Bailys

Camera System

Introduction

Bailys' camera system was created out of an effort to curb the malicious actions by those who falsely claim illegal behavior against Bailys. The system was created with an extreme number of cameras in order to hopefully capture all events which may happen during the restaurant and nightclub hours. Baily's camera system would have been impossible if it wasn't for the other projects which were implemented earlier. The camera system as a whole is composed of three main parts: pfSense, ZoneMinder, and FreeNAS in order to properly function with 38 cameras. PfSense is the router, which segments the network into secure subnets for not only PCI compliance, but also for managing network IP resources. ZoneMinder, is the software installed over Ubuntu 18.04, in order to manage and render the live streams which are being broadcasted by the Amcrest IP cameras. Finally, FreeNAS stores all of the recordings which have been generated by ZoneMinder in a 15TB volume. Currently, the system will store video up to 7 days, although new methods are being discovered in order to conserve drive space more effectively.

Networking

Networking, in terms of hardware, involves the use of Ubiquiti Tough Switches which provide the cameras with 48 volts of POE (Power Over Ethernet). The tough switches are connected directly to the same network as the MICROS POS terminals and server. They are given IP addresses between 192.168.100.200 to 192.168.100.106. PfSense provides the VLAN tag of 30 in order to instruct the Ubiquiti Tough Switches to utilize the PfSense DHCP server to produce a network subnet in the range of: 192.168.8.0/24. This is to allow all 38 cameras, and any future additions to all be contained within the .8 subnet, to allow more free IP address space for the MICROS .100 subnet. Managing the Ubiquiti Tough Switches will require a system which is connected to the MICROS network, and can ping the switches by their .100 IP addresses.

None of the cameras, or any part other than ZoneMinder is accessible through WiFi, in order to promote system reliability, as well as security. It is impossible to completely control what goes through the air, or where the signal travels, but through a hard-line CAT5/6 setup, control and security can be achieved with relative ease. Almost the entire network of cameras is supported by CAT6 cabling, in order to ensure that switches in the network are running at Gigabit speeds. The pathway from Store Room C to the main office where the servers are currently located, are supported by a CAT5 cable. This setup will soon change, where the servers will be deployed in Store Room C, and the entire system will then be supported on CAT6. Currently the CAT5 path is running in Gigabit, so the performance improvement will most likely only be marginal if measurable at all. The purpose of CAT6 was for preference to ensure that Gigabit will be achieved, as CAT6 is “certified” for Gigabit.

Recording

Recording requires the use of ZoneMinder and FreeNAS. ZoneMinder is a PHP/C++ based application which runs on top of an Ubuntu 18.04 Linux server, which requires extensive setup time as it requires Apache and MySQL to be installed before ZoneMinder can be run. The system allows for any internet enabled device on the networks OTD, and OTD-EXT to view the cameras utilizing a simple web browser. The URL in order to access ZoneMinder is currently: http://192.168.100.57/zm which is the IP address of the Ubuntu server, followed by "zm" to stand for ZoneMinder. ZoneMinder stores the processed video within FreeNAS through an iSCSI virtual drive. The file formatting of the stored video is actually a collection of JPG images, which are later combined by using ffmpeg to produce an swf or mpeg video file. Currently almost all of the cameras are setup within ZoneMinder for motion detection, as this method saves drive space and network traffic/bandwidth while there is no movement. The motion detection is typically set to high sensitivity, in order to record as much video as possible without having the recording running continuously.

Storage

FreeNAS is where all of the video is stored from the ZoneMinder Ubuntu server. The ffmpeg files are saved to a virtual iSCSI device. ZoneMinder cannot store it's video files within a typical Microsoft SMB style share, as FreeNAS and SMB do not seem to have proper support for symlinking. If ZoneMinder ever attempts to utilize an SMB file share, it will simply throw an error in the log, and no video will be recorded. ISCSI on the other hand, natively supports symlinking, as it takes SCSI commands through a set of drivers in order to operate exactly as a dedicated hard drive. ISCSI allows to trick ZoneMinder into thinking it is storing to a physical drive, avoiding any incompatibility issues with the file sharing service. Unintentially, it was discovered that by switching from SMB to iSCSI, performance was improved, and it allowed for easier drive space allocation on the NAS, by specifying a maximum drive size for the iSCSI volume. Note: For an iSCSI volume over 4TB, G-Parted must be used instead of the default Linux tool, "fdisk." If a GPT partition is not created for a volume larger than 4TB, Linux will create a DOS volume where any sectors beyond the 4TB mark will be left "unallocated." After using G-Parted, it will still be necessary to create an EXT-4 filesystem, and a few symlinks for ZoneMinder to store it's files in without changing any of it's default settings.

