Fehlerbehebung bei Zugriffslisten über Virtual Private Network auf RV016-, RV042-, RV042G- und RV082-VPN-Routern

Ziele

Eine Zugriffskontrollliste (ACL) ist eine Sammlung von Bedingungen für die Genehmigung und die Ablehnung. Eine ACL gibt an, welchen Benutzer- oder Systemprozessen Zugriff auf bestimmte Ressourcen gewährt wird. Eine ACL kann ungerechtfertigte Versuche blockieren, auf Netzwerkressourcen zuzugreifen. Das Problem kann in dieser Situation auftreten, wenn Sie auf beiden Routern ACLs konfiguriert haben, aber einer der Router nicht zwischen der Liste zulässiger und abgelehnter Zugriffe unterscheiden kann, die von der ACL zugelassen werden. Zenmap, ein Open-Source-Tool zur Überprüfung des Typs der aktiven Paketfilter/Firewalls, wird zum Testen der Konfiguration verwendet.

In diesem Artikel wird die Fehlerbehebung für zulässige ACLs erläutert, die nicht über Gateway-to-Gateway-VPN zwischen zwei VPN-Routern funktionieren.

Unterstützte Geräte

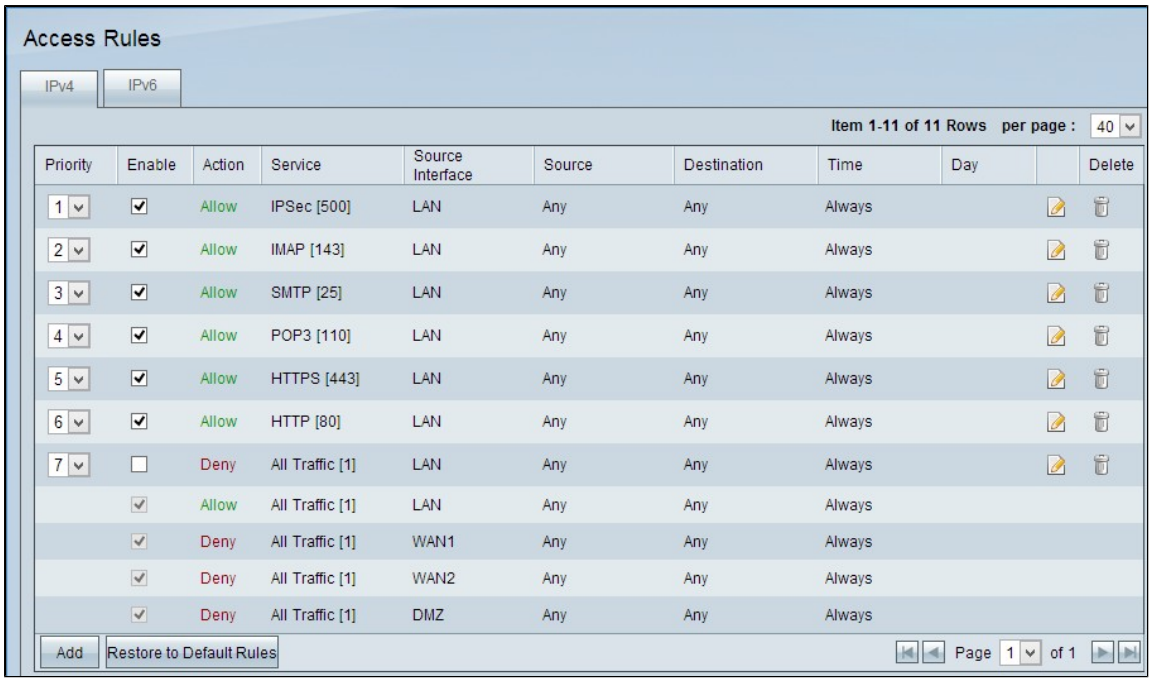
RV016
â€¢RV042
ãƒ» RV042G
RV082

Software-Version

ãƒ» v4.2.2.08

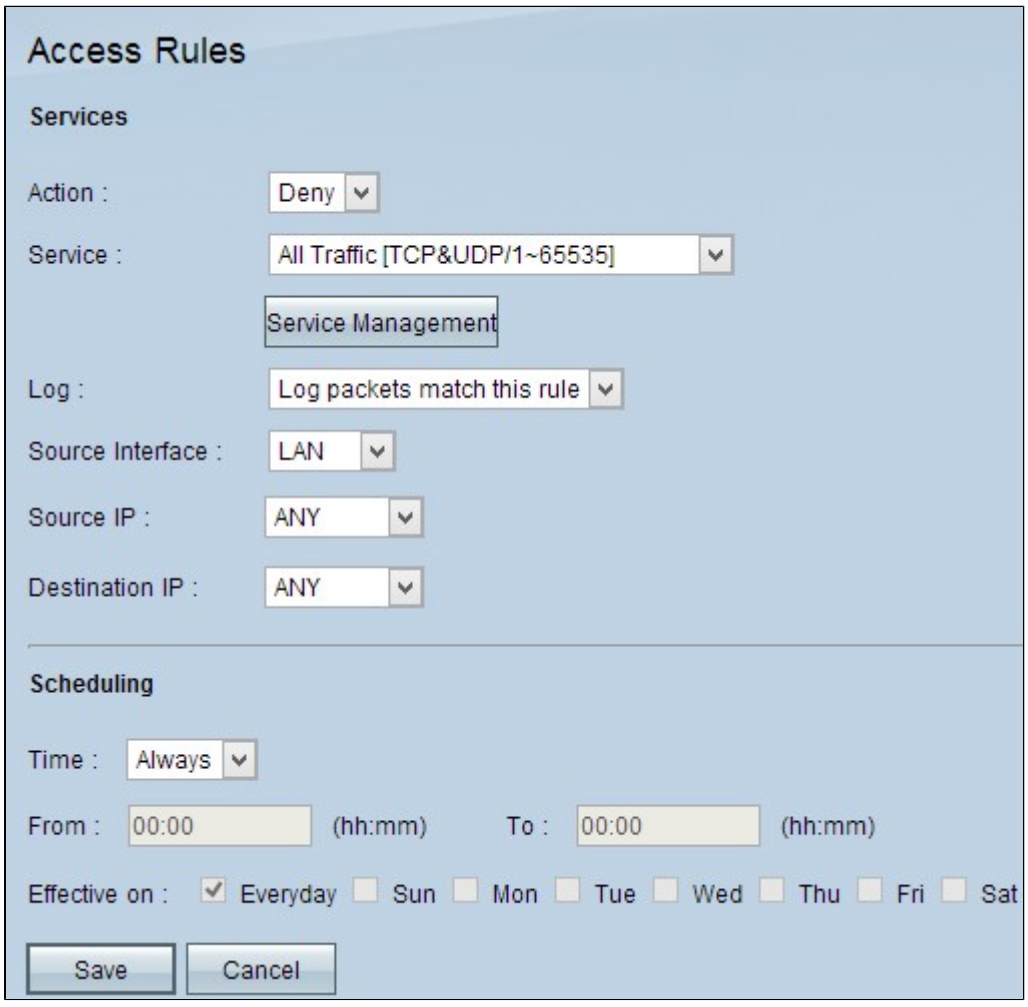
Konfiguration von ACL über VPN

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Access Rules aus**. Die Seite *Zugriffsregel* wird geöffnet:

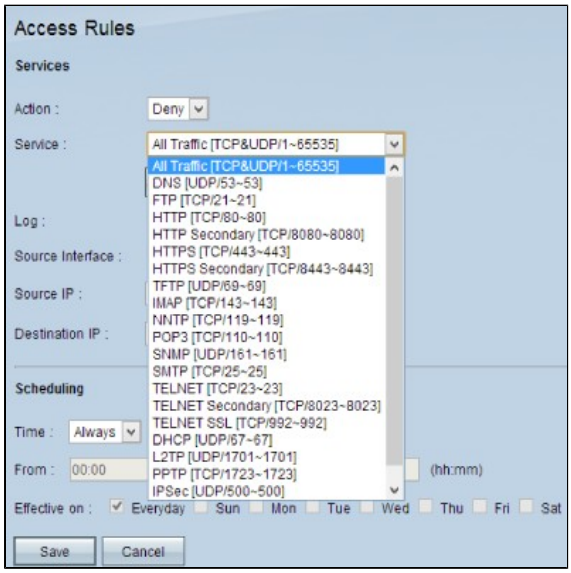


Hinweis: Die Standardzugriffsregeln können nicht bearbeitet werden. Die im obigen Bild erwähnten, vom Benutzer konfigurierten Zugriffsregeln können mit dem folgenden Prozess bearbeitet werden.

