A Basic Guide to keeping your CCTV system secure online.

In a modern-day security system, access to a CCTV system from any location around the world and more commonly smart phone devices and tablets is now an essential part of any system specification.

Unfortunately, in most cases people do not take the necessary steps to ensure that their CCTV system is as safe and secure as it should be once remote access has been enabled.

There are many ways of securing online systems and this document will only cover the most basic and common processes.

Best Security Measures

P2P

P2P is the current recommended way to keep your security system safe online. Using P2P takes very little configuration so it is quick and easy to set up for both engineers and end users. The NVR generates a unique QR code which can be scanned by the LILIN Viewer app, this will then import all the connection settings for the NVR directly in to the LILIN Viewer app. Using P2P there is no need for any port forwarding on site.

P2P works by the NVR establishing an outbound connection to the P2P server, the LILIN Viewer also connects to the P2P server and the P2P server connects the NVR and App together so video and data can flow seamlessly between the 2 devices.

The only drawback of using P2P is there is a slight delay (4 – 5 seconds) in connection when the app is first opened, this is while the secure connection in between the app and the NVR established within the P2P server.

It is still strongly recommended to change the password on your NVR to a strong password.

Please note P2P is not supported by every product. Please check your product specification/documentation to confirm P2P is supported.

VPN

One of the most secure way of securing your CCTV system for remote access is to use a VPN connection. A VPN connection requires specific VPN enabled equipment usually found in Premium Home/SME/Enterprise routers and firewall equipment.

For more information on VPN click here - http://en.wikipedia.org/wiki/Virtual_private_network

Using a VPN connection means you do not have to set up any port forwarding on your router to remotely access the system, instead VPN access is configured meaning any device that wishes to connect to the system requires a VPN client configuring on that device. The VPN client on the remote device is started and a connect established between the client device and the router/firewall on the site with the CCTV system. This forms a secure tunnel and the client device is issued an IP address on the local network meaning the client device now behaves like it is connected to the local network even though it can be anywhere in the world. All the CCTV devices are then accessed using their internal IP address.

For the average home or SOHO, a VPN connection is just not a viable cost option, so if your router does not support VPN the information below will help make your system as secure as possible.

Essentials Security Measures

Change ALL the default passwords to a 'Strong' password

Change ALL default passwords for ALL users on ALL devices that can be accessed remotely from the internet. Default usernames and passwords for most devices are very well known by unauthorized users looking to access systems online and the default usernames and password are the details an unauthorized user will try first. Most people are unaware that there are actual large default username and password reference databases online, making the unauthorized user's job even easier.

Enable Brute Force Account Lock Feature

All current LILIN NVR models have an account lock feature which can be enabled, this feature is essential if you are opening any port forwarding to an NVR. This feature will disable web GUI logins for a specified amount of time once an incorrect password has been entered more than the specified times.

Do not use the main administrator account for daily use

As on any I.T. based system it is not recommended that you use the Administrator account for daily usage. Although you may want administrator privileges when connecting to your device, using the administrator account is still not advised. Instead setup another user account and grant that user administrator privileges or any other level access rights required. The less access rights you grant to remote users the safer your system will be should anyone gain unauthorized access.