There is a **known issue with iSCSI and FreeNAS.** In the event that ZoneMinder is throwing an error stating that it is unable to symlink, along with many read/write errors, ensure that the iSCSI service has been started in FreeNAS. It is important to run the *sudo service zoneminder stop* command on the Camera Server, as well as restarting the server with: *sudo shutdown -r now* There are a few rare scenarios where FreeNAS will not boot with iSCSI online in the event of a power failure, or a hard system reboot. In this scenario, the Camera Server will need a full restart, in order to restart it's iSCSI virtual drive. Although the setup may seem temperamental, having each system on a UPS power backup system will prevent this issue, and most likely will never arise again.

PfSense

PfSense also provides the firewall settings to properly isolate subnets from one another, and manage what devices are accessible between each subnet. For the ZoneMinder camera server, this means PfSense can be configured where the server can access the .8 subnet where the cameras operate. PfSense also provides network access to the Internet by explicitly allowing the camera server while everything else on the .100 network remains blocked. Currently, the .100 network is labeled as "BRIDGEWIFILAN," and firewall settings affecting the .100 MICROS network are the settings listed under BRIDGEWIFILAN. The cameras are placed in an isolated .8 subnet that does not allow any data other than explicitly defined live video streams to leave the subnet. This is to prevent any outside malicious attackers from being able to access the cameras directly. The NAS has been placed within the .2 subnet by the ip: 192.168.2.8. The .2 subnet is managed directly from the Fronteir/FiOS router, and is not managed by PfSense. Although the NAS is not directly managed by PfSense, there are firewall settings provided that restricts or allows access for the camera server and the NAS to communicate. This is similar to "port forwarding" in the common traditional ISP routers.

Permissions

The NAS, and other Unix-like systems such as the Camera Server perform permissions in a way which may be confusing for the average Windows user, or even an Administrator. In Unix based systems, permissions are based on ownership and groups. Each user has their own folder on the NAS, and the ownership is bound to their User, and the Group that their user account is defined under. The user account inherits it's permissions from the group. Currently there are two groups, Trusted, and Bailys. The Trusted account allows the power user permissions such as "sudo," and other elevated permissions for system administration. Permissions are currently being perfected, but if there is a chance that user X writes a file to user Y, and user Y does not have the permission to modify the file that user X has written, it will require an administrator to properly assign permissions, at least upon a group level, in order to allow user Y to modify the file. Hopefully once perfected, anyone who is within the Bailys group, will be able to modify each others files, unless explicitly specified.

In order to change the ownership of a directory or file, the *chown* command should be used. The syntax for this command is: *sudo chown user:group fileName* or in case of a directory: *sudo chown -R user:group directoryName*. The "-R" tag is to specify that the command should be done recursively. In other words, the "-R" tag will change the ownership of every file, in every sub-directory within the directory specified. Without the tag, only the directory listed will change in ownership, while all of the files contained within will stay unchanged.

ZoneMinder Installation

Probably the most difficult process of setting up the software for the camera system was involved with ZoneMinder. The software does not support SMB shares despite what the documentation states, so simply attempting to store camera video in a shared folder from a NAS is impossible. In order to provide ZoneMinder with storage for camera video ("events"), an iSCSI device had to be created in order to prevent any incompatibility issues.

The installation instructions are found here:
https://zoneminder.readthedocs.io/en/stable/installationguide/ubuntu.html

It is also important to note that at the time of this writing, ZoneMinder does not support Ubuntu 18.04 officially, but it was found that the sources for Ubuntu 17.04 worked without an issue. When installing the PPA, it is important to select the PPA for Ubuntu 17.04, if the 18.04 PPA hasn't been created yet, or simply isn't supported. Most likely, a new PPA hasn't been created yet, simply due to the fact that 18.04 has been just released. The difference between 17.04 and 18.04 is merely an updated GUI, and a newer Linux kernel version. The camera server is currently running the 17.04 PPA without any issues, although it is recommended to use the correct PPA when it becomes available.

The guide for setting up an iSCSI share on FreeNAS can be found here:
http://thesolving.com/storage/how-to-create-an-iscsi-target-with-freenas/

In the guide above, it shows how to connect to the iSCSI from a Windows machine. It is important to follow instructions for Ubuntu Linux, on how to install the correct drivers, and format the drive for use.

