

Konfigurieren der DMZ auf dem Router der Serie RV34x

Ziel

In diesem Dokument wird erläutert, wie Sie den DMZ-Host (DMZ) und die Hardware-DMZ auf Routern der Serie RV34x konfigurieren.

Einführung

Eine DMZ ist ein Ort in einem Netzwerk, das für das Internet geöffnet ist und Ihr Local Area Network (LAN) hinter einer Firewall sichert. Durch die Trennung des Hauptnetzwerks von einem einzigen Host oder einem kompletten Subnetz oder einem "Subnetz" wird sichergestellt, dass Personen, die Ihren Service wie Internetspiele, Videokonferenzen, Web- oder E-Mail-Server über die DMZ besuchen, keinen Zugriff auf Ihr LAN haben. Cisco bietet zwei Methoden zur Verwendung von DMZs an: DMZ-Host und Hardware-DMZ. Der DMZ-Host ermöglicht es einem Host im LAN, dem Internet verfügbar zu machen, während die Hardware-DMZ (Subnetz/Bereich) ein für die Öffentlichkeit offenes Subnetz ist.

Bei der Planung der DMZ können Sie eine private oder eine öffentliche IP-Adresse verwenden. Eine private IP-Adresse ist für Sie nur im LAN eindeutig. Eine öffentliche IP-Adresse ist für Ihr Unternehmen eindeutig und wird von Ihrem Internetdienstanbieter (Internet Service Provider, ISP) zugewiesen. Um eine öffentliche IP-Adresse zu erhalten, müssen Sie sich an Ihren ISP wenden.

Die meisten Benutzer würden die Hardware-DMZ verwenden, da sie automatisch ein VLAN und ein eigenes Netzwerksegment einrichten. Für "Hardware DMZ" wird Subnetz- oder Bereichsoption verwendet. Die Konfiguration des DMZ-Hosts ist einfacher, da Sie keine Zugriffsregeln konfigurieren müssen, aber weniger sicher.

WAN-zu-DMZ ist der gängigste Anwendungsfall und LAN-zu-DMZ. DMZ-zu-WAN ist ebenfalls zulässig, da DMZ-Systeme möglicherweise Betriebssystem-Patches oder -Updates benötigen. DMZ-zu-LAN sollte jedoch blockiert werden, da es sich um ein potenzielles Sicherheitsloch handeln könnte. Hacker im Internet verwenden beispielsweise DMZ als Jumper-Server.

Der Unterschied zwischen DMZ-Host und Hardware-DMZ im Anwendungsfall ist:

Wenn Sie etwas für das Internet verfügbar machen möchten, aber über einen All-in-One-Server verfügen oder über keine öffentlichen IP-Adressen, sollten Sie den DMZ-Host verwenden. Platzieren Sie den Server in einem Ihrer VLANs, und richten Sie ihn als DMZ-Host ein. Anschließend kann der externe Benutzer über die WAN-IP des Routers auf den Server zugreifen.

Wenn Sie im Internet etwas verfügbar machen möchten und Sie über mehrere Server (jeweils mit einem bestimmten Service) und die gleiche Anzahl öffentlicher IP-Adressen verfügen, sollten Sie Hardware-DMZ verwenden. Verbinden Sie diese Server mit dem angegebenen DMZ-Port (d. h. LAN 4 für RV340), und konfigurieren Sie sie mit denselben öffentlichen IP-Adressen, die Sie im Router oder Subnetz konfigurieren). Anschließend kann der externe

Benutzer über diese IP-Adressen auf jeden Server zugreifen.

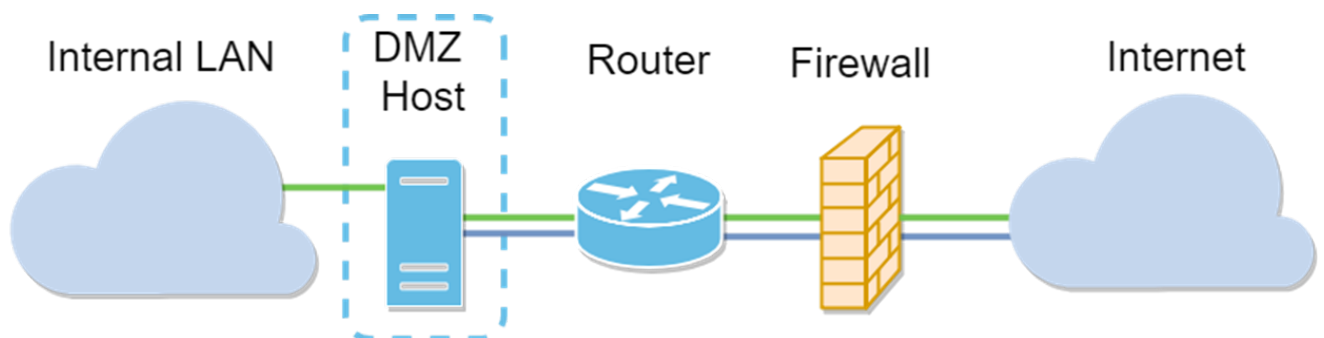
DMZ	Vergleichen	Kontrast
Host	Trennung des Datenverkehrs	Ein Host, vollständig für das Internet geöffnet
Subnetz/Bereich	Trennung des Datenverkehrs	Mehrere Geräte und Typen, vollständig offen für das Internet.

Hinweis: In diesem Beispiel wird bei der Konfiguration des DMZ-Subnetzes ein Switch am DMZ-Port des Routers angeschlossen.

Weitere Informationen zum Aktivieren von SSH auf einem Switch finden Sie in diesem Artikel: [Aktivieren des SSH-Service für Managed Switches der Serien 300 und 500](#).