Recommended Security Measures

Change the default ports used by each device accessible remotely

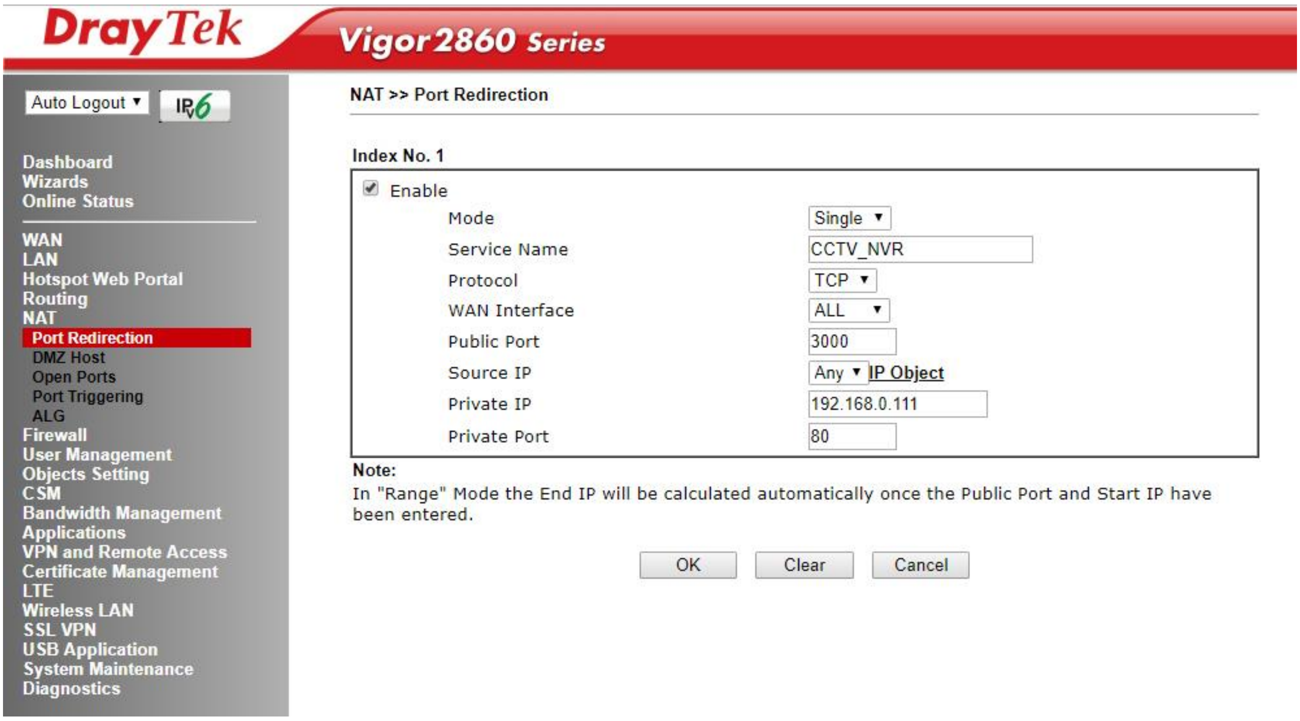
Port redirection

If you need to open ports in your firewall, most modern routers now support a feature known as port redirection. If your router supports this feature, it is recommended to use this rather than change the HTTP ports on all the local devices.

Port redirection allows you to have devices using the same internal/private port number and specify a unique external/public port number.

Please see your router documentation for instructions of how to use and configure port redirection on your specific router.

Example of port redirection for an NVR



NAT >> Port Redirection

Index No. 1

☑ Enable

Mode	Single ▾
Service Name	CCTV_NVR
Protocol	TCP ▾
WAN Interface	ALL ▾
Public Port	3000
Source IP	Any ▾ IP Object
Private IP	192.168.0.111
Private Port	80

Note:
In "Range" Mode the End IP will be calculated automatically once the Public Port and Start IP have been entered.

If Port redirection is not supported

Change the default ports used by all CCTV devices on the network that can be accessed remotely via the internet. As default ALL LILIN devices use port 80 and other default ports such as RTSP port 554 and 3100. These port numbers can be changed under the network menu on your LILIN equipment.

Alternatively, some routers support a feature called 'Port mapping'. This allows all the device's ports to be left as default and then specify non-standard ports to use when accessing the device remotely from the internet.

E.G. Incoming port 5000 on the router can be mapped to device 192.168.1.2 port 80. This port redirection is handled internally by the router not the CCTV equipment so accessing the security system from an internal device would not change.

Changing all of these ports on the devices will make an unauthorized users life harder. People often use tools to scan for a router's 'open ports' and live devices responding on these ports. These scans are usually run in large batches and only the default and most commonly used ports are usually scanned, so by adjusting the default ports your devices may not appear in any generic none targeted IP scans.

Only open the exact/minimum ports required to remotely access your system

Open ONLY the basic ports required to access your system, any extra open ports can pose an additional security risk to your system. Modern CCTV equipment heavily resembles PC equipment, they also share a lot of traits such as operating systems and services. Opening port ranges and other none required ports can result in unrestricted access to equipment’s ‘operating systems’ allowing command line administration of the CCTV equipment. This could result in a number of unwanted consequences.

Lock remote access connection from specific IP addresses

Lock any remote access down to specific static IP address or IP address range. This is a very easy way of making your system safer. Allowing access to only pre-specified IP addresses means only incoming requests from a predefined destination IP address are allowed. This method is best used in site to site security where a static IP address is available on both sites.

Locking access to a pre-specified IP address or IP address range is a viable option for all users. With some basic research, access to your security system can be secured down by IP address to requests from specified Internet Service Providers or even specific countries of origin. Countries and Internet Service Providers are allocated pre-set IP ranges by the internet governing body. By adding these IP ranges to your router/firewall you will automatically deny access from a remote access request with an origin outside of the specified IP address range.

Disable remote ping responses from the router

Stop your router from responding to Ping requests from a WAN IP addresses. Ping requests are the most common give away that there is an internet connected device at the end of an IP address. Large batches of IP address are pinged to give an unauthorized user a shorter list of known active devices to target. By not appearing on these huge lists your system will hopefully remain undetected for much longer.

Never use the DMZ feature on your router

Do not use the DMZ feature of your router/firewall. The DMZ will port forward ALL ports to the specified DMZ server/device. The danger here is that some equipment run extra services such as 'Telnet'. Allowing access to this service means an unauthorized user can access the Operating System of the camera or NVR/DVR and perform functions such that could have detrimental effects to the system.

See ‘Only open the exact ports you need to remotely access your system’ above

Set up an incoming connection schedule in your router

Set up an incoming connection schedule on the router to allow specific timed access to rules in the router/firewall. Most router/firewalls support scheduled access to the firewall rules, allowing rules to be turned on and off at certain specified times of the day. This will once again limit the amount of time your internet connected system will be accessible from the internet therefore making the system more secure.