Synology QuickConnect White Paper

Last Jun 7, 2023

Table of Contents

Executive Summary

Network-attached storage (NAS) systems are helping small and medium-sized businesses (SMB) achieve big things. From freelancers to thriving startups with several hundred employees, accessing valuable data from different devices and locations is crucial to the success of any business. Unlike larger enterprises, SMBs generally have limited IT resources to help them enable and secure remote access around the clock.

Configuring a static public IP address, manually defining port forwarding rules and complicated network settings can also stretch a small business thin and even compromise data security. Thankfully, affordable and easy-to-use NAS servers with simplified web-based connectivity overcome these challenges and make enabling and securing remote access to important business files a breeze, allowing small and medium-sized enterprises to focus on what they do best and achieve their goals.

The Future of Connectivity for Consumers and Businesses

The operations and personnel of modern SMBs are no longer confined to a single office or region. Both employees and consumers are increasingly becoming accustomed to performing everyday tasks on their personal mobile devices, not just on desktop computers in an office space.

To remain competitive in this changing landscape, everyone needs to be able to collaborate and securely share information anywhere, anytime. Just like larger enterprises, small businesses today are expected to store and provide immediate access to documents, videos, images, and other types of files. Aside from securing these files, small businesses also need to grant access to employees with multiple devices and different permission levels.

The Promise of Network-Attached Storage

NAS have become popular among smaller businesses that do not require dedicated enterprise-class data centers. In fact, the global NAS market is booming and expects to see a compound annual growth rate (CAGR) of 21% from 2016 to 2023. However, enabling remote computers and mobile devices access to files on a private NAS server from over the Internet presents several challenges for SMBs.

In order for remote employees to access work files and other assets on a NAS server from outside the business's private LAN, there must be a reliable way to connect from a public network. However, typical methods, such as static public (external) IP addresses or port forwarding, can be cumbersome to implement and maintain, and also expose the organization to new threats.

The Shortfalls of Static External IP Addresses

The external IP address assigned to an organization's router by its Internet service provider (ISP) allows communication between a private network and the public Internet. Although external IP addresses can be either static or dynamic, most businesses prefer having a static IP address because a permanent address is easier for remote devices to find and connect to than a constantly changing (or dynamic) address. However, due to the limited number of public IP addresses available for allocation and the need for ISPs to provide 24/7 support, static public IP addresses are more expensive than dynamic public IP addresses.

Consequently, most customers, including many small businesses, are assigned a dynamic public IP address. Another drawback to owning a static public IP address is that devices need to be configured manually, requiring more effort and IT resources than many small businesses can afford. Having a static IP address can also expose the private network to security threats since a fixed address gives potential attackers more time to pinpoint and exploit vulnerabilities than addresses that are constantly changing.

The Problems of Port Forwarding

Aside from using static external IP addresses, SMBs can also configure port forwarding rules using network address translation (NAT) on their router to map external IP addresses and ports with private IP addresses and ports. Although port forwarding is an effective way to allow remote access to endpoints hidden within a private network, the rules need to be manually created and configured for every device and internal resource on the private network.

Modifying or adding new rules also requires complicated manual configuration, which would further stretch the limited IT resources of most small businesses. As with using a static external IP address, port forwarding can also expose the private LAN to greater cybersecurity risks since hackers can simply scan for open ports that can be used to break into the private network and access internal systems.

Simple and Secure Web Management for NAS

To overcome the drawbacks of using a static public IP address and configuring complicated port forwarding rules, Synology QuickConnect provides easy and secure access to Synology NAS servers over the Internet. With QuickConnect, IT administrators do not need to manually configure devices or complex port forwarding rules in order for remote employees to access resources on the company's private LAN.

What is QuickConnect?

As the name entails, QuickConnect is designed to make connecting to Synology NAS servers easy and quick. Setting up a server and correctly offering its services usually requires a certain level of knowledge in IT administration. QuickConnect seeks to remove that necessity and, through technology that causes the least network overhead, make connecting to Synology NAS servers effortless for anyone.

This means QuickConnect removes several barriers that are often encountered by users trying to set up a NAS server. Namely, QuickConnect users do not need to own a static external IP address, set up NAT port-forwarding rules, or switching between WAN/LAN addresses when the client device is relocated.

