



Control4 MyHome: Remote Access Configuration

Document: DOC-00036

Revision: A

Date: 01/09/2012

Copyright © 2012 Control4. All Rights Reserved.

Saved: 1/9/2012 8:54:00 PM

DOC-00036 MyHome-
Remote Access
Configuration_V2

Page 1 of 22

Control4 MyHome: Remote Access Configuration

About Control4

Control4, a leading provider of the operating system for the smart home, delivers intelligent control of consumer electronics products, appliances and networking systems through an easy-to-use and intuitive software interface. Founded in 2003, the company delivers affordable automation and control of lighting, music, video, HVAC, security, and energy management systems to the broad market through more than 1,600 custom integrators, retail outlets, and distributors in over 65 countries. Control4 is the platform of choice for major consumer electronics companies, hotels, businesses and utilities that require an intelligent, open and affordable control solution. For more information visit www.control4.com. For more information visit www.control4.com.

Disclaimer

The information in this document is provided in connection with Control4 products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Control4's terms and conditions for the license of such products, Control4 Corporation and its affiliates, ("Control4") assume no liability whatsoever, and Control4 disclaims any express or implied warranty, relating to the sale and/or use of Control4 products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Control4 products are not intended for use in medical, life saving, or life sustaining applications.

Information regarding third-party products is provided solely for educational purposes. Control4 is not responsible for the performance or support of third-party products and does not make any representations or warranties whatsoever regarding the quality, reliability, functionality or compatibility of these products. The reader is advised that third parties can have intellectual property rights that can be relevant to this document and the technologies discussed herein, and is advised to seek the advice of competent legal counsel, without obligation of Control4.

Control4 retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Control4 makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein.

Copyright

©2012 Control4. All rights reserved. Control4, the Control4 logo, the 4-ball logo, the Control4 Certified logo, theControl4 iQ logo, Everyday Easy, and InfinityEdge are registered trademarks or trademarks of Control4 Corporation in the United States and/or other countries. Other brands and names are the property of their respective owners.

Contact Information

Control4 Corporation
11734 S. Election Road
Salt Lake City, UT 84020 USA
<http://www.control4.com>

Copyright © 2012 Control4. All Rights Reserved.

Contents

1. Introduction	5
1.1 Purpose.....	5
1.2 Scope.....	5
1.3 Keywords and Definitions	6
1.4 Related Documents	6
2. Internet Addressing Solutions.....	6
2.1 Static IP Addresses	7
Table 1. Comcast Business Service Dynamic IP vs. Static IP Comparison	7
2.2 Dynamic DNS Services	8
2.3 Dynamic DNS Service Configuration Examples.....	8
2.3.1 Netgear ProSafe VPN Firewall SRXN3205.....	8
Figure 1. Create New DDNS Service Provider Account.....	9
Figure 2. Configure Netgear SRXN3205 for DDNS Service.....	9
2.3.2 Cisco RV 120W Wireless N VPN Firewall.....	10
Figure 3. Configure Cisco RV 120W for DDNS Service	10
3. Virtual Private Network Broadband Router and Client Configuration	10
3.1 Router and VPN Client Configuration Examples.....	11
3.1.1 Netgear ProSafe VPN Firewall SRXN3205.....	11
Figure 4. Netgear VPN Configuration	11
Figure 5. IKE Policies	12
Figure 6. Netgear Create User Account.....	12
Table 2. Apple iOS settings for VPN Client in IPSec Mode.....	13
3.1.2 Cisco RV 120W Wireless N VPN Firewall.....	13
Figure 7. Enable Remote Management.....	14
Figure 8. Disable Block Fragmented Packets.....	14
Figure 9. Advanced VPN Setup.....	15
Figure 10. VPN Policy	16
Figure 11. Establish the VPN User Accounts	16
Figure 12. VPN Client Connection.....	17
3.2 MyHome Configuration.....	17
Figure 13. Director Screen	18
4. Port Forwarding Configuration.....	18
4.1 Port Configuration	18

Control4 MyHome: Remote Access Configuration

Table 3. Ports Utilized by MyHome Application	19
Figure 14. Firewall Access Rules	20
Figure 15. Firewall Access Rules (con't).....	21
4.2 MyHome Application Configuration.....	22
5. Conclusion	22

1. Introduction

The Control4® MyHome™ family of applications offers a convenient and flexible way to turn you and your customer's smartphone, tablet or computer into the familiar and graphically-rich Control4 touch interface. MyHome applications are an affordable way to extend the capabilities of the Control4 home-automation experience and manage a home automation system more effectively, including lighting, temperature, music, movies, and security.

In a Control4-enabled smart home, the MyHome applications work with your Control4 system over the home's WiFi network securely, because only authorized devices can connect to your system and to a properly-configured WiFi network.

MyHome applications also can be used outside the home, but care should be taken to properly configure the home network first to keep it secure when using it outside the home environment.

1.1 Purpose

This document is intended for Control4 Dealers and Installers who want to set up MyHome for their customers to use outside the home.

This white paper describes different remote access configuration solutions to set up when using MyHome applications outside the home—and the benefits and limitations of each option so that a Dealer can discuss the tradeoffs with their customers to identify the optimal approach.

1.2 Scope

To configure your customer's home for remote access by the MyHome application, you will need to

- establish a method for addressing the home from any Internet connection through either a static Internet protocol ("IP") address or a dynamic DNS service ("DynDNS") as described in "Internet Addressing Solutions."
- install a broadband router that supports virtual private network ("VPN") client access and configure your mobile devices to establish VPN connections with your home as described in "Virtual Private Network Broadband Router and Client Connection."

