



DVR Network Security

Table of Contents

TABLE OF CONTENTS	2
GETTING STARTED	4
INTRODUCTION.....	4
DISCLAIMER	4
BACKGROUND INFORMATION	4
GENERAL BEST PRACTICES	4
USE THE EQUIPMENT ONLY AS SURVEILLANCE EQUIPMENT.....	5
USE A STRONG PASSWORD POLICY	5
A WORD ON DEFAULT PASSWORDS	5
PASSWORD STRENGTH.....	6
USER SPECIFIC PERMISSIONS	6
NETWORKING BEST PRACTICES	6
USE WINDOWS FIREWALL OR ANOTHER SOFTWARE FIREWALL.....	6
A WORD ON STANDARD PORTS.....	7
THE BASICS	7
TAKING IT A STEP FURTHER	8
USE A HARDWARE FIREWALL INSIDE YOUR NETWORK	8
USE AN SSL CERTIFICATE IF POSSIBLE	9
USE A VPN CONNECTION FOR VIDEO	9
ISOLATE YOUR SURVEILLANCE EQUIPMENT.....	9
ADDITIONAL RESOURCES	9
NETWORKING	9
DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)	9
IP ADDRESSING	9
LOCAL AREA NETWORKS (LAN)	9
NETWORK ADDRESS TRANSLATION (NAT)	9
PORT FORWARDING	10
PORTS	10
ROUTING / ROUTER CONFIGURATION	10
SUBNET / SUBNET MASKING	10
TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL (TCP/IP)	10
USER DATAGRAM PROTOCOL	10
WIDE AREA NETWORKS (WAN)	10
FIREWALLS	10

GENERAL INFORMATION	10
COMMON PORT NUMBERS.....	10
SOFTWARE FIREWALLS	11

Apex CCTV

Getting Started

Introduction

This document is intended to give some background on security networkable DVRs and IP cameras. This is background information applicable to most products, and is not specific to any of the products that we carry.

Disclaimer

This document requires a basic understanding of networking principles including, but not limited to, network address translation (NAT), transmission control protocol/internet protocol (TCP/IP), user datagram protocol (UDP), subnet and subnet mask configuration, dynamic host configuration protocol (DHCP), IP addresses, routing and router configuration, public vs. private networks, etc...

The basic knowledge described above is outside the scope of this document, and will be covered briefly or not at all, and only as it applies to an individual step you need to take in configuring your product. Please find other resources in the "Additional Resources" section at the end of this document.

Background Information

There are some inherent security advantages to networkable digital video recorders, the primary of which is that they are uncommon, compared to say a windows system, and therefore their target footprint for attacks is much smaller than that of widely distributed systems. Unlike Windows or other common operating systems, the number of DVR installations is relatively small, and a hacker cannot readily make assumptions about which DVR, IP Camera, or software package you are using. Most businesses, however, run Windows or Linux operating systems, and thousands of individuals work hard to penetrate these high-value targets because copies of the environments are easy to set up and repeatedly test attacks against.

Many attacks come through well-documented and known techniques that are shared amongst the hacker sub-culture and are therefore common knowledge. This is simply not the case with surveillance systems.

However, as with any networked computer system, surveillance equipment is as secure as you make it. Leaving default usernames and passwords in place, for example, is begging for trouble. Taking even a few simple steps to secure your surveillance installation can make it very difficult to penetrate, and will discourage all but the most persistent hackers from even making the attempt.

General Best Practices

Here is a list of general best practices for all data security that apply to windows based DVRs as well.

Use the Equipment Only as Surveillance Equipment

This is particularly true of DVRs that are built on the windows operating system. Running unneeded services on the system, surfing the internet, checking your email, and the like all present possible routes of exploitation for hackers and/or viruses.

A (non-comprehensive) list of services and other programs that may be pre-configured that should be disabled might be:

- 1) Internet information services
 - a. Your DVR probably has a built-in web server included with its software package, and on top of being a security hole, this can conflict with other web servers running on port 80.
- 2) Windows file and printer sharing.
- 3) FTP servers of any kind.
- 4) Database servers of any kind.
- 5) Mail servers of any kind.
 - a. If you must run an SMTP server for your DVR software to send notifications, make sure it is not an open relay that can be exploited by spammers.
- 6) Windows shared folders.
- 7) Message Queuing service.
- 8) SNMP service.
- 9) Remote Desktop Connection.
- 10) Windows Remote Assistance.
- 11) Windows Messenger or Windows Live Messenger.
- 12) Any email clients such as Outlook or Outlook Express.

