

Opzioni DMZ per router RV160/RV260

Obiettivo

Questo documento descrive le due opzioni per la configurazione di una zona demilitarizzata: host DMZ e subnet DMZ sui router serie RV160X/RV260X.

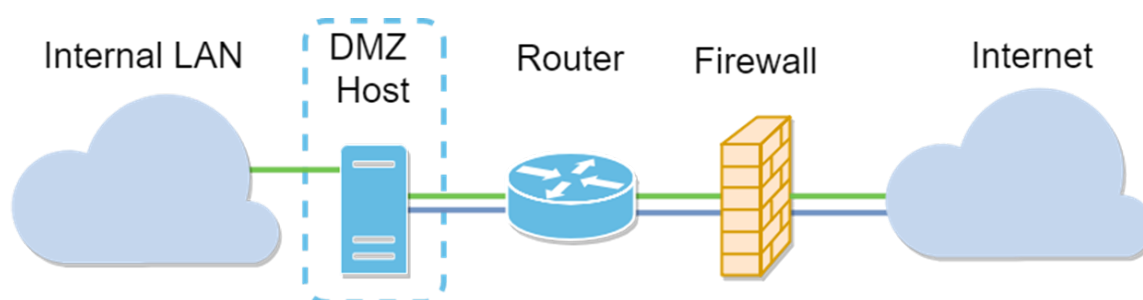
Requisiti

- RV160X
- RV260X

Introduzione

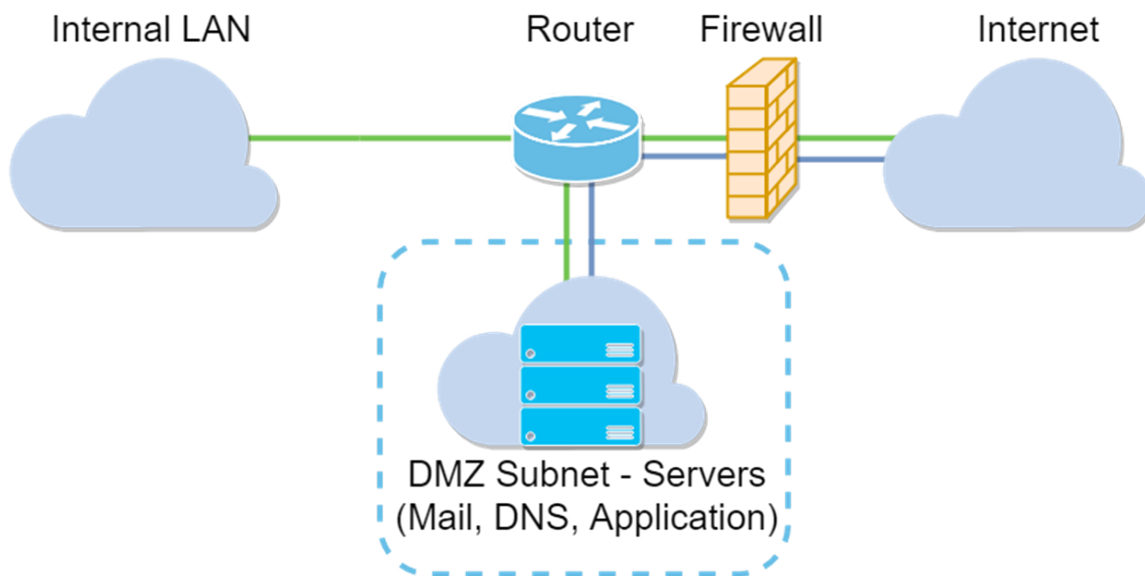
Una zona demilitarizzata è una posizione in una rete aperta a Internet che protegge la rete locale (LAN) da un firewall. La separazione della rete principale da un singolo host o da un'intera sottorete, o "subnet", garantisce che gli utenti che visitano il server del sito Web tramite la DMZ non abbiano accesso alla LAN. Cisco offre due metodi per utilizzare le DMZ nella rete, entrambi dotati di importanti differenze nel modo in cui operano. I riferimenti visivi riportati di seguito evidenziano la differenza tra le due modalità operative.

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



Tipo DMZ	Confronta	Contrasto
Host	Separa il traffico	Host singolo, completamente aperto a Internet
Subnet/Intervallo	Separa il traffico	Più dispositivi e tipi, completamente aperti a Internet. Disponibile solo su hardware RV260.