This white paper describes the key attributes of these major steps. Configuring broadband routers to enable VPN connections can be very complex. The examples we provided have worked in actual homes, but we have not provided an exhaustive list of possible configurations. In most cases, the manufacturer of the networking equipment will be able to provide the best support for these products. Dealers and installers should contact them directly to get the latest information regarding their products and their VPN capabilities or limitations.

Alternatively, a broadband router could be configured to support 'port forwarding,' which would also enable remote access by the MyHome application, but without a need for a VPN client on the mobile device. This approach introduces numerous security risks that could enable a malicious Internet user to gain unauthorized access to the Control4 system outside the home. Control4 does not recommend this approach for customer installations, but the details and a description of the security risks are also described in this white paper.

IMPORTANT: Control4 recommends that remote access using the MyHome application only be implemented securely with a Control4-supported broadband router that offers VPN connections.

1.3 Keywords and Definitions

Keywords	Definitions
Domain name system (DNS)	A naming system that translates computer host names into IP addresses.
Dynamic DNS service (DDNS)	A service used to update in real time the Domain Name System (DNS) name servers to keep them up to date with the current IP address of a home's broadband connection.
Internet protocol (IP)	The main protocol used across the Internet for data packet transfers across networks.
Internet Service Provider (ISP)	Companies that offer Internet access to their customers for a fee.
Port forwarding	A router configuration whereby an incoming data packet's destination address is translated to a new destination and that data packet is sent to that new destination.
Remote Access	The ability to access a computer or network from a remote location.
Virtual private network (VPN)	The use of private communications over a public network through the Internet and Intranets. A login and password are usually required to access the VPN.

1.4 Related Documents

Document Title	Document Location
Control4 Supported Networking Equipment	Control4 Dealer portal at: http://www.control4.com/dealer/products/myhome/

2. Internet Addressing Solutions

Most homeowners obtain their broadband Internet access from an Internet Service Provider (ISP) that allocates a numeric IP address for their home. This numeric IP address is similar to the street address for the home, but identifies a 'virtual' location for the home on the Internet. Many ISPs offer both "static" IP addresses—which means they are stable, unchanging addresses—and "dynamic" IP addresses—which can change from one session on the Internet to the next. While it would be easier for homeowners who want to access their home remotely over the Internet to have a static IP address, most ISPs only offer such an address at an extra cost. Instead, ISPs typically provide dynamic IP addresses so that they can rapidly expand their networks for new users, reconfigure networks to optimize traffic, and make changes without regard to the IP addresses they have allocated to each user to keep their administrative costs low.

Control4 MyHome: Remote Access Configuration

Currently, remote access to the Control4® system using the MyHome™ application requires that a user or Dealer knows and is able to enter their home's IP address. However, a numeric IP address is not only inconvenient to remember, but a connection is impossible if the IP address changes (which the ISP has the right to do) and the user is unaware of the change.

To overcome these limitations, the Dealer can work with the homeowner to establish a static IP address for the home or use a dynamic DNS (DDNS) service provider to create a static name that connects a user to a home's broadband IP address.

Two solutions are described below that you can set up for the homeowner:

- Obtain a static IP address from the ISP, or
- Assign a DNS hostname using a DDNS service provider.

2.1 Static IP Addresses

A static IP address offers the very best performance with the MyHome application and is the preferred option for homeowners that seek the highest levels of service. To obtain a static IP address, the Dealer will need to contact the homeowner's ISP. Most ISPs offer static IP addresses at an additional cost, but the benefit is a more stable remote connection to the home.

When coupled with a broadband router supporting VPNs, the homeowner may also benefit by having more robust remote access to all of their Internet-connected electronics. In many cases, homeowners that have remote access to their corporate network already have static IP addresses because many corporate IT staffs require it to "white list" access from the remote IP address to the corporate network.

The details of obtaining a static IP address will vary based on the ISP and are beyond the scope of this white paper.

As an example of one ISP with static IP capabilities, Comcast® offers a business-class level of service for which static IP addresses are available at an additional cost over the standard monthly Internet access charges. More information can be found here: <http://business.comcast.com>.

A table published by Comcast on their website describing the differences in service and their cost as of January 1, 2012 is shown below.

Table 1. Comcast Business Service Dynamic IP vs. Static IP Comparison

Dynamic IP vs. Static IP

Your Business Uses:	Dynamic IP	Static IP
A Single Computer	No additional hardware or special configuration required.	No additional hardware or special configuration required.
Multiple Computers	Requires a router.	Requires a switch or hub.
VPN Compatibility	Requires a router for multiple computers. Special configuration may be required.	Requires a switch or hub for multiple computers. No special configuration required.
Remote Management	Difficult to configure and may require a special configuration to router.	No special configuration required.
Hosted Servers	Requires outside-hosted dynamic DNS. Firewall may limit mail server.	All ports available. No special configuration required.
Pricing	Included with Business Class Internet Service.	Static IPs available: 1 - \$14.95/mo., 5 - \$19.95/mo., 13 - \$34.95/mo.

Please [Get a Free Quote](#) or call (866) 621-1191 to speak to a dedicated local Business Class representative to order business services from Comcast, or to have any questions you may have answered.

Source: Comcast website as of 1/6/2012. <http://business.comcast.com>

Copyright © 2012 Control4. All Rights Reserved.

