Konfiguration eines demilitarisierten Zonenports mit Subnetzmaske auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Eine DMZ (De-Militarized Zone) ist ein Teil eines internen Netzwerks einer Organisation, das für ein nicht vertrauenswürdiges Netzwerk wie das Internet verfügbar gemacht wird. Eine DMZ trägt zur Verbesserung der Sicherheit im internen Netzwerk eines Unternehmens bei. Anstatt alle internen Ressourcen über das Internet verfügbar zu machen, sind nur bestimmte Hosts wie Webserver verfügbar.

Wenn eine Zugriffskontrollliste (ACL) an eine Schnittstelle gebunden ist, werden ACE-Regeln (Access Control Element) auf Pakete angewendet, die an dieser Schnittstelle ankommen. Pakete, die keinem der ACEs in der ACL entsprechen, werden einer Standardregel zugeordnet, deren Aktion darin besteht, nicht übereinstimmende Pakete zu verwerfen. In diesem Artikel wird erläutert, wie der DMZ-Port konfiguriert wird und wie Datenverkehr von der DMZ zu bestimmten Ziel-IP-Adressen zugelassen wird.

Unterstützte Geräte

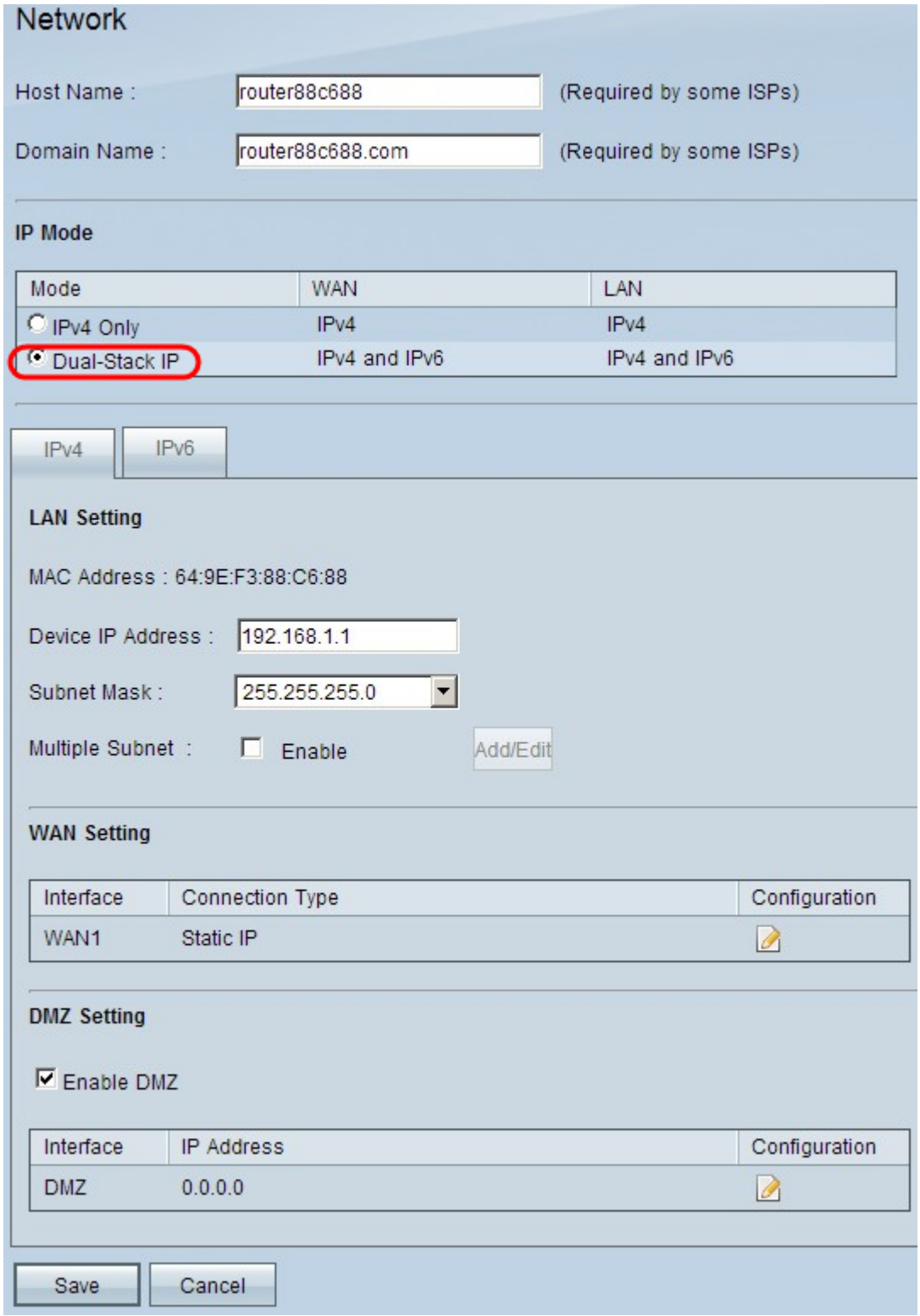
RV016
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

