Aktivieren des öffentlichen WAN-Zugriffs mit DDNS und Port Forwarding

Dieses Dokument beschreibt die erforderlichen Schritte für die dynamische DNS (DDNS)-Konfiguration und Port Forwarding auf Cisco Small Business-Routern. Ziel ist der sichere Zugriff aus dem Internet auf einen internen Webserver und eine IP-Videokamera.

Überblick

Cisco Small Business-Router bieten eine erweiterte Netzwerklösung zur gemeinsamen Nutzung des Internets, die speziell auf die Bedürfnisse kleiner und mittlerer Unternehmen zugeschnitten ist. Mit dieser Lösung können mehrere Computer in einem Büro die Internetverbindung über integrierte Switch-Ports, angeschlossene Switches oder Wireless Access Points gemeinsam nutzen. Über die 10/100-Ethernet-WAN-Schnittstelle des Routers wird eine direkte Verbindung zum Breitband-DSL- oder zu einem Kabelmodem mit integrierten VPN- und Firewall-Funktionen hergestellt.

Der Zugriff aus dem Internet auf interne Netzwerkserver, Netzwerkdienste oder IP-Videoüberwachungskameras stellt jedoch aus den folgenden Gründen eine Herausforderung dar:

- Das interne LAN (Local Area Network) muss umfassend vor den unautorisierten Benutzern aus dem Internet geschützt werden. Dies geschieht mit Firewalls, die eingehende Verbindungen verhindern, autorisierten Zugriff auf bestimmte Netzwerkressourcen aber zulassen.
- Den Hosts im internen Netzwerk werden private IP-Adressen zugewiesen, um die Verwendung der knapp werdenden öffentlichen IP-Adressen zu verringern. Damit diese Hosts mit dem Internet kommunizieren können, muss mithilfe von NAT (Network Address Translation) jede private in eine öffentliche IP-Adresse übersetzt werden.
- In vielen kleineren und mittleren Unternehmen werden heutzutage Breitband-Internetverbindungen verwendet. Die Breitband-Internetverbindung erhält vom Service Provider eine dynamische öffentliche IP-Adresse zugeordnet, die sich im Gegensatz zu einer statischen Adresse häufig ändern kann.

Die Kombination von DDNS- und Port Forwarding-Funktionen stellt eine einfache Lösung für einen kontrollierten sicheren Zugriff auf die WAN-Schnittstelle des Routers und das interne Netzwerk aus dem Internet dar.

Hauptmerkmale

Dynamisches DNS

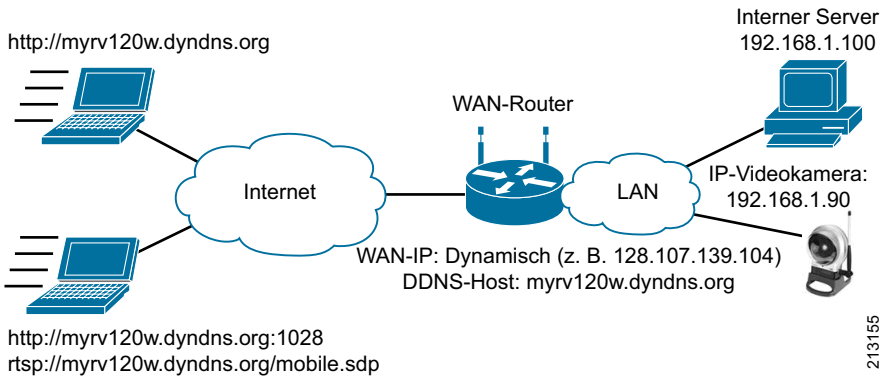
Dynamisches DNS (DDNS) dient zum Zuordnen von Internetdomänennamen zu IP-Adressen. Anders als DNS, das nur statische IP-Adressen verarbeiten kann, wurde DDNS für dynamische IP-Adressen entwickelt, wie sie beispielsweise von DHCP-Services zugewiesen werden. DDNS eignet sich perfekt für Netzwerke kleinerer und mittlerer Unternehmen, die dynamische öffentliche Adressen von Internet Service Providern erhalten.