2.2 Dynamic DNS Services

For homeowners who are unable to obtain a static IP address, unwilling to incur the additional cost or prefer the simplicity of remembering a hostname, a DDNS service provider can be used to overcome the limitations of dynamic IP addresses. The DDNS service provider allocates a static hostname (e.g., homeownername.ddnsservice.org) to the user. The static hostname is used by the DDNS provider to redirect queries to the current IP address of the home.

Whenever the ISP allocates a new IP address, software running on the broadband router or a computer at the home communicates the new IP address to the DDNS provider. The ultimate result is that homeowners can connect with their homes by using their own hostname, for example, homeowner.ddnsservice.org instead of an unknown varying IP address.

The downside of using the DDNS service provider is that there may be times during which the home's IP address has changed, but this change has not been communicated back to the DDNS service. During these brief periods, the use of the hostname would be unsuccessful. The DDNS service provider will be pointing to the old IP address until it receives notification that the address has changed. Unfortunately, the DDNS service provider won't be able to distinguish between a changed IP address, an Internet access outage, or some other error, and the user will only know that their MyHome application is unable to connect.

On a positive note, changes in the dynamic IP address allocated to a home are typically infrequent (sometimes as long as months or years between changes) and the delay in the notification of the IP address change to the DDNS provider is also usually very short (less than five (5) minutes). Most users will never experience any problems, but the Dealer should communicate the potential problem to their customers to properly set expectations and avoid unnecessary service calls.

Unfortunately, the configuration of dynamic domain name services is not standardized and varies based on the DDNS service provider, the broadband router that supports such a service, or the software application that is installed in the home to enable this service.

As with many aspects of third party products and services that interact with the Control4 system, the Dealer should adopt a preferred service and test it in their own homes before implementing it for a customer.

Control4 maintains a list of supported networking solutions which can be found on our Dealer website. This list identifies which solutions support DDNS services.

Note: Control4 makes no representations or warranties regarding such third-party products or services.

2.3 Dynamic DNS Service Configuration Examples

2.3.1 Netgear ProSafe VPN Firewall SRXN3205

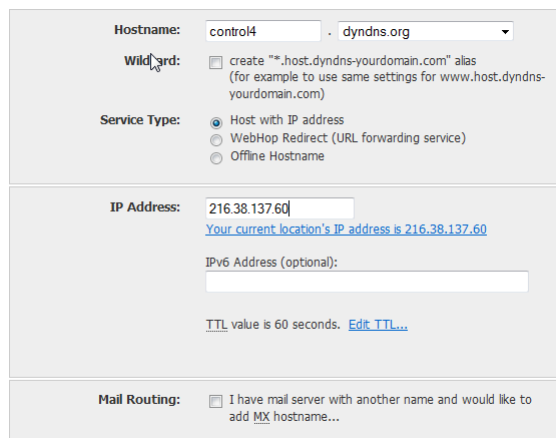
The following steps demonstrate how to configure a Netgear® ProSafe VPN Firewall SRXN3205 for use with Dynamic Network Services, Inc, a leading DDNS service provider. More information regarding Dyn can be found here: <http://dyn.com>. They currently offer a free trial of their DDNS service here: <http://dyn.com/dns/dyndns-pro-free-trial/>.

Control4 MyHome: Remote Access Configuration

To configure this firewall for DDNS:

1. Create a new account with a DDNS service provider and define your hostname. In the screen below from the Dyn website, we chose control4.dyndns.org as the hostname we'll use to enable remote access for the MyHome application. We also entered our current IP address assuming this was being set up at the home. If set up prior to being at the installation site, it may take a few moments for the DDNS service to update with the home's IP address before using the MyHome application.

Figure 1. Create New DDNS Service Provider Account

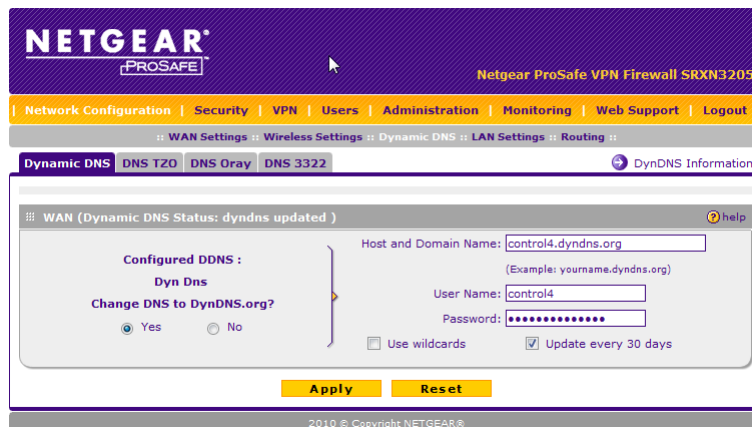


The screenshot shows a web form for creating a new DDNS account. The form is divided into several sections:

- Hostname:** A text input field containing "control4" and a dropdown menu showing ". dyndns.org".
- Wildcard:** A checkbox labeled "create '*.host.dyndns-yourdomain.com' alias (for example to use same settings for www.host.dyndns-yourdomain.com)".
- Service Type:** Three radio buttons: "Host with IP address" (selected), "WebHop Redirect (URL forwarding service)", and "Offline Hostname".
- IP Address:** A text input field containing "216.38.137.60". Below it, a link says "Your current location's IP address is 216.38.137.60".
- IPv6 Address (optional):** An empty text input field.
- TTL value:** A label "TTL value is 60 seconds." with a link "Edit TTL...".
- Mail Routing:** A checkbox labeled "I have mail server with another name and would like to add MX hostname...".

