

Konfiguration der Firewall-Zugriffsregel zum Blockieren von Ping-Paketen aus zwei verschiedenen Netzwerken auf den VPN-Routern RV016, RV042, RV042G und RV082

Ziel

Auf einem Router können zwei verschiedene Netzwerke erforderlich sein, um den Internetzugriff für Geräte bereitzustellen, die sich nicht im gleichen Netzwerk wie der Router befinden. Dies kann durch eine Zugriffsregel erreicht werden, die auf verschiedenen Kriterien basiert, um den Zugriff auf ein Netzwerk oder einen IP-Adressbereich zu erlauben oder zu verweigern. Eine Zugriffsregel erleichtert dem Router die Bestimmung, welcher Datenverkehr die Firewall passieren darf, und erhöht die Sicherheit des Routers.

In diesem Artikel wird erläutert, wie Ping-Pakete von zwei verschiedenen Netzwerken auf RV016-, RV042-, RV042G- und RV082-VPN-Routern mithilfe einer Zugriffsregel blockiert werden.

Unterstützte Geräte

RV016
RV042
RV042G
RV082

Software-Version

v4.2.1.02

Konfiguration von Zugriffsregeln

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

Access Rules

IPv4 IPv6

Item 1-

Priority	Enable	Action	Service	Source Interface	Source	Destination	Time
	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always
	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always

Add Restore to Default Rules

Schritt 2: Klicken Sie auf **Hinzufügen**, um eine Zugriffsregel hinzuzufügen. Die Seite *Access Rules Services* wird geöffnet:

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Schritt 3: Wählen Sie in der Dropdown-Liste Action (Aktion) die gewünschte Aktion aus, die den Datenverkehr passieren lässt, wenn **Allow (Zulassen)** ausgewählt ist. Andernfalls wählen Sie **Verweigern**, um den Datenverkehr abzulehnen.

Schritt 4: Wählen Sie den entsprechenden Service aus der Dropdown-Liste aus.

Hinweis: Wenn der gewünschte Service verfügbar ist, fahren Sie mit Schritt 10 fort.

Schritt 5: Wenn der entsprechende Service nicht verfügbar ist, klicken Sie auf **Service Management**, und das Fenster *Service Management* wird angezeigt:

Service Name :

Protocol :

Port Range : to

All Traffic [TCP&UDP/1~65535]
 DNS [UDP/53~53]
 FTP [TCP/21~21]
 HTTP [TCP/80~80]
 HTTP Secondary [TCP/8080~8080]
 HTTPS [TCP/443~443]
 HTTPS Secondary [TCP/8443~8443]
 TFTP [UDP/69~69]
 IMAP [TCP/143~143]
 NNTP [TCP/119~119]
 POP3 [TCP/110~110]
 SNMP [UDP/161~161]

Schritt 6: Geben Sie den gewünschten Servicenamen in das Feld "Servicename" ein.

Schritt 7. Wählen Sie in der Dropdown-Liste "Protocol" (Protokoll) einen geeigneten Protokolltyp aus:

~f» TCP - Das Transmission Control Protocol ist ein Protokoll, das von Anwendungen verwendet wird, die eine garantierte Übermittlung erfordern.

~f» UDP - User Datagram Protocol verwendet Datagram-Sockets, um die Kommunikation zwischen Host und Host herzustellen.

~f» IPv6 - Leitet Internet-Datenverkehr zwischen Hosts in Paketen weiter, die über Netzwerke geroutet werden, die durch Routing-Adressen spezifiziert sind.

Schritt 8: Geben Sie im Feld Port Range (Port-Bereich) den Port-Bereich ein, der für den Service gilt.

Schritt 9. Klicken Sie auf **Add to List**, um den Service der Dropdown-Liste "Service" auf der Seite *Access Rules* hinzuzufügen.

Schritt 10. Klicken Sie auf **OK**, um das Fenster zu schließen, und der Benutzer wird auf die Seite *Zugriffsregeln* zurückgeführt.

Access Rules

Services

Action :

Service :

Log :

Source Interface :

Source IP :

Destination IP : to

Schritt 11. Wählen Sie **Protokollpakete, die dieser Regel entsprechen**, um die eingehenden Pakete zu protokollieren, die der Zugriffsregel in der Dropdown-Liste "Protokoll" entsprechen.

Schritt 12: Wählen Sie in der Dropdown-Liste "Source Interface" (Quellschnittstelle) eine Schnittstelle aus, die von dieser Regel betroffen ist. Die Quellschnittstelle ist die Schnittstelle, von der aus der Datenverkehr initiiert wird.

âf» LAN - Der Port des lokalen Netzwerks verbindet Computer in unmittelbarer Nähe in einem Netzwerk wie einem Bürogebäude oder einer Schule.

âf» WAN1 - Der WAN-Port verbindet Computer in einem großen Bereich eines Netzwerks. Dies kann jedes Netzwerk sein, das eine Region oder sogar ein Land verbindet. Es wird von Unternehmen und Behörden verwendet, um Verbindungen zu anderen Standorten herzustellen.

âf» WAN2 - Wie Port WAN1, mit der Ausnahme, dass es sich um ein zweites Netzwerk handelt.

âf» DMZ - Ermöglicht es externem Datenverkehr, auf einen Computer im Netzwerk zuzugreifen, ohne das LAN freizulegen.

âf» BELIEBIG â€” Ermöglicht die Verwendung jeder beliebigen Schnittstelle.

Access Rules

Services

Action :

Service :

Service Management

Log : Log packets match this rule

Source Interface :

Source IP :

Destination IP : to

Schritt 13: Wählen Sie eine Option aus, um die Quell-IP-Adresse anzugeben, die das Netzwerk für den Datenverkehr über die Schnittstelle verwendet, und zwar aus der Dropdown-Liste "Source IP" (Quell-IP):

âf» Any (Beliebig): Jede IP-Adresse wird für die Weiterleitung von Datenverkehr verwendet. Rechts neben der Dropdown-Liste stehen keine Felder zur Verfügung.

âf» Single - Eine einzelne IP-Adresse wird für die Weiterleitung des Datenverkehrs verwendet. Geben Sie die gewünschte IP-Adresse in das Feld rechts neben der Dropdown-Liste ein.

âf» Bereich - Eine IP-Adresse für den Bereich wird für die Weiterleitung von Datenverkehr verwendet. Geben Sie den gewünschten IP-Adressbereich in die Felder rechts neben der Dropdown-Liste ein.

Schritt 14: Wählen Sie aus der Dropdown-Liste Destination IP (Ziel-IP) eine Option aus, um die Ziel-IP-Adresse anzugeben, die das Netzwerk für den Datenverkehr über die Schnittstelle verwendet:

âf» Any (Beliebig): Jede IP-Adresse wird für die Weiterleitung von Datenverkehr verwendet. Rechts neben der Dropdown-Liste stehen keine Felder zur Verfügung.

âf» Single - Eine einzelne IP-Adresse wird für die Weiterleitung des Datenverkehrs verwendet. Geben Sie die gewünschte IP-Adresse in das Feld rechts neben der Dropdown-Liste ein.

âf» Bereich - Eine IP-Adresse für den Bereich wird für die Weiterleitung von Datenverkehr verwendet. Geben Sie den gewünschten IP-Adressbereich in die Felder rechts neben der Dropdown-Liste ein.

Schritt 15: Klicken Sie auf **Speichern**, um die Einstellungen zu übernehmen.

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.