VPN’s and Mobile Apps for Security Camera Systems: EyeSpyF-Xpert

Contents:
1.0 Introduction p2
1.1 Ok, what is the problem? p2
1.2 Port Forwarding and Edge based Solutions p2
1.3 What is a VPN? p2
1.4 Security advantages of a VPN p2
1.5 Types of VPN p3
2.0 VPN and AXIS Camera Companion p4
2.1 Speed of performance p4
3.0 How to set up a VPN on the Synology DiskStation NAS p5
3.1 Three types of VPN! p6
3.1.1 PTTTP p8
3.1.2 OpenVPN p10
3.1.3 L2TP p11
4.0 Testing the VPN p14
5.0 Connecting to the VPN via a Mobile device. p15
5.1 Advantages of a VPN for connecting via Mobile p18
1.0 Introduction
In this article we explore how a VPN can be used to help with remote access to Security Camera Systems via Mobile Apps. We will focus on the AXIS Camera Companion System and corresponding Mobile App but the general case is true for many Security Camera Systems and Mobile Apps.

1.1 Ok, what is the problem?
Generally, IP Security Camera Systems run on a LAN. Often there is no need for remote access. But the introduction of Mobile Apps suddenly creates the need for Remote Access. If the Mobile Device is running on the same LAN as the Security Camera System then access to the Camera System via Mobile App is relatively simple. The difficulty arises when the user moves the Mobile Device into another LAN or onto a Mobile Network. From the users point of view the App won’t work anymore. Of course trying to contain the Mobile device within the are of the LAN is futile.

The reason the App won’t work when it is moved outside the area of the LAN is because remote access is not set up on the Security Camera System. To enable remote access the System Manager must set up port forwarding (http://portforward.com) to an externally addressable IP address. The external IP address port details can be saved in the Mobile App. Better Mobile Apps automatically detect when they are on the same LAN as the Camera System or if they are remote and switch from local address to remote address automatically maintaining uninterrupted connectivity.

Setting up port forwarding is a technical chore and some System Managers may feel it is a security risk.

1.2 Port Forwarding and Edge based Solutions
Edge technology based solutions such as AXIS Camera Companion feel the Port Forwarding problem more acutely. A server style Security Camera System often requires just one open port to gain access to the system and all cameras that are connected to it, however an edge based system where there is no central server may need multiple open ports, one for each camera.

The AXIS Camera Companion has got the ability to support up to 16 cameras. If you want remote access to all 16 cameras via the mobile app you will need 16 port forwarding rules. This can be tedious and some routers may not even allow you to set up large number of port forwarding rules. This constraint can restrict you from being able to gain remote access to a full AXIS Camera Companion Site.

1.3 What is a VPN?
A Virtual Private Network (VPN) (http://en.wikipedia.org/wiki/Virtual_private_network) extends a private network across a public network such as the internet. It allows a computer to send and receive data across a public network as if it was connected directly to the private network and it benefits from the functionality, security and management features of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of various virtual tunnelling protocols or traffic encryption.

From a user perspective, accessing the data on a VPN is exactly the same as if they were connected directly to the private network. VPNs allow employees to connected securely to the companies intranet from outside of the office in order to access data.

1.4 Security advantages of a VPN
Public WiFi offers no encryption security to its users and your signals are broadcast for anyone tech savvy to eavesdrop. If you are connected to a public network via a VPN then all of the data that was once easy to intercept is now encrypted and no one else can see it. Much like a firewall protects the data on your computer, a VPN protects your data when you are online.

1.5 Types of VPN

Server VPN software:
A VPN can come in several different formats. You can buy VPN software and put it on a server within your LAN.

Router VPN:
Some brands of routers have VPN software built in.

NAS box VPN:
Some Network Addressable Storage devices have a VPN feature.

If the VPN is mounted on the router than no additional ports need to be opened. The router VPN software handles the port management from its own VPN to the LAN. If the VPN is mounted on a NAS box or on a server within the LAN then a port must be opened to that device. This is still a technical burden but it is secure as you can control who connects to it and all data transfer is encrypted.
2.0 VPN and AXIS Camera Companion
We decided to try out the VPN software on our Synology Diskstation device (http://www.expertreviews.co.uk/network-storage/277309/synology-ds110j) we have in the office with a view to using it with AXIS Camera Companion (http://www.axis.com/en/products/cam_companion_software/index.htm) and corresponding Mobile App (http://www.eyespyfx.com/companion.php).

2.1 Speed of performance
A VPN encrypts all data that is transferred through it. Encryption is a processor task. The speed of the transfer may be affected if the processor in the VPN device is slow. If the VPN is located in the Router that may offer a speed advantage over VPN’s that are located behind the router. In our case we set up a VPN on a NAS box behind the router. The NAS box is busy doing other tasks and so its processor is already busy. The VPN is an additional load. In our test performance was slightly slower than directly accessing the cameras via open ports but acceptable.
3.0 How to set up a VPN on the Synology DiskStation

First you will have to connect to the web interface of your Synology DiskStation NAS Box using the username and password that you have been assigned.

Once you have logged in you should go to the package centre and find the VPN package. Download and install this package.

Once you have installed the VPN Package you should start to run it.
You should now click on the main menu and choose “VPN Server”. This will show you options to configure your VPN.