2. Configure the home's broadband router using the information established with the DDNS service provider (see the screen below).

Figure 2. Configure Netgear SRXN3205 for DDNS Service



The screenshot shows the Netgear ProSafe VPN Firewall SRXN3205 web interface. The navigation bar includes "Network Configuration", "Security", "VPN", "Users", "Administration", "Monitoring", "Web Support", and "Logout". The "Dynamic DNS" section is active, showing "DNS TZO", "DNS Oray", and "DNS 3322". The "WAN (Dynamic DNS Status: dyndns updated)" section is expanded, showing the following configuration:

- Host and Domain Name:** "control4.dyndns.org" (with an example: "yourname.dyndns.org").
- User Name:** "control4".
- Password:** A masked password field.
- Use wildcards:** An unchecked checkbox.
- Update every 30 days:** A checked checkbox.

Buttons for "Apply" and "Reset" are visible at the bottom of the configuration area. The footer indicates "2010 © Copyright NETGEAR®".

When completed and the broadband router checks in with the DDNS service provider, the homeowner can now access their home network via their hostname once the MyHome application and the VPN are properly configured.

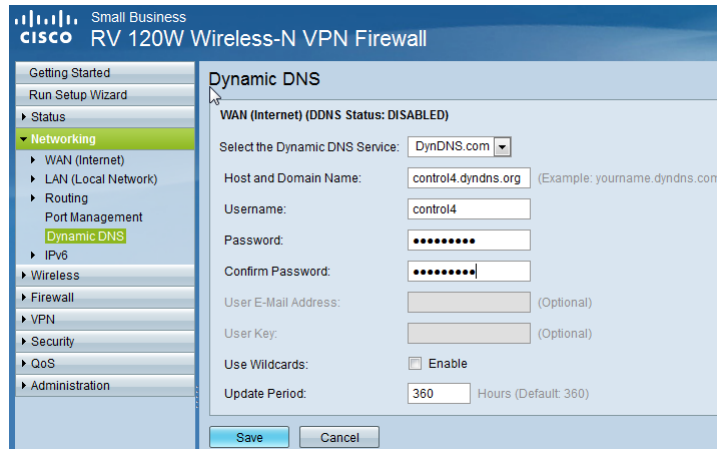
Copyright © 2012 Control4. All Rights Reserved.

Control4 MyHome: Remote Access Configuration

2.3.2 Cisco RV 120W Wireless N VPN Firewall

The following screen illustrates a similar configuration for the Cisco® RV 120W Small Business Wireless N VPN Firewall.

Figure 3. Configure Cisco RV 120W for DDNS Service



The screenshot shows the configuration page for Dynamic DNS on a Cisco RV 120W Wireless-N VPN Firewall. The interface is titled "Small Business Cisco RV 120W Wireless-N VPN Firewall". On the left is a navigation tree with "Dynamic DNS" selected under the "Networking" section. The main content area shows the "Dynamic DNS" configuration for the "WAN (Internet) (DDNS Status: DISABLED)". The "Select the Dynamic DNS Service" dropdown is set to "DynDNS.com". The "Host and Domain Name" field contains "control4.dydns.org" with a note "(Example: yourname.dydns.com)". The "Username" field contains "control4". The "Password" and "Confirm Password" fields are masked with dots. The "User E-Mail Address" and "User Key" fields are optional and empty. The "Use Wildcards" checkbox is unchecked. The "Update Period" is set to "360 Hours (Default: 360)". At the bottom are "Save" and "Cancel" buttons.

When completed and the broadband router checks in with the DDNS service provider, the homeowner can now access their home network via their hostname once the MyHome application and the VPN are properly configured.

3. Virtual Private Network Broadband Router and Client Configuration

A virtual private network (VPN) is a secure connection made by traveling users over the public Internet or telecommunication networks to a centralized network. In the context of a homeowner, a VPN is a private connection between their personal computer—or mobile device—to their home network from a location outside their home. VPNs typically require remote users of the network to be authenticated, and they often secure data with encryption technologies to prevent disclosure of private information. With a VPN connection, the user should experience the connection to their home network just as if they were at home. Using this method, a MyHome user can experience the same benefits of the Control4 system securely outside their home.

To enable a VPN connection, the home network will require a broadband router that supports this functionality and mobile devices that can be configured for VPN connections. Ideally, VPN support is built directly into the router and the mobile device. Fortunately, there are a number of broadband routers that offer VPN capabilities. In addition, Apple® iPods and iPads as well as many Android® mobile devices provide direct VPN support.

In the following section, we provide some examples of broadband routers and mobile devices that have been configured to support VPN connections. As you might expect, different routers vary in the support of VPN functionality, and the matching configuration on the mobile device can be difficult to ascertain. It is essential that Dealers identify a solution they feel works well. Care should be taken to

Copyright © 2012 Control4. All Rights Reserved.

Control4 MyHome: Remote Access Configuration

attempt this configuration first on a demo system or in their home before attempting at a customer site.

3.1 Router and VPN Client Configuration Examples

3.1.1 Netgear ProSafe VPN Firewall SRXN3205

The following VPN router and client configuration example utilize a Netgear ProSafe VPN Firewall SRXN3205 and an Apple iPad.