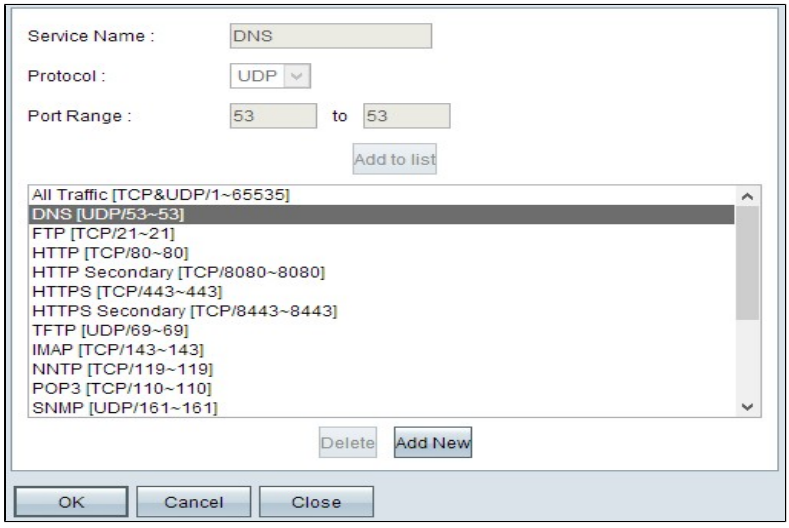
Schritt 2: Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue Zugriffsregel hinzuzufügen. Die Seite "*Zugriffsregeln*" wird geändert, um die Bereiche "Services" und "Planung" anzuzeigen. Das Hinzufügen einer Zugriffsregel wird in den folgenden Schritten erläutert.



Schritt 3: Wählen Sie in der Dropdown-Liste Aktion die Option **Verweigern** aus, um den Dienst abzulehnen.



Schritt 4: Wählen Sie in der Dropdown-Liste "**Service**" den erforderlichen Service aus, der auf die Regel angewendet wird.



Schritt 5: (Optional) Um einen Service hinzuzufügen, der nicht in der Dropdown-Liste "Service" enthalten ist, klicken Sie auf **Service Management**. In Service Management kann nach Bedarf ein Service erstellt werden. Nachdem ein Dienst erstellt wurde, klicken Sie auf **OK**, um die Einstellungen zu speichern.

Schritt 6: Wählen Sie **Protokollpakete, die dieser Regel entsprechen,** aus der Dropdown-Liste "Protokoll" aus, und zwar nur für Protokolle, die übereinstimmen, oder **Nicht protokollieren** für Protokolle, die nicht mit der Zugriffsregel übereinstimmen.

Schritt 7. Wählen Sie in der Dropdown-Liste "Source Interface" (Quellschnittstelle) einen Schnittstellentyp aus, der die Quelle für die Zugriffsregeln darstellt. Folgende Optionen sind verfügbar:

ãƒ» LAN â€" Wählen Sie LAN aus, wenn die Quellschnittstelle das LAN ist.

ãƒ» WAN - Wählen Sie WAN, wenn die Quellschnittstelle der ISP ist.

ãƒ» DMZ - Wählen Sie DMZ, wenn die Quellschnittstelle die entmilitarisierte Zone ist.

ãƒ» BELIEBIG â€" Wählen Sie BELIEBIG, um die Quellschnittstelle als eine der oben genannten Schnittstellen zu definieren.

Schritt 8: Wählen Sie in der Dropdown-Liste Source IP (Quell-IP) die gewünschte(n) Quelladresse(n) aus, die auf die Zugriffsregel angewendet werden soll(en). Folgende Optionen sind verfügbar:

ãƒ» Einfach - Wählen Sie Einfach, wenn es sich um eine einzelne IP-Adresse handelt, und geben Sie die IP-Adresse ein.

ãƒ» Bereich - Wählen Sie Bereich, wenn es sich um einen IP-Adressbereich handelt, und geben Sie die erste und letzte IP-Adresse in den Bereich ein.

ãƒ» ANY (BELIEBIG) - Wählen Sie ANY (BELIEBIG) aus, um die Regeln auf alle Quell-IP-Adressen anzuwenden.

Schritt 9. Wählen Sie in der Dropdown-Liste Destination IP (Ziel-IP) die gewünschte(n) Zieladresse(n) aus, die für die Zugriffsregel gilt. Folgende Optionen sind verfügbar:

ãƒ» Einfach - Wählen Sie Einfach, wenn es sich um eine einzelne IP-Adresse handelt, und geben Sie die IP-Adresse ein.

ãƒ» Bereich - Wählen Sie Bereich, wenn es sich um einen IP-Adressbereich handelt, und geben Sie die erste und letzte IP-Adresse in den Bereich ein.

ãƒ» ANY (BELIEBIG) - Wählen Sie ANY (BELIEBIG) aus, um die Regeln auf alle Ziel-IP-Adressen anzuwenden.