Einige DDNS-Provider, wie z. B. dyndns.com, bieten ihre DDNS-Services gebührenfrei an. Melden Sie sich einfach bei einem DDNS-Provider an, fügen Sie den FQDN (Fully Qualified Domain Name, vollqualifizierter Domänenname) des Routers hinzu, und konfigurieren Sie den Cisco Router so, dass die WAN-IP-Adresse mit dem entsprechenden FQDN automatisch aktualisiert wird. Jetzt sind Sie in der Lage, über den FDQN auf die Netzwerkressource und den WAN-Router zuzugreifen, ohne die aktuelle öffentliche IP-Adresse kennen zu müssen.

Port Forwarding

Mithilfe von Port Forwarding wird ein bestimmter TCP- oder UDP-Port für einen Server hinter der Router-Firewall geöffnet, um über diesen Port eingehenden Verkehr zuzulassen und direkt an den angegebenen Server weiterzuleiten. Somit werden Verbindungen zwischen externen Hosts und Services innerhalb eines privaten LAN ermöglicht.

Abbildung 1 Netzwerkdiagramm zu DDNS und Port Forwarding



Beschriebene Produkte

- Cisco RV120W Wireless-N VPN-Firewall-Router (GUI-Konfigurationsanzeigen dieses Routers werden in diesem Dokument als Beispiel verwendet)
- Cisco RV220W Wireless-N Netzwerksicherheits-Firewall
- Cisco Small Business-Router: RV042, RV082, RV016, RVL200, WRVS4400N, RVS4000 und WRV210

Design-Tipps

WAN-IP-Adresse – Internet Service Provider stellen zwei Arten von WAN-IP-Adressen bereit: dynamisch zugewiesene und statisch zugewiesene IP-Adressen. Bei statischen IP-Adressen kann der Benutzer die IP-Adresse mithilfe von Port Forwarding verwenden, um auch ohne DDNS die oben genannten Ziele zu erreichen.

DDNS – Ein Konto bei einem DDNS-Provider wie dyndns.com oder tzo.com ist erforderlich. Innerhalb dieses Kontos werden verschiedene DDNS-Hosteinträge erstellt. Der Administrator muss einen DDNS-Hostnamen für die WAN-IP-Adresse erstellen. Der DDNS-Eintrag wird durch den Router sofort über HTTP aktualisiert, sobald sich die IP-Adresse ändert.

Port Forwarding – Die Server-Ports, die vom Server verwendet werden, müssen bekannt sein. Allgemeine Server-Ports, wie die Ports für Web-Service oder E-Mail-Service, sind auf dem Router für eine vereinfachte Konfiguration vordefiniert. Ein beliebiger benutzerdefinierter Service kann auch anhand seiner TCP- oder UDP-Portnummer erstellt werden. Port Forwarding vereinfacht die Konfiguration mehrerer Server, wenn Sie auf diesen Servern unterschiedliche Services bereitstellen.

LAN-IP-Adresse – Es wird dringend empfohlen, dass der interne Server oder die IP-Kamera für das Port Forwarding mit lokalen statischen IP-Adressen konfiguriert werden, statt die DHCP-Adresse vom Router zu beziehen. Sobald sich die IP-Adresse des internen Geräts ändert, würde bei Verwendung einer DHCP-Adresse die Port Forwarding-Regel außer Kraft gesetzt. Wird die statische IP-Adresse direkt auf dem Host konfiguriert, darf sie sich nicht im gleichen Bereich wie der DHCP-Adresspool befinden.

Netzwerkdiagramm

Abbildung 1 zeigt eine Beispielimplementierung von DDNS und Port Forwarding mithilfe eines Cisco Small Business-Routers.

Der WAN-Router bezieht seine IP-Adresse dynamisch, und Firewall und NAT sind standardmäßig aktiviert. In diesem Beispiel kann auf den WAN-Router über seinen FQDN (myrv120w.dyndns.org) zugegriffen werden. Dazu muss der DDNS-Hosteintrag *myrv120w.dyndns.org* der dynamischen IP-Adresse der WAN-Schnittstelle des Routers zugeordnet werden.

