About "Port Forwarding"

Mar. 2018

About “port forwarding”

It is well known that the Internet is flooded with constant cyber-attacks. Once connected to the Internet, devices will face all kinds of cyber security problems. Therefore, it is generally recommended that devices not be directly connected to the Internet, unless there are special access purposes. Without direct access to the Internet, the probability of a device being attacked will be greatly reduced. However, this does not preclude the possibility of an attack. When it is necessary to make a device Internet-facing, it is important to protect them using a defense in depth approach. Firewalls, VPNs, intrusion detection, encryption and two factor authentication on Internet facing devices are all effective ways of reducing the risk of attack and alerting you of anomalous network traffic.

If P2P or VPN solutions fail to meet the needs of users, who want to have a quick and steady access to the specified port service of the device through the Internet, users may have to choose the traditional "port forwarding" scheme. While this provides easy access to devices, special consideration should be given to cybersecurity controls because these devices will be visible from the internet. If one decides to use this method, it is highly recommended that additional host-based security controls are used to better secure the device. As shown in our "IPC Security Guide" and "NVR Security Guide," we have provided a number of recommendations to better secure these devices:

1) Minimize the number of ports exposed to the Internet. Do not set the IP address of the device to DMZ, which will expose your device directly to the Internet. Only forward the network ports that must be used. For example, to use web services, only port 443 is forwarded.

2) Avoid using generic ports and reconfigure them as custom ports. After changing the default port, you will reduce the risk that the attacker may guess the port you are using. For example, port 443 is usually used for HTTP. It is recommended that the user configure a custom port for the specified service instead of port 443, and the custom port should conform to the TCP/IP port rule (1 -- 65535)

3) Enable IP filtering. If you have static IP addresses on your remote devices, you can create a filter rule with an IP range (your ISP at home, your mobile provider, etc.) and only allow the devices that are specified in IP address filter rule to access the system.

The above security suggestions can enhance the security to a certain extent, but

these are not enough, and users still need to do the followings as basic points:

1) Set a strong password. See NIST recommendations for strong password creation. https://pages.nist.gov/800-63-3/sp800-63b.html
2) Upgrade to the latest device firmware released by Hikvision, in a timely manner.

If possible, placing your Internet connected devices behind a VPN can enhance the system security substantially. While Hikvision devices do not currently have built in VPNs, it is possible to implement VPN servers in front of Hikvision devices.