Schritt 10. Wählen Sie in der Dropdown-Liste Zeit (Time) eine Methode aus, mit der definiert werden soll, wann die Regeln aktiv sind. Dazu gehören:

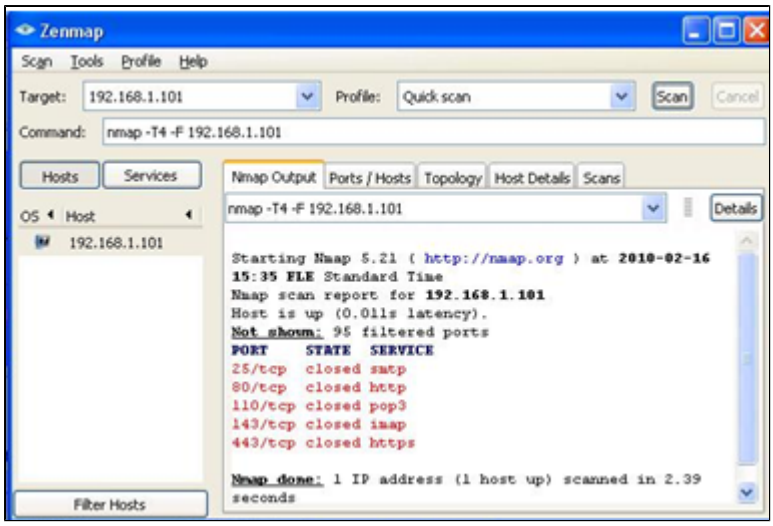
ãƒ» Immer - Wenn Sie Immer aus der Dropdown-Liste "Zeit" wählen, werden die Zugriffsregeln immer auf den Datenverkehr angewendet.

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. Aktivieren Sie nach der Angabe des Zeitintervalls die Kontrollkästchen für die Tage, an denen die Zugriffsregeln im Feld "Gültig am" aktiviert werden sollen.

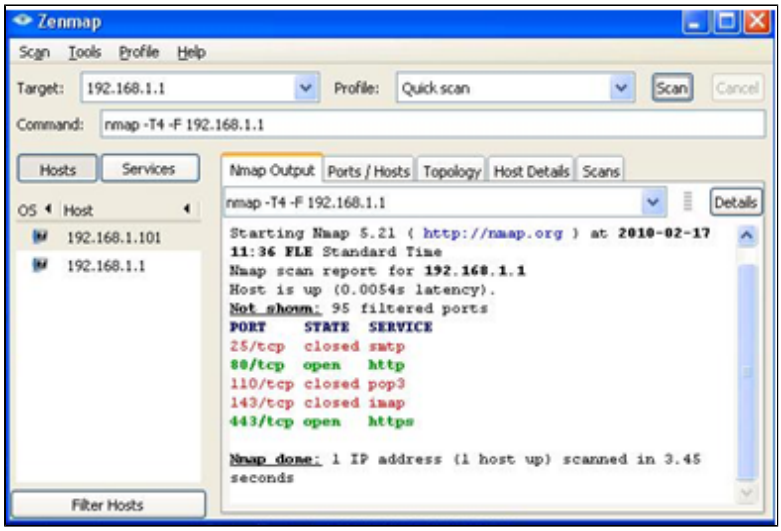
Schritt 11. Klicken Sie auf **Speichern**, um Ihre Einstellungen zu speichern.

Schritt 12: Wiederholen Sie die Schritte 2 bis 10, wobei die Felder mit den entsprechenden Feldern im Bild übereinstimmen. Hierbei werden die Zugriffsregeln für die einzelnen Kunden angewendet. Die ersten 7 lassen einige Dienste zu; die 8. verweigert jeglichen anderen Verkehr. Diese Konfiguration wird auch auf dem zweiten Router vorgenommen. IPSec-Port 500 ist zulässig.

Hinweis: Führen Sie diese Schritte für beide Router aus, um zu überprüfen, ob die Zugriffsregeln wie gewünscht konfiguriert wurden.