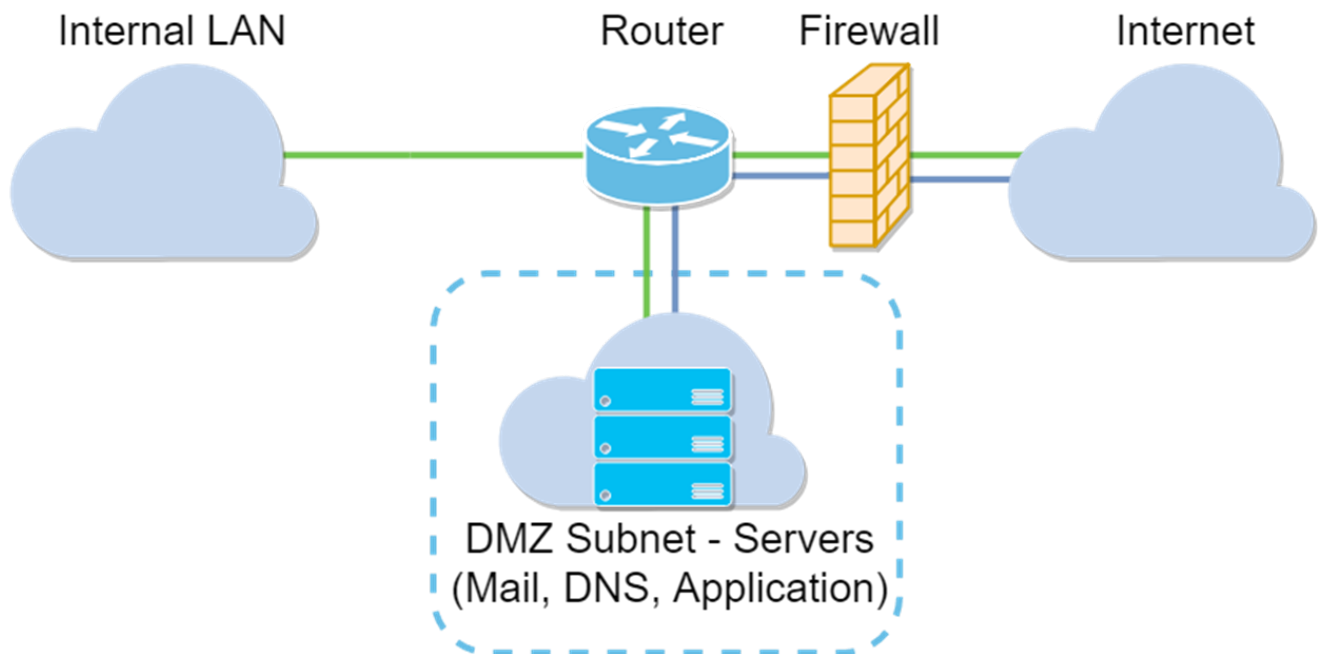
Weitere Informationen zur Konfiguration der DMZ auf dem RV160/RV260 finden Sie in diesem Artikel: [DMZ-Optionen für Router der Serien RV160 und RV260](#).

Host-DMZ-Topologie



Hinweis: Wenn Sie eine Host-DMZ verwenden und der Host von einem Angreifer kompromittiert wird, kann Ihr internes LAN möglicherweise weiteren Sicherheitsrisiken ausgesetzt sein.

Subnetz-DMZ-Topologie



Anwendbare Geräte

RV34x

Softwareversion

1.0.2.16

Konfigurieren des DMZ-Hosts

Schritt 1: Melden Sie sich auf der Webkonfigurationsseite Ihres Routers an.



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.

Schritt 2: Navigieren Sie zu **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

Schritt 3: Aktivieren Sie im Feld *DMZ Host* das **Kontrollkästchen Enable (Aktivieren)**, um den DMZ Host zu aktivieren.

DMZ Host

DMZ Host: Enable

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

Schritt 4: Geben Sie die IP-Adresse des Hosts in die *IP-Adresse des DMZ-Hosts ein*, die dem Internet zur Verwendung von Diensten wie Internet-Gaming, Videokonferenzen, Web- oder E-Mail-Servern zur Verfügung gestellt wird.

Hinweis: Dem LAN-DMZ-Host muss eine feste oder statische IP-Adresse zugewiesen werden, damit die DMZ-Hostfunktion ordnungsgemäß funktioniert. Vergewissern Sie sich, dass sich der Router im gleichen Netzwerk befindet wie Ihr Router. Sie können dies auch konfigurieren, wenn sich die DMZ in einem anderen VLAN befindet.

DMZ Host

DMZ Host: Enable

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

Schritt 5: Klicken Sie auf **Apply** Save your configuration.

DMZ Host

Enable

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

Der DMZ-Host sollte jetzt erfolgreich aktiviert sein.

Schritt 6: (Optional) In den nächsten Schritten zeigen wir Ihnen eine Möglichkeit zur Überprüfung des DMZ-Hosts. Navigieren Sie zu **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

Schritt 7: (Optional) In diesem Beispiel ist die *Remotewebverwaltung* aktiviert, wobei **HTTPS** ausgewählt ist. Dies ist die Remote-Anmeldung bei der Webkonfigurationsseite über die WAN-IP-Adresse. In diesem Schritt wird die Portnummer auf **6000** angepasst. Der Bereich liegt zwischen **1025** und **65535**.

Hinweis: Wenn Sie dies beim Remotezugriff auf die Webseite konfiguriert haben, wird Ihre Seite möglicherweise am Ladebildschirm hängen. Das bedeutet, dass der Port zu dem geändert wurde, was Sie angepasst haben.

