

Configurazione della DMZ sul router serie RV34x

Obiettivo

L'obiettivo di questo documento è mostrare come configurare la DMZ (Demilitarized Zone) per host e hardware sui router serie RV34x.

Introduzione

Una zona demilitarizzata è una posizione in una rete aperta a Internet che protegge la rete locale (LAN) da un firewall. La separazione della rete principale da un singolo host o da un'intera sottorete o "subnet" garantisce che gli utenti che visitano il servizio, ad esempio i videogiochi Internet, le videoconferenze, il Web o i server di posta elettronica tramite la DMZ, non abbiano accesso alla LAN. Cisco offre due metodi per utilizzare le DMZ, ovvero Host DMZ e DMZ hardware. L'host DMZ consente a un host della LAN di essere esposto a Internet, mentre la DMZ hardware (subnet/intervallo) è una sottorete aperta al pubblico.

Per pianificare la DMZ è possibile utilizzare un indirizzo IP pubblico o privato. Un indirizzo IP privato è univoco solo per l'utente che utilizza la rete LAN. Un indirizzo IP pubblico sarà univoco per l'organizzazione e verrà assegnato dal provider di servizi Internet (ISP). Per ottenere un indirizzo IP pubblico, è necessario contattare l'ISP.

La maggior parte degli utenti utilizza la DMZ hardware perché imposta automaticamente una VLAN e il proprio segmento di rete. Per "Hardware DMZ" stiamo utilizzando l'opzione subnet o range. L'host DMZ è più semplice da configurare poiché non è necessario configurare le regole di accesso, ma è meno sicuro.

WAN-to-DMZ è il caso di utilizzo più comune, così come LAN-to-DMZ. È inoltre consentita la DMZ-to-WAN, poiché le macchine DMZ potrebbero richiedere patch o aggiornamenti del sistema operativo, ma la DMZ-to-LAN dovrebbe essere bloccata perché potrebbe rappresentare un potenziale problema di sicurezza. Ad esempio, gli hacker su Internet utilizzano DMZ come server jumper.

La differenza tra host DMZ e DMZ hardware in termini di utilizzo è la seguente:

Se si desidera esporre qualcosa a Internet, ma si dispone di un server all-in-one o non si dispone di indirizzi IP pubblici di riserva, è consigliabile utilizzare Host DMZ. Posizionare il server in una delle VLAN e configurarlo come host DMZ. L'utente esterno può quindi accedere al server tramite l'IP WAN del router.

Se si desidera esporre qualcosa a Internet e si dispone di più server (ciascuno con un servizio specifico) e della stessa quantità di indirizzi IP pubblici, è consigliabile utilizzare DMZ hardware. Collegare questi server alla porta DMZ specificata (ad esempio, LAN 4 per RV340) e configurarli con gli stessi indirizzi IP pubblici configurati nel router o nella subnet. L'utente esterno potrà quindi accedere a ciascuno dei server tramite gli indirizzi IP specificati.

DMZ	Confronta	Contrasto
Host	Separa il	Host singolo,

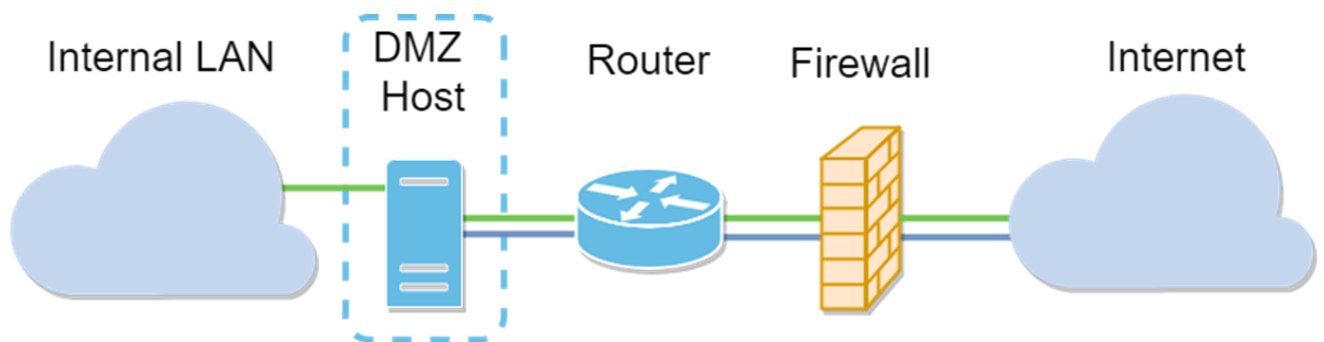
	traffico	completamente aperto a Internet
Subnet/Intervallo	Separa il traffico	Più dispositivi e tipi, completamente aperti a Internet.

Nota: Nell'esempio, uno switch sarà collegato alla porta DMZ del router durante la configurazione della subnet DMZ.

per informazioni su come abilitare SSH su uno switch, fare riferimento a questo articolo: [Abilitazione del servizio SSH sugli switch gestiti serie 300/500.](#)

