ID Systems

Laboratory Informatics & Applications
HL7, HIPAA, MU, POCT Consultation
Application Integration & Connectivity
Facility Command, Control, Security
Facility Automation & Surveillance
Unix, Linux, Cache, U2 Specialist

ID Systems Primer on IP Cam, DVR, & NVR Security

The availability of low cost residential IP (Internet Protocol) Cameras, Digital Video Recorders (DVR), and Network Video Recorders (NVR) has brought significant benefits to individual home security and to “monitoring at a distance”.

Some of our BLOG users have purchased these devices. If you are participating in the Sunrise Terrace Snapshot Repository we have assured you that your personal network remains secure when using the outbound FTP transport configuration provided to you when you added your camera, DVR, or NVR to the Sunrise Terrace Repository site.

Most of these IP devices are capable of additional methods of content sharing and remote access that may have already been activated by the manufacture as part of a vendors “plug and play” or “out of the box” automatic usability features.

In this BLOG POST I will suggest the review of five basic network configuration settings essential to maintaining the security of your personal network and the IP devices attached to that network.

The router hardware supplied by your ISP (Internet Service Providers) is the very first line of defense of your personal network. Your ISP uses the IETF RFC-1918 standards to establish one of three 3 private IP address ranges* for your personal network and the router will apply NAT (Network Address Translation) to connect your personal network to the Internet. This technique effectively prevents outside or external access to your personal home network. However, if you have installed local service on your personal network, such has a Web Server, you or your contractor would have had to re-configure your Internet router to provide external access to those services using protocols that may have exposed your personal network and IP devices on that network to external users.

The first (1) and best way to protect your IP devices from intrusion is to change the manufactures default administrative userID and password, or better yet disable the vendor administrative userID and create your own access credentials! There are lists of camera vendors default userID’s and passwords listed on the Internet. In a world of mass produced IP devices vendors have published instructions on how to configure their IP devices for remote access. Additionally, there are sites on the Internet that search for IP cameras by the manufacturer or geographic location and automatically attempt to log-on to the camera. If you have not changed your camera default administrative userID and password you could become privacy hack victim. Shodan at www.shodanhq.com is one example of such camera hacking service.

Some IP camera manufactures ship their equipment with a service call DDNS service already enabled to ease remote access setup for their customers. DDNS (Dynamic Domain Name Service) is a service often established by the vendor that allows your IP device to send its IP address to the companies DDNS service database. Any user who knows your default DDNS userID can use this information to find their way back to your IP camera, DVR, or NVR. Suggestion two (2) is to disable DDNS service on your IP device unless you are using a DDNS service for your own remote access to IP cameras, DVR's, or NVR's on your network. There are third party DDNS providers that you can use instead of the vendor provided service that are more secure.

DDNS on its own doesn't allow full access to IP devices on your personal network. You or your consultant/contractor would have additionally established a “Port Forwarding” configuration on your Internet Router. Port Forwarding instructs the router to direct an inbound connection request to a specific IP address on your personal network based on a network parameter, typically by using a specific port number. This is the most common way vendor provide remote access to their IP devices on your personal network. I would not recommend the purchase of an IP device that does not allow you to disable the DDNS service.

Suggestion three (3) is to change IP device remote access service to a non-standard port. The well-known port number of the HTTP demon service is 80. Web crawlers and search engines will attempt to use the well-known ports to locate

you IP device during an Internet crawl. Changing the well-known port to something other than one of the popular alternatives (i.e.: 8000 & 8080) will reduce your vulnerability by 90% for an IP device exposed to the Internet. Suggestion four (4) is to monitor your Internet Router activity. Keeping your router visible so you can and monitor the router LED's for transmit and receive activity is an indication of a possible attack. If you see continual strobing (blinking) of these LED's check your Internet Router log. Finally, suggestion five (5) is to check the router log periodically or when you observe continuous or unusual router activity. External access attempts to your personal network will appear in the router log (if you have activated logging) and you can use that data to filter or deny unwanted traffic to your personal network.

These five suggestions are easy to do and are the basis of good Internet security for IP devices on you network.

There are several other tools available to secure your personal network that are more technical or require special hardware and/or services from your ISP. Some of these security enhancements are:

- Do not use your routers default address for a camera
- Update your IP devices firmware (Router & IP devices)
- Install an isolated network for your remote access devices
- Use a VPN Router (this requires special hardware and/or clients)
- Use alternative protocols for camera access (sHTTP, RTSP, etc)

I hope this BLOG POST has been helpful in securing your personal network.

Dav A. Eide
28 Mar 2015

Footnote: IETF RFC-1918 private network ranges start with the IP Addresses: 10.0.0.0, 172.16.0.0, & 192.168.0.0.

11728 136th Avenue East, Puyallup, WA 98374 • Office: 253.445.0961 • Mobile: 206.790.8199 • Fax: 253.445.0470
Email: info@idsystems.org • Web: http://idsystems.org