In addition, do not use the DVR for any business or personal related computing such as running financial packages, storing personal documents, or making online credit card transactions that may be stored in your computer's memory somehow.

Use a Strong Password Policy

There are at least three aspects to take into account.

A Word on Default Passwords

First and foremost, IMMEDIATELY change any default password you were given when you first received your hardware. Using default usernames and passwords is the single most exploited vulnerability on virtually all network hardware. It is also the easiest to prevent. If your system allows it, change *both* the administrative username and password. Keep in mind that defaults are typically readily available on the internet, or from the product manufacturer. If somebody can tell what you have, they can likely get the default login information and compromise your system.

Password Strength

Use a strong password. Do not use your name, business name, address, phone number, email address, birth date, a relative's birthdates, or any other commonly available information. A medium-strong policy is as follows:

- 1) Contains a minimum of eight characters.
- 2) Use three out of the following groups. All four is better:
 - a. CAPITAL LETTERS
 - b. Lowercase letters
 - c. Numbers, such as 1, 2, 3, etc...
 - d. Special Characters such as \$, %, ^, &, etc...

Also, try not to use any common English words or names of any kind.

Completely random passwords, such as "ne@6Sw!z" are the best. However, if you have trouble memorizing such passwords, you can still make a strong password by taking something you like and turn it into a password by capitalizing one or two letters, and replacing letters with symbols that look like them. Take for example: "Bugs Bunny ."

By replacing the letter 'B' with the number '8', the letter 's' with '\$', and the space with an underscore ('_'), we can get something pretty good, and not too hard to remember:

"8ug\$_8unny." If you capitalize a random letter or two, perhaps the 'n' since there are two of them and *that* is easy to remember, you can get something VERY strong:

"8ug\$_8uNNy."

Whatever you do, DO NOT use a default password.

User Specific Permissions

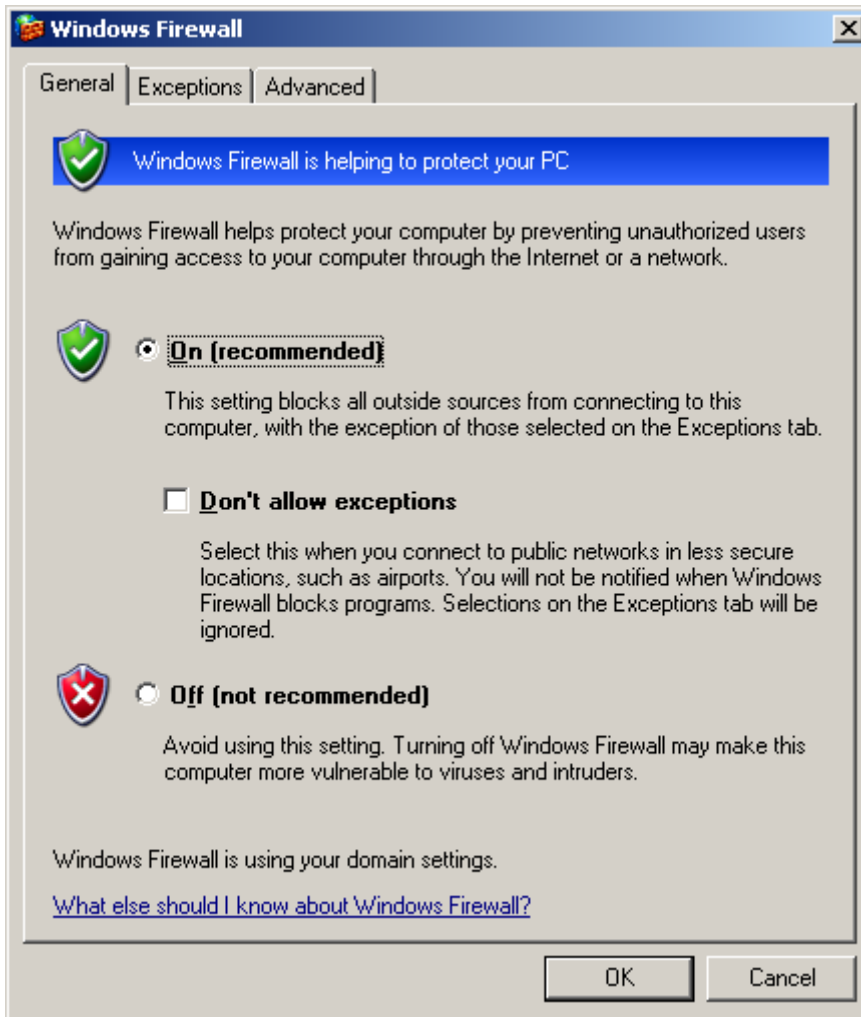
If at all possible, do not allow any access to the equipment from the administrative username or password. If you are the owner, fine, but DON'T give those credentials out to anyone else for remote viewing purposes. If somebody needs access to your equipment, give them their own login, and only grant them the permissions they need to accomplish their purpose.