Port Forwarding wird folgendermaßen konfiguriert:

- Leiten Sie Port 80 an Port 80 auf dem Webserver des internen LAN weiter (192.168.1.100).
- Leiten Sie Port 1028 an Port 80 einer IP-Videokamera weiter (192.168.1.90).
- Leiten Sie das RTSP-Protokoll an den RTSP-Port der Videokamera weiter.

Mithilfe dieser Konfiguration können Remote-PCs und mobile Geräte über Webbrowser und -anwendungen aus dem Internet auf interne Services zugreifen.

DDNS-Konfiguration und Port Forwarding auf Cisco Small Business-Routern

Checkliste für die Vorkonfiguration

Verbinden Sie den WAN-Port des RV-Routers und den Ethernet-Port des DSL- oder Kabelmodems mithilfe eines Ethernet-Kabels. Schalten Sie den RV-Router an, und verbinden Sie die internen PCs, Server und IP-Videokameras mit dem LAN-Switch oder den Switch-Ports am RV-Router. Smart Tips zum Verbinden von Router und Switch mit VLANs und Trunks und zum Abschließen der LAN-Einstellungen finden Sie im entsprechenden Cisco Small Business-Dokument.

Vergewissern Sie sich, dass die lokalen PCs und Server durch die Firewall des RV-Routers geschützt werden und dass die Kommunikation untereinander und mit dem Router funktioniert. Stellen Sie sicher, dass der interne Webserver über die IP-Adresse 192.168.1.100 verfügt, und ändern Sie die statische IP-Adresse der IP-Videokamera WVC210 auf 192.168.1.90. Folgen Sie den Anweisungen *IP Video Surveillance Smart Setup Guide* beim Konfigurieren der IP-Adresse der IP-Videokamera WVC210.

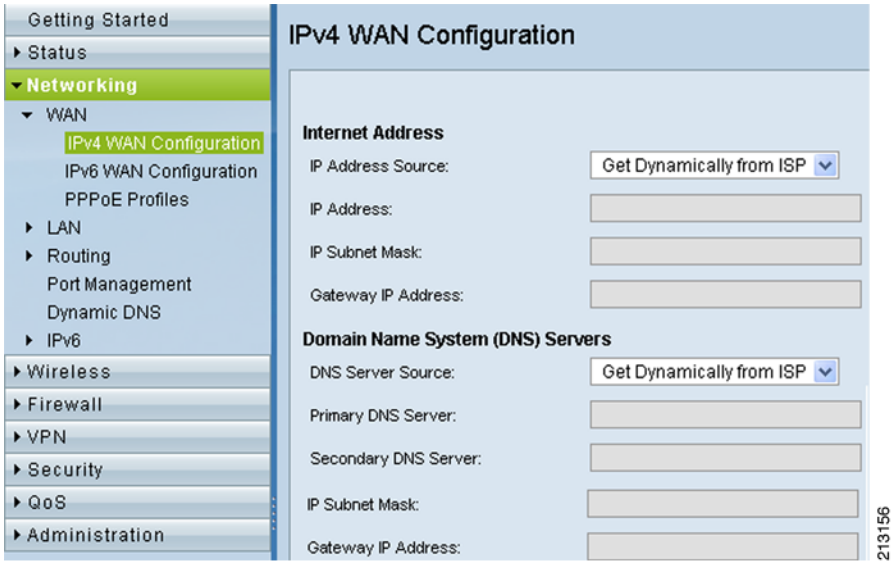
Konfigurieren des WAN-Zugriffs

Die standardmäßige WAN-Einstellung des RV-Routers ist so festgelegt, dass die IP-Adresse dynamisch vom ISP bezogen wird. Firewall und NAT sind ebenfalls standardmäßig aktiviert. Für einen grundlegenden WAN-Zugriff sind keine weiteren Konfigurationseingaben erforderlich.

Schritt 1 Wechseln Sie zu **Networking > WAN > IPv4 WAN Configuration,** und stellen Sie sicher, dass die Internetadressquelle und DNS-Server auf **Get Dynamically from ISP** eingestellt sind.