QuickConnect was initially designed to ensure specific Synology NAS services were always reachable from any network environment, even one that's not port-forwardable. Now it offers a comprehensive solution to guarantee that not only are the services always accessible, but they are also accessed with minimal effort and network overhead. In so doing, QuickConnect delivers the following features:

1. A permanent and easily memorized server ID - a QuickConnect ID - that works in both LAN and over the Internet
2. Server location detection (LAN/WAN detection)
3. QuickConnect hole punching
4. QuickConnect relay service
5. QuickConnect Smart DNS
6. QuickConnect WebRTC
7. QuickConnect web portal

With these features, QuickConnect users enjoy various exclusive benefits, including:

- A personalized server ID

- Anywhere accessibility regardless of network environment
- Assurance that the client device always takes the shortest path to reach the NAS over QuickConnect

A Secured Solution for You and Your Business

In addition to the convenience of integrated web management for NAS servers, Synology QuickConnect takes all the necessary precautions to prevent data leakage and interception. These security measures overcome the main shortfalls associated with using static public IP addresses and port forwarding, and include the following:

- Secured NAS server information and credentials
- End-to-end encryption for data transmission between the NAS and client Device
- A trusted certificate for web portal sessions
- High-security data centers

By providing an integrated and highly-secured web management service for NAS, Synology offers consumers and SMBs an easy yet powerful solution for enabling small business connectivity on a global scale—even without the IT resources of much larger enterprises.

How QuickConnect Works

QuickConnect offers three distinct services–mobile and PC client utility access, a single QuickConnect Web Portal for easy connectivity and port forwarding configuration, and DSM file sharing. All of these services require QuickConnect to guarantee an efficient connection. If QuickConnect is unable to connect to the destination NAS after completing the QuickConnect connectivity procedure, QuickConnect will route the connection through Synology Cloud Services. We will soon explain how QuickConnect works in greater detail.

One Web Portal for Better Connectivity

The QuickConnect Web Portal allows users to easily access their NAS and even enable port forwarding to ensure connectivity with a single, convenient web address, so that they don't have to rely on QuickConnect Relay Service to reroute the connection. Although consumers may not want to configure port forwarding, the best practice for small businesses is to enable port forwarding through the QuickConnect Web Portal for faster connectivity. The QuickConnect Relay Service is the final recourse if all connection attempts are unsuccessful. Although It may take longer to connect to the destination NAS, consumers may still prefer the relay service for its configuration-free connectivity.

QuickConnect Connectivity Procedure

QuickConnect performs a series of attempts to connect the client web portal to the destination NAS using the user’s QuickConnect ID. Below is the connectivity procedure:

1. Perform LAN/WAN detection to verify server reachability with the registered network addresses on the QuickConnect Server.
2. Test hole punching compatibility of the environment in which the Synology NAS is located.
3. Provide a relay service for any NAS not reachable using these methods.

LAN/WAN Detection

When a client attempts to reach a Synology NAS using the server’s QuickConnect ID, a request is sent to Synology QuickConnect Server for the registered information of the NAS. This allows the client to obtain network information about the server to identify possible ways to connect it. The information includes the public IP, LAN IP, and NAT type among others, all of which are necessary for the link and do not compromise the security of the NAS. With the given information, the client can identify whether a direct connection with the IP or domain address can be established over LAN or WAN.

QuickConnect Hole Punching

If no direct connection can be established, the client will attempt to establish a virtual tunnel between the client and the NAS via QuickConnect to allow a temporary direct link for data transmission. This technology allows the server and the client to experience Internet synchronization performance very similar to connecting via WAN IP/DDNS without physically having such an environment.

Hole punching works by initiating a virtual tunnel from the client to the NAS with the aid of the QuickConnect Server.

1. The NAS sends out a request to the QuickConnect Server, and keeps the hole, a random external port punched by the request on the NAT in front of the NAS, open to receive a hole punching request.
2. Similarly, the client sends out a request to the QuickConnect Server to create another hole on the NAT in front of the client.
3. The QuickConnect Server will deliver the hole information of the NAS to the client and vice versa.
4. The NAS will try to establish a connection to the client through the punched hole on the client side.
5. Once the client receives the hole punching request from the NAS, a hole punching response is sent back to the NAS via the punched hole on the NAS side.
6. If the hole punching response arrives at the NAS, a virtual tunnel is successfully created.

