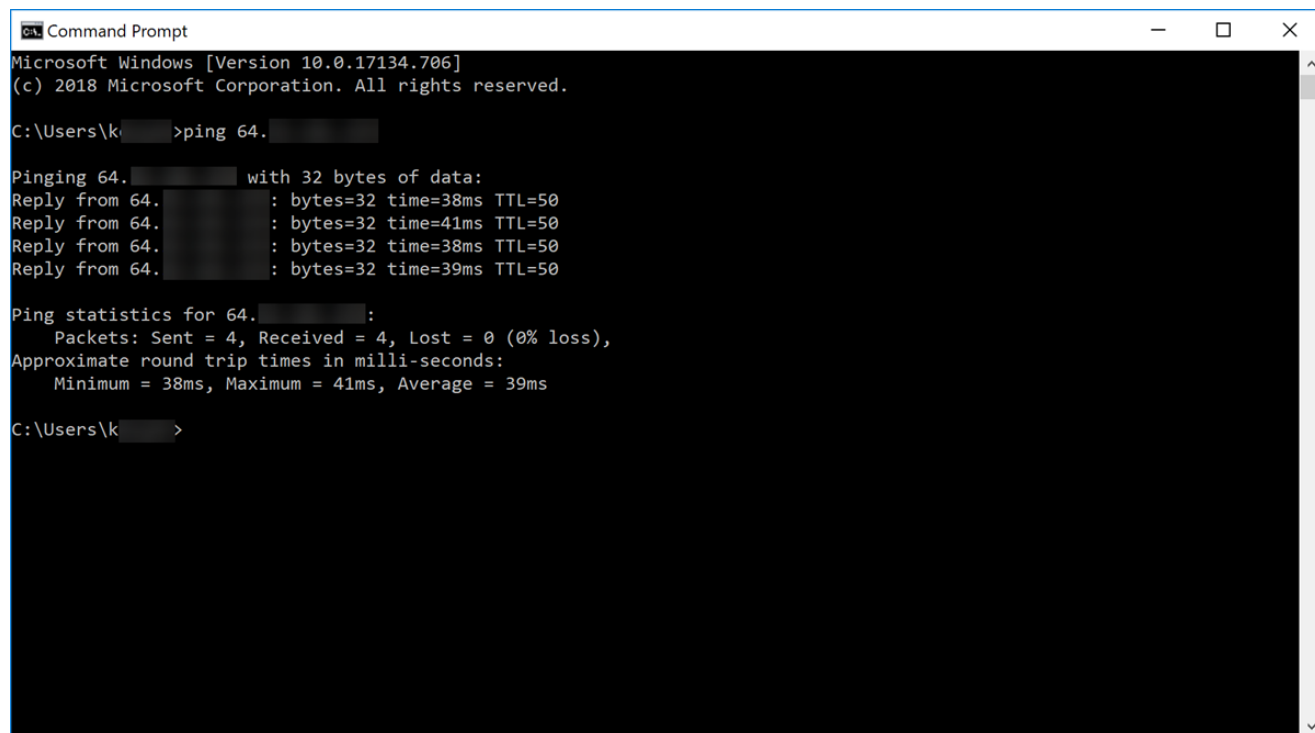


command prompt

步驟8. (可選) 將打開命令提示符視窗。我們將對DMZ IP地址執行ping命令，以檢視是否存在任何連線。使用**ping DMZ_IP_Address**命令。啟動ping時，按下**enter**鍵。如果您收到來自該IP地址的回覆，則意味著您與DMZ之間具有連線。如果您收到任何型別的消息，例如「請求超時」或「目標主機無法訪問」，則應檢查您的配置和連線。

在本例中，我們將鍵入ping **64.x.x.x.x**。64.x.x.x是我們的DMZ公有IP地址。

附註：請閱讀這份出色的文檔：[RV160和RV260路由器故障排除](#)。本故障排除文檔將涵蓋排除連線故障時需要分析的一些方面。即使本文檔適用於RV160和RV260，您仍可以在其中使用一些類似的故障排除步驟。



```
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\k... >ping 64.

Pinging 64. with 32 bytes of data:
Reply from 64. : bytes=32 time=38ms TTL=50
Reply from 64. : bytes=32 time=41ms TTL=50
Reply from 64. : bytes=32 time=38ms TTL=50
Reply from 64. : bytes=32 time=39ms TTL=50

Ping statistics for 64.:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 41ms, Average = 39ms

C:\Users\k... >
```