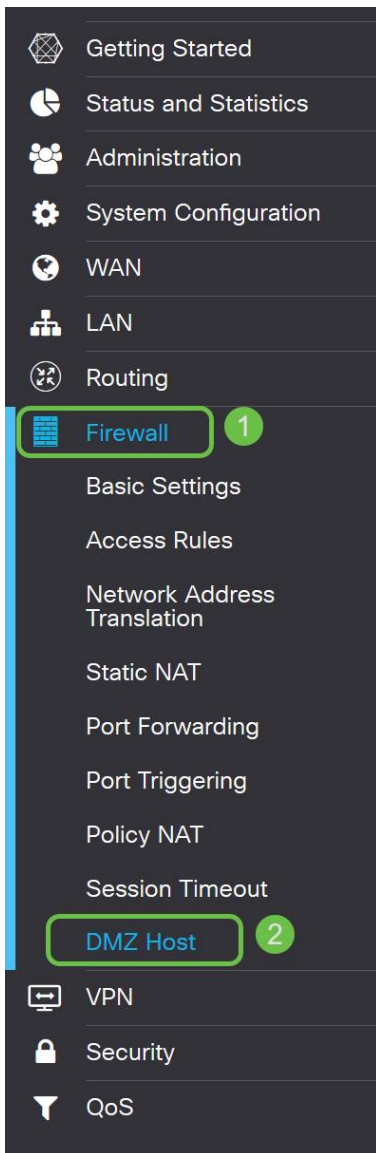
Informazioni sull'indirizzamento IP

In questo articolo vengono utilizzati schemi di indirizzamento IP che presentano alcune sfumature nel loro utilizzo. 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. Per ottenere un indirizzo IP pubblico, è necessario contattare il proprio (ISP).

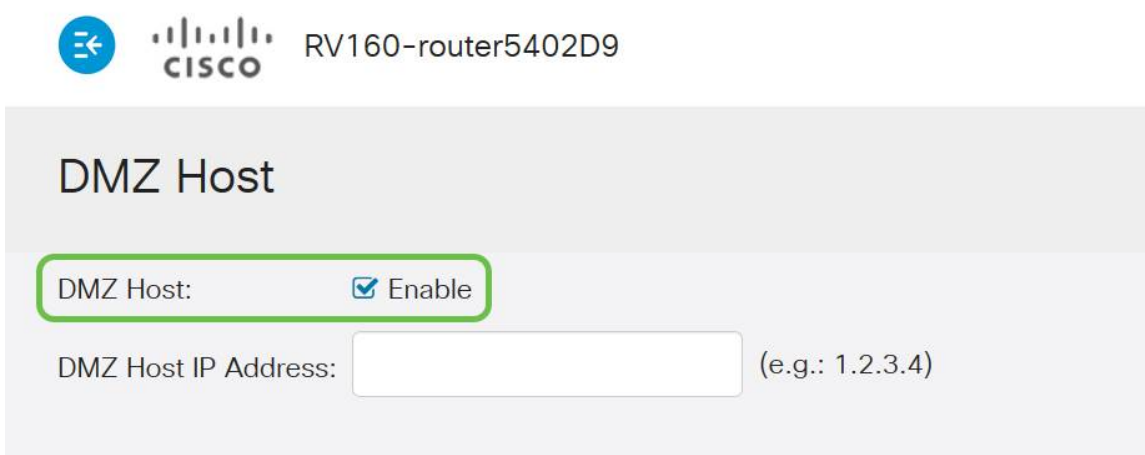
Configurazione dell'host DMZ

Le informazioni richieste per questo metodo includono l'indirizzo IP dell'host desiderato. L'indirizzo IP può essere pubblico o privato, ma l'indirizzo IP pubblico deve trovarsi in una subnet diversa dall'indirizzo IP WAN. L'opzione DMZ Host è disponibile sia su RV160X che su RV260X. Configurare l'host DMZ attenendosi alla seguente procedura.

Passaggio 1. Dopo aver effettuato l'accesso al dispositivo di routing, nella barra dei menu a sinistra fare clic su **Firewall > DMZ Host**.



Passaggio 2. Fare clic sulla casella di controllo **Abilita**.



Passaggio 3. Immettere l'indirizzo IP designato dell'host che si desidera aprire per l'accesso WAN.



RV160-router5402D9

DMZ Host

DMZ Host:

Enable

DMZ Host IP Address:

10.2.

(e.g.: 1.2.3.4)

Passaggio 4. Una volta ottenuto l'indirizzo desiderato, fare clic sul pulsante Applica.