VPN-Router 1

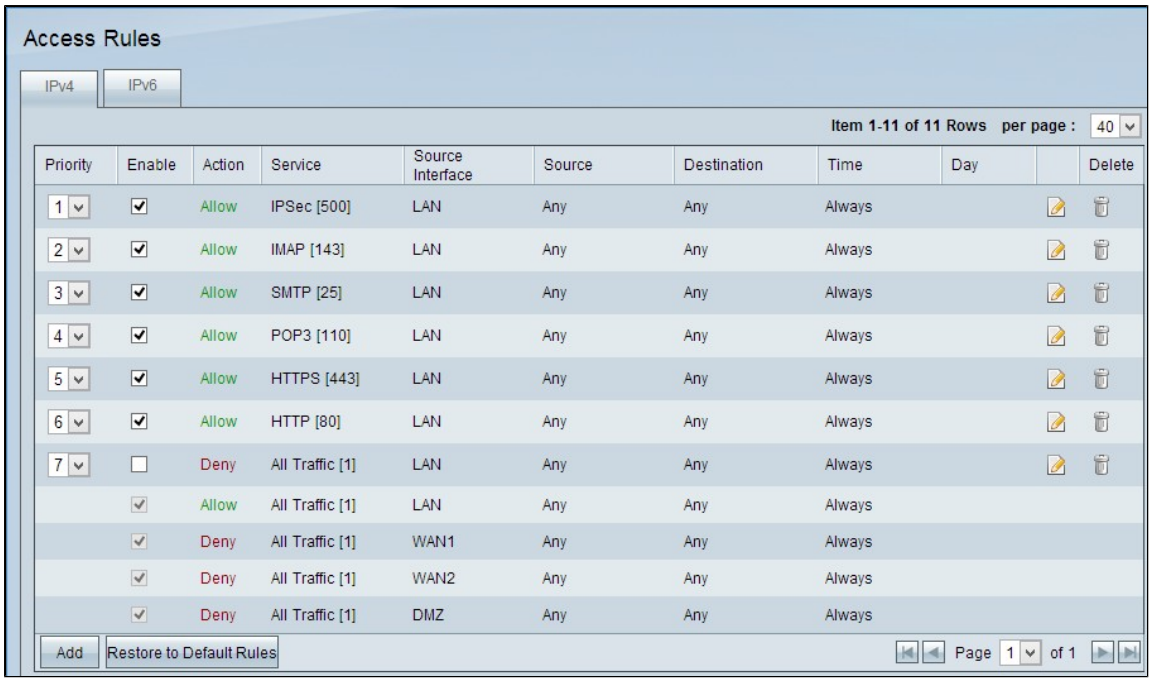


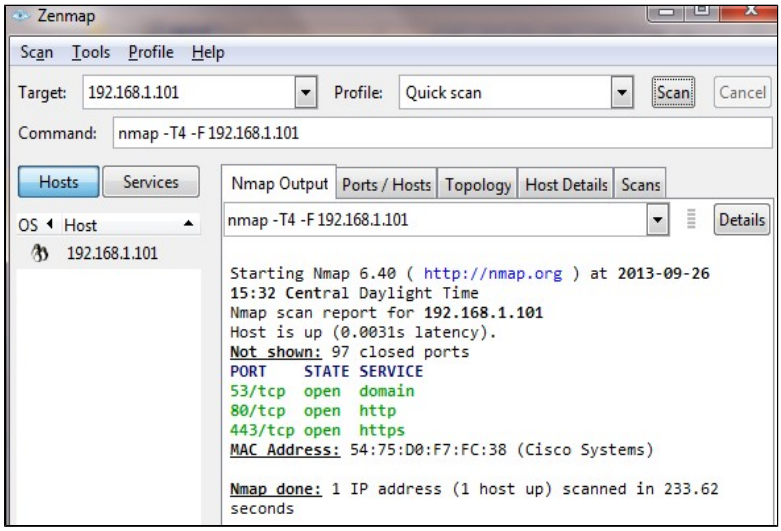
VPN-Router 2

Schritt 13: Installieren Sie Zenmap(NMAP) von http://nmap.org/download.html und starten Sie es auf einem PC im LAN 192.168.2.0.

Hinweis: Dies ist das LAN hinter dem Router mit den sieben zusätzlichen ACLs. Die Ziel-IP-Adresse (192.168.1.101) ist ein PC auf dem Remote-Gateway-LAN.

Schritt 14: Wählen Sie **Schnellsuche** aus dem Profil, und klicken Sie auf **Scannen**. Dadurch können wir die offenen und gefilterten Ports gemäß den ACLs erkennen, das Ergebnis wird in der obigen Abbildung dargestellt. Die Ausgabe zeigt, dass diese Ports geschlossen sind, unabhängig von den zulässigen ACLs, die auf dem RV0xx 1 konfiguriert wurden. Wenn wir versuchen, die Ports zur LAN-IP (192.168.1.1) des Remote-Gateways zu überprüfen, stellen wir fest, dass die Ports 80 und 443 offen sind (die für den PC 192.168.1.101 geschlossen wurden).





Die ACL funktioniert nach dem Entfernen der siebten abgelehnten ACL korrekt und funktioniert einwandfrei, wie wir der Ausgabe entnehmen können.

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.