

DMZ-Optionen für RV160/RV260-Router

Ziel

In diesem Dokument werden die beiden Optionen für die Einrichtung eines DMZ-Hosts der demilitarisierten Zone und eines DMZ-Subnetzes auf Routern der Serien RV160X und RV260X erläutert.

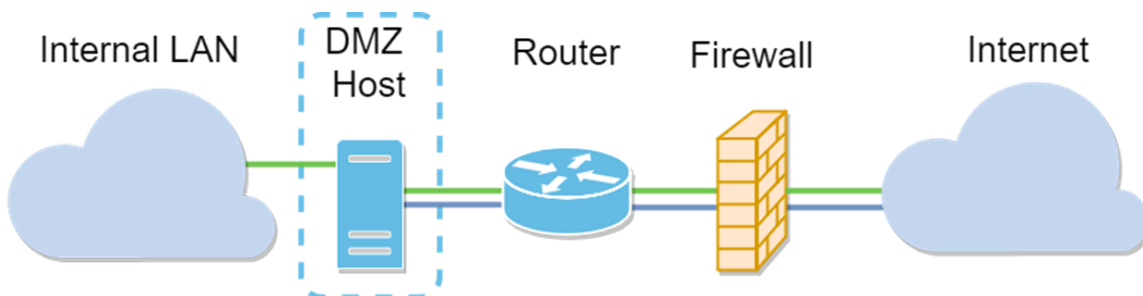
Anforderungen

- RV160X
- RV260X

Einführung

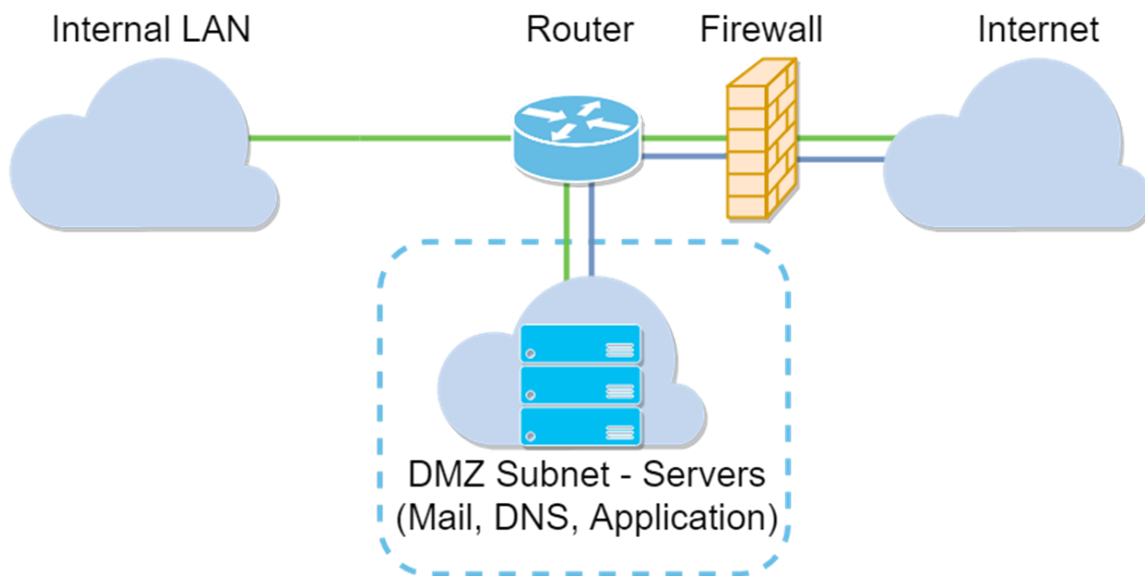
Eine DMZ ist ein Ort in einem Netzwerk, das für das Internet geöffnet ist und gleichzeitig Ihr LAN (Local Area Network) hinter einer Firewall sichert. Durch die Trennung des Hauptnetzwerks von einem einzigen Host oder einem gesamten Subnetz oder einem "Subnetz" wird sichergestellt, dass Personen, die Ihren Webseitenserver über die DMZ besuchen, keinen Zugriff auf Ihr LAN haben. Cisco bietet zwei Methoden für die Verwendung von DMZs in Ihrem Netzwerk, die beide wichtige Unterschiede in ihrer Arbeitsweise aufweisen. Die folgenden visuellen Referenzen verdeutlichen den Unterschied zwischen den beiden Betriebsmodi.

