ReadyNAS Remote – White Paper

NETGEAR
May 2010

NETGEAR® ReadyNAS®
Connect with Innovation™

Table of Contents

Overview 3
Architecture 3
Security 4
Remote Firewall 5
Performance 5

Overview

ReadyNAS Remote is a software application that allows you to create an on-demand virtual private connection between your PC or Mac and your ReadyNAS. This connection is established without the need for any complicated setup – as in the case of traditional VPN application; all you need to do is manage a list of users that are allow to connect to your ReadyNAS. Once the connection is formed, it is just like you are on the same LAN as your ReadyNAS and you can connect to your shared folders using Windows Files Explorer or Mac Finder.

Architecture

The ReadyNAS Remote application runs on your PC or Mac and on your ReadyNAS and forms a direct connection between these two devices. The formation of this connection is facilitated by our ReadyNAS Remote servers. However in 95% of the connections, once the connection is formed our servers are not used of in the connection and there is a direct connection between you and your device. In the few cases when a direct connection cannot be formed, our relay servers are used to create the connection. Regardless of whether you have a direct or relayed connection your data is safe and fully encrypted using our end-to-end security model – only the endpoints can decode the data.

In order to form a connection between your PC or Mac and your ReadyNAS, both devices need to be registered with our ReadyNAS Remote servers. Your ReadyNAS will automatically register itself once the Remote addon has been enabled. Your device uses its unique MAC address as its username but there is no reason to remember this username since invite users from your ReadyNAS. To invite a user to access your ReadyNAS, you can search our global repository of ReadyNAS Remote users and add a user to your allowed list. If you would like to invite someone who is not already registered, you can send out an email invite which contains a link that will prompt the user to register with ReadyNAS Remote and download the client application software on their PC or Mac.

Once these devices (PC or Mac and ReadyNAS) are registered, they log into and form an SSL connection with the ReadyNAS Remote servers. The ReadyNAS Remote servers are then used to form a control channel and route control messages devices. The control channel can is used to send message to the server such as a new user has been added to the allowed list, or to the device informing the ReadyNAS that particular uses has gone offline. The control channel can also be used to route end-to-end control messages between the PC or Mac and the ReadyNAS, as in Figure 1. For example, a user on a PC might be requesting to set up connection to a certain ReadyNAS. In this case, a control message will flow from the PC through the ReadyNAS Remote Servers to the ReadyNAS. The ReadyNAS can then choose to accept or decline the incoming connection request and send a response back to the PC over the same control channel, as shown in Figure 1. If the connection is allowed by the ReadyNAS, the connection setup begins.

During the connection setup phase, our patented NAT traversal technique is used to setup a direct peer-to-peer connection between the PC or Mac clients and the ReadyNAS so no port-forwarding or dynamic DNS is required, as in Figure 1. The connection setup phase requires the use of our ReadyNAS Remote servers, but once the peer-to-peer connection is formed data travels directly[1] between your PC or Mac and your ReadyNAS. As part of the

[1] In approximately 95% of the connection, no relay server is used.

connection setup, 3-DES keys are exchanged which are only shared between the endpoints so the data the flows between the devices is protected by end-to-end encryption.

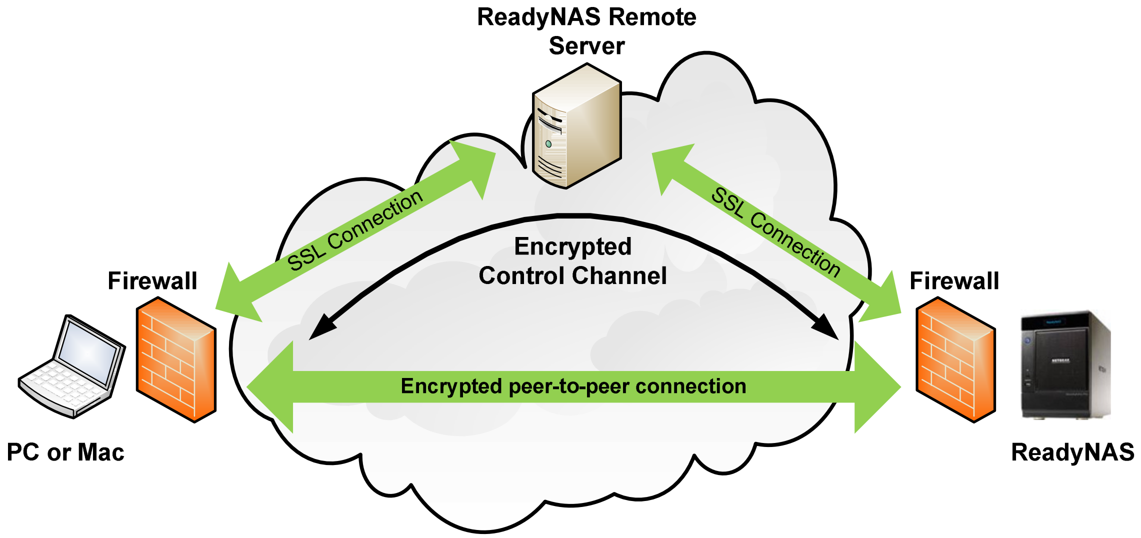


Figure 1: Connection setup with ReadyNAS Remote.