To configure this router for IPsec connections using the Apple iPhone or iPad:

1. Navigate to the VPN>IPSec VPN>Mode Config screen and complete it according to the screen below. The most important items are that you ensure that the IP address pool is something unique that won't conflict with the LAN address of the home LAN or the remote LAN. The example below utilizes 90.90.90.90 to 90.90.90.93. This allows for only four (4) simultaneous connections. It is also important to set the Local IP Address to **0.0.0.0** and the Local Subnet Mask to **0.0.0.0**. These settings cause the associated VPN policy to be applied to all incoming connections regardless of the remote IP address.

Figure 4. Netgear VPN Configuration

The screenshot displays the Netgear ProSafe VPN Firewall SRXN3205 configuration interface. The top navigation bar includes 'Network Configuration', 'Security', 'VPN', 'Users', 'Administration', 'Monitoring', 'Web Support', and 'Logout'. The 'VPN' menu is expanded, showing 'IPSec VPN', 'SSL VPN', 'Certificates', and 'Connection Status'. The 'Edit Mode Config Record' screen is active, showing a 'Record Name' of 'rec1'. The 'Client Pool' section includes three IP pools: 'First Pool' (90.90.90.90 to 90.90.90.93), 'Second Pool' (0.0.0.0 to 0.0.0.0), and 'Third Pool' (0.0.0.0 to 0.0.0.0). The 'WINS Server' and 'DNS Server' sections are also visible. The 'Traffic Tunnel Security Level' section is expanded, showing 'PPS Key Group' set to 'DH Group 2 (1024 bit)', 'SA Lifetime' set to '2600' seconds, 'Encryption Algorithm' set to 'AES-128', and 'Integrity Algorithm' set to 'SHA-1'. The 'Local IP Address' and 'Local Subnet Mask' are both set to '0.0.0.0'. 'Apply' and 'Reset' buttons are at the bottom.

2. Next, navigate to the VPN>IPSec VPN>IKE Policies screen and add a new IKE policy according to the example below. Be sure to select the **Mode Config Record** you created above. The Policy Name is flexible. The Remote Identifier of **0.0.0.0** is particularly important once again to enable a remote connection from any remote IP address. Equally important is the Pre-shared key, which should be unique to each customer and documented for use by the VPN client software.

Control4 MyHome: Remote Access Configuration

Figure 5. IKE Policies

The screenshot shows the 'Edit IKE Policy' configuration page. At the top, a message states 'Operation succeeded.' and there is a link to 'Add New VPN Policy'. The page is divided into several sections:

- Mode Config Record:** Includes a 'Do you want to use Mode Config Record?' section with 'Yes' selected, and a 'Select Mode Config Record:' dropdown set to 'rect1'.
- General:** 'Policy Name' is 'Control4', 'Direction / Type' is 'Responder', and 'Exchange Mode' is 'Aggressive'.
- Local:** 'Identifier Type' is 'FQDN' and 'Identifier' is 'local.com'.
- Remote:** 'Identifier Type' is 'FQDN' and 'Identifier' is '0.0.0.0'.
- IKE SA Parameters:** 'Encryption Algorithm' is 'AES-128', 'Authentication Algorithm' is 'SHA-1', 'Authentication Method' is 'Pre-shared key', 'Pre-shared key' is 'Password', 'Diffie-Hellman (DH) Group' is 'Group 2 (1024 bit)', 'SA-Lifetime (sec)' is '3600', 'Enable Dead Peer Detection' is 'No', 'Detection Period' is '30' seconds, and 'Reconnect after failure count' is '3'.
- Extended Authentication:** 'XAUTH Configuration' has 'Edge Device' selected, and 'Authentication Type' is 'User Database'.

Buttons for 'Apply' and 'Reset' are at the bottom.

Note: The Exchange Mode in the above example was set to **Aggressive**. Multiple forum postings on the Netgear website previously indicated that iPhones and iPads did not support the Aggressive mode, and they recommended **Main** be selected. At the time this white paper was written and using the iOS 5 and the SRXN3205 firmware version 3.0.7-24, this functionality had changed. Aggressive mode was required to make the connection. Once again, Dealers are reminded to find a configuration that works for them, and test it before going to a customer site.

3. Create user accounts for each remote user from the Users>Users screen. The username and password should be unique for each user. Be sure to document this information, as it will be needed to configure the VPN client on the iOS mobile devices. In this case, the user password should be different from the Pre-shared Key above to make the connections as secure as possible.

Figure 6. Netgear Create User Account

The screenshot shows the 'Add User' configuration page in the Netgear ProSafe VPN Firewall SRXN3205 web interface. The breadcrumb trail is 'Network Configuration | Security | VPN | Users | Administration | Monitoring | Web Support | Logout |'. The page title is 'Add User'.

The configuration fields are:

- User Name: 'username'
- User Type: 'Administrator' (dropdown)
- Select Group: 'Control4' (dropdown)
- Password: '*****'
- Confirm Password: '*****'
- Idle Timeout: '10' Minutes

Buttons for 'Apply' and 'Reset' are at the bottom.

Copyright © 2012 Control4. All Rights Reserved.