QuickConnect Smart DNS

With QuickConnect Smart DNS service, clients can easily connect to NAS over HTTPS protocol without complicated certificate configurations. The NAS can automatically obtain the certificates of the domains from Let's Encrypt. When QuickConnect web portal redirects a client to a NAS over HTTPS protocol, the browser will no longer show a prompt window for trusting the certificate.

Note that Smart DNS service is not applicable to DDNS domains.

QuickConnect Relay Service

Once the virtual tunnel is successfully established, the remote client can use this connection to communicate with the NAS directly and no network relay is needed.

In cases where the virtual tunnel cannot be created, a relay service is available for data transmission. When traffic is relayed, it goes through a Synology Relay Server before arriving at its destination. Requiring more time compared to direct connections or QuickConnect hole punching, the QuickConnect relay service serves as the final option for data to be communicated between the NAS and the client.

If the hole punching fails to create a connection, the client will make one last connection attempt by creating a virtual network tunnel using the QuickConnect relay service. The service works as follows:

1. To initiate the relay service, the client will send a request to the QuickConnect server.
2. The QuickConnect server will inform the NAS to create a virtual tunnel between the NAS and the Relay Server.
3. A port will be assigned on the Relay Server, and all network traffic to this port will be redirected via the established virtual tunnel to the NAS.
4. Once the Relay Server is ready, the QuickConnect Server will relay the information back to the client.
5. The client is now able to communicate with the NAS via the relay.

Communicating over the Relay Server can cause a significant delay in data delivery and is thus the last method a client will take in attempt to reach the server.