Networking Best Practices

Here is a list of general best practices for all data security that apply to windows based DVRs as well.

Use Windows Firewall or another Software Firewall

This makes difficult attacks in both directions. The first is attacking your DVR from a compromised PC somewhere else on your network. The 2nd is attacking other machines on your network from a compromised DVR.



When configuring any firewall, you should close all traffic in both directions, and the only open ports that are needed for the services specifically running on each system. Your network probably has a hardware firewall protecting against the internet. Software firewalls can provide at least some protection *between* compromised PCs on your network and other machines.

A Word on Standard Ports

The Basics

Using standard ports can be dangerous as well. If you are using a web server, everyone expects it to run on port 80. So run it on port 4211, or some other random port. The same thing goes for DVRs (most of which HAVE web servers running on port 80). For example, GeoVision webcam server software requires the following ports by default:

80, 4550, 5550, 6550.

It also can use the following ports for certain optional functions:
21, 3550, 5511, etc...

The point is, I know these port numbers without looking them up because I am in the surveillance industry and have done some network configurations with GeoVision products. You can easily configure all of these ports to use different numbers and make someone take the trouble of sniffing them out and trying to figure out which is which. If you run default ports, they don't have to go to this effort.

Taking it a Step Further

Another great trick is to use Network Address Translation (NAT) in your router to forward one public port number to a different local area network port number. That way, if someone is able to exploit your system publicly from say, port 80, then they are *guessing* as to what port the internal traffic is on. They will assume (usually) that there are other vulnerabilities on similar hardware on port 80, but if you are running those services on say, port 85 internally, instead of the public port 80, then they have to figure that out before doing further harm to the rest of our equipment or network. If they cannot remotely install packet sniffing software on your DVR, then they are guessing once the standard port they were expecting fails.

Use a Hardware Firewall inside Your Network

Software firewalls are better than nothing... much better in fact! But a hardware firewall is much harder to penetrate. If you expect an attack to enter your network from say, your DVR, then put a firewall between it and the rest of your network, and use the strictest possible traffic policy. You can use this in conjunction with the NAT trick in the prior step to really shore things up on the LAN side.

Your traffic policy should take the following into account:

- 1) Only allow needed ports in and out from the DVR(s).
- 2) Only allow specific IP addresses or ranges through the DVR that need access.
 - a. If you run a machine shop and you want to keep an eye on your workers, they probably don't need network access to the DVR at all. Take it away based on their IP addresses.
 - b. This is valid for both public and private networks. If you need to view from home, and have a static IP address at your house, then allow that one address and block all others to the surveillance equipment.
- 3) Translate traffic to a different subnet on the DVR side of the firewall (Requires a router with a firewall).
 - a. Example: Your standard IP address formats are the typical 192.168.1.x. Place the public address on the router on that format, but the LAN interface on 20.10.10.x or some other, different interface. This obscures IP addresses when trying outbound attacks from the DVR and makes further network discovery difficult.

Use an SSL Certificate if Possible

Get one from Thawte or VeriSign or GoDaddy or another reputable company and set the DVR to refuse non SSL connections.

This makes transmitted data extremely difficult to read, even if someone IS sniffing packets and has the necessary codec to play back your video available. Note that this can affect streaming video performance.

As with other items, use a non-standard (443) port for your secure transmission.

Use a VPN Connection for Video

By requiring a VPN connection to your network rather than publicly opening ports, you further secure your equipment from outside attack.

Isolate Your Surveillance Equipment

If you *really* want to protect your LAN, run your surveillance equipment on a completely separate internet connection and just don't connect it to the rest of your network. This makes further exploits from a compromised DVR impossible.