Control4 MyHome: Remote Access Configuration

- Using the information created in the above steps, the Dealer or homeowner can now configure the VPN client on their iPhone, iPod Touch or iPad with the following information:

Table 2. Apple iOS settings for VPN Client in IPsec Mode

Parameter	Input
Server	Homeowners Static IP Address of Hostname from DDNS service provider
Account	Username created in Step 3 for each account
Password	Password created in Step 3 for each account
Use Certificate	Off
Group Name	Group for Username as shown in Step 3
Secret	This is the Pre-shared key created in Step 2
Proxy	Off

3.1.2 Cisco RV 120W Wireless N VPN Firewall

The following example uses Cisco's RV 120W Wireless N VPN Firewall, which supports IPsec connections. Despite the fact that Apple's iPod and iPad use IPsec client technology from Cisco, they are not currently able to connect directly to this firewall due to current limitations of the respective implementations. However, Cisco's QuickVPN client provides an easy way to establish a VPN connection with the RV 120W from a PC running the MyHome application.

To configure the Cisco router for IPsec connections:

- Log into the router as the **admin** and enable Remote Management from the Administration>Management Interface>'Web Access' screen (see the screen below) and keep the Port Number as the default of **443** (yes, this is a known limitation of the router that is required for enabling a VPN).

Note: You should definitely change the default admin password to avoid unauthorized access.

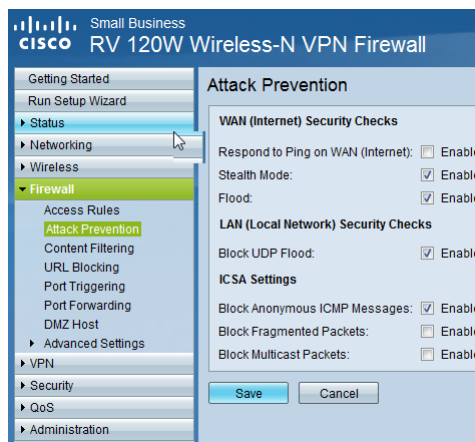
Control4 MyHome: Remote Access Configuration

Figure 7. Enable Remote Management



2. Navigate to the Firewall>Attack Prevention screen and disable the **Block Fragmented Packets** security check (it's another limitation of this router and not a normal VPN set up requirement). See the screen below.

Figure 8. Disable Block Fragmented Packets



3. Now set up the VPN configuration:
 - a. Navigate to the 'VPN/Advanced VPN Setup' screen and Add to the IKE Policy Table.
 - b. Configure the IKE policy as shown in the screen below. Both the Policy Name and Pre-Shared Key can be unique to each installation. Obviously, the Pre-Share Key SHOULD be unique, and you'll want to document it for the homeowner in many VPN configurations.
 - c. Click **Save** to save the policy.

Copyright © 2012 Control4. All Rights Reserved.

Control4 MyHome: Remote Access Configuration

Figure 9. Advanced VPN Setup

The screenshot displays the configuration interface for a Cisco RV 120W Wireless-N VPN Firewall. The left sidebar shows a navigation tree with 'VPN' expanded to 'Advanced VPN Setup'. The main content area is titled 'Advanced VPN Setup' and contains the following configuration sections:

- Add / Edit IKE Policy Configuration**
 - Policy Name: Control4
 - Direction / Type: Responder
 - Exchange Mode: Aggressive
- Local**
 - Identifier Type: FQDN
 - Identifier: local.com
- Remote**
 - Identifier Type: FQDN
 - Identifier: remote.com
- IKE SA Parameters**
 - Encryption Algorithm: 3DES
 - Authentication Algorithm: SHA-1
 - Authentication Method: Pre-Shared Key
 - Pre-Shared Key: Control4
 - Diffie-Hellman (DH) Group: Group2 (1024 bit)
 - SA-Lifetime: 28800 Seconds
 - Dead Peer Detection: Enable
 - Detection Period: 10 (Range: 10 - 999)
 - Reconnect after Failure Count: 3 (Range: 3 - 99)
- Extended Authentication**
 - XAUTH Type: Edge Device
 - Authentication Type: User Database
 - Username: [Empty field]
 - Password: [Empty field]

- Next, add an entry to the VPN Policy table using the settings below. Note that I have made the name of the VPN policy match the IKE policy; but more importantly, be sure to select the matching IKE policy. The VPN Policy table is accessible from the same 'VPN/Advanced VPN Setup' screen.

Advanced users may choose different starting IP address and subnets depending on the IP address configuration of the router. In the screen below, the router remained at the default 192.168.1.1 on the LAN side of the network.

Control4 MyHome: Remote Access Configuration

Figure 10. VPN Policy

Small Business
cisco RV 120W Wireless-N VPN Firewall

Getting Started
Run Setup Wizard
Status
Networking
Wireless
Firewall
VPN
IPsec
Basic VPN Setup
Advanced VPN Setup
VPN Users
VPN Passthrough
Security
QoS
Administration

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

NETBIOS: Enable

Local Traffic Selection

Local IP:

Start Address:

End Address:

Subnet Mask:

Remote Traffic Selection

Remote IP:

Start Address:

End Address:

Subnet Mask:

Split DNS

Split DNS: Enable

Domain Name Server 1:

Domain Name Server 2: (Optional)

Domain Name 1:

Domain Name 2: (Optional)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

SA-Lifetime:

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

5. Establish accounts for each VPN user via the VPN>'VPN Users' screen.
 - a. Press the **Add** button to add a new user.
 - b. Enter a unique Username and Password.
 - c. Select **QuickVPN** as the Protocol.