RAID 1

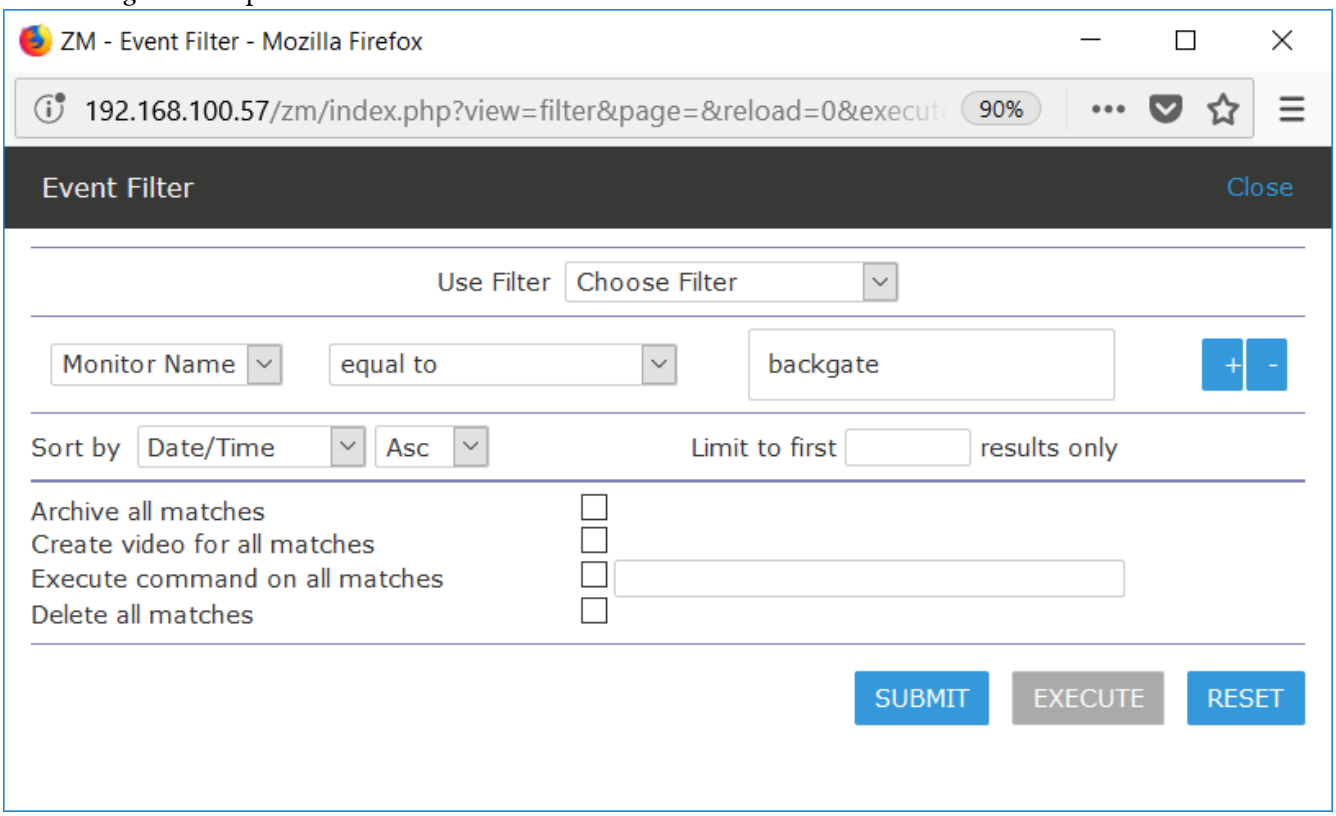
The camera server utilizes a RAID 1 setup with SSD's, this is to ensure some kind of system data security in the event that one of the drives fail. It is important to realize that this RAID setup is not configured in the BIOS, but setup entirely in Linux at the software level. RAID support in Ubuntu 18.04 appears to be limited, although it still exists. In order to properly setup RAID before installing Ubuntu, it is important to boot the system in live desktop, and format the drives before starting the install. Some documentation and instructions can be found at:
https://help.ubuntu.com/lts/serverguide/advanced-installation.html
Be sure to verify that the drives are *NOT* setup in RAID mode, as Ubuntu only supports software-based RAID, and not hardware.