Hinweis Wird die IP-Adresse vom ISP statisch zugewiesen, stellen Sie die IP-Adressquelle auf „Use Static IP Address“ ein, und geben Sie die IP-Adresse, die Subnetzmaske und alle Standardrouterinformationen ein, die Sie vom ISP erhalten haben.

Abbildung 2 Überprüfen der WAN-Konfiguration



Schritt 2 Wechseln Sie zu **Status > System Status**, und überprüfen Sie im Abschnitt **WAN information (IPv4)**, ob der Router seine IP-Adresse, Subnetzmaske, Gateway und DNS-Informationen vom ISP erhalten hat, und dass NAT aktiviert ist.

Konfigurieren der DDNS-Einstellungen

In diesem Abschnitt wird der DDNS-Eintrag *myrv120w.dyndns.org* für den WAN-Router erstellt und der Router so konfiguriert, dass dieser DDNS-Eintrag automatisch auf seine aktuelle WAN-IP-Adresse aktualisiert wird, sobald sich diese ändert.

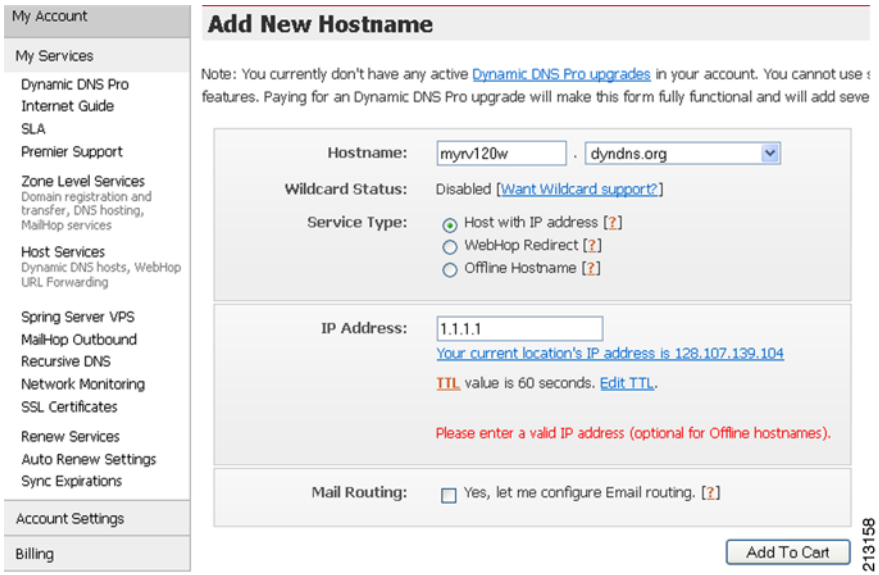
Schritt 1 Konfigurieren Sie das DDNS-Konto.

1. Wenn Sie noch nicht über ein DDNS-Konto verfügen, gehen Sie zu www.dyndns.com, um ein DDNS-Konto zu beantragen.

Eine gültige E-Mailadresse ist zum Aktivieren des Kontos erforderlich. Der Basisdienst ist gebührenfrei.

2. Ist das Konto geprüft und aktiviert, melden Sie sich an, und wechseln Sie zu **My Services > My Hosts**. Klicken Sie auf **Add Host Service**, um einen neuen DDNS-Hostnamen für den RV-Router zu erstellen.

Abbildung 3 Hinzufügen eines neuen Hostnamen über die dyndns.com-Website



In diesem Beispiel wird der Hostname „myrv120w.dyndns.org“ für den RV-Router erstellt.