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



DMZ-Typ	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. Nur auf RV260-Hardware verfügbar.

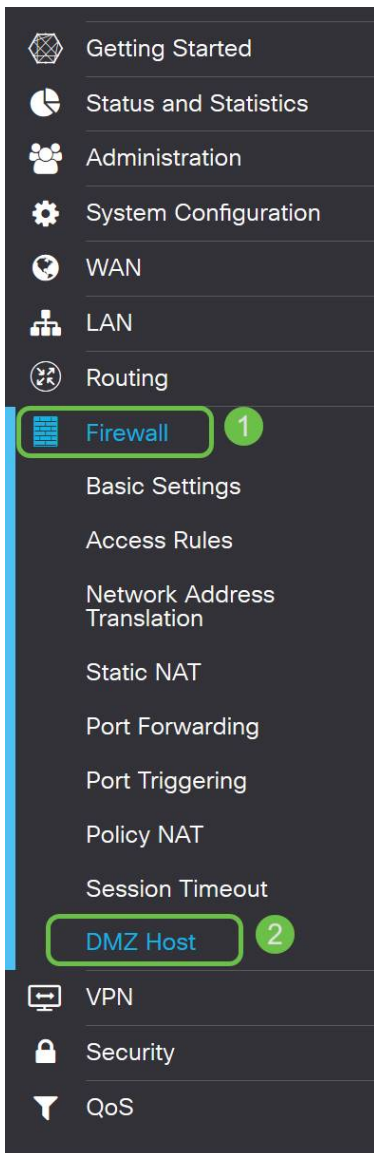
IP-Adressierung

In diesem Artikel werden IP-Adressierungsschemata verwendet, die in ihrer Verwendung einige Nuancen enthalten. 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 zugewiesen. Um eine öffentliche IP-Adresse zu erhalten, müssen Sie sich an Ihren (ISP) wenden.

Konfigurieren des DMZ-Hosts

Die für diese Methode erforderlichen Informationen umfassen die IP-Adresse des beabsichtigten Hosts. Die IP-Adresse kann entweder öffentlich oder privat sein, die öffentliche IP-Adresse sollte sich jedoch in einem anderen Subnetz als die WAN-IP-Adresse befinden. Die DMZ-Host-Option ist auf dem RV160X und dem RV260X verfügbar. Konfigurieren Sie den DMZ-Host wie unten beschrieben.

Schritt 1: Nachdem Sie sich bei Ihrem Routing-Gerät angemeldet haben, klicken Sie in der linken Menüleiste auf **Firewall > DMZ Host**.



Schritt 2: Klicken Sie auf das Kontrollkästchen **Aktivieren**.



DMZ Host

DMZ Host: Enable

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

Schritt 3: Geben Sie die festgelegte IP-Adresse des Hosts ein, der für den WAN-Zugriff geöffnet werden soll.



RV160-router5402D9

DMZ Host

DMZ Host: Enable

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

Schritt 4: Wenn Sie mit Ihrer Adressierung zufrieden sind, klicken Sie auf die Schaltfläche "Anwenden".

Apply

Cancel

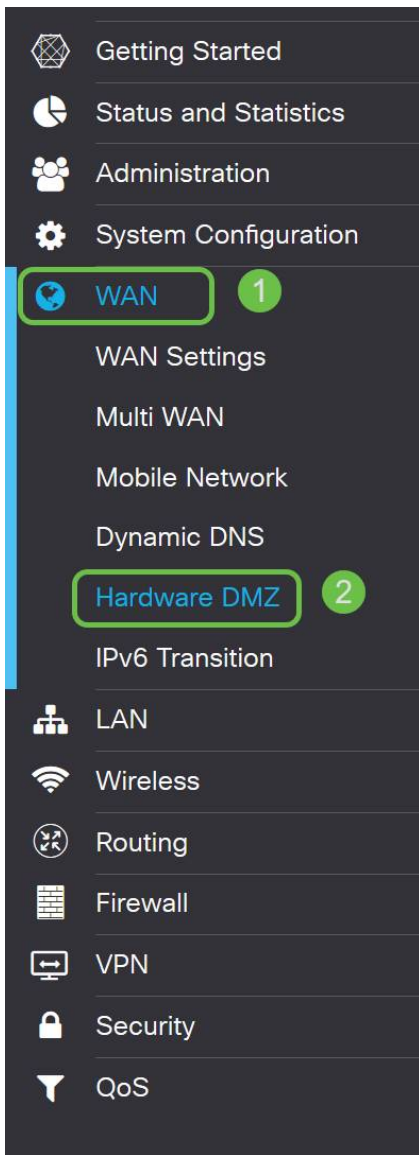
Hinweis: Wenn Sie nur mit einer RV160X-Serie arbeiten und die Überprüfungsanweisungen überspringen möchten, [klicken Sie hier, um zum Abschnitt dieses Dokuments zu gelangen](#).