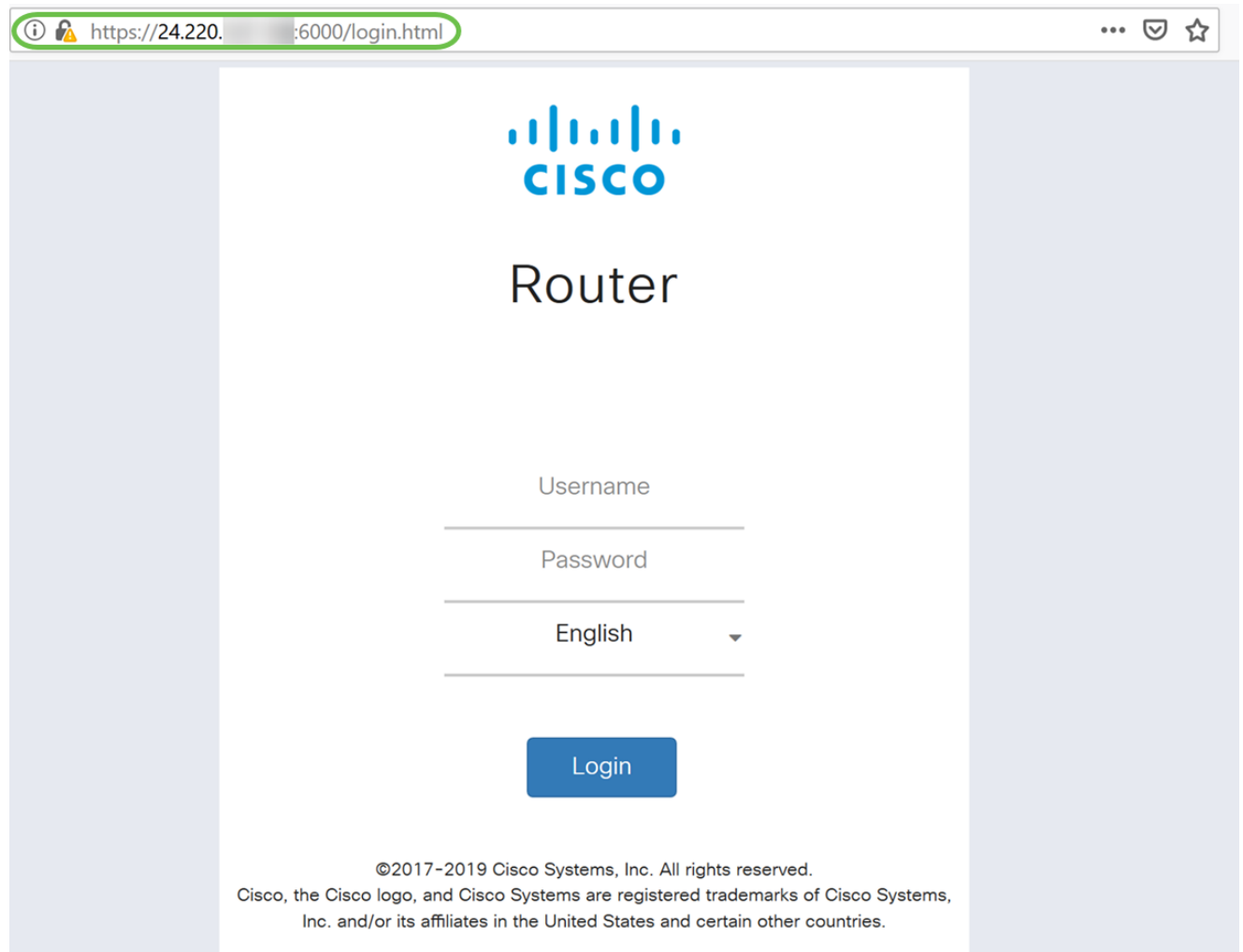
Remote Web Management: Enable

HTTP HTTPS

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

Schritt 8: Stellen Sie sicher, dass Sie auf die Webkonfigurationsseite des Routers zugreifen können, indem Sie **https://[WANIPaddress]:port** eingeben, wobei die WAN-IP-Adresse die tatsächliche WAN-IP-Adresse des Routers ist, und anschließend **:port** für die Portnummer, die Sie in Schritt 5 für diesen Abschnitt festgelegt haben. In diesem Beispiel haben wir **https://24.220.x.x:6000** eingegeben, aber Sie würden die tatsächlichen Zahlen und nicht **x** angeben. Mit dem **x** wird unsere öffentliche WAN-IP-Adresse ausgeblendet.

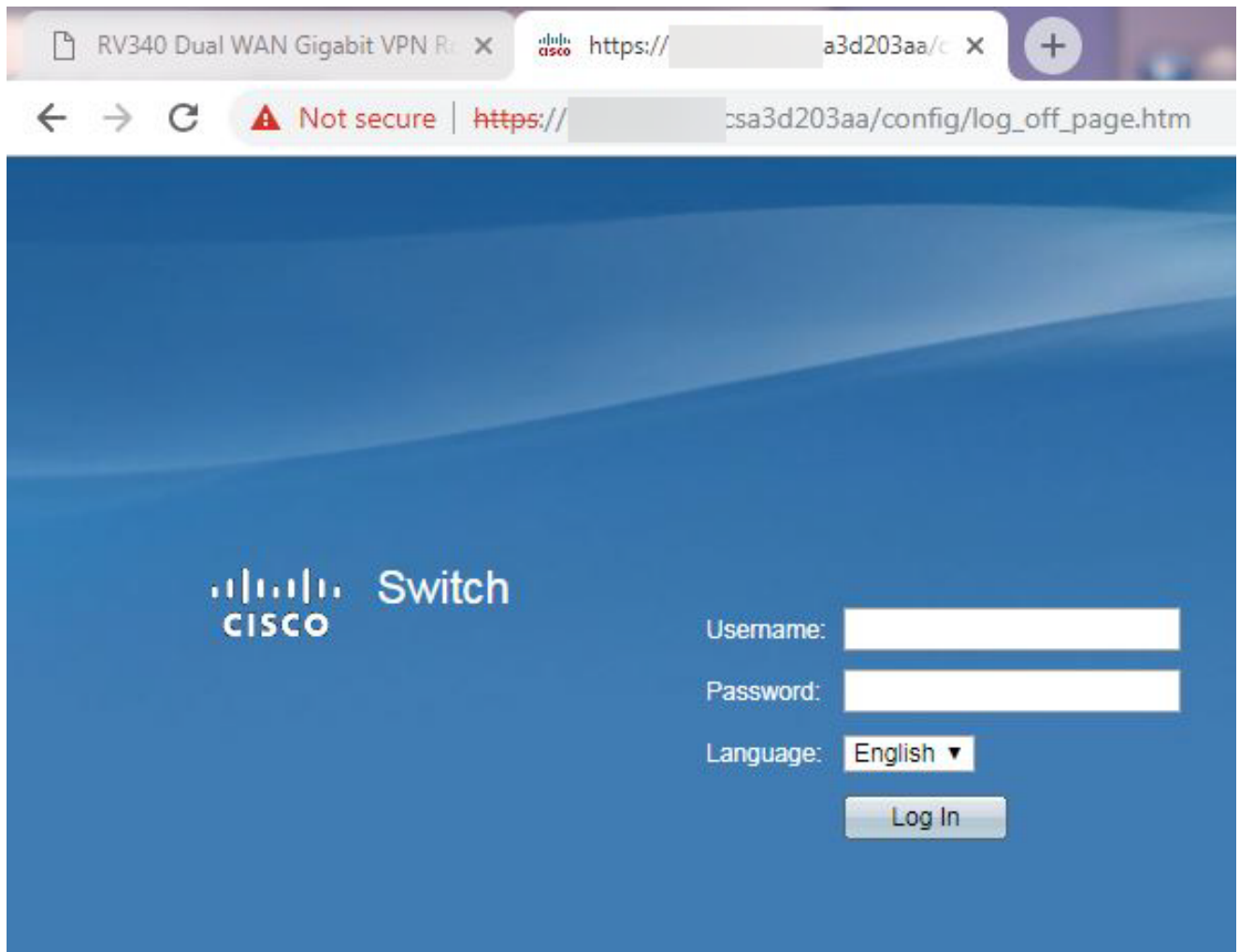
Hinweis: Vergewissern Sie sich, dass Sie nicht über das VPN verbunden sind. Wenn Sie sich manchmal im VPN befinden, können Sie nicht auf die Webseite zur Konfiguration zugreifen.