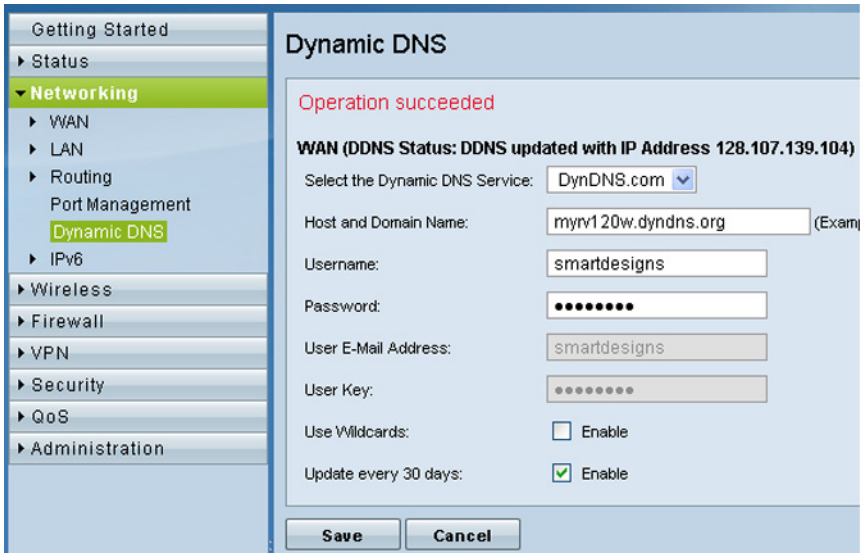
3. Geben Sie eine beliebige IP-Adresse, wie 1.1.1.1, ein, und klicken Sie **Add to Cart**, um die Konfiguration abzuschließen.

Schritt 2 Konfigurieren Sie den Cisco-Router.

1. Melden Sie sich beim RV-Router an, und wechseln Sie zu **Networking > Dynamic DNS**, um *DynDNS.com* als DDNS-Service auszuwählen.
2. Geben Sie als Host- und Domänennamen *myrv120w.dyndns.org* und danach Benutzernamen und Kennwort Ihres dyndns.com-Kontos ein.
3. Markieren Sie **Update every 30 days** für aktuelle Hostinformationen von DynDNS.com, und halten Sie das Abonnement auch über die 30-tägige Demoversion hinaus aufrecht.
4. Klicken Sie auf **Save**, damit der Router sofort den DDNS-Eintrag online mit seiner aktuellen WAN-IP-Adresse aktualisiert.

Auf der Seite mit den DDNS-Einstellungen werden jetzt die folgenden Meldungen angezeigt: *Operation succeeded* und *WAN (DDNS Status: DDNS updated with IP address 128.107.139.104)*.

Abbildung 4 Seite mit den DDNS-Einstellungen



Hinweis Damit die DDNS-Einstellungen sofort übernommen werden können, muss der Router über eine aktive Internetverbindung verfügen. Sie können sich ebenfalls über dyndns.com anmelden, um zu überprüfen, ob der Hosteintrag die neue aktualisierte IP-Adresse anzeigt.

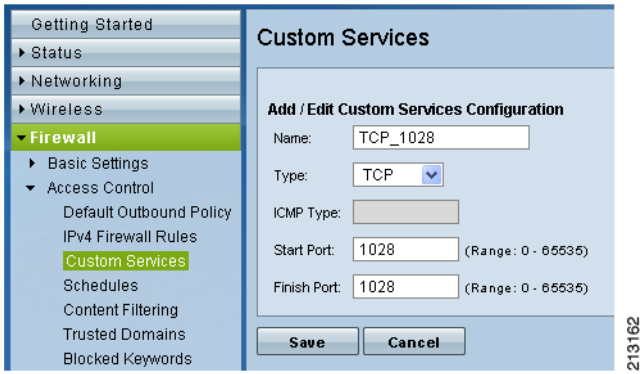
Konfigurieren von Port Forwarding

In diesem Abschnitt konfigurieren Sie Port Forwarding für den internen Webserver mit der IP-Adresse 192.168.1.100 und eine interne IP-Videokamera mit der IP-Adresse 192.168.1.90. So können Benutzer aus dem Internet mithilfe von http://myrv120w.dyndns.org auf den Webserver zugreifen. Auf die Webseite der IP-Videokamera kann über http://myrv120w.dyndns.org:1028 ebenfalls zugegriffen werden. Alternativ steht den Benutzern der RTSP-Stream der IP-Videokamera direkt über rtsp://myrv120w.dyndns.org/mobile.sdp zur Verfügung.