Konfigurieren der Hardware-DMZ

Diese Methode ist nur für die Serie RV260X verfügbar und erfordert je nach gewählter Methode unterschiedliche IP-Adressierungsinformationen. Beide Methoden verwenden tatsächlich Subnetzwerke, um die Zone zu definieren. Der Unterschied besteht darin, wie viel des Subnetzwerks zum Erstellen der entmilitarisierten Zone verwendet wird. In diesem Fall sind die Optionen - *alle* oder *einige*. Die Subnetz-Methode (*all*) erfordert neben der Subnetzmaske die IP-Adresse der DMZ selbst. Diese Methode belegt alle IP-Adressen, die zu diesem Subnetz gehören. Die Range-Methode (*einige*) hingegen ermöglicht die Definition eines kontinuierlichen Bereichs von IP-Adressen, die sich innerhalb der DMZ befinden.

Hinweis: In beiden Fällen müssen Sie mit Ihrem ISP zusammenarbeiten, um das IP-Adressierungsschema des Subnetzwerks zu definieren.

Schritt 1: Klicken Sie nach der Anmeldung bei Ihrem RV260X-Gerät auf **WAN > Hardware DMZ**.



Hinweis: Die Screenshots stammen von der RV260X-Benutzeroberfläche. Unten sehen Sie den Screenshot der Hardware-DMZ-Optionen, der auf dieser Seite angezeigt wird.



Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

Schritt 2: Klicken Sie auf das Kontrollkästchen **Aktivieren (LAN8 in DMZ-Port ändern)**. Dadurch wird der 8. Port des Routers in ein "Fenster" für die DMZ in Dienste umgewandelt, die eine höhere Sicherheit erfordern.

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

Schritt 3: Nachdem Sie auf *Aktivieren* geklickt haben, wird unter den auswählbaren Optionen eine Informationsmeldung angezeigt. Überprüfen Sie die Details zu Punkten, die sich auf Ihr Netzwerk auswirken können, und klicken Sie auf **OK**. **Ich stimme dem Kontrollkästchen oben zu.**

 When hardware DMZ is enabled, the dedicated DMZ Port (LAN8) will be:

- * Disabled as Port Mirror function, if Port Mirror Destination is DMZ Port (LAN > Port Settings);
- * Removed from LAG Port (LAN > Port Settings);
- * Removed from Monitoring Port of Port Mirror (LAN > Port Settings);
- * Changed to "Force Authorized" in Administrative State (LAN > 802.1X Configuration);
- * Changed to "Excluded" in "Assign VLANs to ports" table (LAN > VLAN Settings).

OK, I agree with the above.

Schritt 4: Der nächste Schritt teilt sich in zwei mögliche Optionen auf: Subnet und Range. In unserem Beispiel unten haben wir die **Subnet**-Methode ausgewählt.

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address: 164.33.100.250

Subnet Mask: 255.255.255.248

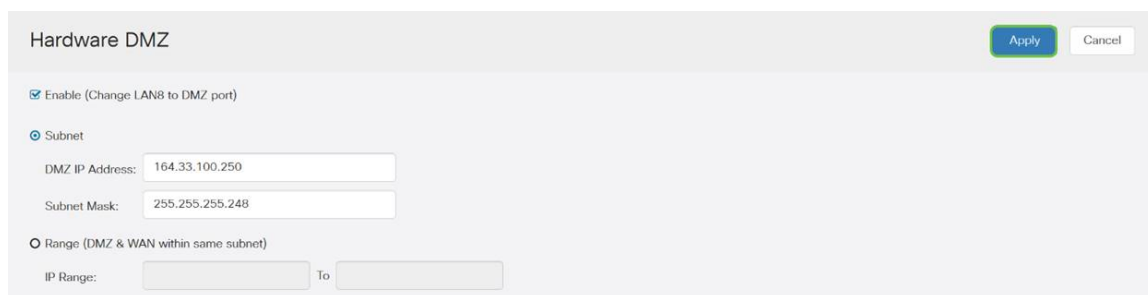
Range (DMZ & WAN within same subnet)

IP Range:

To

Hinweis: Wenn Sie die Range-Methode verwenden möchten, müssen Sie auf die Schaltfläche **Range** Radial klicken und dann den IP-Adressbereich eingeben, der vom ISP zugewiesen wurde.