Security

ReadyNAS Remote offers users end-to-end security to access their data remotely. Our security model is outlined below:

1. ReadyNAS Remote running on the ReadyNAS securely (SSL) authenticates with and connects to ReadyNAS Remote server.
2. The administrator of the ReadyNAS securely (SSL) logs into the ReadyNAS Remote configuration page locally and adds registered ReadyNAS Remote users to allowed list (access control list).
3. On the Window or Mac clients, registered users securely (SSL) authenticate with and connect to the ReadyNAS Remote sever.
4. Once the user is authenticated the ReadyNAS Remote server will send over SSL to the PC or Mac, a list of ReadyNAS devices to which the authenticated user has been granted access.
5. Using the control channel setup with the ReadyNAS Remote server, the PC or Mac client sends a connection setup request to the ReadyNAS. If the requesting user is in the locally managed access control list located on the ReadyNAS, the connection setup is allowed to proceed.
6. During the connection setup, the PC or Mac clients then exchange 3-DES keys with the ReadyNAS so that the keys are only know by the two endpoints.
7. Once the connection is formed, all data is encrypted and transported directly between the two endpoints and only the endpoint can decrypt the data.
8. To access files that are password protected and not public, the user will be prompted for local Linux user credentials to access the folder - the same as if you were on the LAN.

There is no way that anyone that is not in the locally managed access control list or who has not been authenticated with the ReadyNAS Remote server can access your ReadyNAS.
Even though ReadyNAS Remote could be used as a VPN connection to your ReadyNAS, as only layer of protection we have only allowed it to transport CIFS/SMB and AFP traffic

between your PC or Mac and your ReadyNAS; all other ports on the virtual network are blocked.

Remote Firewall

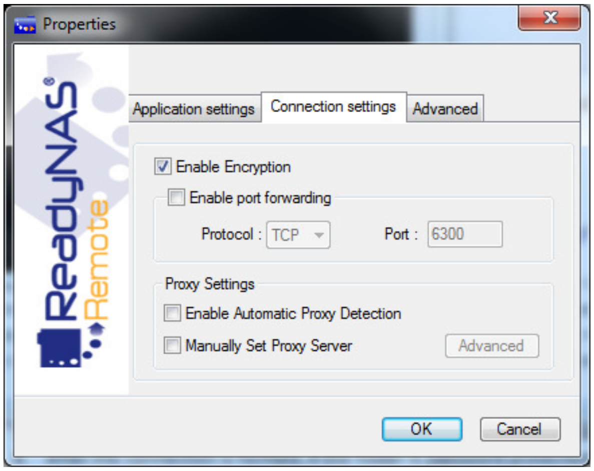
ReadyNAS Remote has a firewall built-in that protects both the ReadyNAS and the remote user from access to unauthorized services after the peer-to-peer connection is formed. The ReadyNAS typically is running many other services apart from Folder Sharing. These include services such as media streaming, ftp and http services. The remote user is allowed access only to Folder Sharing and should not be able to access other services. The firewall prevents the remote user from accessing the other services.

The firewall blocks any incoming packets to ports other than the Folder Sharing ports. Hence if remote users try to access ports other than Folder Sharing ports they will be blocked. The firewall is also running on the ReadyNAS Remote application on the PC or MAC side and prevents packets on the PC destined for other services on the ReadyNAS to be dropped at the source itself.

Performance

As is the case with any VPN application, ReadyNAS Remote introduces marginal bandwidth overhead in order to tunnel from the private network interface. The overhead is an additional TCP or UDP header and the relative overhead depends on the size of the packet that is transmitted. On average, the overhead introduced by ReadyNAS Remote is approximately 5%.

Since ReadyNAS Remote is a user space application (as opposed to a kernel application) it does consume some CPU resource. All traffic that flows over the virtual network is encrypted and firewalled (packet inspected) to only allow CIFS/SMB and AFP traffic. The amount of CPU resources used will depend on the data transfer rate. For example, if you are using ReadyNAS Remote and transferring data over 100 Mbps LAN you may see some measurable CPU usage. The CPU usage maybe reduced by not encrypting the traffic flow. We do not suggest you disable encryption, but if you are comfortable with you networking environment and need to boost performance it is an option. To disable encryption, go to Properties in the Mac or Windows client, you have the option to disable Encryption which may improve performance as in Figure 2.



Properties

Application settings | Connection settings | Advanced

☑ Enable Encryption

☐ Enable port forwarding

Protocol : TCP   Port : 6300

Proxy Settings

☐ Enable Automatic Proxy Detection

☐ Manually Set Proxy Server   Advanced

OK   Cancel

Figure 2: Connection settings dialog.