3.1 Three types of VPN!

When we got to the point of configuring the VPN we were faced with a choice of three types of VPN:
**PPTP** (Point-to-Point Tunnelling Protocol) is a commonly used VPN solution supported by most clients (including Windows, Mac, Linux, and mobile devices including Android and iOS). PPTP is the easiest to set up.

**OpenVPN** is an open source solution for implementing VPN. It protects the VPN connection with the SSL/TLS encryption mechanism. OpenVPN was not available on our office Router so we could not use this one. OpenVPN is the perhaps the most secure but it has the greatest overhead in terms of set up.

**L2TP** (Layer 2 Tunnelling Protocol) over IPSec provides virtual private networks with increased security and is supported by most clients (such as Windows, Mac, Linux, and mobile devices). L2TP is more secure than PPTP is marginally more difficult to set up. It is supported on iOS and Android devices.

The next section gives the set up procedure for each of the 3 VPN types:

1. PPTP
2. OpenVPN
3. L2TP
3.1.1 PPTP

Tick Enable PPTP VPN server.

Now modify the below advanced options according to your needs.

- **Dynamic IP address**: Enter a network address here. VPN Server will assign virtual IP addresses to VPN clients according to the value entered. For example, if you enter "10.0.0.0," the virtual IP address assigned to VPN clients will range from "10.0.0.1" to "10.0.0.[Maximum connection number]" in our case 5" for PPTP.

- **Maximum connection number**: Specify the maximum number of concurrent VPN connections.

- **Authentication**: Choose one of the following options:
  - **PAP**: This authentication method does not encrypt VPN clients' passwords during authentication.
  - **MS-CHAP v2**: This authentication method encrypts VPN clients' passwords during authentication using Microsoft CHAP version 2.

- **Encryption**: If you selected **MS-CHAP v2** above, choose one of the following encryption options:
  - **No MPPE**: VPN connections will not be protected with any encryption mechanism.
  - **Require MPPE (40/128 bit)**: VPN connections will be protected with a 40-bit or 128-bit encryption mechanism, depending on the client's settings.
  - **Maximum MPPE (128 bit)**: VPN connections will be protected with 128-bit encryption mechanism, which provides the highest level of security.

- **MTU**: Specify the maximum transmission unit to limit the size of data packets transmitted via the VPN.

- **Use manual DNS**: Specify the IP address of a DNS server to push to VPN clients. If this option is disabled, the DNS server used by the DiskStation will be pushed to clients.
When you have finished editing the details click **Apply**.
3.1.2 OpenVPN

Tick Enable OpenVPN server.

Now modify the below advanced options according to your needs.

- **Dynamic IP address**: Enter a network address here. VPN Server will assign virtual IP addresses to VPN clients according to the value entered. For example, if you enter "10.0.0.0," the virtual IP address assigned to VPN clients will range from "10.0.0.1" to "10.0.0. [Maximum connection number]" for PPTP.

- **Maximum connection number**: Specify the number of concurrent VPN connections.

- **Enable compression on VPN link**: Enable this option if you want to compress data during transfer. This option can increase transmission speed, but might consume more system resources.
When you have finished editing the details click **Apply.**
3.1.3 L2TP

Tick Enable L2TP/IPSec VPN server.

Now modify the below advanced options according to your needs.

- **Dynamic IP address**: Enter a network address here. VPN Server will assign virtual IP addresses to VPN clients according to the value entered. For example, if you enter "10.0.0.0," the virtual IP address assigned to VPN clients will range from "10.0.0.1" to "10.0.0.[Maximum connection number]" for PPTP.
- **Maximum connection number**: Specify the maximum number of concurrent VPN connections.
- **Authentication**: Choose one of the following options:
  - **PAP**: This authentication method does not encrypt VPN clients' passwords during authentication.
  - **MS-CHAP v2**: This authentication method encrypts VPN clients' passwords during authentication using Microsoft CHAP version 2.
- **Use manual DNS**: Specify the IP address of a DNS server to push to VPN clients. If this option is disabled, the DNS server used by the DiskStation will be pushed to clients.
- **IKE authentication**: Enter and confirm a pre-shared key. This secret key should be given to the VPN user in order to authenticate the connection.
When you have finished editing the details click **Apply**.
4.0 Testing the VPN

To ensure that the VPN has been enabled correctly you should click on status and ensure that the correct one is enabled (in our case PPTP).

Now you should go to the Privilege tab and ensure that the correct users have got access as shown below.
5.0 Connecting to the VPN via a Mobile device.
In this example we will use an Android Tablet. A VPN profile can be created and managed at Settings > Wireless & networks > VPN. Remember to select and enter the correct protocol, server address, and pre-shared key.

After creating the profile, we'll connect to the VPN Server using the Synology NAS box username and password.
Once you have connected to the VPN from your mobile device you should go back to the web view of your diskstation and open the VPN Settings again. If you look at the connection list you should now see that the mobile device account that you used in the last step is now connected to the VPN.
You have now successfully set up and connected to your VPN Server.
You can now logon to your Mobile App, in this case Viewer for AXIS Camera Companion using the VPN as the connection.

5.1 Advantages of a VPN for connecting via Mobile

Ease of use:
By using a VPN, will also bypass the need to carry out a lot of the port forwarding for each camera required without the use of a VPN. Using a VPN you will be required to open only one port which allows the VPN to connect and then the mobile device will connect to the network via the VPN rather than making a direct connection like before.

Secure:
The VPN is more secure than opening multiple ports. All data traffic is encrypted and the devices that can connect are controlled and monitored.