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

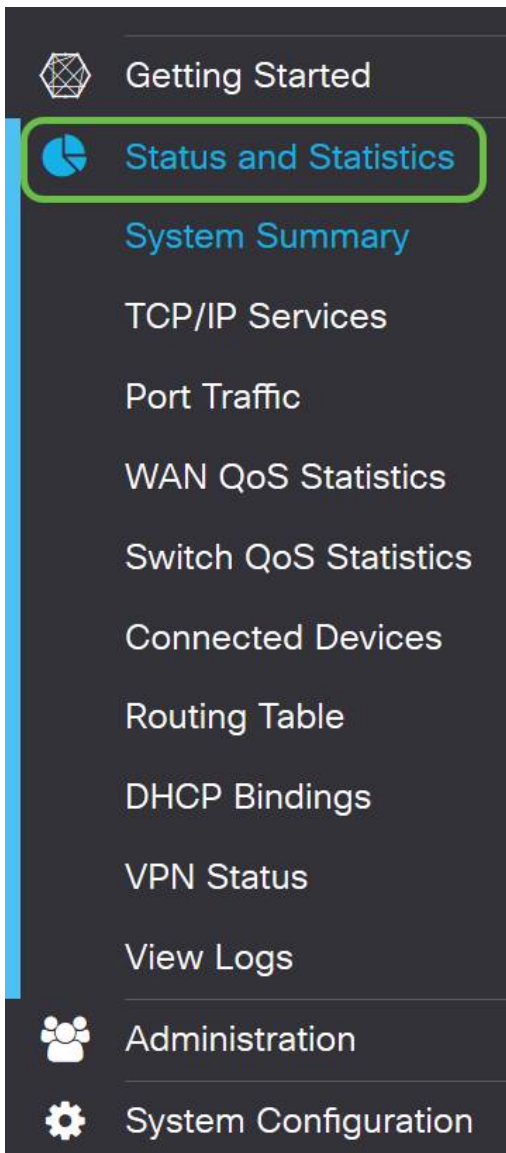


The screenshot shows the 'Hardware DMZ' configuration page. The 'Enable' checkbox is checked. The 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range' radio button is unselected. The 'IP Range' and 'To' fields are empty. In the top right corner, the 'Apply' button is highlighted with a green border, and the 'Cancel' button is visible next to it.

Überprüfen der ordnungsgemäßen Einrichtung der DMZ

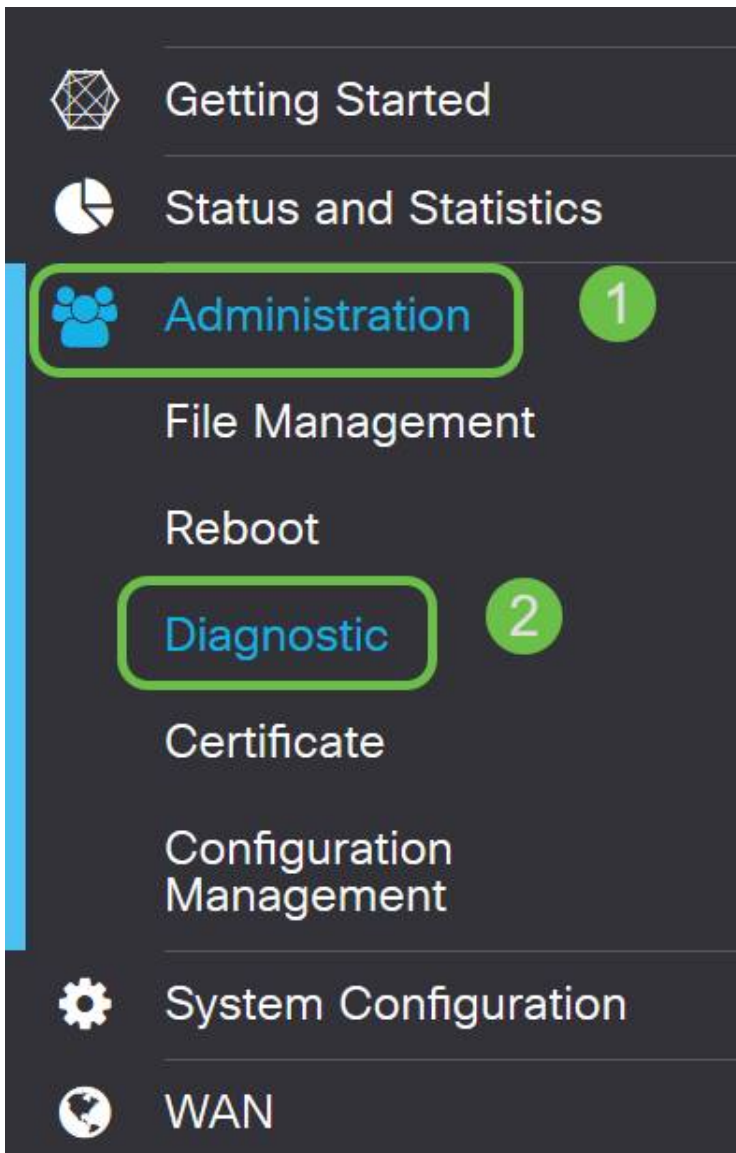
Die Überprüfung, ob die DMZ so konfiguriert ist, dass sie Datenverkehr von Quellen außerhalb ihrer Zone angemessen akzeptiert, reicht ein Ping-Test aus. Zuerst aber wird die Administrationsschnittstelle angehalten, um den Status der DMZ zu überprüfen.