Additional Resources

Networking

Dynamic Host Configuration Protocol (DHCP)

http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

<http://www.dhcp.org/>

http://www.dhcp-handbook.com/dhcp_faq.html

<http://www.webopedia.com/TERM/D/DHCP.html>

IP Addressing

http://en.wikipedia.org/wiki/IP_address

http://www.3com.com/other/pdfs/infra/corpinfo/en_US/501302.pdf

<http://computer.howstuffworks.com/question549.htm>

http://www.webopedia.com/TERM/I/IP_address.html

Local Area Networks (LAN)

http://en.wikipedia.org/wiki/Local_area_network

http://compnetworking.about.com/cs/lanvlanwan/g/bldef_lan.htm

http://www.webopedia.com/TERM/L/local_area_network_LAN.html

Network Address Translation (NAT)

http://en.wikipedia.org/wiki/Network_address_translation

<http://computer.howstuffworks.com/nat.htm>

<http://www.webopedia.com/TERM/N/NAT.html>

Port Forwarding

<http://www.portforward.com/>

http://en.wikipedia.org/wiki/Port_forwarding

<http://www.zeropaid.com/news/6160/Introduction+to+Port+Forwarding>

Ports

http://en.wikipedia.org/wiki/Computer_port_%28software%29

<http://itmanagement.webopedia.com/TERM/P/port.html>

Routing / Router Configuration

<http://en.wikipedia.org/wiki/Routing>

http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm

<http://www.webopedia.com/TERM/R/routing.html>

Subnet / Subnet Masking

<http://en.wikipedia.org/wiki/Subnetwork>

<http://www.networkcomputing.com/unixworld/tutorial/001.html>

<http://www.webopedia.com/TERM/S/subnet.html>

Transmission Control Protocol / Internet Protocol (TCP/IP)

http://en.wikipedia.org/wiki/Internet_protocol_suite

http://www.webopedia.com/TERM/T/TCP_IP.html

User Datagram Protocol

http://en.wikipedia.org/wiki/User_Datagram_Protocol

<http://www.webopedia.com/TERM/U/UDP.html>

Wide Area Networks (WAN)

http://en.wikipedia.org/wiki/Wide_area_network

http://www.webopedia.com/TERM/W/wide_area_network_WAN.html

Firewalls

While firewall configuration is outside the scope of this document, various hardware and software firewalls can create configuration and remote access problems for various security products. The following information is intended to help provide starting points for troubleshooting firewall issues. Links to many common software firewall products and vendors are provided.

General Information

[http://en.wikipedia.org/wiki/Firewall_\(networking\)](http://en.wikipedia.org/wiki/Firewall_(networking))

<http://www.howstuffworks.com/firewall.htm>

<http://www.webopedia.com/TERM/f/firewall.html>

Common Port Numbers

<http://www.iana.org/assignments/port-numbers>

http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
http://www.webopedia.com/quick_ref/portnumbers.asp

Software Firewalls

BlackICE PC Protection

<http://www.iss.net/>

BullGuard Suite

<http://www.bullguard.com/default.aspx>

Comodo Personal Firewall

<http://www.personalfirewall.comodo.com/>

F-Secure Internet Security

http://www.f-secure.com/home_user/products_a-z/fsis2007.html

Jetico Personal Firewall

<http://www.jetico.com/>

Kaspersky Internet Security

<http://www.kaspersky.com/>

LavaSoft Personal Firewall

http://www.lavasoftusa.com/products/lavasoft_personal_firewall.php

McAfee Personal Firewall

<http://us.mcafee.com/default.asp>

Microsoft Windows Firewall

http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx

NeT Firewall

<http://www.ntkernel.com/w&p.php?id=18>

Norman Personal Firewall

http://www.norman.com/products_npf.shtml

OutpostPro Firewall

<http://www.agnitum.com/>

Panda Platinum Internet Security

http://us.pandasoftware.com/products/platinum_is/

pcInternet Patrol

<http://www.pcinternetpatrol.com/>

Preventon

<http://www.preventon.com/>

PrivateFirewall

<http://www.privacyware.com/features.html>

Terminet

<http://www.infotecs.biz/Soft/terminet.htm>

Trend Micro PC-cillin Internet Security

<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>

VisNetic Firewall

<http://www.deerfield.com/products/visnetic-firewall/>

Webroot Personal Firewall

<http://send.onenetworkdirect.net/z/11246/CD45178/>

Apex CCTV