SSH Remote Access

The camera system may be accessed using SSH remotely, or if a computer monitor is not installed on the machine. This is the preferred method for accessing and managing the server, as it keeps CPU usage to a minimum to prevent any lost or skipped frames in the recording from cameras. Using SSH to access the camera server on Linux is quite easy, although on Windows, it may require a few extra steps, such as installing Putty. Putty is a small program for Windows which will allow for a connection to the Linux server through SSH. Please remember that all SSH connections, unless explicitly defined on the server will require knowledge of the BASH (Born Again SHell) set of commands. Both freeNAS, and Ubuntu Linux are setup for BASH.

Find A Recording

One of the most important tasks for a camera system is the ability to record, then the ability to view those recordings. ZoneMinder can be a bit confusing at first when attempting to look up and see what was recorded on each camera. The system utilizes "filters" to manage much of it's data management tasks. A better term than "filters" would most likely be, tasks. In order to view past recordings, click on Filters, and set it up as the image below specifies.



In this filter, it will locate all "events" matching the monitor name *backgate,* since the beginning of time. Currently, the NAS will store 9 days worth of recordings, although in a system which records longer, it may be necessary to also filter for date/time by clicking the plus symbol on the upper right hand side. After one clicks submit on the filter, a list of *events* will display, and by clicking on the event id, the recording will begin to play.

Backup Recording

As stated earlier, the next most important feature of a camera system is the ability to backup, or extract recordings from the system. There are currently a few methods to extract a recording from the server, although the most common method is to utilize a filter to find all recordings from a single camera/monitor, then generate a video file, and finally download the file.

If a large recording is not downloading after making an mpeg conversion, it is probably because the file size is too large. The default php maximum download size is only 128MB, this has now been changed to 2048MB. In order to change this setting once again, an administrator will need to SSH into the Ubuntu server while utilizing PUTTY, and modify a php config file. This file is located at:
/etc/php/7.2/apache2/php.ini
The config file will need to be modified by utilizing vim with administrator privileges. The line to modify is:
memory_limit = 2048M
Once this has been configured, the system will now be able to convert, and allow the download of a recording up to 2GB in size. The maximum recording size should be around 1GB during nightclub, so this should provide plenty of head-room for the future.

There may still be some instances where the video recording won't initiate a download. In these situations where a video has been created, and the video won't download, the user can click on “export” above the recording preview, and check the box to export all video. Select Zip as the file type, and click download when ready. If all else fails, the video file can still be pulled by browsing through the ZoneMinder directories on the NAS. It is best to have someone experienced with Linux based systems to browse through the directories on the NAS.

Restart Zoneminder

There may be a few instances where it is better to restart ZoneMinder it's self, rather than the entire server as a whole. A case for this, may be that there are other services running on the server, while ZoneMinder it's self is having issues with recording. The way to go about this is to restart the service individually by utilizing a linux shell:

sudo service zoneminder restart

This service restart command is not completely unique. The service command is an internal script/program in Linux for managing all kinds of other services. To learn more about Linux services, the man page can easily be viewed by typing in the shell:

man service

After the ZoneMinder service has restarted, it may take a moment before everything comes back online. It can easily be determined when the application has completed starting up by looking in either the "System Information" application in the GUI, or *htop* in the shell. To view *htop* in the shell, just type ***htop***, and hit enter. When the system is ready, the CPU usage on each core will be around 40 to 60% and remain steady. Another way to ensure that the system is ready, is to simply give it two to three minutes, and that should be plenty of time for the system to become ready.

Setup Tools

Due to the nature of the Camera System being a decentralized machine made of many networked segments, there are multiple tools and concepts that must be understood and utilized, in order to properly maintain the system. There is one networked segment which was not mentioned earlier, and that is the Cameras themselves. It may seem illogical to make the cameras as their own segment in the entirety of the Camera System, although, each camera is a server in it's self, which requires firmware and holds settings which can only be configured by accessing each camera directly. There are a few main tools for configuring the cameras individually:

Amcrest IP Config: lists all Amcrest IP cameras locaed on the .8 VLAN network. This is the most useful configuration tool for rapidly changing all of the basic settings for each camera.

Amcrest Web View Chrome Plugin: allows for fine tuning of each camera, and setting profiles for Day/Night recording. The Amcrest Web View is the only tool which can accurately set the date/time stamp, removing the Amcrest logo, and modifying the video output label in the lower left hand corner. Because these stamps are already handled on it's own by the ZoneMinder service, the most important functionality for future reference is the Day/Night profiles.

Hard Reset Cameras

There are some situations where a camera may need to be reset that is no longer accessible to the online configuration tools. A reset of a camera which requires accessing the hardware it's self, rather than utilizing software, is called a "Hard Reset." One of the issues with the Amcrest IP2M-852EW cameras is that, due to their IP67 weatherproofing standard, there is no accessible reset button from the outside. This is to ensure that no water or moisture can leak into the camera housing, even in the event of a water blast. The reset involves a physical disassembly of the camera housing.