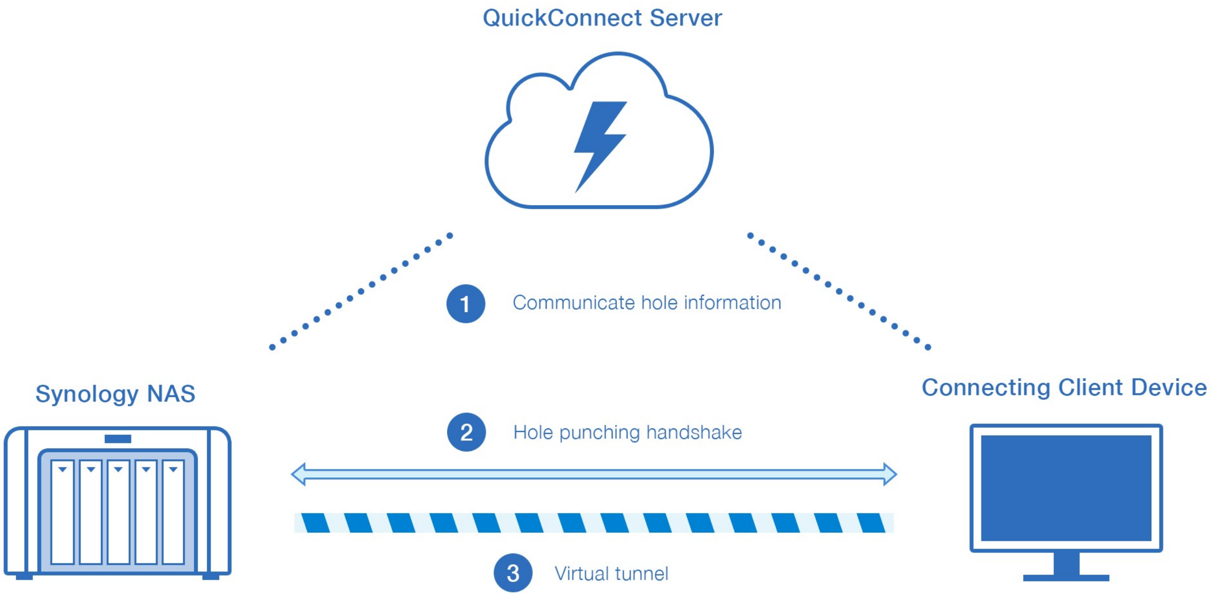

Figure 1: QuickConnect hole punching mechanism

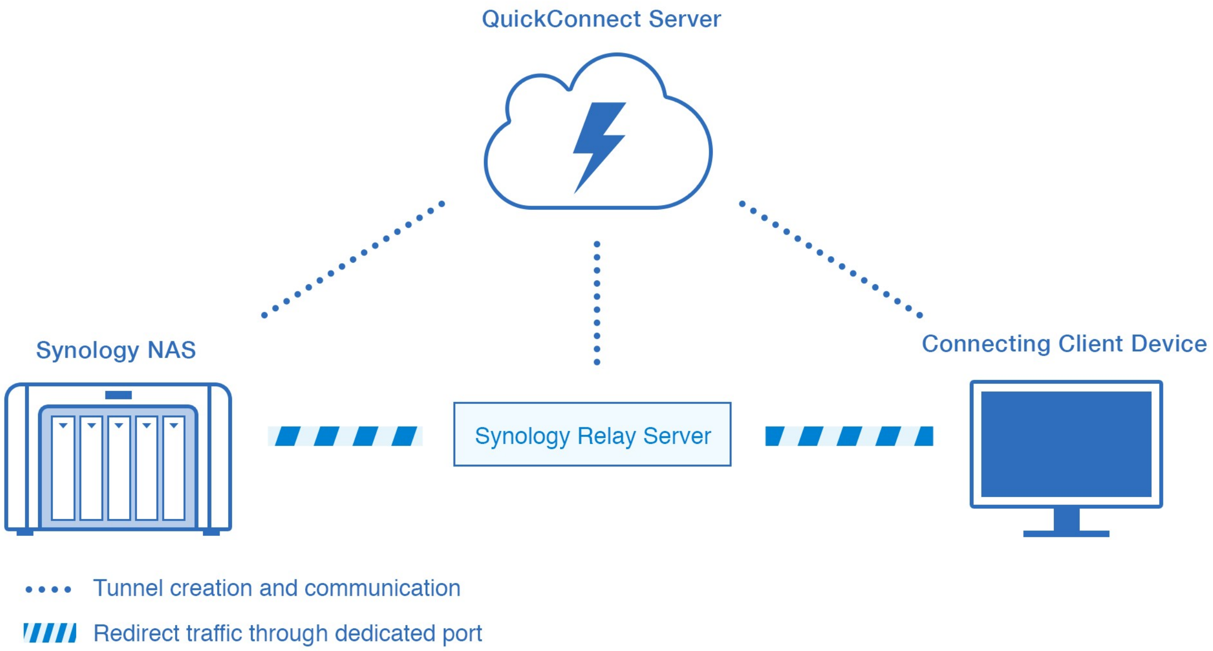

Figure 2: QuickConnect relay service

QuickConnect Services

We customize QuickConnect for each Synology application: mobile and PC client utility access, QuickConnect Web Portal, and DSM file sharing. These applications leverage different advantages of QuickConnect to deliver the same convenience and efficiency.

Mobile and PC Utility Access

QuickConnect allows Synology client software such as Synology Drive, and mobile applications such as DS file to access a Synology NAS using QuickConnect ID instead of using IP address and DDNS. In so doing, QuickConnect directs the client PC or mobile device to reach the NAS by way of LAN, WAN, hole punching or, if none of the above is available, through Synology's relay service.