步驟9. (可選) 我們也可以執行tracert命令來檢視封包到達目的地所行經的路徑。使用**tracert DMZ_IP_Address**命令並按**Enter**鍵啟動進程。在此範例中，我們可以看到追蹤過程在抵達終端的DMZ IP位址時已完成。到達目的地後，也會顯示「跟蹤完成」。

```
Command Prompt
Microsoft Windows [Version 10.0.17134.706]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\k...>tracert 64.

Tracing route to ip-64-... [64. ]
over a maximum of 30 hops:

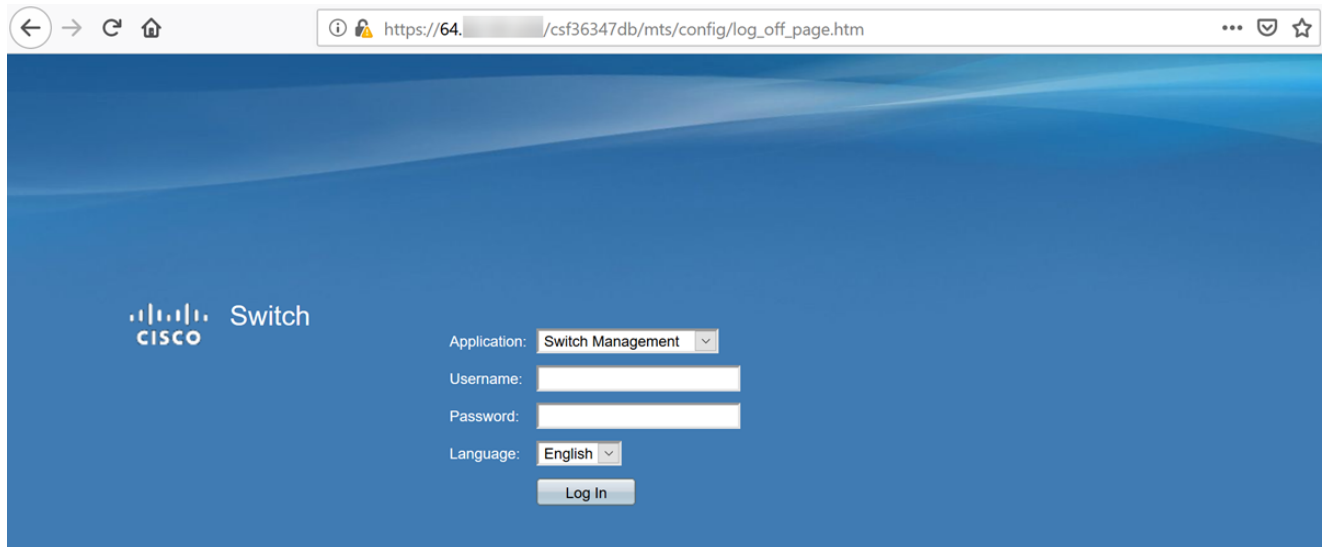
  1    3 ms    4 ms    3 ms  testwifi.here [192.168.86.1]
  2   14 ms   15 ms   18 ms  96.
  3   15 ms   14 ms   13 ms  po- [68. ]
  4   73 ms   40 ms   54 ms  be- [162. ]
  5   40 ms   23 ms   62 ms  be- [68. ]
  6   17 ms   16 ms   17 ms  be- [68. ]
  7   18 ms   19 ms   22 ms  be- [68. ]
  8   23 ms   23 ms   20 ms  173.
  9   18 ms   16 ms   16 ms  xe- [89. ]
 10   17 ms   15 ms   20 ms  ae22- [173. ]
 11   21 ms   25 ms   28 ms  ae22- [173. ]
 12   23 ms   22 ms   22 ms  xe-7- [89. ]
 13   24 ms   22 ms   22 ms  ip4. [173. ]
 14   24 ms   21 ms   22 ms  66.
 15   37 ms   *       31 ms  216- [216. ]
 16   28 ms   28 ms   27 ms  ip- [64. ]
 17   30 ms   30 ms   26 ms  ip- [64. ]

Trace complete.

C:\Users\keyven>
```

步驟10。(可選)在本範例中，有一個交換器連線到DMZ連線埠，其靜態IP位址為64.x.x.x (公共IP位址)。通過在頂部的瀏覽器中輸入公共IP地址，可以嘗試訪問交換機的圖形使用者介面(GUI)。

已輸入https://64.x.x.x，並進入交換器的GUI頁面。



現在，您應該瞭解幾種方法以驗證DMZ是否正常工作。

配置訪問規則 (可選)

如果您已為硬體DMZ配置公用IP地址或IP地址範圍，本節將向您展示如何為DMZ配置訪問規則的示例。DMZ應正常工作，而無需配置訪問規則。配置訪問規則是可選的，但建議將其配置為提供訪問網路的基本安全級別。例如，如果預設情況下不配置訪問規則，則允許通過路由器的所有資料包到達網路的所有部分。訪問規則可以允許一台主機、IP地址範圍或網路，同時阻止另一台主機、IP地址範圍或網路訪問同一區域 (主機或網路)。通過使用訪問規則，我們可以確定在路由器介面轉發或阻止哪些型別的流量。

步驟1.導覽至Firewall > Access Rules。



System Configuration



WAN



LAN



Routing



Firewall 1

Basic Settings

Access Rules 2

Network Address Translation

Static NAT

Port Forwarding

Port Triggering

Session Timeout




DMZ Host



VPN

步驟2.在IPv4訪問規則表中，按一下**Plus**圖示新增新的IPv4訪問規則。

IPv4 Access Rules Table

  	Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination
	1001	<input checked="" type="checkbox"/>	Allowed	IPv4: Pi-Prob...	WAN1	Any	VLAN	10.2.0.120
	4001	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any
	4002	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any