ãƒ» v4.2.2.08

DMZ-Konfiguration mit Subnetz

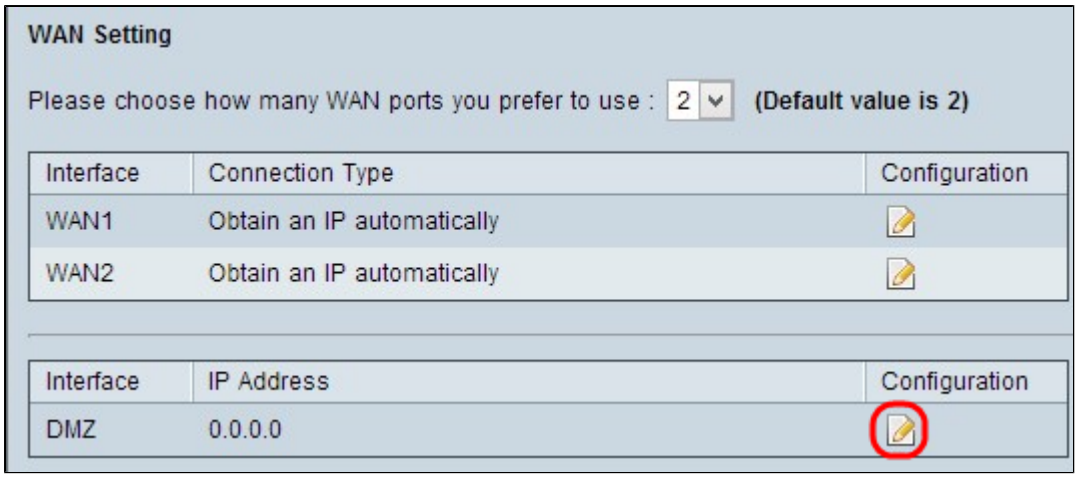
Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Setup > Network (Setup > Netzwerk)**. Die Seite *Netzwerk* wird geöffnet:



Schritt 2: Um die DMZ für eine IPv4- oder IPv6-Adresse zu konfigurieren, klicken Sie auf die entsprechende Registerkarte im Feld für die LAN-Einstellung.

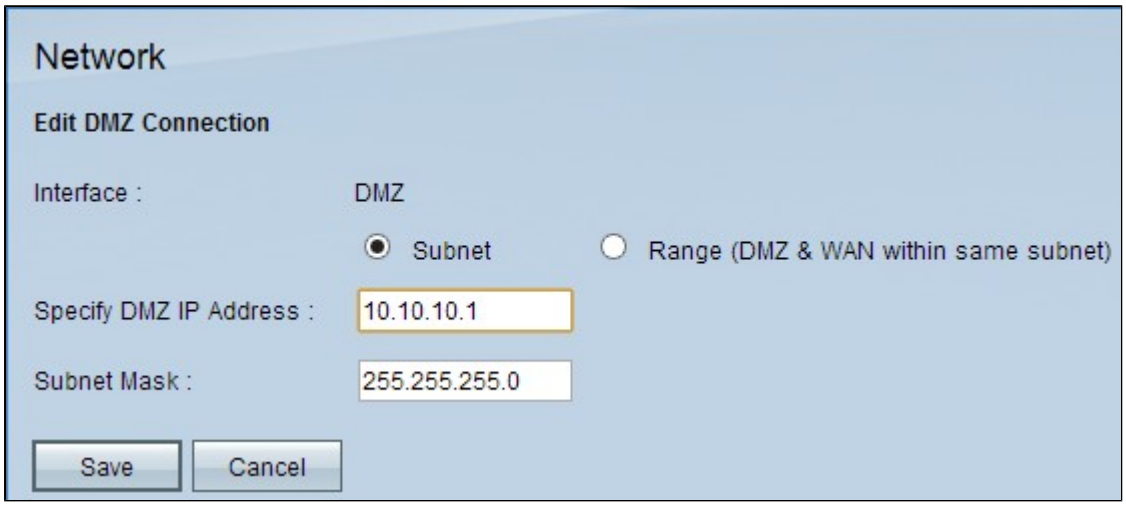
Hinweis: Dual-Stack IP im Bereich *IP Mode (IP-Modus*) muss aktiviert sein, wenn Sie IPv6 konfigurieren möchten.