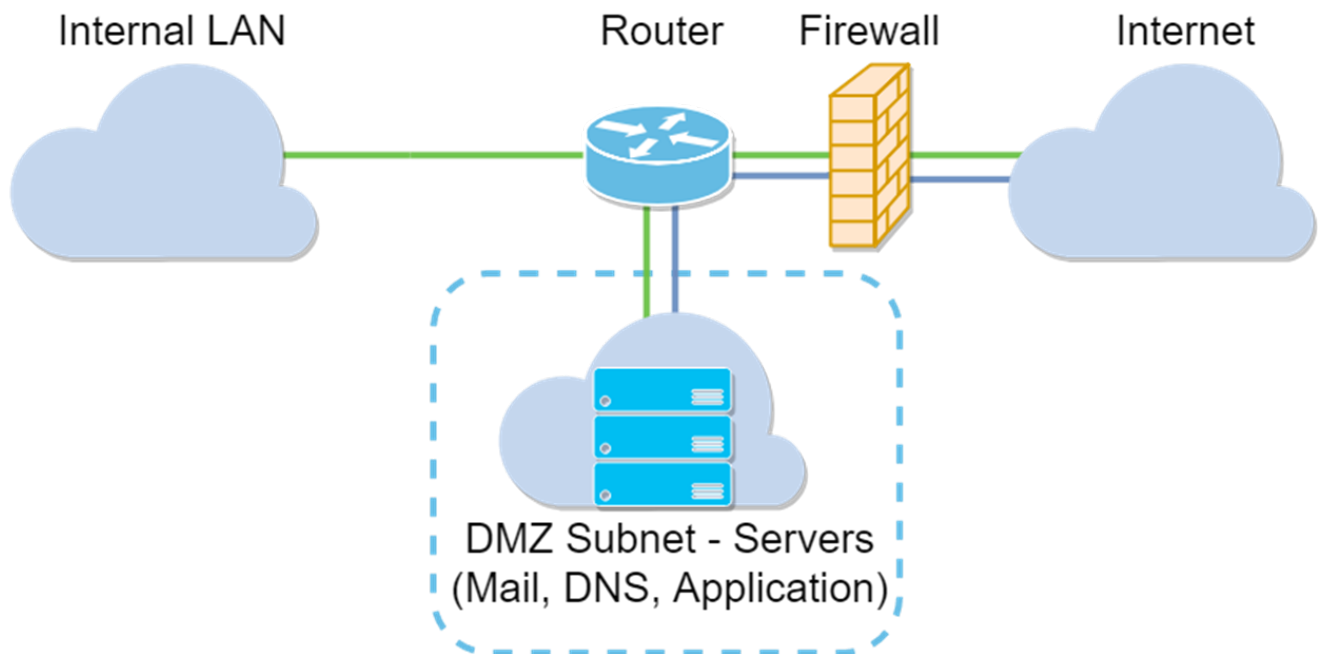
Per informazioni su come configurare DMZ su RV160/RV260, vedere questo articolo: [Opzioni DMZ per router RV160/RV260.](#)

Topologia DMZ host



Nota: Quando si utilizza una DMZ dell'host, se l'host è compromesso da un fattore dannoso, la LAN interna potrebbe essere soggetta a ulteriori intrusioni.

Topologia Subnet DMZ



Dispositivi interessati

RV34x

Versione del software

1.0.02.16

Configurazione dell'host DMZ

Passaggio 1. Accedere alla pagina di configurazione Web del router.



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.

Passaggio 2. Passare a **Firewall > Host DMZ**.



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

Passaggio 3. Nel campo *Host DMZ*, selezionare la casella di controllo **Abilita** per abilitare Host DMZ.

DMZ Host

DMZ Host: Enable

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

Passaggio 4. Immettere l'indirizzo IP dell'host nella *DMZ* che verrà esposto a Internet per l'utilizzo di servizi quali giochi Internet, videoconferenze, Web o server di posta elettronica.

Nota: Affinché la funzionalità host DMZ funzioni correttamente, è necessario assegnare all'host LAN DMZ un indirizzo IP fisso o statico. Accertarsi che si trovi sulla stessa rete del router. È possibile configurare questa condizione anche quando la DMZ si trova su un'altra VLAN.

DMZ Host

DMZ Host: Enable

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

Passaggio 5. Fare clic su **Apply** save the configuration (Applica e salva la configurazione).

DMZ Host

Enable

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

A questo punto è necessario aver abilitato correttamente l'host DMZ.

Passaggio 6. (Facoltativo) Nei passaggi successivi, verrà visualizzato un modo per verificare l'host DMZ. Passare a **Firewall > Impostazioni di base**.



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

Passaggio 7. (Facoltativo) In questo esempio, *Gestione Web remota* è abilitata con **HTTPS** selezionato. In questo modo, è possibile accedere alla pagina di configurazione Web in remoto tramite l'indirizzo IP WAN. In questo passaggio verrà impostato il numero di porta **6000**. L'intervallo è compreso tra **1025 e 65535**.

Nota: Se la configurazione è stata eseguita durante l'accesso remoto alla pagina di gestione Web, la pagina potrebbe bloccarsi nella schermata di caricamento. Ciò significa che la porta è stata modificata in base alle modifiche apportate.