Schritt 9: Sie sollten jetzt über die WAN-IP-Adresse auf die Webseite zur Konfiguration des Geräts im DMZ-Port zugreifen können, ohne die Portnummer hinzuzufügen.

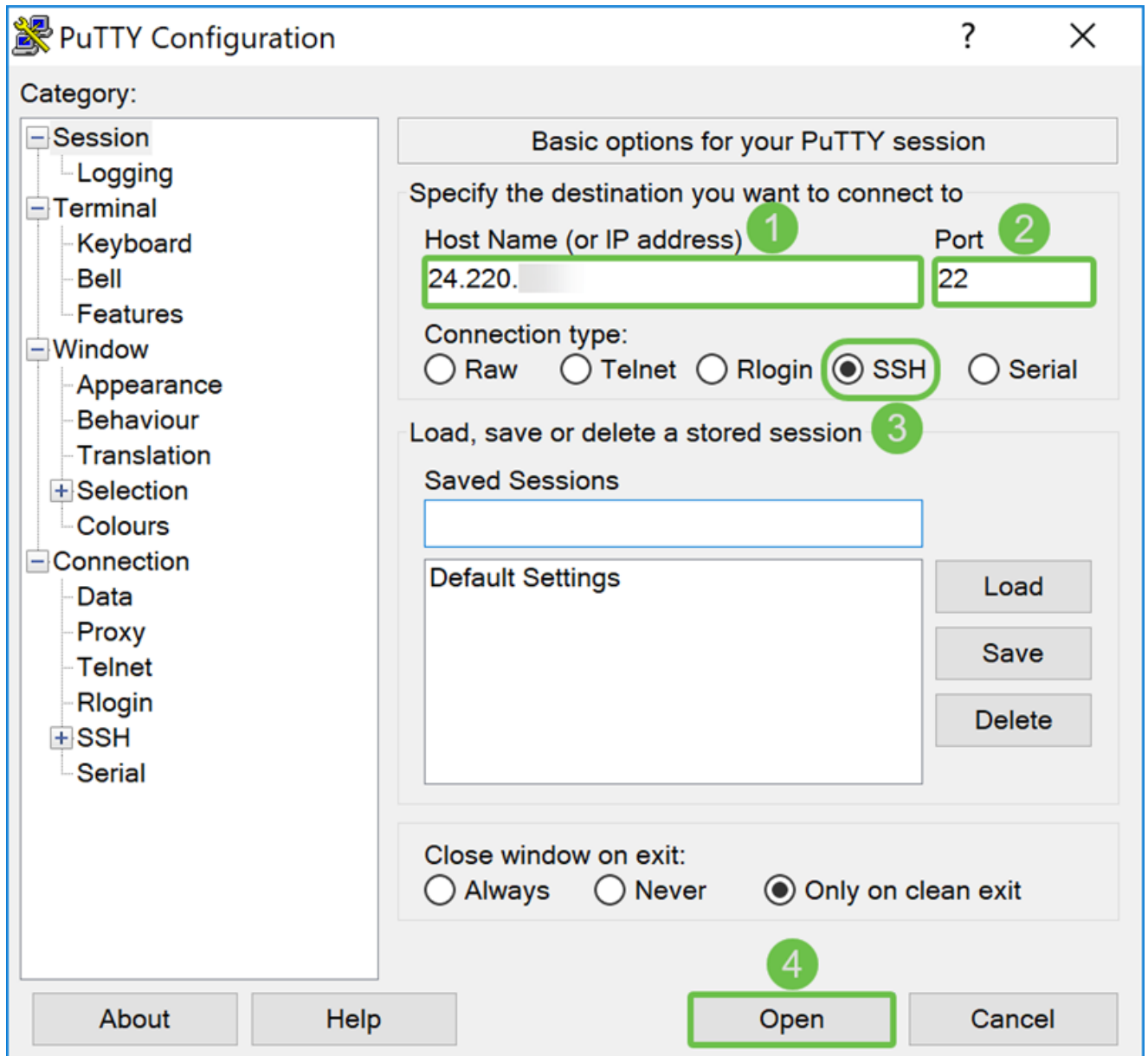
<https://24.220.x.x:6000>: zeigt die Webkonfigurationsseite des Routers an.

<https://24.220.x.x> - zeigt die Webseite für die Konfiguration des Switches an.