Schritt 3: Blättern Sie nach unten zum Feld DMZ-Einstellung, und klicken Sie auf das Optionsfeld **DMZ aktivieren**, um DMZ zu aktivieren.



Schritt 4: Klicken Sie auf das Symbol für die **DMZ-Konfiguration**, um das Subnetz zu konfigurieren. Die Konfiguration kann für IPv4 und IPv6 folgendermaßen erfolgen:

IPv4-Konfiguration



Schritt 5: Klicken Sie auf das Optionsfeld **Subnetz**, um die DMZ für ein anderes Subnetz als das WAN zu konfigurieren. Für Subnetz-IP sollte Folgendes konfiguriert werden:

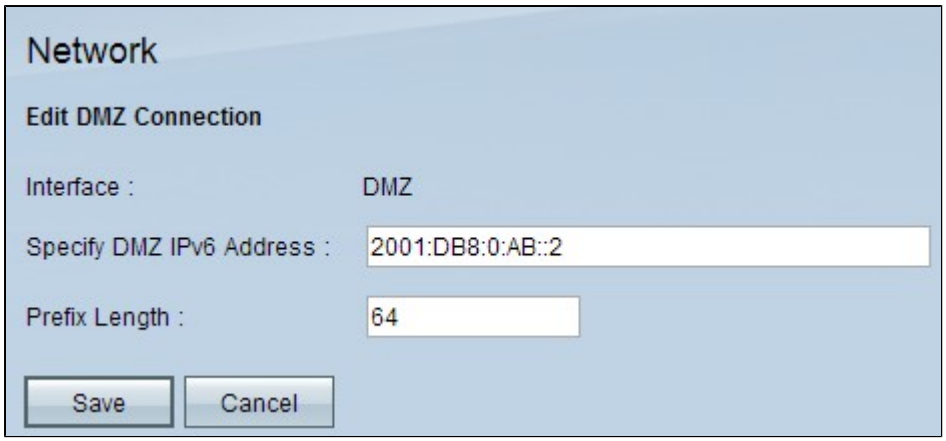
ãƒ» DMZ-IP-Adresse angeben â€" Geben Sie die DMZ-IP-Adresse in das Feld **DMZ-IP-Adresse angeben ein**.

ãƒ» Subnetzmaske â€" Geben Sie die Subnetzmaske in das Feld **Subnetzmaske ein.**

Warnung: Hosts mit einer IP-Adresse in der DMZ sind nicht so sicher wie Hosts innerhalb Ihres internen LAN.

Schritt 6: Klicken Sie auf **Range** (Bereich), um die DMZ so zu konfigurieren, dass sie sich im selben Subnetz wie das WAN befindet. Der Bereich der IP-Adressen muss in das Feld **IP Range for DMZ port (IP-Bereich für DMZ-Port)** eingegeben werden.

IPv6-Konfiguration



Hinweis: Für die IPv6-Konfiguration sind folgende Optionen verfügbar:

Schritt 7. DMZ-IPv6-Adresse angeben â€" Geben Sie die IPv6-Adresse ein.