步驟3.確保選中**Enable**覈取方塊。這將啟用規則。

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

步驟4.在Action欄位中，在下拉式清單中選擇**Allow**。

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

步驟5.在 *Services* 欄位中選擇服務。我們將以所有流量形式保留。

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

Schedule Name:

- All Traffic
- BGP
- DNS-TCP
- DNS-UDP
- ESP
- FTP
- HTTP
- HTTPS
- ICMP Destination Unreachable
- ICMP Ping Reply
- ICMP Ping Request
- ICMP Redirect Message
- ICMP Router Advertisement
- ICMP Router Solicitation
- ICMP Source Quench

步驟6.從下拉選單中選擇 **Never** 或 **True**

True — 匹配規則。

Never — 不需要日誌。

在本例中，我們將將其保留為**True**。

Rule Status:	<input checked="" type="checkbox"/> Enable
Action:	Allow
Services:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 All Traffic
Log:	True
Source Interface:	WAN1
Source Address:	Any
Destination Interface:	WAN1
Destination Address:	Any

步驟7.從下拉選單中選擇 *Source Interface* 和 *Source Address*。

在本範例中，選擇了 **DMZ** 和 **Any**。

Rule Status:	<input checked="" type="checkbox"/> Enable
Action:	Allow
Services:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 All Traffic
Log:	True
Source Interface:	DMZ 1
Source Address:	Any 2
Destination Interface:	WAN1
Destination Address:	Any

步驟8.從下拉選單中選擇 *Destination Interface* 和 *Destination Address*。

在本範例中，選擇了 **DMZ** 和 **Any**。

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface: 1

Destination Address: 2

步驟9.在 *Scheduling* 部分，從下拉選單中選擇一個時間以應用防火牆規則。如果要配置自己的計畫，請按一下 [此處連結](#)。

在本例中，我們將使用 **ANYTIME** 作為計畫。

Scheduling

Schedule Name: Click [here](#) to configure the schedules

步驟10.按一下 **Apply** 新增新規則。此規則表示將允許流向任何DMZ的任何DMZ流量。

Access Rules

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Scheduling

Schedule Name: Click [here](#) to configure the schedules

這裡是一個建立的示例。您可以看到，我們在規則中新增了DMZ無法與VLAN 1中的任何目的

地進行通訊的規則。這是因為我們不希望DMZ能夠訪問VLAN 1中的任何內容。

IPv4 Access Rules Table

Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination	Schedule	Configure
1	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	DMZ	Any	DMZ	Any	ANYTIME	▲ ▼ ⚙
2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN1	Any	Any	Any	ANYTIME	▲ ▼ ⚙
3	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	DMZ	Any	VLAN1	Any	ANYTIME	▲ ▼ ⚙
1001	<input checked="" type="checkbox"/>	Allowed	IPv4: Pi-Probe-2	WAN1	Any	VLAN	10.2.0.120	ANYTIME	
4001	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any	ANYTIME	
4002	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any	ANYTIME	

使用路由器檢驗

步驟1。若要確認您的裝置是否已連線路由器上的DMZ連線埠，請導覽至**Status & Statistics**，該頁面將會自動載入**System Summary**頁面。連線埠4或LAN 4會將DMZ的狀態列為「UP」。

。

Port Status

Port ID	1	2	3	4/DMZ	Internet	Internet	USB	USB
Interface	LAN	LAN	LAN	LAN	WAN1	WAN2	USB1	USB2
Link Status	↓	↑	↓	↑	↓	↑	↓	↓
Speed	--	1000Mbps	--	1000Mbps	--	1000Mbps	N/A	N/A

對裝置的IP執行ping操作將讓我們知道裝置的可達性狀態。使用使用的公用IP地址驗證任何特定服務/埠的DMZ配置是有益的。

步驟2.導覽至**Administration > Diagnostic**。



Getting Started



Status and Statistics



Administration

1

File Management

Reboot

Diagnostic

2

Certificate

Configuration
Management



System Configuration

步驟3.輸入DMZ的IP地址，然後點選Ping按鈕。

在本示例中，我們將使用在[DMZ主機](#)部分中配置的DMZ的IP地址。

附註：如果ping成功，您將看到如下所示的消息。如果ping失敗，則表示無法訪問DMZ。檢查您的DMZ設定，確保它們配置正確。

Ping or Trace on IP Address

IP Address/Domain Name: (e.g.: 1.2.3.4 or abc.com or fe80::10)

```
64 bytes from 10.1.1.2: icmp_seq=0 ttl=64 time=0.543 ms
64 bytes from 10.1.1.2: icmp_seq=1 ttl=64 time=0.331 ms
64 bytes from 10.1.1.2: icmp_seq=2 ttl=64 time=0.332 ms
64 bytes from 10.1.1.2: icmp_seq=3 ttl=64 time=0.326 ms
```

結論

完成DMZ設定後，您應該能夠從LAN外部訪問服務。