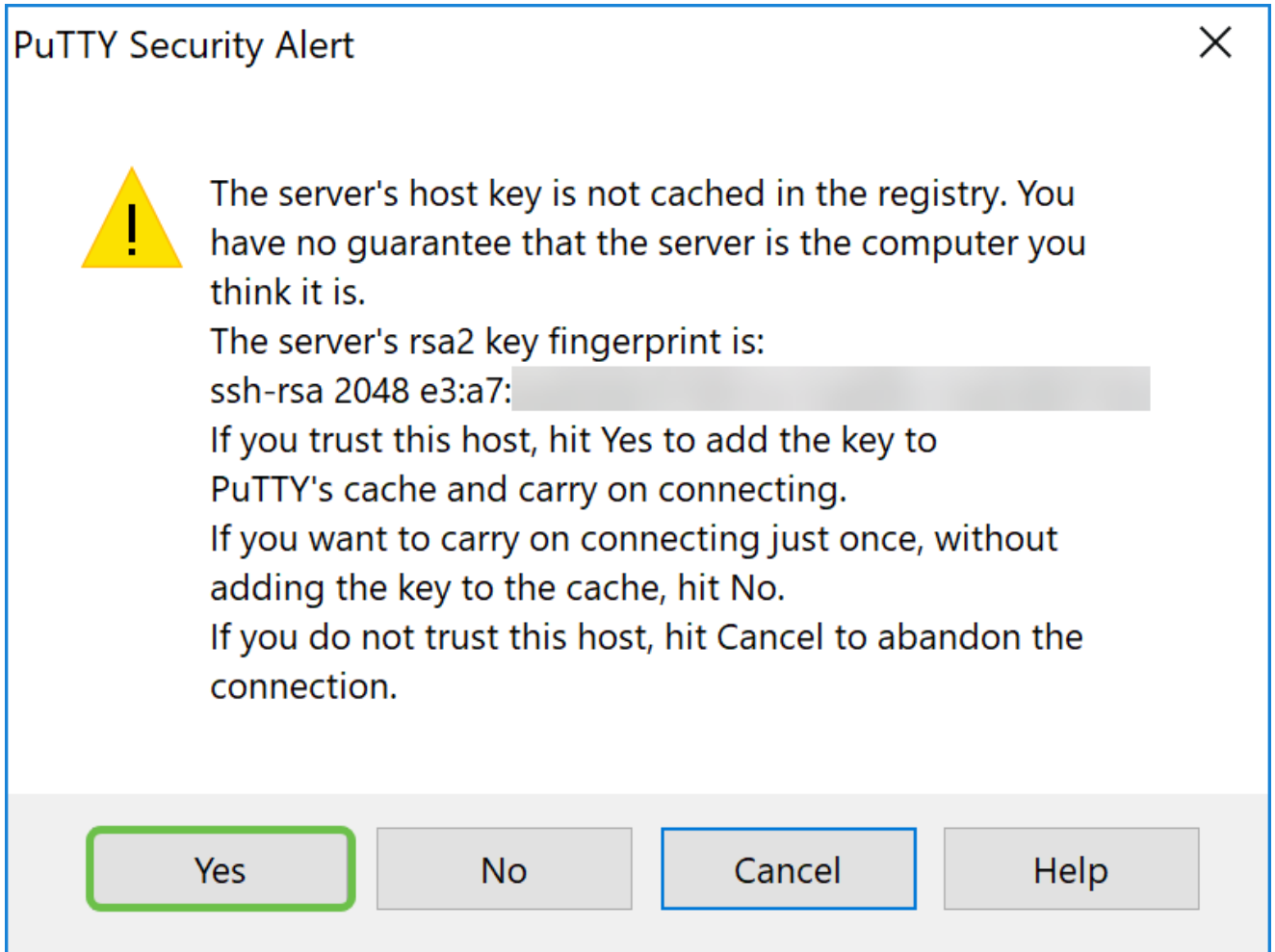


Schritt 10: Wir verwenden PuTTY für SSH im Switch. Geben Sie die **öffentliche IP-Adresse** Ihres Geräts im *Feld Hostname (oder IP-Adresse)* ein. Stellen Sie sicher, dass Port **22** eingegeben und **SSH** ausgewählt ist. Klicken Sie auf **Öffnen**, um die Verbindung zu starten.

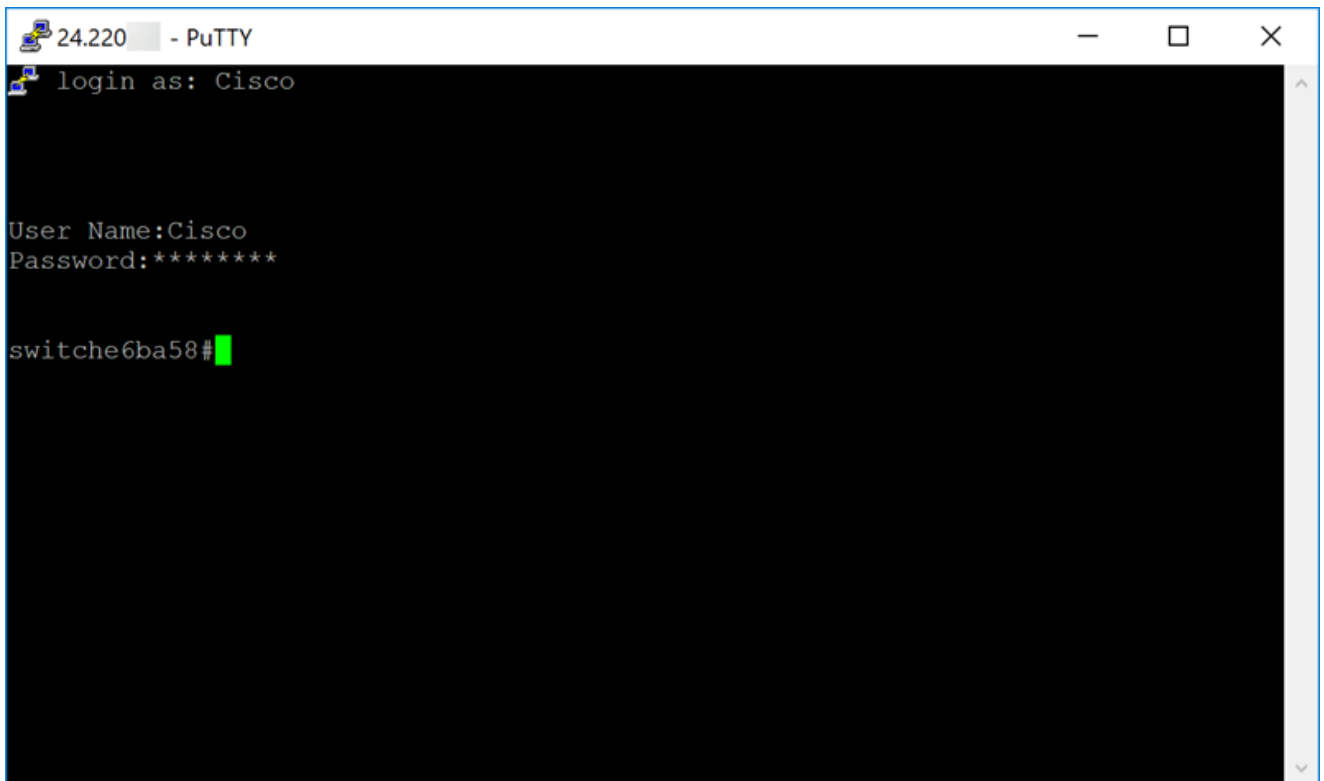
Hinweis: Wenn Sie SSH in den Switch einbinden möchten, denken Sie daran, SSH zuerst auf dem Switch zu aktivieren. In den meisten Switches können Sie zu **Security > TCP/UDP Services** navigieren, um den **SSH-Dienst** zu aktivieren. Um SSH mit Windows zu verwenden, können Sie PuTTY herunterladen. Weitere Informationen finden Sie in diesem Dokument: [Zugriff auf eine SMB-Switch-CLI mit SSH oder Telnet](#). SSH wird empfohlen, Telnet jedoch nicht, da SSH sicherer ist.