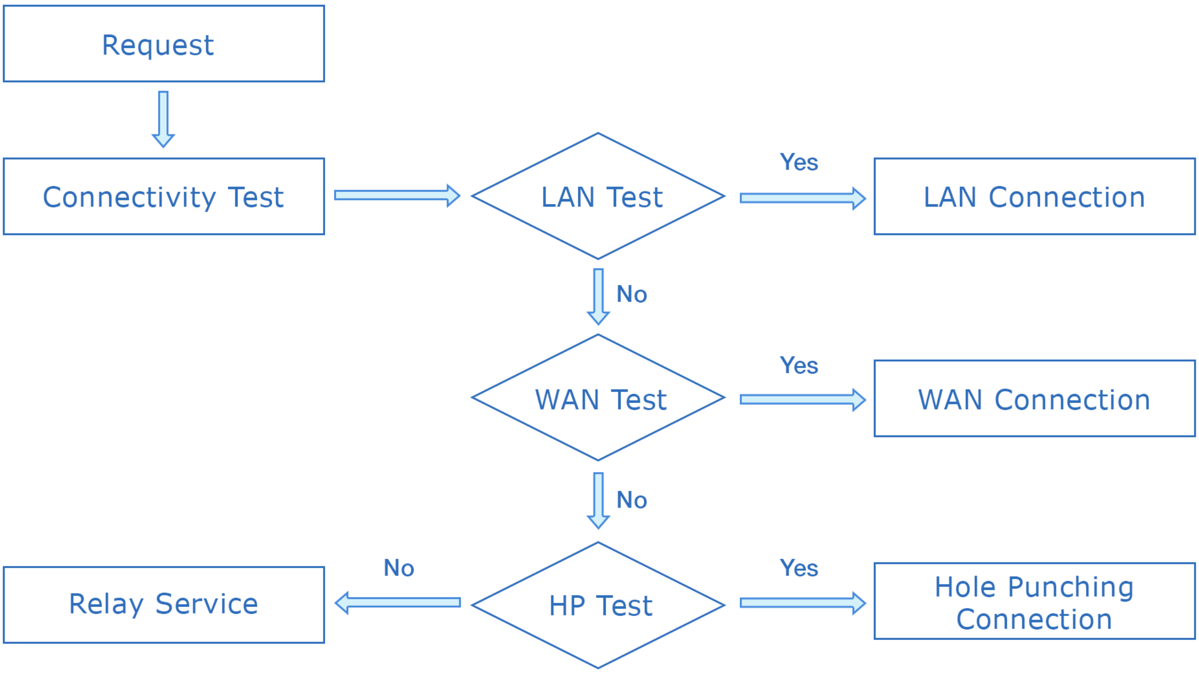

Figure 3: Workflow for mobile and PC utility access over QuickConnect

QuickConnect WebRTC

When direct connections are not possible, a client device can communicate with the NAS via the QuickConnect relay service. However, because the relay service has limited bandwidth, increasing usage may lower the transmission rates. To improve transmission rates, hole punching is implemented using WebRTC, allowing data to be partially transmitted through a virtual tunnel instead of relying solely on the relay service. Some data still need to be transmitted via the QuickConnect relay service due to browser limitations.

QuickConnect Web Portal

QuickConnect Web Portal allows the web interface of a Synology NAS, including the DSM management interface, Photo Station and various application portals, to be accessed from a browser anywhere with a consistent address that can be bookmarked.

A typical address of the DSM management interface powered by QuickConnect Web Portal looks like:

- quickconnect.to/[QuickConnect ID] (e.g., quickconnect.to/tenni)

A Photo Station address would look like:

- quickconnect.to/[QuickConnect ID]/photo (e.g., quickconnect.to/tenni/photo)

An application alias is required for DSM Application Portal to be accessed with the QuickConnect address. A typical address for File Station's application portal looks like:

- quickconnect.to/[QuickConnect ID]/[alias] (e.g., quickconnect.to/tenni/file)

These addresses are universal. When the QuickConnect Server receives a request for these addresses, it initiates the QuickConnect connectivity procedure to verify NAS location and accessibility. In cases where QuickConnect fails to locate a LAN or WAN address to redirect the browser to, Synology offers QuickConnect Portal Server that functions as a proxy between a Synology NAS and the connecting web browser.

The QuickConnect connectivity procedure helps redirect the browser to establish the best possible path to the desired web page. For example, the Portal Server will redirect the client browser to the LAN address (e.g., http://192.168.17.99:5000/) or WAN address (e.g., http://tenni.synology.me:5000) if these addresses are reachable.