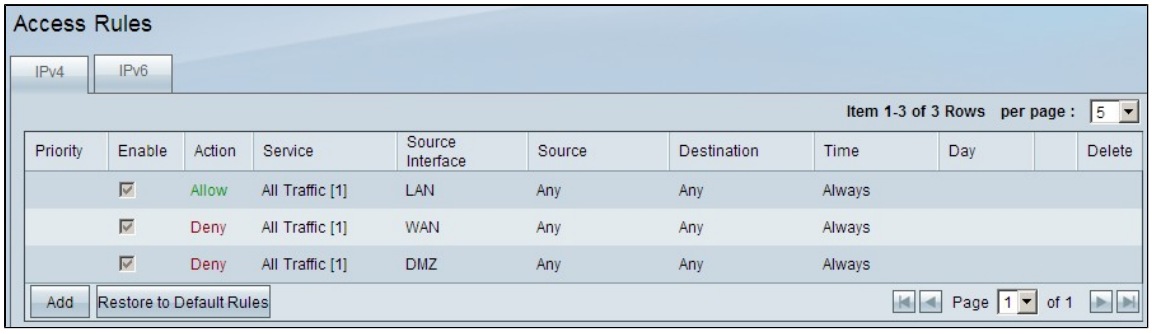
Schritt 8: Präfixlänge - Die Präfixlänge der oben genannten DMZ-IP-Adressdomäne ist einzugeben.

Schritt 9. Klicken Sie auf **Speichern**, um die Konfiguration zu speichern.

Konfiguration von Zugriffsregeln

Mit dieser Konfiguration werden die Zugriffslisten für die IPs definiert, die in den mehreren Subnetzmasken konfiguriert sind.

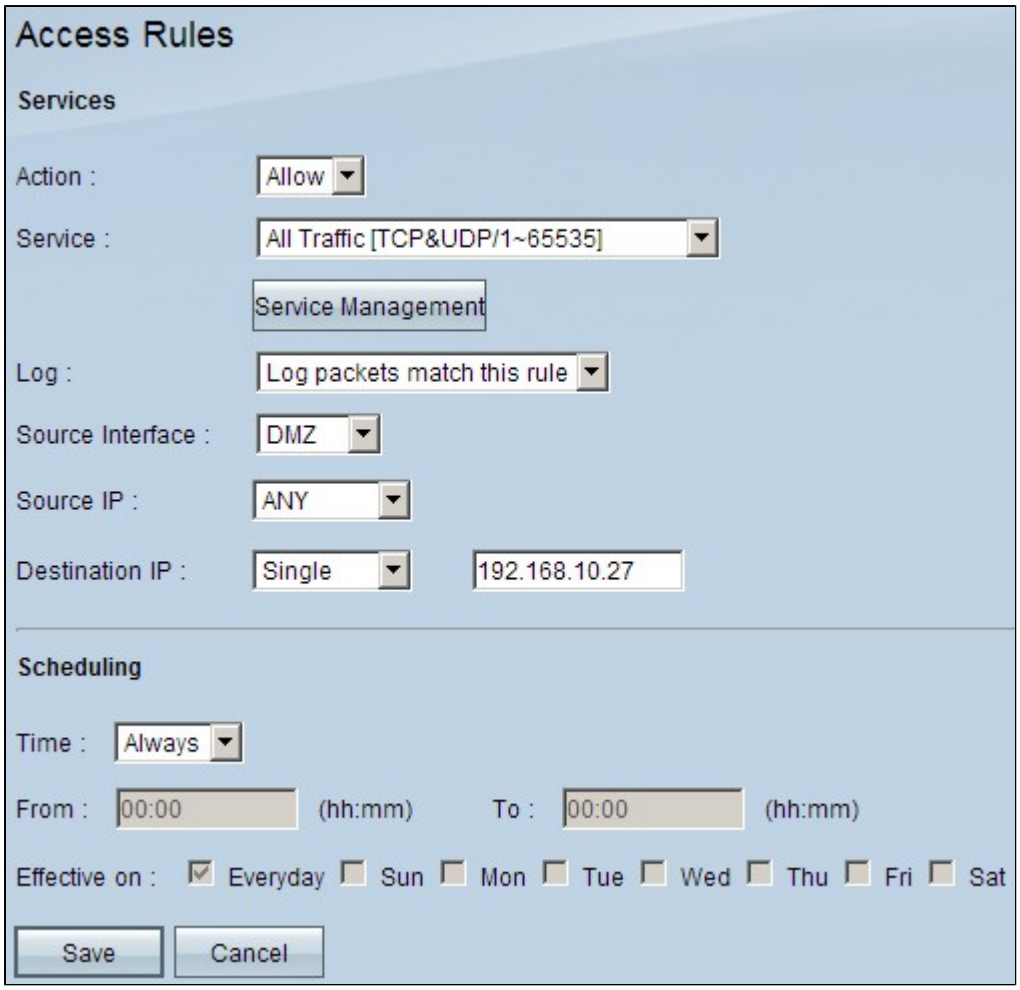
Schritt 1: Melden Sie sich beim Router-Konfigurationsprogramm an, und wählen Sie **Firewall > Access Rules**. Die Seite *Zugriffsregeln* wird geöffnet:



Hinweis: Die Standardzugriffsregeln können nicht bearbeitet werden.