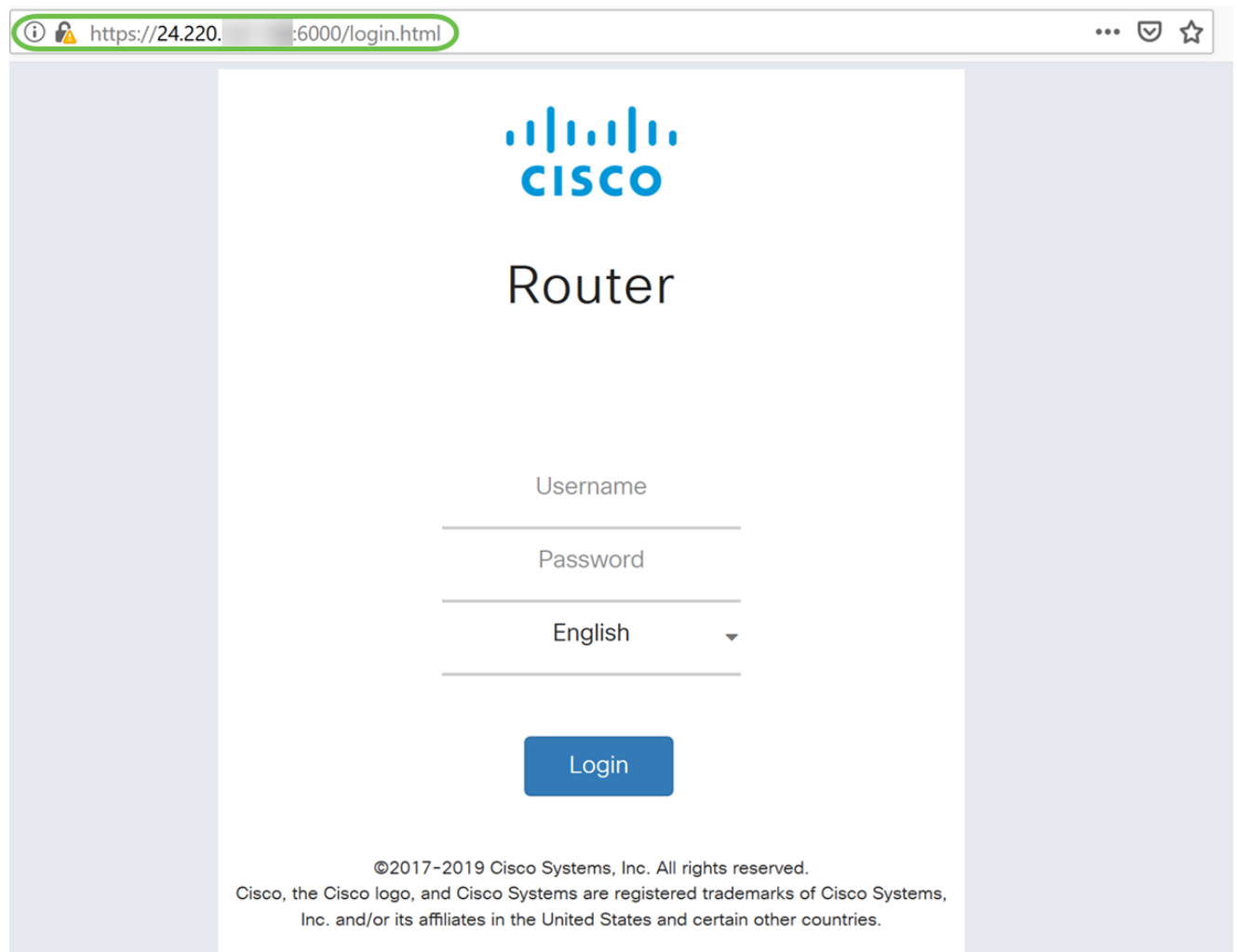
Remote Web Management: Enable

HTTP HTTPS

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

Passaggio 8. Verificare di poter accedere alla pagina di configurazione Web del router digitando **https://[indirizzoIPWAN]:porta**, dove indirizzo IP WAN è l'indirizzo IP WAN effettivo del router e quindi **:porta** per il numero di porta impostato nel passaggio 5 per questa sezione. In questo esempio è stato immesso **https://24.220.x.x:6000**, ma è necessario includere i numeri effettivi e non **x**. La **x** sta per nascondere il nostro indirizzo IP WAN pubblico.

Nota: Accertati di non essere connesso alla VPN. A volte, essere connesso alla VPN non ti consente di accedere alla pagina di configurazione Web.

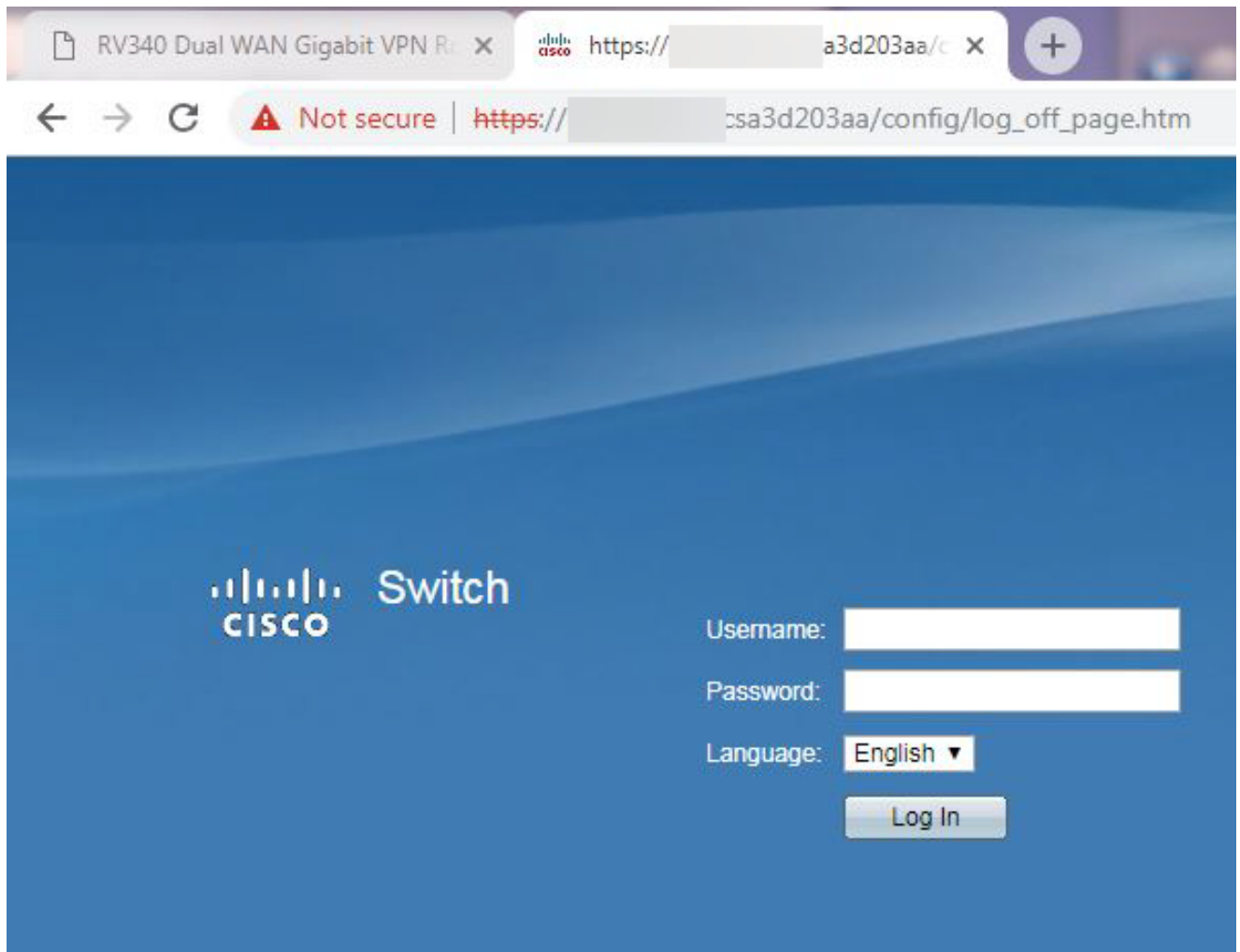


Passaggio 9. A questo punto, dovrebbe essere possibile accedere alla pagina di

configurazione Web del dispositivo nella porta DMZ utilizzando l'indirizzo IP WAN senza aggiungere il numero di porta.