Figure 11. Establish the VPN User Accounts

Small Business
cisco RV 120W Wireless-N VPN Firewall

Getting Started
Run Setup Wizard
Status
Networking
Wireless
Firewall
VPN
IPsec
Basic VPN Setup
Advanced VPN Setup
VPN Users
VPN Passthrough
Security
QoS
Administration

VPN Users

PPTP Server Configuration

PPTP Server: Enable

Starting IP Address: (xxxx.xxxx.xxxx.xxxx)

Ending IP Address: (xxxx.xxxx.xxxx.xxxx)

VPN Client Setting Table

No.	Enabled	Username	Password	Allow User to Change Password	Protocol
1	<input checked="" type="checkbox"/>	Control4	*****	<input type="checkbox"/>	QuickVPN

Please click 'Save' button to take Add/Edit/Delete Operation into effect

6. You are now ready to configure the Cisco QuickVPN client on the personal computer. In the screen below

Control4 MyHome: Remote Access Configuration

- the Profile Name matches the Policy Name on the router,
- the User Name matches the VPN username account created on the router along with the assigned password, and
- the Server Address matches the Static IP address of the home network; or in the example below, the hostname established with the DDNS service provider.

Click **Connect**. If everything is entered correctly, the PC will establish a VPN connection with the broadband router.

Figure 12. VPN Client Connection



Note: We plan to update these instructions once Apple and Cisco address the current issues with the IPSEC VPN client on the iPod, iPhone and iPad. At the present time, there is not a QuickVPN client for Android either.

3.2 MyHome Configuration

By using a VPN connection between the Control4 system and the mobile device, no special configuration of the MyHome application is required.

To configure MyHome:

1. From the **More...**'>'Director' screen (see the screen below for an example), the user or Dealer selects the Director of the Primary Controller.
2. Enter the Primary Controller's IP address on the home network.
3. Press the **Connect** button.
4. Identify the mobile device to the project.
5. Update the project.
6. Given the limited bandwidth of many remote connections, we recommend that this process initially be completed on the LAN inside the home. The homeowner should also be informed not to update the project outside the home to avoid performance problems.

Control4 MyHome: Remote Access Configuration

Figure 13. Director Screen



4. Port Forwarding Configuration

The MyHome application can also remotely access a homeowner's Control4 system using a technique called 'port forwarding.' Essentially, the broadband router is configured so that when a user addresses it from the Internet side—whether through a static IP address or DDNS approach—open ports route these interactions directly to the Primary Controller.

This approach eliminates the need for a VPN client on the mobile device. However, port forwarding introduces numerous security risks that could enable a malicious Internet user to gain unauthorized access to the Control4 system or the home network from outside the home.

Port forwarding is analogous to leaving the front door of your home open to visitors with the caveat that anyone can come inside somewhat invisibly (through the anonymity of remote Internet interactions).

The port forwarding approach is an excellent way for Control4 Dealers to demonstrate the functionality of the MyHome application with fully-configured systems to help homeowners understand the potential of the Control4 platform within the home. However, this approach was never intended to be an acceptable solution for remote access beyond its use with demo systems.

IMPORTANT: Control4 does not recommend or approve of port forwarding for remote access using the MyHome application due to the security risks. Dealers and homeowners that use this technique assume any and all associated risks for such actions. Control4 requires Dealers to fully inform the homeowner of all associated risks and acquire written permission from any such homeowner before attempting any remote access through port forwarding from the home.

4.1 Port Configuration

The procedure for enabling port forwarding on a broadband router will differ based on the manufacturer. The specific ports and the functionality they support are listed in the table below.

Note: To ensure maximum flexibility, both the TCP and UDP ports should be forwarded.

Control4 MyHome: Remote Access Configuration

In using this approach, the ports should be forward to the LAN's IP address for the Control4 Primary Controller in the home. This Controller should either be allocated a static IP address within that network, or its IP address should be reserved with the router's DHCP server functionality.

Table 3. Ports Utilized by MyHome Application

Port	Function	Comments
5020	Enables unsecure communications with Director.	Most of the MyHome functionality is enabled by forwarding this port.
5021	Enables SSL secured communications with Director.	In cases where the MyHome – PC application has SSL enabled, this port would also need forwarding.
80	Enables delivery of artwork for albums, movies and radio stations.	This port is one of the most highly used on the Internet including for typical HTTP traffic. Forwarding this port is the most risky, but is required to demonstrate some of the graphical functionality.

As an example of proper configuration, the following steps demonstrate how to configure a Cisco RV 120W Small Business Wireless N VPN router to enable the port forwarding approach described above.

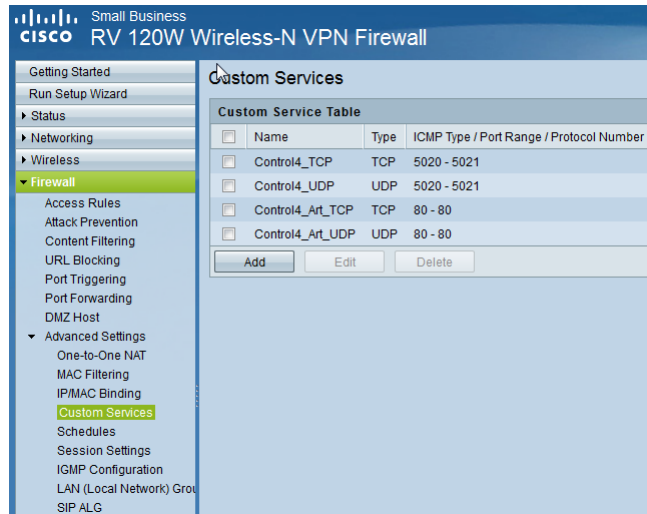
Note: The RV 120W has a known limitation in that "Internet NAT redirection does not work using firewall port-forwarding rules." This limitation provides an excellent example of the importance of identifying networking equipment that works in 'real world' environments, and learning its limitations in a demo installation before attempting an installation in a client's home is essential. In writing this white paper, the author spent many hours debugging this issue before finding the limitation and workaround documented in the latest firmware release notes.