In order to disassemble the camera housing, the black front cover face must be removed by placing a credit card, or any other thin non metallic wedge in order to *slowly* peel off the glued cover. Once the face is removed, four screw holes will be exposed. Ensure that an over-sized screw driver is utilized for these screws, as they are constructed with soft aluminum pot-metal, and can strip very easily with the incorrect screw driver. A known screwdriver that seems to work best can be found at Harbor Freight in the size: *PH1x3"* as it seems to grip the screws very securely. This could possibly be due to design, rather than defect, as the camera housing is composed of an aircraft grade aluminum, a soft metal screw will most likely strip it's Philips head, before the threading.

After the screws are removed, the housing comes apart in two halves, be sure to separate the two halves slowly, as the IR LED power connector is still attached to the main board. The reset button will be located next to this power connector. According to the instructions provided by Amcrest, press and hold the reset button for 45 seconds.

After the hard reset, assemble the camera while being careful not to over-tighten the screws, and pay attention to the two alignment notches in the housing. Simply tighten the screws until they seem to be tight. The camera utilizes a silicone gasket which doesn't require much pressure in order to create a seal. As long as the housing doesn't flex, and the two halves appear to be flush with each other, the screws are probably tight enough.

NTP Time

The PfSense router maintains an activated feature that can sync multiple devices to one single time server. The cameras and viewing stations are to be synced to this NTP time service, and is typically the same ip as the systems gateway address. This ensures that all systems are synced to the same time. Without this synchronization, ZoneMinder will throw some seemingly random errors which all eventually point to issues with https, or other encrypted certificate based communications. The server and client cannot create a stable encrypted session with each other, unless their clocks are properly synced.

This also appears to be an issue with the cameras as well. If all of the cameras are not properly synchronized to ZoneMinder, this may cause buffer overrun issues. This is being investigated further as of 10/11/2018, however, it is at least important to synchronize the cameras, simply for an accurate timestamp.

Simple QA

Q. Why are all the recordings in black and white?
A. The image is most likely in black and white in order to save data storage space on the NAS, although, ***in some instances the camera it's self may be in night vision,*** in which case, the cameras output will only be available in black and white. The camera will not record in color during night vision mode, as it is utilizing IR LED's to produce light which the camera will be sensitive to. The camera it's self has an IR shield during daylight color mode, but when in night vision mode, that IR shield is removed, and colors will no longer be accurate anyways, if the camera was somehow forced into color vision mode.

Q. Why is the video so choppy in Montage Mode?
A. The video in montage mode will be choppy, and there doesn't appear to be a method to change this as of yet. The thing is, ZoneMinder was created to be able to run on some pretty dated hardware, and still perform properly. If each video tile was able to run smoothly, it would eat up quite a bit of CPU resources, and network resources. The infrastructure could most likely handle a smoother video playback in montage mode, although, this is the way ZoneMinder was created, and ***it does not mean anything is wrong with the recording, this is simply the way the creators have setup the system.***

Q. Why is the video playback choppy and at low frame-rate?
A. The playback is *not* reflecting what is actually stored on disk. The video output viewed may be choppy depending on system load. If there are a massive number of cameras (such as we have here), ZoneMinder will drop frames from being sent to the client in order to ensure that the video being recorded is at top quality. In order to view the recording smoothly, the recording must be converted to ***mpeg,*** viewed through VLC, or any other desktop media player.

Q. Why is the frame-rate so low in the recordings?
A. Almost all of the video being outputted from the cameras are at 10fps, this is the lowest frame-rate which can be utilized before the human eye will determine the video playback to be choppy. ***5 to10FPS is an industry standard,*** as it allows for video to play smoothly, without consuming all of the storage space on the NAS. In standard 1080p, video is typically recorded at 30fps, if all the cameras were to record at that speed, Baily's would have to triple it's storage space on the NAS.

Q. Why don't I have permissions to change some of the settings?
A. All other accounts, other than root can change system level settings. Linux and ZoneMinder are very sensitive to changes to it's config. Accounts have been created to be highly limited in order to ensure that the system won't be crippled from a simple mistake. In order to change system level settings, the password will have to be recovered from Baily's password repository system, which is covered in another document. ***It is highly unlikely that any system settings will need to be changed, and it should only be changed by someone who truly understands how Linux works with symlinks!***