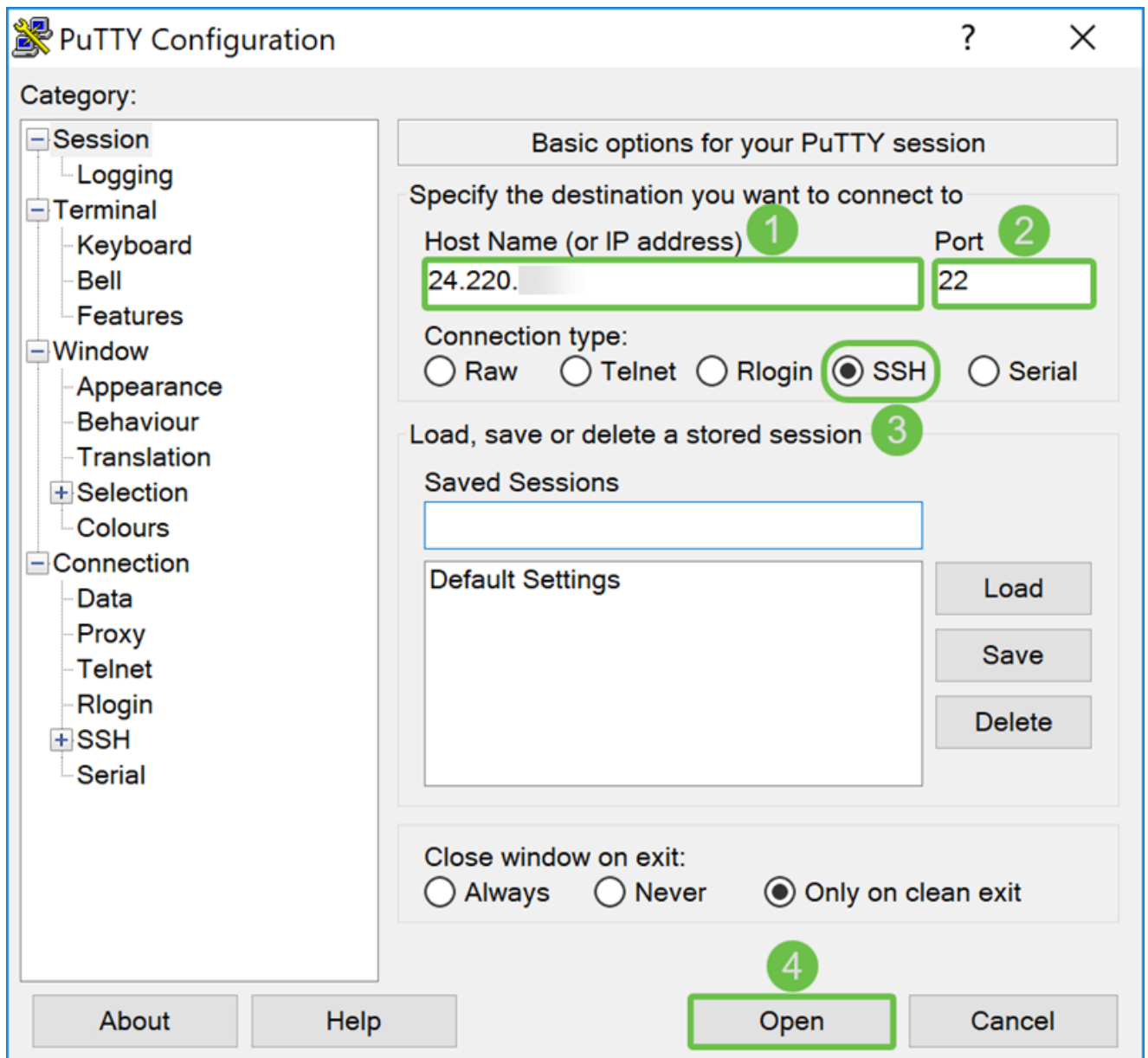
<https://24.220.x.x:6000> - visualizza la pagina di configurazione web del router.

<https://24.220.x.x> - visualizza la pagina di configurazione web dello switch.