To configure a Cisco router to enable the port forwarding:

1. Establish the definitions for the various Control4 services based on the ports and protocol types used. As shown in the table above, services were created for ports 5020, 5021 and 80 for both the TCP and UDP protocols.

Control4 MyHome: Remote Access Configuration

Figure 14. Firewall Access Rules



2. Create the firewall access rules to enable the MyHome application to remotely access Director on the Primary Controller inside the home's Control4 system.

Note: In the following example, the IP address of the Primary Controller on the LAN is 192.168.1.161, so any incoming access directed at ports 5020, 5021 or 80 will now be directed at the IP address of the Primary Controller.

The following excerpt is taken from the RV 120W Release Notes for Firmware version 1.0.2.6:

“Internet NAT redirection does not work using firewall port-forwarding rules. Description—A LAN client cannot access a service by using the WAN IP address of the LAN device (such as an IP camera or an FTP server). Work Around—Enable access to the service by creating a firewall access rule on the Firewall > Access Rules page. After clicking Add to add a rule, make the following selections:

- *Connection Type—Inbound (WAN (Internet > LAN (Local Network))*
- *Action—Always Allow*
- *Service—Specify HTTP for web server or, if the service uses a custom port, you can add it.*
- *Send to Local Server (DNAT IP)—Enter the internal IP address of the server.*
- *Make sure the Rule Status is set to Enabled and save the settings.*

After this you will be able to access the server via FQDN from both internal and external hosts. Note that it is not necessary to create a port forwarding rule; when applying the access rule, the router creates the corresponding port forward.”

Control4 MyHome: Remote Access Configuration

Figure 15. Firewall Access Rules (con't)

The screenshot shows the 'Access Rules' configuration page for a Cisco RV 120W Wireless-N VPN Firewall. The left sidebar contains a navigation menu with 'Firewall' expanded to 'Access Rules'. The main area is titled 'Add / Edit Access Rule Configuration'. The 'Connection Type' is set to 'Inbound (WAN (Internet) > LAN (Local Network))'. The 'Action' is 'Always Allow'. The 'Service' is 'Control4_TCP'. The 'Source IP' is 'Any'. The 'Destination IP' is 'Any'. The 'Rule Status' is 'Enabled'. There are 'Save', 'Cancel', and 'Back' buttons at the bottom.

The screenshot shows the 'Access Rules' configuration page for a Cisco RV 120W Wireless-N VPN Firewall, displaying the 'Access Rule Table'. The 'Default Outbound Policy' is set to 'Allow'. The table lists four rules, all with an 'Always Allow' action and 'Enabled' status. The 'Connection Type' for all rules is 'Inbound (WAN (Internet) > LAN (Local Network))' and the 'Destination IP' is 'Any'. There are 'Add Rule', 'Edit Rule', 'Enable', 'Disable', 'Delete', and 'Reorder' buttons below the table, along with 'Save' and 'Cancel' buttons at the bottom.

Action	Service	Status	Connection Type	Source IP	Destination IP
Always Allow	Control4_TCP	Enabled	Inbound (WAN (Internet) > LAN (Local Network))	Any	Any
Always Allow	Control4_UDP	Enabled	Inbound (WAN (Internet) > LAN (Local Network))	Any	Any
Always Allow	Control4_Art_TCP	Enabled	Inbound (WAN (Internet) > LAN (Local Network))	Any	Any
Always Allow	Control4_Art_UDP	Enabled	Inbound (WAN (Internet) > LAN (Local Network))	Any	Any

3. With the broadband router now properly configured, the last step is to point the MyHome application at the home's IP address. This is described in the following section.

4.2 MyHome Application Configuration

By utilizing the port forwarding approach, the mobile device is not treated as a local device in the same manner as using the VPN approach. As a result, the designation of Director's IP address will be based on the preferred Internet addressing solution.

If the Control4 system's public Internet address is static, then the Dealer needs only to enter that static IP address on the **More...>**Director screen in the MyHome application.

If a DDNS is used, the Dealer enters the hostname provided by the DDNS service provider.

Note: The MyHome – PC version only supports the numeric IP address. The other MyHome application versions for iOS and Android support entry of a hostname. The Dealer can ignore error messages from the application indicating the device is not currently connected to WiFi, but remember that updating the project will take time over low bandwidth remote-access connections.

5. Conclusion

With a robust broadband Internet connection and the proper home network configuration, Control4 users can extend their home automation systems for access outside the home.

To summarize, the key elements we've discussed in this white paper include

- knowing the home's public Internet address,
- installing a broadband router that supports secure connections with the home, and
- configuring the homeowner's mobile devices to reflect the idiosyncrasies of the broadband router's VPN implementation.

By selecting quality networking equipment and familiarizing themselves with its capabilities and limitations before arriving at the customer's home, Dealers can provide remote access using the MyHome application and ensure a high-quality Control4 experience.

As networking technologies and solutions evolve quickly, Dealers should check the Control4 website often to review the list of supported networking solutions, and identify those that support DDNS and VPN capabilities when the customer requires a remote access solution.