Apply

Cancel

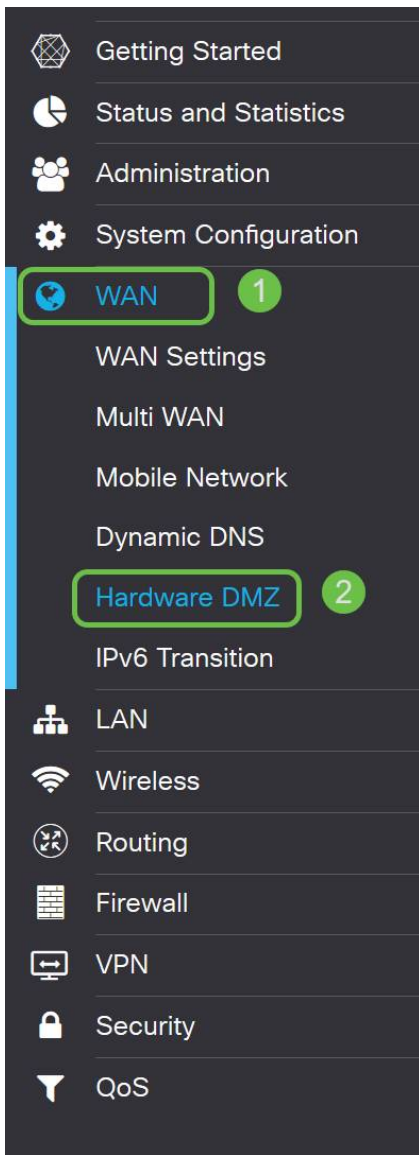
Nota: Se si utilizza solo una serie RV160X e si desidera passare alle istruzioni di verifica, [fare clic qui per passare alla sezione corrispondente del presente documento](#).

Configurazione di DMZ hardware

Disponibile solo per la serie RV260X, questo metodo richiede informazioni di indirizzamento IP diverse a seconda del metodo scelto. Entrambi i metodi utilizzano infatti le sottoreti per definire la zona, la differenza è la quantità di sottorete utilizzata per creare la zona demilitarizzata. In questo caso, le opzioni sono *tutte* o *alcune*. Il metodo Subnet (*all*) richiede l'indirizzo IP della DMZ stessa, insieme alla subnet mask. Questo metodo occupa tutti gli indirizzi IP che appartengono alla sottorete specificata, mentre il metodo Range (*some*) consente di definire un intervallo continuo di indirizzi IP da posizionare nella DMZ.

Nota: In entrambi i casi, sarà necessario collaborare con l'ISP per definire lo schema di indirizzamento IP della sottorete.

Passaggio 1. Dopo aver effettuato l'accesso al dispositivo RV260X, fare clic su **WAN > DMZ hardware**



Nota: Gli screenshot sono tratti dall'interfaccia utente di RV260X. Di seguito è riportata la schermata delle opzioni DMZ hardware che verrà visualizzata in questa pagina.



Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet

DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

Passaggio 2. Selezionare la casella di controllo **Abilita (Cambia LAN8 in porta DMZ)**. In questo modo, l'ottava porta del router viene convertita in una "finestra" DMZ only per offrire servizi che richiedono una sicurezza avanzata.

Hardware DMZ

Enable (Change LAN8 to DMZ port)

Subnet


DMZ IP Address:

Subnet Mask:

Range (DMZ & WAN within same subnet)

IP Range: To

Passaggio 3. Dopo aver fatto clic su **Abilita**, viene visualizzato un messaggio informativo sotto le opzioni selezionabili. Esaminare i dettagli relativi ai punti che possono influire sulla rete e fare clic su **OK**. **Accetto la casella di controllo precedente.**

 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.

Passo 4: il passo successivo si divide in due potenziali opzioni, Subnet e Intervallo. Nell'esempio seguente è stato selezionato il metodo **Subnet**.

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

Nota: Se si intende utilizzare il metodo Range, sarà necessario fare clic sul pulsante radiale **Range**, quindi immettere l'intervallo di indirizzi IP assegnato dall'ISP.