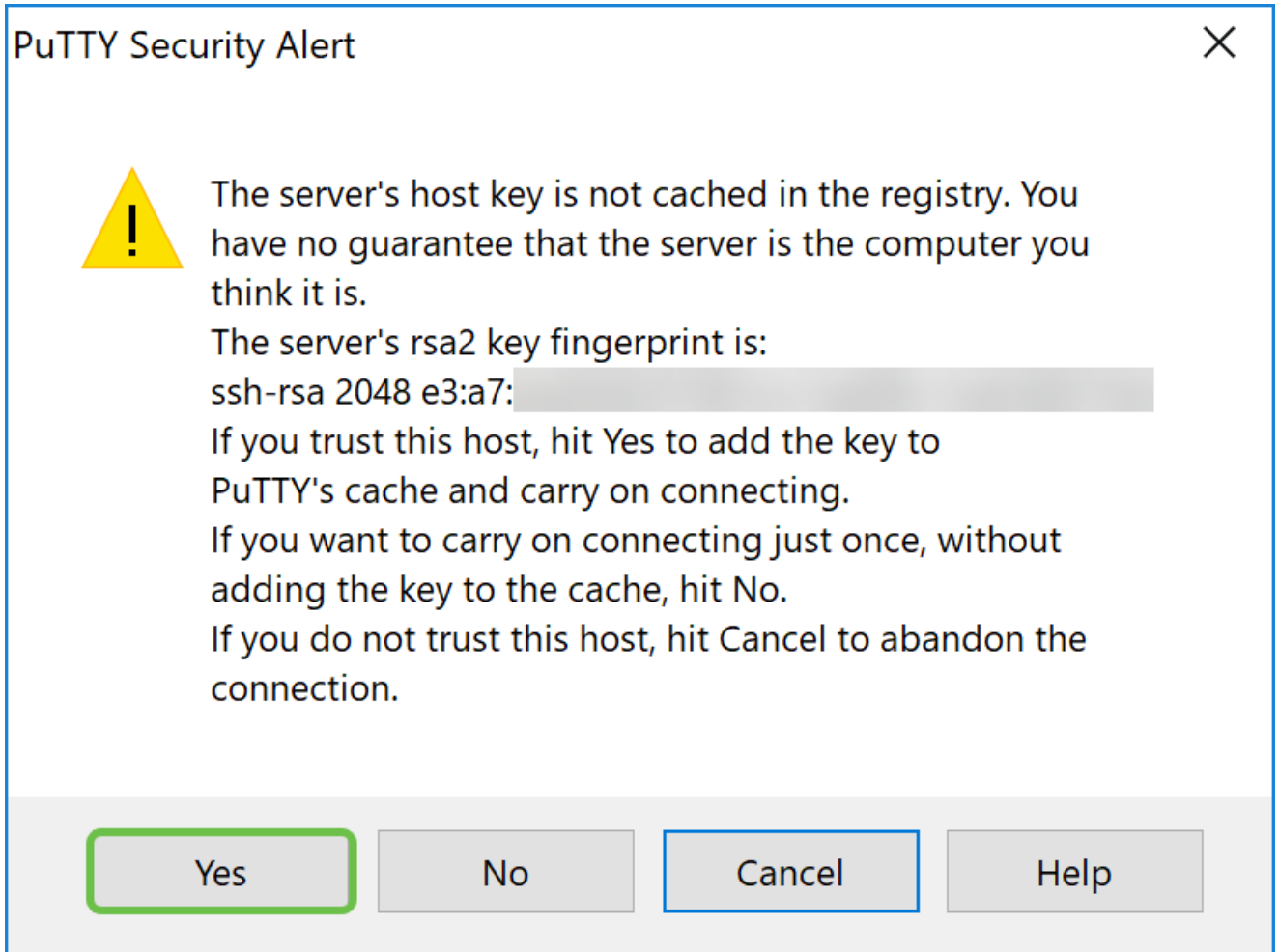


Passaggio 10. Useremo PuTTY per SSH sullo switch. Immettere l'**indirizzo IP pubblico** del dispositivo nel campo *Nome host (o indirizzo IP)*. Verificare che la porta **22** sia stata immessa e che **SSH** sia selezionato. Fare clic su **Apri** per avviare la connessione.

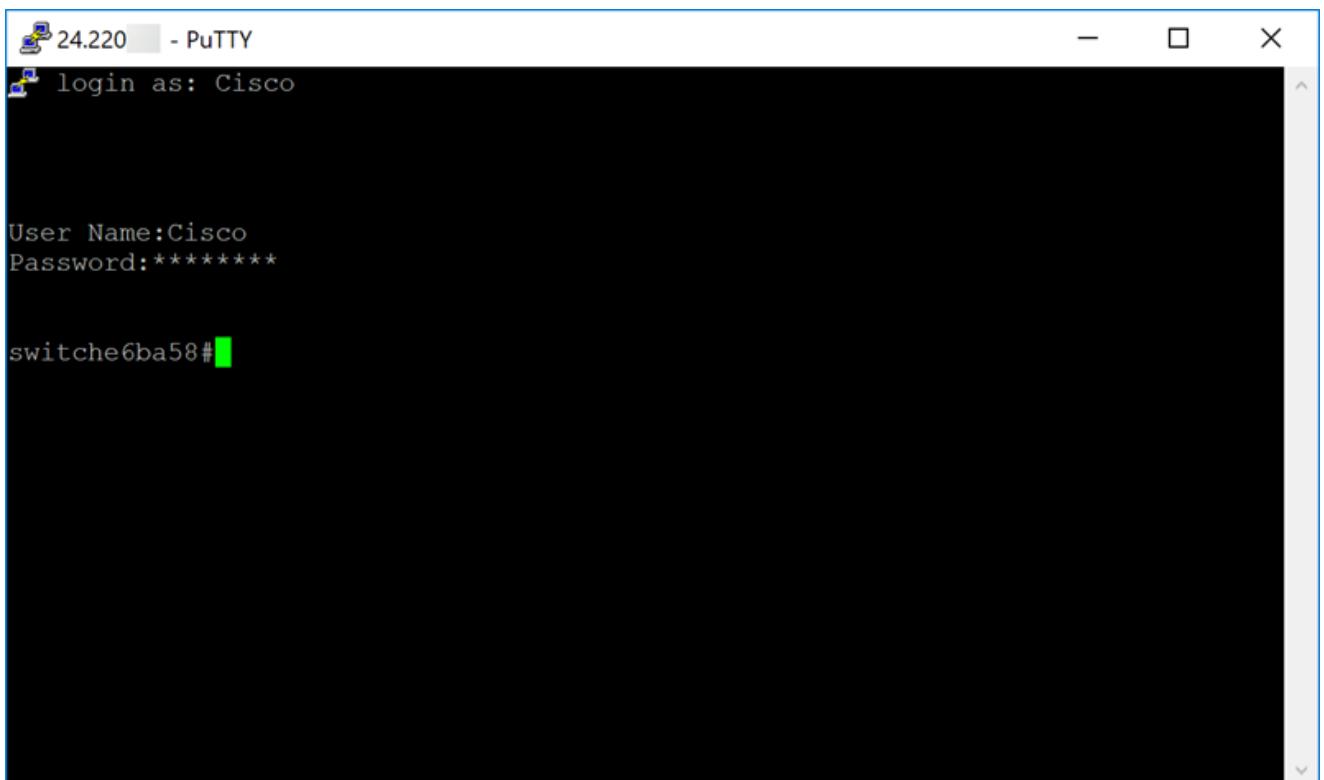
Nota: Per abilitare il protocollo SSH sullo switch, occorre prima abilitarlo. Nella maggior parte degli switch, è possibile selezionare **Security > TCP/UDP Services** (Sicurezza > Servizi TCP/UDP) per abilitare il **servizio SSH**. Per il protocollo SSH con Windows, è possibile scaricare PuTTY. Per ulteriori informazioni su: [Come accedere alla CLI di uno switch per PMI utilizzando SSH o Telnet](#). Si consiglia SSH e Telnet non perché SSH è più sicuro.