Schritt 11: Eine *PuTTY*-Sicherheitswarnung kann angezeigt werden. Klicken Sie auf **Ja**, um mit der Verbindung fortzufahren.



Schritt 12: Wenn die Verbindung erfolgreich hergestellt wurde, werden Sie aufgefordert, sich mit Ihren Anmeldeinformationen anzumelden.



Konfigurieren der Hardware-DMZ

Schritt 1: Wenn Sie Hardware-DMZ anstelle des DMZ-Hosts konfigurieren möchten, wählen Sie **WAN > Hardware DMZ aus**.



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

Schritt 2: Aktivieren Sie das **Kontrollkästchen Aktivieren**, um den LAN4-Port in den DMZ-Port zu ändern.

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

Schritt 3: Eine Warnmeldung wird angezeigt. Klicken Sie auf **Yes** (Ja), um die Änderungen zu akzeptieren, die der Router am DMZ-Port (LAN4) vornehmen würde, oder **No (Nein)**, um die Änderungen abzulehnen.

Wenn die DMZ auf "enable" gesetzt ist, wird die Konfiguration des DMZ-Ports (LAN4) wie folgt automatisch geändert:

Entfernen Sie den LAG-Port (Abschnitt "LAN > Porteinstellungen").

Wird die Funktion zur Portspiegelung deaktivieren, wenn das Ziel der Portspiegelung der DMZ-Port ist (Abschnitt "LAN > Porteinstellungen")

Aus Überwachungsport für Port-Spiegelung entfernen (Abschnitt "LAN > Porteinstellungen")

Verwaltungsstatus zu "Force Authorized" (Befehl "Network > 802.1X")

Der Wert des DMZ-Ports in der Tabelle "VLANs an Port Table" wird in "Exclude" (Abschnitt "LAN > VLAN-Mitgliedschaft") geändert.

In diesem Beispiel klicken wir auf **Ja**.

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

Schritt 4: Wählen Sie entweder **Subnetz** oder **Bereich** (DMZ und WAN im gleichen Subnetz) . In diesem Beispiel wählen wir **Subnet** aus.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

Schritt 5: Geben Sie die **DMZ-IP-Adresse** und die **Subnetzmaske ein**. Alles, was an das LAN4-Segment angeschlossen ist, muss in diesem Netzwerk vorhanden sein.

Hinweis: Stellen Sie sicher, dass das mit dem DMZ-Port verbundene Gerät über diese statische IP-Adresse verfügt. Diese IP-Adresse muss sich möglicherweise außerhalb Ihres WAN-Subnetzes befinden.

In diesem Beispiel wird eine öffentliche IP-Adresse für die DMZ verwendet.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address: 1

Subnet Mask: 2

Range (DMZ & WAN within same subnet)

IP Range: to

Hinweis: Wenn Sie die *Range*-Methode verwenden möchten, müssen Sie auf das Optionsfeld **Range** klicken und dann den Bereich der IP-Adressen eingeben, die von Ihrem ISP zugewiesen wurden. Dies wird in der Regel verwendet, wenn Sie mehrere öffentliche IP-Adressen von Ihrem ISP für mehrere Geräte im DMZ-Netzwerk haben.

Wenn Sie eine einzige öffentliche IP-Adresse haben und das Subnetz für Sie nicht funktioniert, geben Sie in beiden Feldern unter dem Feld *IP Range (IP-Bereich)* die einzige öffentliche IP-Adresse ein. Bei der IP-Adresse muss es sich um eine andere freie IP-Adresse als das WAN-IP-Subnetz handeln. Die IP-Adresse des WAN darf nicht verwendet werden. Wenn Sie beispielsweise eine einzige öffentliche IP-Adresse von 24.100.50.1 erhalten, die sich im gleichen Subnetz wie Ihre WAN-IP-Adresse befindet, geben Sie **24.100.50.1 bis 24.100.50.1** in das Feld *IP-Bereich ein*.

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

1 Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: **2** to

Schritt 6: Klicken Sie in der rechten oberen Ecke auf **Apply (Übernehmen)**, um die DMZ-Einstellungen zu übernehmen.

Hardware DMZ

Enable (Change LAN4 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: to

Sie sollten die Hardware-DMZ erfolgreich aktiviert haben.

Schritt 7: (Optional) Um dies zu überprüfen, öffnen Sie die Eingabeaufforderung auf Ihrem PC, indem Sie zur Suchleiste unten links navigieren und die **Eingabeaufforderung** eingeben. Klicken Sie auf die Anwendung **für die Eingabeaufforderung**, wenn sie angezeigt wird.

Hinweis: In diesem Beispiel verwenden wir Windows 10.