Schritt 1 Erstellen Sie einen neuen Service, der für Port Forwarding verwendet werden kann.

1. Wechseln Sie zu **Firewall > Access Control > Custom Service**.
2. Klicken Sie auf **Add**, um einen Service für TCP-Port 1028 zu erstellen.
3. Geben Sie als Namen „TCP_1028“ ein, legen Sie „TCP“ als Typ und den Start-Port sowie den End-Port als „1028“ fest.

Abbildung 5 Bildschirm „Custom Services“



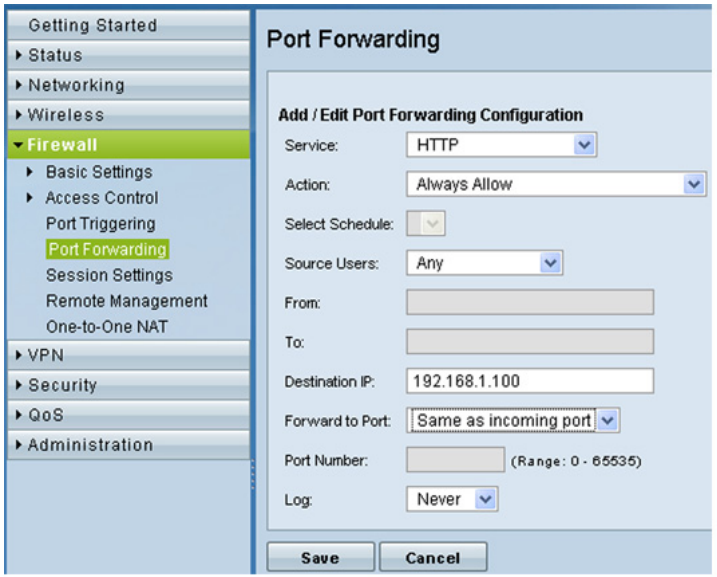
Schritt 2 Fügen Sie die erste Port Forwarding-Regel für internen Webserverzugriff hinzu.

Nach dem Erstellen dieser Regel wird der HTTP-Verkehr (TCP-Port 80) auf den HTTP-Port für den internen Webserver (192.168.1.100) umgeleitet.

1. Wechseln Sie zu **Firewall > Port Forwarding**, und klicken Sie auf **Hinzufügen**.
2. Wählen Sie **HTTP in Service** aus, ändern Sie die Aktion zu **Always Allow**, und wählen Sie dann **Any** aus der Pulldown-Liste „Source Users“ aus.
3. Geben Sie die interne Webserver-IP-Adresse (*192.168.1.100)* als Ziel-IP ein.
4. Wählen Sie unter „Forward to Port“ den Eintrag **Same as incoming port** aus, und klicken Sie auf **Save**.

In der Zusammenfassung wird jetzt eine Regel angezeigt.

Abbildung 6 Bildschirm „Port Forwarding“



Hinweis Beim Definieren von Regeln bezieht sich die Quelle auf Benutzer aus dem Internet und das Ziel auf das interne LAN des Unternehmens.

Schritt 3 Wiederholen Sie den Vorgang aus Schritt 2, um die zweite Regel für das Anzeigen der Webseite der IP-Videokamera zu erstellen.

Nach dem Erstellen dieser Regel wird der TCP-Verkehr an TCP-Port 1028 an den HTTP-Port des internen Servers 192.168.1.90 weitergeleitet.

1. Wählen Sie für diese Regel im Service-Abschnitt **TCP_1028** aus.
2. Ändern Sie die Aktion auf **Always Allow**, und wählen Sie dann **Any** aus der Pulldown-Liste „Source Users“ aus.
3. Geben Sie die IP-Adresse der IP-Kamera (192.168.1.90) ein, wählen Sie **Specify Port** aus der Pulldown-Liste „Forward to Port“ aus, geben Sie „Port 80“ als Port-Nummer an, und klicken Sie dann auf **Save**.