Passaggio 11. È possibile che venga visualizzato un *avviso di sicurezza PuTTY*. Fare clic su **Sì** per continuare la connessione.



Passaggio 12. Se la connessione ha esito positivo, verrà richiesto di eseguire l'accesso con le credenziali.



Configurazione di DMZ hardware

Passaggio 1. Se si desidera configurare la DMZ hardware anziché l'host DMZ, selezionare **WAN > DMZ hardware**.



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

Passaggio 2. Selezionare la casella di controllo **Enable** per modificare la porta LAN4 in DMZ.

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

Passaggio 3. Viene visualizzato un messaggio di avvertenza. Fare clic su **Sì** per accettare le modifiche che il router apporterebbe alla porta DMZ (LAN4) o su **No** per negarle.

Quando DMZ è impostato su enable, la configurazione della porta DMZ (LAN4) viene modificata automaticamente come segue:

Rimuovi dalla porta LAG (sezione "LAN > Impostazioni porta")

Disabilita la funzione Port Mirror se la destinazione Port Mirror è una porta DMZ (sezione "LAN > Impostazioni porta")

Rimuovi dalla porta di monitoraggio del mirroring della porta (sezione "LAN > Impostazioni porta")

Stato amministrativo su "Forza autorizzazione" (sezione "LAN > 802.1X")

Il valore della porta DMZ nella tabella "VLAN su tabella porte" verrà modificato in "Escludi" (sezione "LAN > Appartenenza VLAN")

In questo esempio verrà fatto clic su **Sì**.

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

Passaggio 4. Selezionare **Subnet** o **Range** (DMZ e WAN nella stessa subnet). In questo esempio verrà selezionata la **subnet**.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

Passaggio 5. Inserire l'**indirizzo IP** della **DMZ** e la **subnet mask**. Tutto ciò che è collegato al segmento LAN4 deve essere inserito in questa rete.

Nota: Verificare che il dispositivo collegato alla porta DMZ disponga di tale indirizzo IP statico. Potrebbe essere necessario che l'indirizzo IP sia esterno alla subnet WAN.

In questo esempio, verrà utilizzato un indirizzo IP pubblico per la DMZ.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address: 1

Subnet Mask: 2

Range (DMZ & WAN within same subnet)

IP Range: to

Nota: Se si intende utilizzare il metodo *Range*, sarà necessario fare clic sul pulsante di opzione **Range**, quindi immettere l'intervallo di indirizzi IP assegnato dall'ISP. Questa opzione viene in genere utilizzata quando l'ISP dispone di più indirizzi IP pubblici per più dispositivi nella rete DMZ.

Se si dispone di un solo indirizzo IP pubblico e la subnet non funziona, immettere l'indirizzo IP pubblico in entrambi i campi sotto il campo *Intervallo IP*. L'indirizzo IP deve essere un indirizzo IP libero diverso dalla subnet IP WAN, non può utilizzare l'indirizzo IP WAN. Ad esempio, se si ha un solo indirizzo IP pubblico di 24.100.50.1 che si trova all'interno della stessa subnet dell'indirizzo IP WAN, immettere **24.100.50.1 to 24.100.50.1** nel campo *Intervallo IP*.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

1 Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: **2** to

Passaggio 6. Fare clic su **Apply** (Applica) nell'angolo in alto a destra per accettare le impostazioni DMZ.

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

DMZ hardware dovrebbe essere stato abilitato correttamente.

Passaggio 7. (Facoltativo) Per verificare questa condizione, aprire il prompt dei comandi sul PC spostandosi sulla barra di ricerca in basso a sinistra e digitando **prompt dei comandi**. Fare clic sull'applicazione del **prompt dei comandi** quando viene visualizzata.

Nota: Per questo esempio viene utilizzato Windows 10.