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

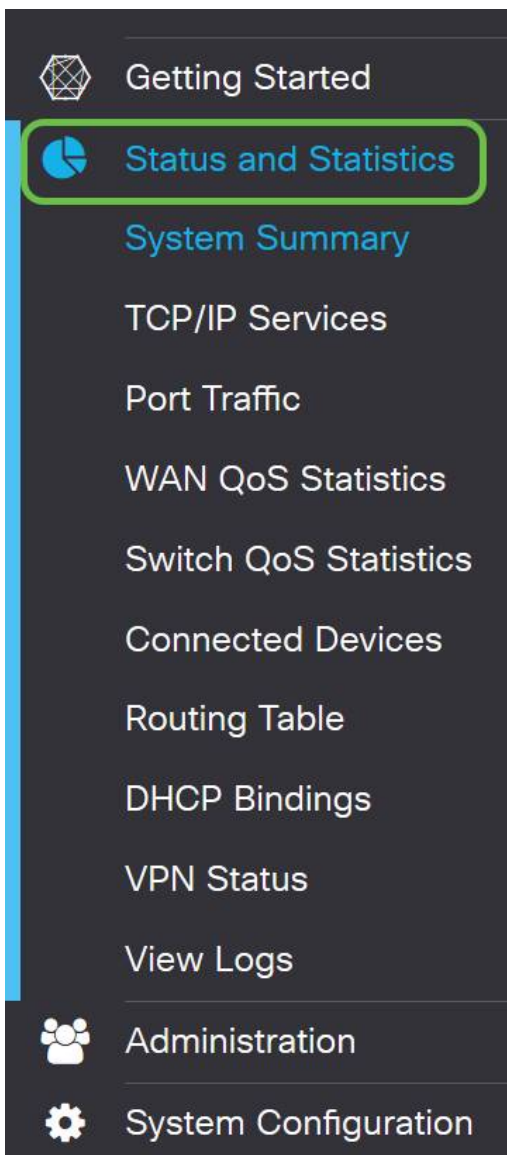


The screenshot shows the 'Hardware DMZ' configuration page. The 'Enable' checkbox is checked. The 'Subnet' radio button is selected. The 'DMZ IP Address' field contains '164.33.100.250' and the 'Subnet Mask' field contains '255.255.255.248'. The 'Range' radio button is unselected. The 'IP Range' and '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.

Verifica della corretta configurazione della DMZ

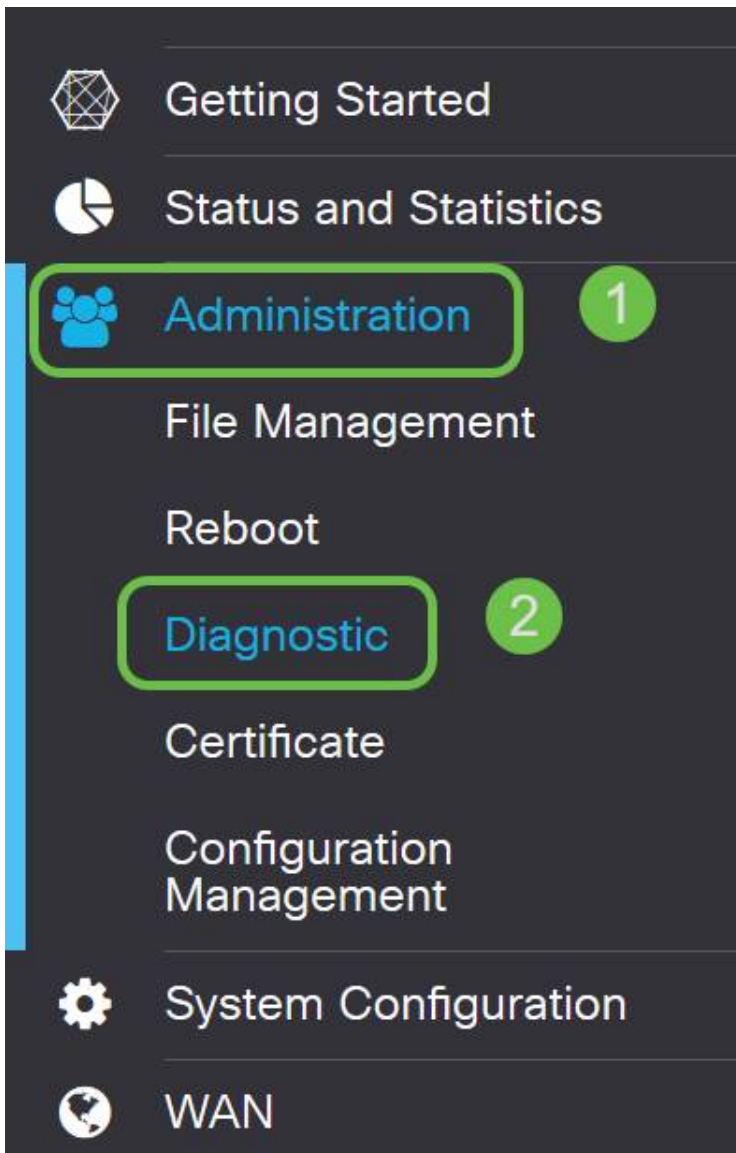
Per verificare che la DMZ sia configurata in modo da accettare in modo appropriato il traffico proveniente da fonti esterne alla sua zona, è sufficiente un test ping. Per prima cosa, ci fermeremo all'interfaccia amministrativa per controllare lo stato della DMZ.

Passaggio 1. Per verificare che la DMZ sia configurata, passare a **Stato e statistiche**, la pagina caricherà automaticamente la pagina di riepilogo del sistema. La porta 8 o "Lan 8" visualizzerà lo stato della DMZ come "*Connesso*".



È possibile utilizzare la funzionalità ping ICMP per verificare se la DMZ funziona come previsto. Il messaggio ICMP, o semplicemente "ping", cerca di bussare alla porta della DMZ. Se la DMZ risponde dicendo "Ciao", il ping è completato.

Passaggio 2. Per individuare la funzione ping nel browser, fare clic su **Amministrazione > Diagnostica**.



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



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

Conclusioni

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