The following image illustrates the process used by the QuickConnect Web Portal:

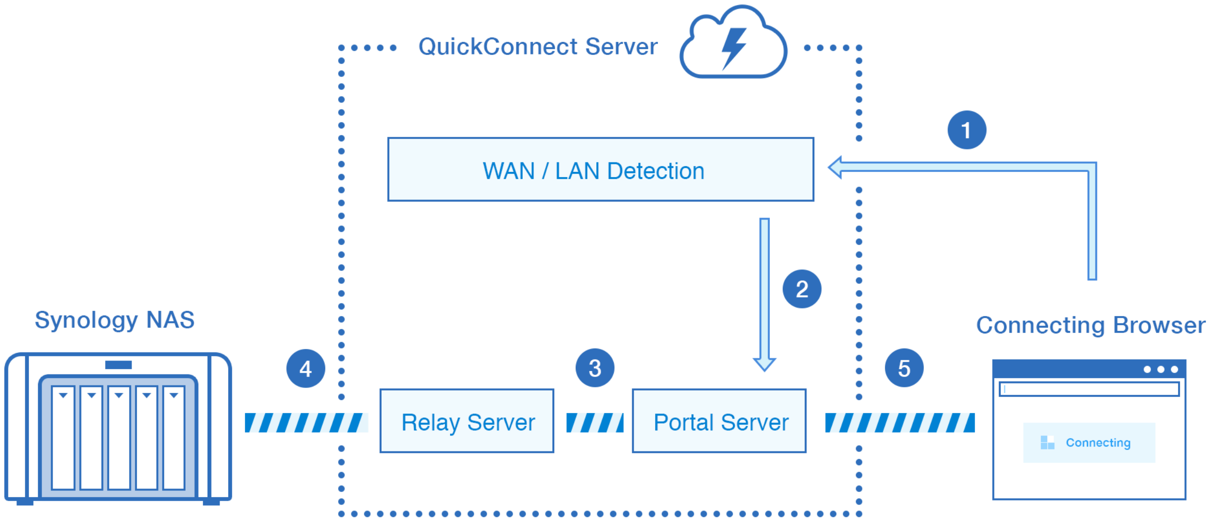

Figure 4: QuickConnect Web Portal

1. The client performs the QuickConnect connectivity procedure.

2. The browser is redirected to the Portal Server if the results of the LAN/WAN connectivity procedure are unsuccessful.
3. The Portal Server invokes a virtual network tunnel from the Relay Server to the NAS.
4. The Portal Server serves as a proxy to handle all the traffic between the NAS and the client browser via the virtual network tunnel.
5. The client browser is now able to access the intended NAS web pages via the Portal Server.

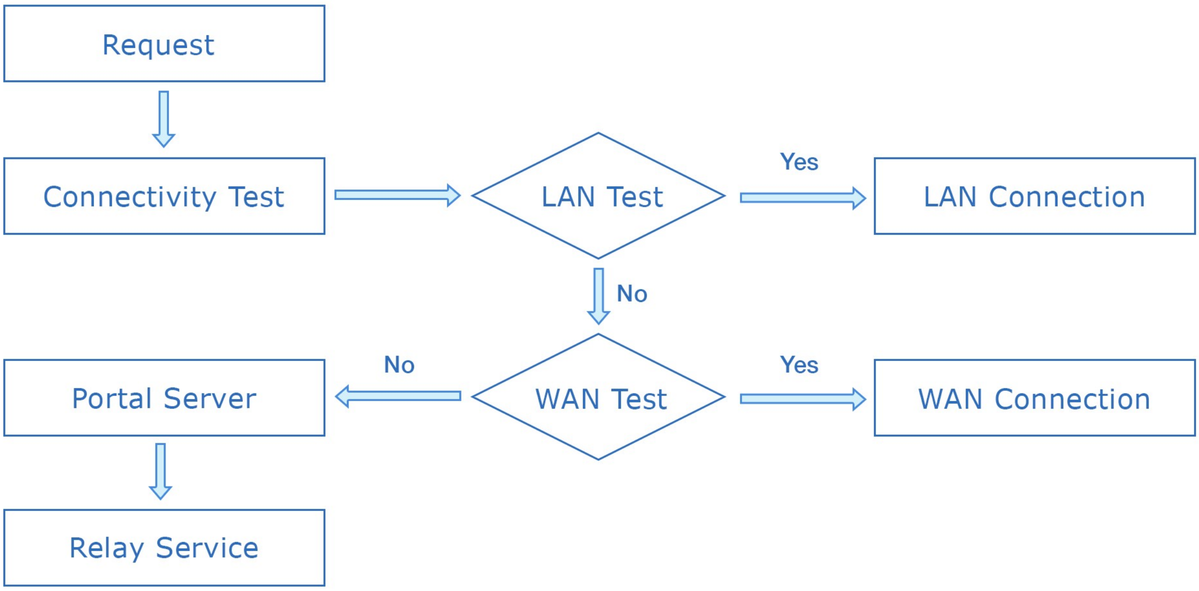

Figure 5: Workflow for QuickConnect Web Portal

To summarize, the benefits of QuickConnect Web Portal are:

1. QuickConnect connectivity procedure guarantees an efficient connection.
2. Web portal uses standard ports that are firewall-friendly for web browsing.
3. Permanent URLs that can be bookmarked.

File Sharing Service over QuickConnect

File sharing is a native DSM service that allows a file to be shared with a URL. A shared link takes the form of any of the following:

- http://gofile.me/2dRzN/lt1zrMTz
  QuickConnect enabled
- http://nnicole.synology.me:5000/fbsharing/ljjl5jbS
  DDNS enabled
- http://192.168.17.99:5000/fbsharing/pDWQYwq
  Link begins with the server's IP address

When QuickConnect is enabled, a file sharing link always takes the form in the "gofile.me" domain. By way of the connectivity procedure, this link allows the connecting browser to take the best possible path to access the shared files. That is to say, the client browser will be redirected to the shared link's LAN/WAN address if available, before attempting through the relay tunnel.

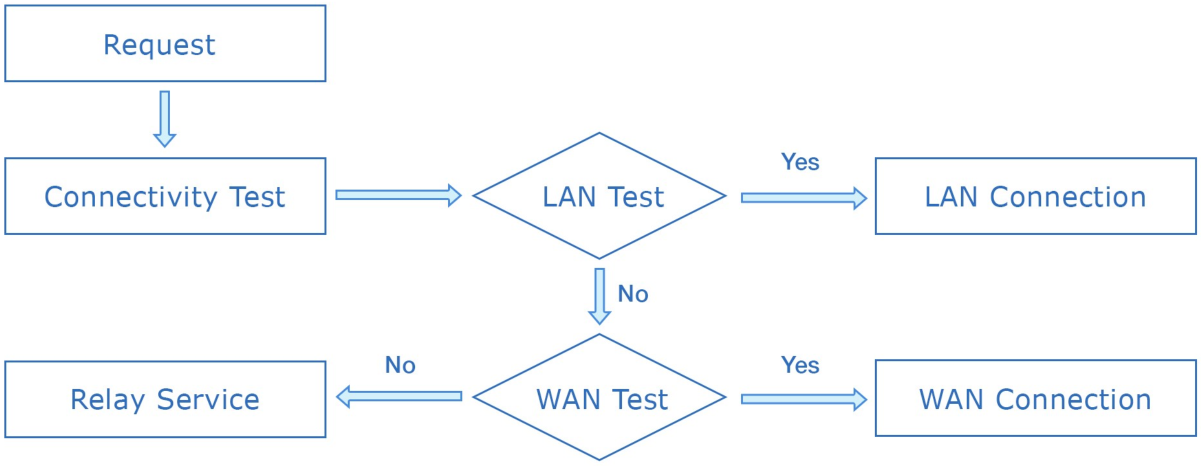

Figure 6: Workflow for file sharing over QuickConnect

URLs of Different Connection Types

Types of different connections can be identified by the URL formats. URL formats and the corresponding connection types are listed as follows:

- [ip].[alias].direct.quickconnect.to
  Direct connection over LAN
- [alias].direct.quickconnect.to
  Direct connection over WAN
- [alias].[relay_server_id].quickconnect.to
  Relay connection of DSM web pages
- gofile-[sharing_id].[relay_server_id].quickconnect.to
  Relay connection of gofile sharing web pages

Supported Services

The supported services/applications are as follows.