Filters



Best match

2



Command Prompt

App



1

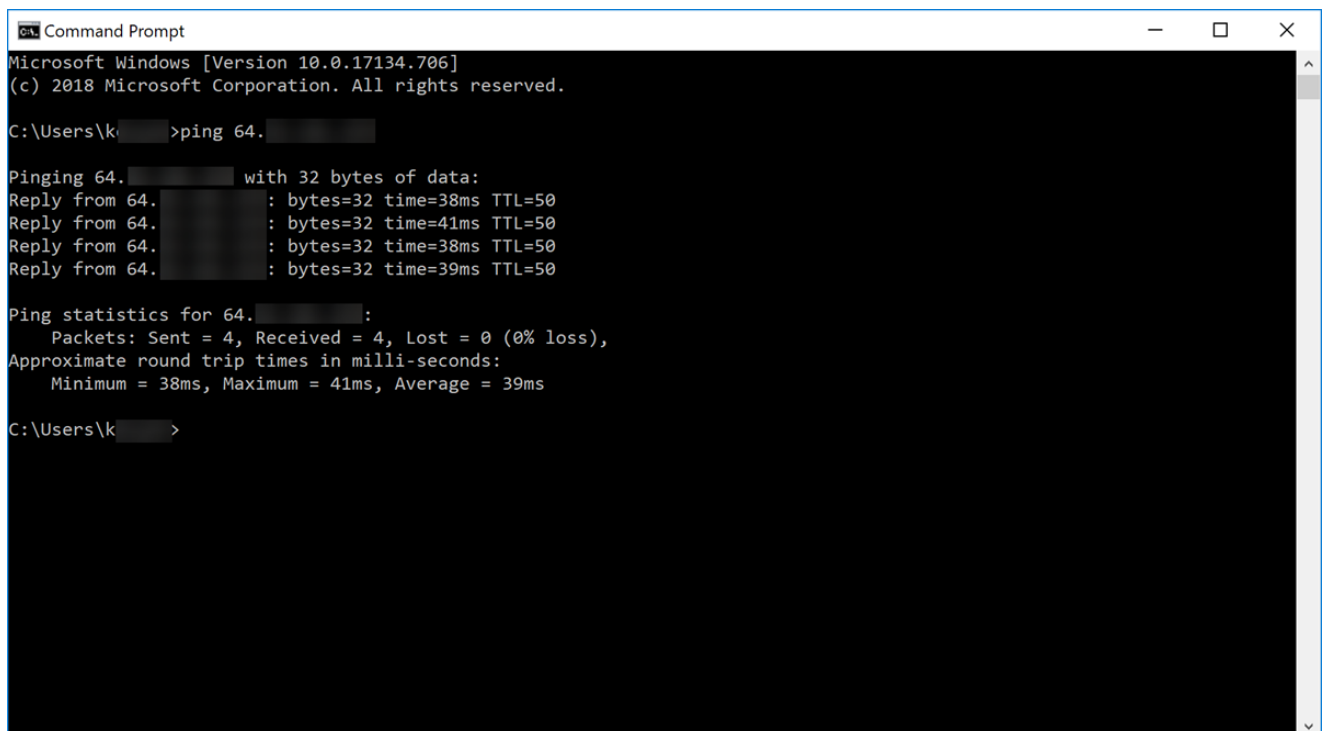


command prompt

Passaggio 8. (Facoltativo) Verrà visualizzata una finestra del *prompt dei comandi*. Verrà eseguito un comando ping sull'indirizzo IP DMZ per verificare se è disponibile connettività. Usare il comando **ping** *DMZ_IP_Address*. Premere **Invio** per avviare il ping. Se si ricevono risposte da quell'indirizzo IP, significa che si dispone di connettività tra l'utente e la DMZ. Se sono stati ricevuti messaggi del tipo "Richiesta scaduta" o "Host di destinazione irraggiungibile", verificare la configurazione e le connessioni.

Nell'esempio, verrà digitato ping **64.x.x.x**. 64.x.x.x è il nostro indirizzo IP pubblico per la DMZ.

Nota: Leggi questo fantastico documento: [Risoluzione dei problemi sui router RV160 e RV260](#). Questo documento di risoluzione dei problemi copre alcune aree da analizzare durante la risoluzione dei problemi di connettività. Anche se il presente documento è per RV160 e RV260, è possibile eseguire procedure di risoluzione dei problemi simili.



```
Command Prompt
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... >
```

Passaggio 9. (Facoltativo) È possibile anche eseguire un comando traceroute per verificare il percorso dei pacchetti alla destinazione. Usare il comando **tracert** *DMZ_IP_Address* e premere **Invio** per avviare il processo. Nell'esempio, la traccia è completa quando viene raggiunto l'indirizzo IP DMZ alla fine. Viene inoltre visualizzato "Trace complete" (Traccia completata) una volta raggiunto il punto di destinazione.

```
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:

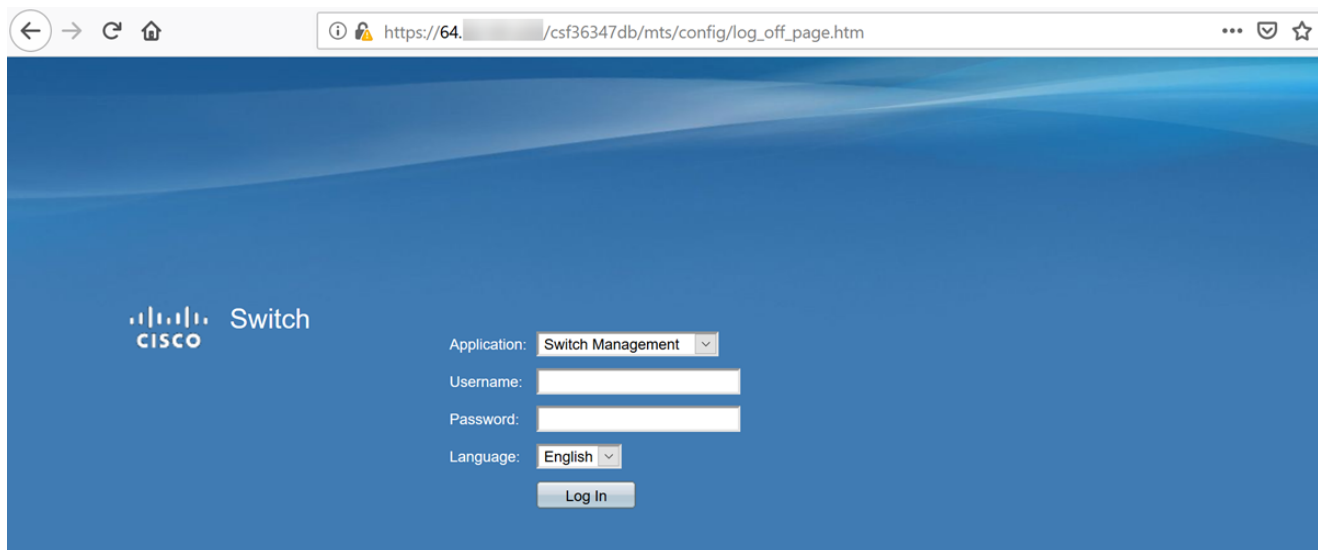
  1    3 ms    4 ms    3 ms  testwifi.here [192.168.86.1]
  2   14 ms   15 ms   18 ms  96. ...
  3   15 ms   14 ms   13 ms  po-... [68. ...]
  4   73 ms   40 ms   54 ms  be-... [162. ...]
  5   40 ms   23 ms   62 ms  be-... [68. ...]
  6   17 ms   16 ms   17 ms  be-... [68. ...]
  7   18 ms   19 ms   22 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>
```

Passaggio 10. (Facoltativo) Nell'esempio, è presente uno switch collegato alla porta DMZ con l'indirizzo IP statico 64.x.x.x (indirizzo IP pubblico). Per accedere all'interfaccia grafica dello switch, immettere l'indirizzo IP pubblico nel browser in alto.