Filters 



Best match

2



Command Prompt

App



1

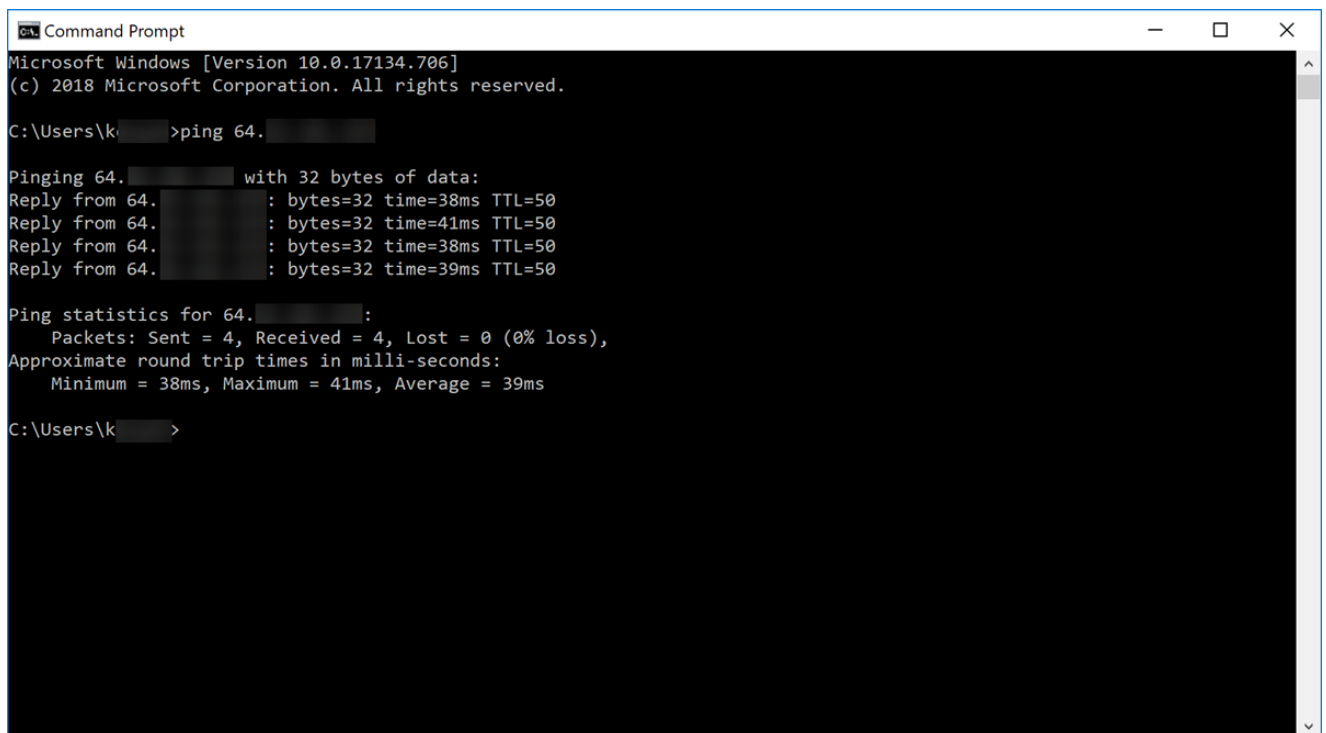


command prompt

Schritt 8: (Optional) Das Fenster *Eingabeaufforderung* wird geöffnet. Wir führen einen Ping-Befehl zur DMZ-IP-Adresse aus, um festzustellen, ob eine Verbindung besteht. Verwenden Sie den Befehl **ping DMZ_IP_Adress**. Drücken Sie die **Eingabetaste**, wenn Sie den Ping starten möchten. Wenn Sie Antworten von dieser IP-Adresse erhalten, bedeutet dies, dass Sie eine Verbindung zwischen Ihnen und der DMZ haben. Wenn Sie eine Art von Nachrichten wie "Request timed out" (Zeitüberschreitung der Anfrage) oder "Destination host unreachable" (Zielhost nicht erreichbar) erhalten haben, sollten Sie Ihre Konfiguration und Verbindungen überprüfen.

In diesem Beispiel geben wir ping **64.x.x.x ein**. 64.x.x.x ist unsere öffentliche IP-Adresse für die DMZ.

Hinweis: Mehr dazu in diesem Dokument: [Fehlerbehebung bei Routern der Serien RV160 und RV260](#). Dieses Dokument zur Fehlerbehebung behandelt einige Bereiche, die bei der Behebung von Verbindungsproblemen analysiert werden müssen. Obwohl dieses Dokument für den RV160 und den RV260 gilt, können Sie hier möglicherweise einige ähnliche Fehlerbehebungsschritte ausführen.



```
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...>
```

Schritt 9: (Optional) Wir können auch einen Traceroute-Befehl ausführen, um den Pfad anzuzeigen, den die Pakete für den Zugang zum Ziel verwenden. Verwenden Sie den Befehl **tracert DMZ_IP_Adress**, und drücken Sie die Eingabetaste, um den Vorgang zu starten. In diesem Beispiel sehen wir, dass die Ablaufverfolgung abgeschlossen ist, wenn sie am Ende die DMZ-IP-Adresse erreicht. Sobald der Empfänger erreicht ist, wird auch "Trace complete" (Ablaufverfolgung abgeschlossen) angezeigt.

```

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. ]

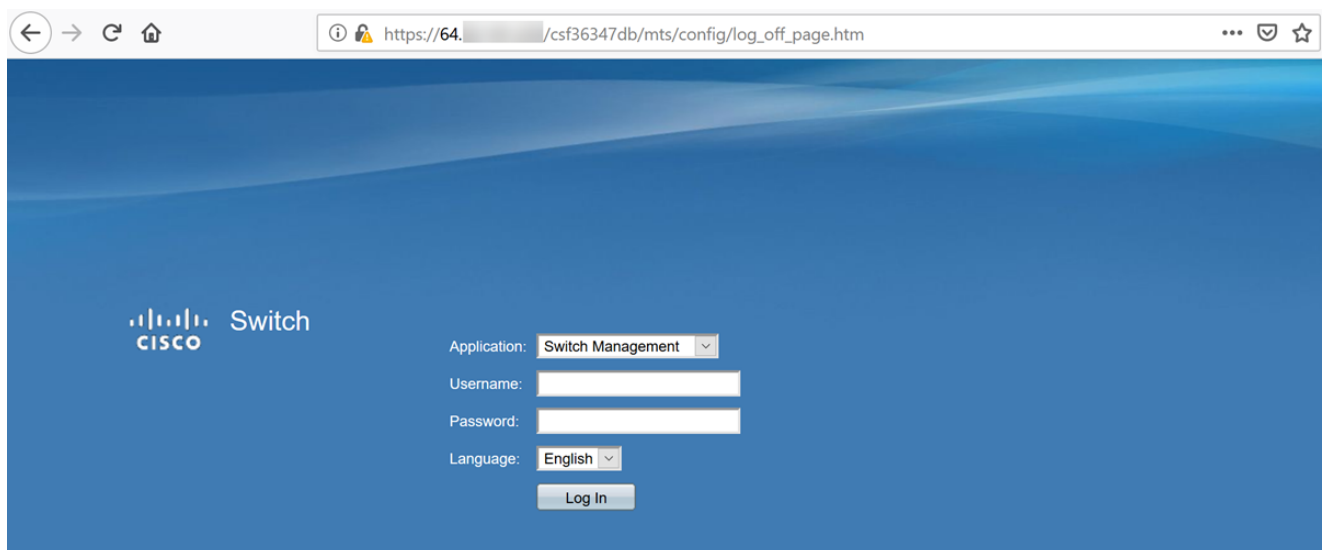
Trace complete.

C:\Users\keyven>

```

Schritt 10: (Optional) In diesem Beispiel ist ein Switch mit der statischen IP-Adresse 64.x.x.x (öffentliche IP-Adresse) mit dem DMZ-Port verbunden. Sie können versuchen, auf die grafische Benutzeroberfläche (GUI) des Switches zuzugreifen, indem Sie die öffentliche IP-Adresse im Browser oben eingeben.