PC utilities and mobile applications	DSM native services	QuickConnect Web Portal

Chat DS audio DS cloud DS cam DS download DS file DS finder DS note DS video LiveCam MailPlus Synology Drive (desktop and mobile) Synology Photos	CMS File sharing	Application Portal Audio Station DiskStation Manager Download Station File Station Note Station Surveillance Station Synology Photos Video Station

QuickConnect Security

Even though QuickConnect provides convenient NAS management over the web, businesses can rest assured that all of their private data is protected at all times. In fact, Synology goes to great lengths to ensure that the NAS server data, data transmissions, web portal, and even the data centers for the Synology QuickConnect Servers are impeccably secured.

Synology NAS Information

To enable the QuickConnect service2, the Synology NAS must be registered under the QuickConnect Server. This means the Synology NAS reports its status, such as network environments and supported services, to the QuickConnect Server.

The reported information (i.e. the public IP address, LAN address, NAT type, etc.) is required for the connectivity procedure. Synology safeguards users' digital privacy. The retrieved information is only used by Synology in order to deliver the QuickConnect service.

Relay Tunnel

With SSL enabled, data transmission over the network virtual tunnel is secured with end-to-end encryption. Therefore, QuickConnect guarantees confidentiality and integrity of data transmission between the Synology NAS and client devices.

QuickConnect Web Portal

QuickConnect Web Portal is secured by end-to-end encryption when the browser is redirected to the Synology NAS using LAN or WAN connection. Otherwise, the request is directed to the Portal

Server.

In such conditions, the Portal Server offers a trusted certificate for the connecting browser to verify the identity of the Portal Server. This helps us combat man-in-the-middle attacks by preventing messages from being intercepted by devices imitating the Portal Server.

The Portal Server would then decrypt and modify the specific HTTP headers so as to inform the destination NAS of the identity of the connecting client. Having done so, the Portal Server then sends the data to the destination Synology NAS via the network virtual tunnel. Once again, data transmission over the virtual network tunnel is secured with end-to-end encryption if SSL is enabled.

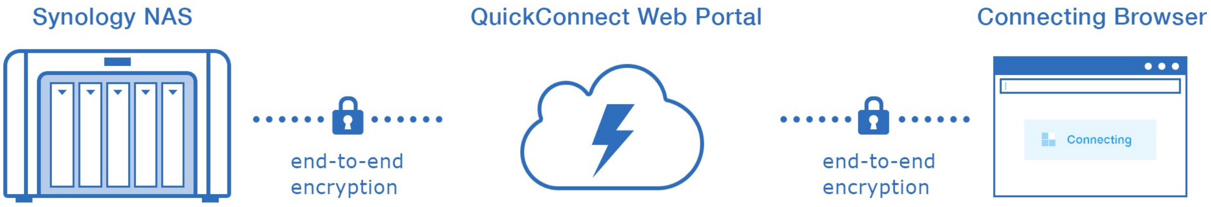

Figure 7: Security mechanism of the QuickConnect Web Portal

While providing the promised services, QuickConnect makes no use of collected data from registered Synology NAS servers except in delivering such services. For more details, visit the Privacy Terms on our official website.

Facility Security

Synology QuickConnect Servers are hosted in data centers in a total of eight sites around the globe to provide high-quality and stable service. All data centers are staffed 24/7, guarded with surveillance systems and strict policies governing personnel access. Facilities are also well equipped to ensure power supply and network availability in the event of outage or preventable disasters.

Conclusion

All businesses have big aspirations, no matter their size. But for individual consumers and smaller companies that lack the deep pockets and extensive IT resources of larger enterprises, enabling employees to access valuable data from anywhere poses additional challenges. Although many small and mediumsized businesses are installing NAS servers on private LANs, granting remote access over the Internet often requires additional IT expertise to manually configure devices and complex port forwarding rules.

With Synology QuickConnect, any user and business can enjoy anywhere access to data stored on a Synology NAS, as well as the QuickConnect web management interface, from any network environment. Eliminating the need to set up complicated port forwarding and firewall rules for cross-network connections, Synology QuickConnect makes all of this possible with a simple, personalized QuickConnect ID and securely guides the connecting device via the shortest route across networks to the destination NAS.

To find out how your business can start reaping the benefits of NAS today, visit www.synology.com or refer to the following links.

- Subscribe to Synology eNews for the latest insights at Synology Account
- Try out a live demo for the latest DSM at https://demo.synology.com