Schritt 1: Um zu überprüfen, ob die DMZ konfiguriert ist, navigieren Sie zu **Status & Statistics**, die Seite Systemübersicht wird automatisch geladen. Port 8 oder "Lan 8" listet den Status der DMZ als "*Connected*" auf.

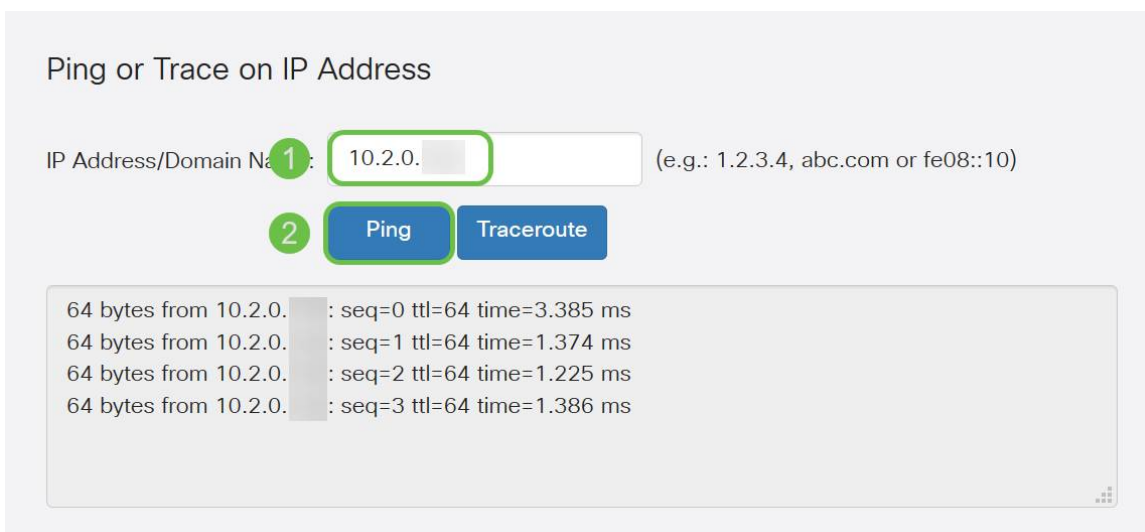


Mit der Trusty ICMP-Ping-Funktion können wir testen, ob die DMZ wie erwartet funktioniert. Die ICMP-Meldung oder einfach "ping" versucht, an die Tür der DMZ zu klopfen. Wenn die DMZ mit "Hello" antwortet, ist der Ping abgeschlossen.

Schritt 2: Um in Ihrem Browser zur Ping-Funktion zu navigieren, klicken Sie auf **Administration > Diagnostic (Verwaltung > Diagnose)**.



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



Wenn der Ping erfolgreich ist, wird eine Meldung wie oben 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.

Schlussfolgerung

Nachdem Sie die Einrichtung der DMZ abgeschlossen haben, sollten Sie in der Lage sein, von außerhalb des LAN auf die Services zuzugreifen.