Wir haben <https://64.x.x.x> eingegeben, wodurch wir zur GUI-Seite des Switches gelangen.



Sie sollten jetzt einige Möglichkeiten kennen, um sicherzustellen, dass Ihre DMZ ordnungsgemäß funktioniert.

Konfigurieren von Zugriffsregeln (optional)

Wenn Sie eine öffentliche IP-Adresse oder einen IP-Adressbereich für die Hardware-DMZ konfiguriert haben, wird in diesem Abschnitt ein Beispiel für die Konfiguration von Zugriffsregeln für die DMZ angezeigt. Die DMZ sollte ordnungsgemäß arbeiten, ohne Zugriffsregeln konfigurieren zu müssen. Die Konfiguration von Zugriffsregeln ist optional, es wird jedoch empfohlen, sie so zu konfigurieren, dass sie eine grundlegende Sicherheitsstufe für den Zugriff auf Ihr Netzwerk bieten. Wenn wir beispielsweise die Zugriffsregeln nicht

standardmäßig konfigurieren, können alle Pakete, die den Router durchlaufen, in alle Teile unseres Netzwerks gelangen. Zugriffsregeln können einem Host, einem Bereich von IP-Adressen oder einem Netzwerk erlauben und gleichzeitig verhindern, dass ein anderer Host, ein Bereich von IP-Adressen oder ein Netzwerk auf denselben Bereich (Host oder Netzwerk) zugreift. Mithilfe von Zugriffsregeln können wir entscheiden, welche Arten von Datenverkehr an den Router-Schnittstellen weitergeleitet oder blockiert werden.

Schritt 1: Navigieren Sie zu **Firewall > Zugriffsregeln**.



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

Schritt 2: Klicken Sie in der *Tabelle mit den IPv4-Zugriffsregeln* auf das **Plus**-Symbol, um eine neue IPv4-Zugriffsregel hinzuzufügen.

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

Schritt 3: Stellen Sie sicher, dass das Kontrollkästchen **Aktivieren** aktiviert ist. Dadurch wird die Regel aktiviert.

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Schritt 4: Wählen Sie im Feld *Aktion* in der Dropdown-Liste die Option **Zulassen**.

Rule Status: Enable

Action:

Services: IPv4 IPv6

Log:

Source Interface:

Source Address:

Destination Interface:

Destination Address:

Schritt 5: Wählen Sie einen **Service** im Feld *Services aus*. Wir verlassen es als **Gesamter Datenverkehr**.

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

Schritt 6: Wählen Sie aus der Dropdown-Liste **Never** oder **True aus**.

True: Entspricht den Regeln.

Nie - Kein Protokoll erforderlich.

In diesem Beispiel wird es als **True** belassen.

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

Schritt 7: Wählen Sie die *Quellschnittstelle* und die *Quelladresse* aus der Dropdown-Liste aus.

In diesem Beispiel wurden **DMZ** und **Any** ausgewählt.

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

Schritt 8: Wählen Sie die *Zielschnittstelle* und die *Zieladresse* aus der Dropdown-Liste aus.

In diesem Beispiel wurden **DMZ** und **Any** ausgewählt.

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
Source Address:	Any
Destination Interface:	DMZ 1
Destination Address:	Any 2

Schritt 9: Wählen Sie im Abschnitt *Planung* eine Zeit aus der Dropdown-Liste aus, um die Firewall-Regel anzuwenden. Wenn Sie Ihren eigenen Zeitplan konfigurieren möchten, klicken Sie auf den Link [here](#).

In diesem Beispiel verwenden wir **ANYTIME** als unseren Zeitplan.

Scheduling

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

Schritt 10: Klicken Sie auf **Übernehmen**, um die neue Regel hinzuzufügen. Diese Regel besagt, dass jeder DMZ-Datenverkehr, der an eine DMZ geleitet wird, zulässig ist.

Access Rules Apply Cancel

Rule Status: Enable

Action: Allow

Services: IPv4 IPv6 All Traffic

Log: True

Source Interface: DMZ

Source Address: Any

Destination Interface: DMZ

Destination Address: Any

Scheduling

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

Hier ein Beispiel, das erstellt wurde. Wie Sie sehen, haben wir in einer Regel hinzugefügt, dass die DMZ mit keinem Ziel in VLAN 1 kommunizieren kann. Der Grund hierfür ist, dass die DMZ nicht auf irgendetwas von VLAN 1 zugreifen kann.

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	

Überprüfen der Verwendung des Routers

Schritt 1: Um zu überprüfen, ob Ihr Gerät im DMZ-Port des Routers angeschlossen ist, navigieren Sie zu **Status & Statistics**, die Seite lädt die Seite *Systemübersicht* automatisch. Port 4 oder LAN 4 listet den Status der DMZ als "UP" auf.

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

Wenn Sie die IP-Adresse des Geräts anpingen, wird uns der Erreichbarkeitsstatus des Geräts mitgeteilt. Es empfiehlt sich, die DMZ-Konfiguration für einen bestimmten Service/Port mithilfe der öffentlichen IP-Adresse zu überprüfen.

Schritt 2: Navigieren Sie zu **Administration > Diagnostic (Verwaltung > Diagnose)**.



Getting Started



Status and Statistics



Administration

1

File Management

Reboot

Diagnostic

2

Certificate

Configuration
Management



System Configuration

Schritt 3: Geben Sie die **IP-Adresse der DMZ ein**, und klicken Sie auf die Schaltfläche **Ping**.

In diesem Beispiel wird die IP-Adresse der DMZ verwendet, die im [DMZ-Host](#)-Abschnitt konfiguriert wurde.

Hinweis: Wenn der Ping erfolgreich ist, wird eine Meldung wie unten gezeigt angezeigt. Wenn der Ping fehlschlägt, bedeutet dies, dass die DMZ nicht erreicht werden kann. Überprüfen Sie Ihre DMZ-Einstellungen, um sicherzustellen, dass sie korrekt konfiguriert sind.

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
```

Schlussfolgerung

Nachdem Sie die Einrichtung der DMZ abgeschlossen haben, sollten Sie von außerhalb des LAN auf die Services zugreifen können.