Schritt 4 Wiederholen Sie den Vorgang aus Schritt 2, um die dritte Regel für das Weiterleiten des RTSP: TCP-Services an denselben Port der IP-Videokamera (192.168.1.90) zu erstellen.

Nach Abschließen dieses Schrittes werden alle drei Regeln angezeigt, wie in Abbildung 7 dargestellt.

Abbildung 7 Port Forwarding-Einträge

Validieren der Konfiguration

Schritt 1 Navigieren Sie im Webbrowser eines mit dem Internet verbundenen Client-PC oder Laptops zu http://myrv120w.dyndns.org.

Der Webbrowser sollte jetzt den Inhalt der internen Website anzeigen.

Schritt 2 Navigieren Sie im Webbrowser eines mit dem Internet verbundenen Client-PC oder Laptops zu http://myrv120w.dyndns.org:1028.

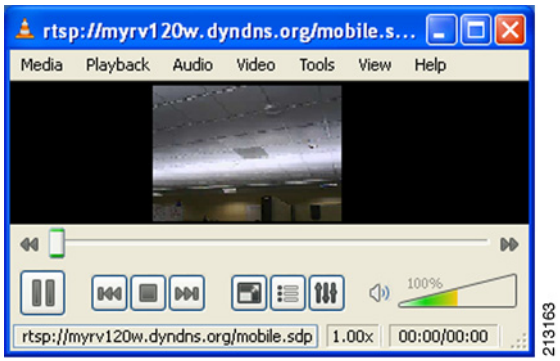
Der Webbrowser sollte jetzt die Webseite und den Videostream der IP-Videokamera WVC210 anzeigen.

Abbildung 8 Überprüfen von TCP-Port Forwarding

Schritt 3 Starten Sie auf einem mit dem Internet verbundenen Smartphone oder Laptop ein Medienwiedergabegerät wie den VLC Player, um den RTSP-Stream der IP-Videokamera WVC210 über den Link RTSP://myrv120w.dyndns.org/mobile.sdp anzuzeigen.

Hinweis Zum Überprüfen von RTSP-Port Forwarding sollte auf der IP-Videokamera WVC210 bereits Mobile Streaming aktiviert sein.

Abbildung 9 Überprüfen von RTSP-Port Forwarding



Weitere verwandte Features

Demilitarisierte Zone (DMZ)

Der Cisco RV-Router unterstützt ebenfalls eine DMZ-Option. Bei einer DMZ handelt es sich um ein Subnetz, auf das vom Internet zugegriffen werden kann, obwohl es sich hinter der Firewall befindet. Durch die DMZ-Funktion werden Pakete von einer bestimmten WAN-Port-IP-Adresse an eine spezielle IP-Adresse im LAN umgeleitet.

Firewall-Regeln können so konfiguriert werden, dass der Zugriff auf bestimmte Services und Ports in der DMZ sowohl aus dem LAN als auch aus dem Internet zugelassen wird. Im Falle eines Angriffs auf einen der DMZ-Knoten wird das LAN nicht notwendigerweise gefährdet. Die DMZ kann außerdem mit DDNS verwendet werden, etwa wenn ein Einzelserver in einem Netzwerk mehrere Services anbietet, die auch aus dem Internet verfügbar sein müssen.

One-to-One NAT

Der Cisco RV-Router unterstützt One-to-One NAT. Damit sehen Systeme hinter einer Firewall mit privaten IP-Adressen so aus, als verfügten sie über öffentliche IP-Adressen. One-to-One NAT kann verwendet werden, wenn der ISP einen Pool mit statischen öffentlichen IP-Adressen bereitstellt. Der privaten Adresse jedes Servers hinter der Firewall wird eine eindeutige öffentliche IP-Adresse zugeordnet. Dies ist besonders dann eine sinnvolle Lösung, wenn kleinere oder mittlere Unternehmen über T1 oder Business Class-Breitbandverbindungen verfügen. Allerdings haben diese Services bedeutend höhere Kosten zur Folge. One-to-One NAT ist immer dann erforderlich, wenn mehrere Server denselben Port verwenden, beispielsweise wenn mehrere Webserver Port 80 verwenden.