Schritt 2: Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Zugriffsregel hinzuzufügen. Die Seite "*Zugriffsregeln*" wird geändert, um die Bereiche "Services" und "Planung" anzuzeigen.

Hinweis: Diese Konfiguration kann sowohl für IPv4 als auch für IPv6 vorgenommen werden, indem die entsprechenden Registerkarten auf der Seite *Access Rules (Zugriffsregeln)* ausgewählt werden. Die für IPv4 und IPv6 spezifischen Konfigurationsschritte werden in den folgenden Schritten erläutert.



Schritt 3: Wählen Sie **Zulassen** aus der Dropdown-Liste Aktion aus, um den Dienst zuzulassen.

Schritt 4: Wählen Sie **in** der Dropdown-Liste "Service" die Option **Gesamter Datenverkehr [TCP&UDP/1~65535**] aus, um alle Services für die DMZ zu aktivieren.

Schritt 5: Wählen Sie **Protokollpakete, die dieser Regel entsprechen,** aus der Dropdown-Liste aus, um nur Protokolle auszuwählen, die der Zugriffsregel entsprechen.

Schritt 6: Wählen Sie **DMZ** aus der Dropdown-Liste Source Interface (Quellschnittstelle) aus, die die Quelle für die Zugriffsregeln darstellt.

Schritt 7. Wählen Sie **Any (Beliebig**) aus der Dropdown-Liste Source IP (Quell-IP) aus.

Schritt 8: Wählen Sie eine der folgenden verfügbaren Optionen aus der Dropdown-Liste Destination IP (Ziel-IP) aus.

ãƒ» Einzel - Wählen Sie eine Einzel-IP-Adresse, um diese Regel auf eine einzelne IP-Adresse anzuwenden.

ãƒ» Bereich - Wählen Sie den Bereich aus, um diese Regel auf einen IP-Adressbereich anzuwenden. Geben Sie die erste und letzte IP-Adresse des Bereichs ein. Diese Option ist nur in IPv4 verfügbar.

ãƒ» Subnetz â€" Wählen Sie Subnetz aus, um diese Regeln auf ein Subnetz anzuwenden. Geben Sie die IP-Adresse und die CIDR-Notation ein, die für die Zuweisung von IP-Adressen und die Weiterleitung von Internetprotokollpaketen für das Subnetz verwendet wird. Diese Option ist nur bei IPv6 verfügbar.

ãƒ» Beliebig - Wählen Sie Beliebig aus, um die Regel auf eine beliebige IP-Adresse anzuwenden.

Timesaver: Fahren Sie mit Schritt 10 fort, wenn Sie IPv6-Zugriffsregeln konfigurieren.

Schritt 9. Wählen Sie in der Dropdown-Liste Zeit (Time) eine Methode aus, mit der definiert werden soll, wann die Regeln aktiv sind. Dazu gehören:

ãƒ» Immer - Wenn Sie Immer aus der Dropdown-Liste "Zeit" wählen, werden die Zugriffsregeln immer auf den Datenverkehr angewendet.

ãƒ» Intervall - Sie können ein bestimmtes Zeitintervall auswählen, in dem die Zugriffsregeln aktiv sind, wenn Sie in der Dropdown-Liste Zeit die Option Intervall auswählen. Nachdem Sie das Zeitintervall festgelegt haben, wählen Sie die Tage aus, an denen die Zugriffsregeln in den Kontrollkästchen "Gültig für" aktiviert werden sollen.

Schritt 10. Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern.

Schritt 11. Klicken Sie auf das Symbol **Bearbeiten**, um die erstellte Zugriffsregel zu bearbeiten.

Schritt 12: Klicken Sie auf das Symbol **Löschen**, um die erstellte Zugriffsregel zu löschen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.