È stato immesso <https://64.x.x.x>, che consente di accedere alla pagina GUI dello switch.



A questo punto, è necessario conoscere un paio di metodi per verificare che la DMZ funzioni correttamente.

Configurazione delle regole di accesso (facoltativo)

Se è stato configurato un indirizzo IP pubblico o un intervallo di indirizzi IP per la DMZ hardware, in questa sezione verrà illustrato un esempio di configurazione delle regole di accesso per la DMZ. DMZ dovrebbe funzionare correttamente senza dover configurare le regole di accesso. La configurazione delle regole di accesso è facoltativa, ma è consigliabile configurarla in modo da garantire un livello di protezione di base per l'accesso alla rete. Ad esempio, se non si configurano le regole di accesso per impostazione predefinita, tutti i pacchetti che passano attraverso il router potrebbero essere autorizzati a tutte le parti della

rete. Le regole di accesso possono consentire a un host, a un intervallo di indirizzi IP o a una rete di accedere alla stessa area (host o rete), impedendo a un altro host, a un intervallo di indirizzi IP o a una rete di accedere alla stessa area. Utilizzando le regole di accesso, possiamo decidere quali tipi di traffico inoltrare o bloccare sulle interfacce del router.

Passaggio 1. Passare a **Firewall > Regole di accesso**.



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

Passaggio 2. Nella *tabella Regole di accesso IPv4*, fare clic sull'icona **Plus** per aggiungere una nuova regola di accesso IPv4.

IPv4 Access Rules Table

  	Priority	Enable	Action	Services	Source Interface	Source	Destination Interface	Destination
	1001	 	Allowed	IPv4: Pi-Prob...	WAN1	Any	VLAN	10.2.0.120
	4001	 	Allowed	IPv4: All Traffic	VLAN	Any	WAN	Any
	4002	 	Denied	IPv4: All Traffic	WAN	Any	VLAN	Any

Passaggio 3. Verificare che la casella di controllo **Abilita** sia selezionata. La regola verrà attivata.

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Passaggio 4. Nel campo *Azione*, selezionare **Consenti** nell'elenco a discesa.

Rule Status: Enable

Action: Allow

Services: IPv4 IPv6 All Traffic

Log: True

Source Interface: WAN1

Source Address: Any

Destination Interface: WAN1

Destination Address: Any

Passaggio 5. Selezionare un **servizio** nel campo *Servizi*. Lo lasceremo come **All Traffic**.

Rule Status: Enable

Action: Allow

Services: IPv4 IPv6 All Traffic

Log: True

Source Interface: WAN1

Source Address: Any

Destination Interface: WAN1

Destination Address: Any

Scheduling

Schedule Name: ANYTIME

- 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

Passaggio 6. Selezionare **Never** o **True** dall'elenco a discesa

True - Corrisponde alle regole.

Mai - Nessun registro richiesto.

In questo esempio, la lasceremo come **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

Passaggio 7. Selezionare l'*interfaccia di origine* e l'*indirizzo di origine* dall'elenco a discesa.

Nell'esempio sono state selezionate le opzioni **DMZ** e **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

Passaggio 8. Selezionare l'*interfaccia di destinazione* e l'*indirizzo di destinazione* dall'elenco a discesa.

Nell'esempio sono state selezionate le opzioni **DMZ** e **Any**.

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface: 1

Destination Address: 2

Passaggio 9. Nella sezione *Pianificazione* selezionare un'ora dall'elenco a discesa per applicare la regola firewall. Per configurare una pianificazione personalizzata, fare clic sul collegamento **qui**.

In questo esempio verrà utilizzato **ANYTIME** come pianificazione.

Scheduling

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

Passaggio 10. Fare clic su **Applica** per aggiungere la nuova regola. Questa regola prevede che sia consentito il traffico DMZ diretto a qualsiasi DMZ.

Access Rules Apply

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](#)

Ecco un esempio che è stato creato. È possibile notare che in una regola è stato aggiunto che la DMZ non è in grado di comunicare con nessuna destinazione nella VLAN 1. Ciò è dovuto al fatto che non si desidera che la DMZ sia in grado di accedere a niente dalla VLAN 1.

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	<input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="↕"/>
2	<input checked="" type="checkbox"/>	Allowed	IPv4: All Traffic	VLAN1	Any	Any	Any	ANYTIME	<input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="↕"/>
3	<input checked="" type="checkbox"/>	Denied	IPv4: All Traffic	DMZ	Any	VLAN1	Any	ANYTIME	<input type="button" value="▲"/> <input type="button" value="▼"/> <input type="button" value="↕"/>
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	

Verifica dell'utilizzo del router

Passaggio 1. Per verificare che il dispositivo sia connesso alla porta DMZ sul router, passare a **Stato e statistiche**, la pagina caricherà automaticamente la pagina *Riepilogo sistema*. La porta 4 o la LAN 4 visualizzeranno lo stato della DMZ come "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

Il ping dell'IP del dispositivo ci consentirà di conoscere lo stato di raggiungibilità del dispositivo. È consigliabile verificare la configurazione della DMZ per ogni servizio/porta

specifica utilizzando l'indirizzo IP pubblico utilizzato.

Passaggio 2. Passare a **Amministrazione > Diagnostica**.



Getting Started



Status and Statistics



Administration

1

File Management

Reboot

Diagnostic

2

Certificate

Configuration
Management



System Configuration

Passaggio 3. Immettere l'indirizzo IP della DMZ e fare clic sul pulsante Ping.

In questo esempio, verrà utilizzato l'indirizzo IP della DMZ configurata nella sezione [Host DMZ](#).

Nota: Se il ping ha esito positivo, verrà visualizzato un messaggio simile a quello mostrato di seguito. Se il ping ha esito negativo, la DMZ non è raggiungibile. Verificare che le impostazioni della zona demilitarizzata siano configurate correttamente.

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
```

Conclusioni

Una volta completata la configurazione della DMZ, dovrebbe essere possibile accedere ai servizi dall'esterno della LAN.