Terafence CCTV Cyber Security Solution White Paper

A Technical Report from Terafence Research Lab

Contents

Technology Introduction to CCTV Surveillance System

The precursors of modern video surveillance were Closed-Circuit Television (CCTV) systems, used analog signals over coax cables to communicate in a closed infrastructure. No networking features existed, and the entire system was closed to any external electronic access, hence – Closed Circuit TV. As technology advanced, digital cameras supporting TCP/IP communication came into existence and got integrated into the organization LAN infrastructure. Nowadays, video surveillance with IP cameras is used not only in large corporations and highly secure locations, but also in most public buildings and increasingly in private home automation systems, and for many organizations are consider “Eyes and Ears” for everything outside the Security Operation Center (SOC) by providing visual information.

Modern video surveillance systems are composed of the following main components:

- IP Cameras, which provide video monitoring of physical locations. They can be grouped into CCTV (analog) and IP (digital) cameras, which, as opposed to their analog versions, can be directly connected to an Ethernet network. In this work, our focus is on IP cameras only.
- Network Video Recorders, which store camera footage. Dedicated device that records and stores video in a digital format, called a Network Video Recorder (NVR). Some advanced IP camera models also integrate Video Management software (VMS) for local storage of recorder footage.
- Monitors, which are used to watch real-time or recorded footage. Monitors can also be analog or digital, such as a computer, smartphone or almost anything with a screen that can display video.
- Advanced Intelligence / Analytics, Devices dedicated for processing video either for forensics or for real-time processing for pre-configured events and alarms.
- Video Storage, Devices which store video information, either locally or in the cloud.

More complex systems can also contain media servers, gateways, routers, and switches. Based on the components present on an enterprise network, we can differentiate three types of surveillance systems:

- Analog systems contain devices that cannot communicate on the Ethernet network. They are much less prone to cyberattacks and are out of the scope of this report.
- Digital systems comprise IP cameras, NVRs, switches, routers, and digital monitors, which all can send and receive Ethernet network traffic. Most of these devices also support remote access, maintenance, and alerting via HTTP, FTP, SSH, SMTP, and similar protocols, and in some cases, also the old and insecure Telnet protocol. Video streaming uses RTP, RTCP, and RTSP, as explained below.
- Hybrid systems comprise of both digital and analog devices. Besides the devices mentioned above, these systems can also contain video encoders or hybrid DVRs to connect analog cameras to the IP network and video decoders to view the digital data on analog monitors.

The architecture of a hybrid video surveillance system can be quite complex, containing a variety of legacy and new technologies. Figure 2 shows an example of such a system, where the direction of the arrows indicates the direction of data flow.

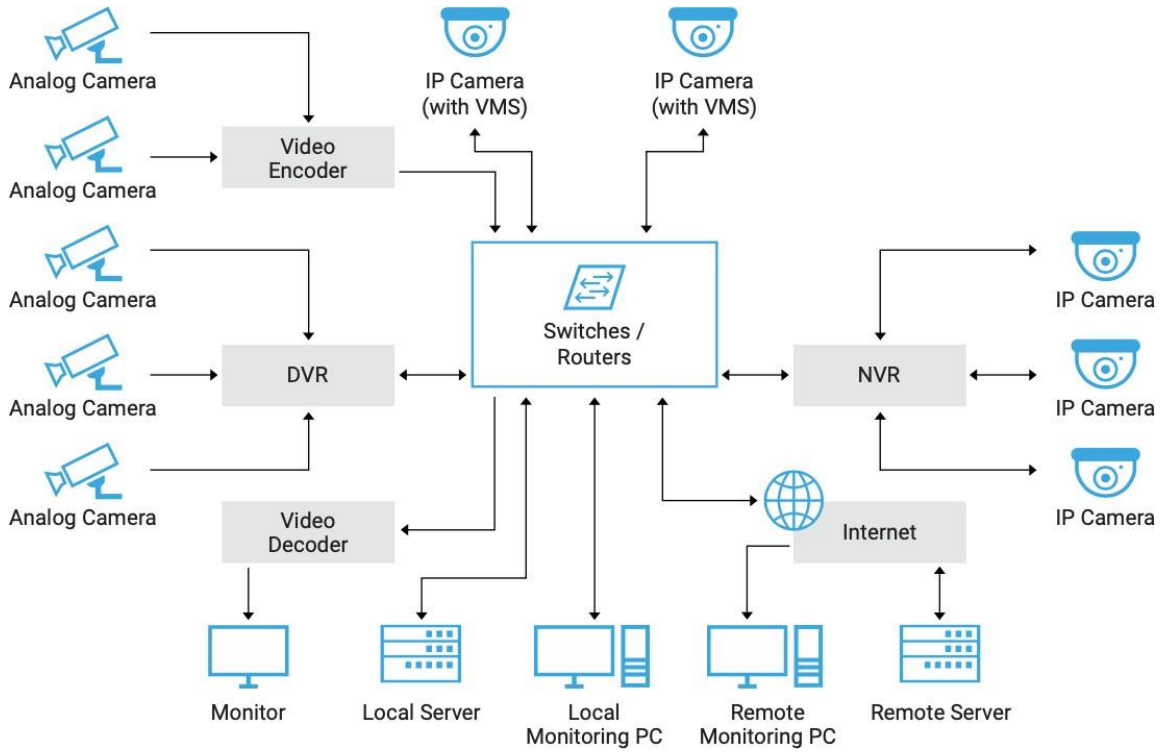


Figure 1 - Surveillance system architecture as found in a modern building

Threat Analysis

Understanding where threats may come from is crucial for establishing protection measures. A recent study by “Frost & Sullivan” suggests the following potential sources:

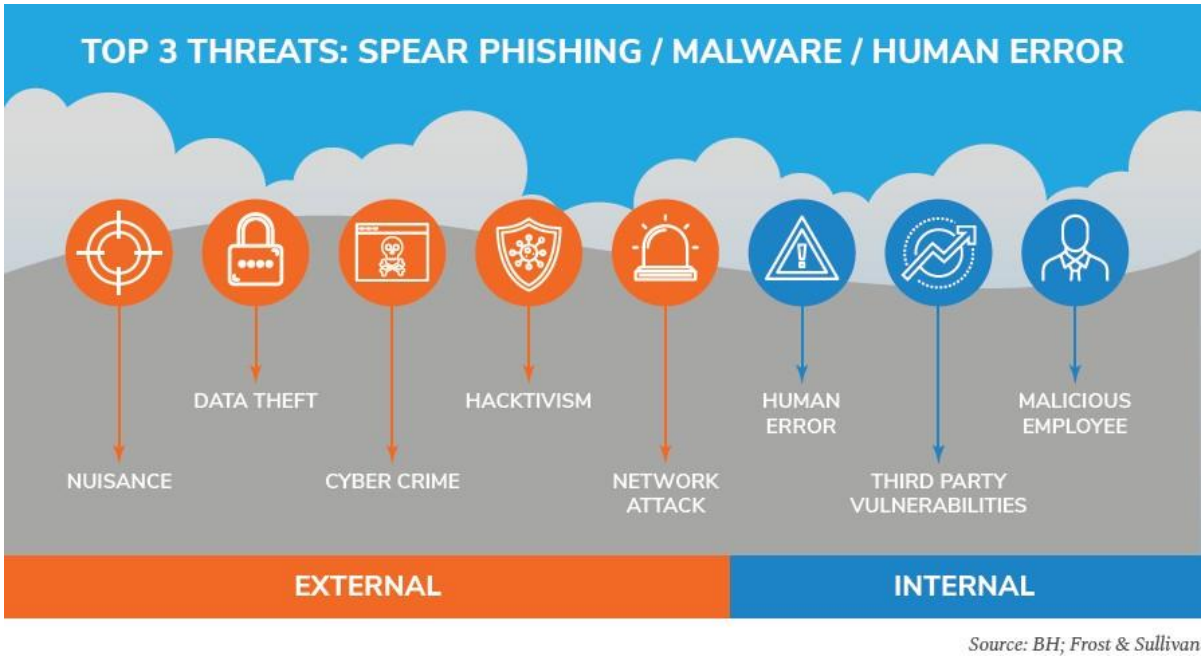


Figure 2 – Threat sources

It is commonly accepted that only 20% of attacks come from the outside (Internet) and 80% come from internal sources. One can have the state-of-the-art network IDS / IPS and FireWall(s) in place but an infected USB-Disk-on-Key inserted on a desktop / server will bypass everything and possibly infecting the entire network or worse, allowing access to hackers, viruses or worse. A laptop that was used outside the organization may have picked up malicious code on someone else’s network, on an open Wi-Fi link in a café, on the train or at the Airport.

As no single solution can provide total security, layered security solutions are often the best way to ensure maximum protection against attacks. Servers and Desktops computers may run tools as protection like FireWall, Anti-Virus and as such, Network access could use NAC to deny connectivity to unknown devices and advanced network behavior tools could monitor traffic for abnormality and attacks.

A major concern arises when attackers take control over **low-maintenance devices**, such as IP-Based CCTV cameras, and use them as an entry point into the organization network. Additionally, taking control over CCTV elements (such as NRV / AI / Forensics) may allow attackers to hide criminal activity or completely blind a SOC during emergencies or terror attacks.

Typically, CCTV systems are handled outside IT "jurisdiction" and quite often serviced by external sub-contractor while the actual infrastructure is shared with IT systems. The Security department is responsible for the CCTV and, in many cases, totally depend on sub-contractor's staff for maintenance, repair and system evolution and even allow remote network access for diagnostics and maintenance, and in worst cases, all without IT department intervention for security (TeamViewer session for example).
A visiting support engineer carrying his LAPTOP coming to update the CCTV elements software / firmware may, unintentionally, carry an undetected virus, trojan hours or ransomware into the network.

CCTV IP-Based cameras should be considered as exceptionally vulnerable for the following suggested reasons:
In many cases the CCTV default admin password is not changed (and can be found in web-sites like – https://learncctv.com/ip-camera-default- password/).
CCTV have good computing resources and are connected to power and network 24/7.

Very few CCTV contain any security tools such as FireWall / Anti-virus etc.

Most CCTV IP cameras run some version of Linux OS, favorite of hackers.

Many CCTVs are not monitored in real-time as the main view screen cannot display all, so are out of SOC's attention, making them susceptible for manipulation, alteration, and abuse.

No CCTV camera will block access to anyone running brute-force password cracking attacks.

Some IP based CCTV camera are physically placed in publicly accessible locations, allowing attacker to use their network cable to hack into the network.

Some CCTV cameras use Wi-Fi to transmit video, allowing Man-in-the- middle attacks and as such.

Few CCTV vendors already include back-door vulnerabilities into their product allowing unauthorized access.

There were incidents were CCTV camera software was modified by attackers to run Bitcoin mining while seemingly operating normally.

In other incidents CCTV cameras were converted to BOTs to be used by companies selling them as resource for cyber-attacks. These companies thrive on devices poorly protected and use them to generate revenue.

It is surprising how easy it is to find CCTV open for direct internet access.

Using websites like “shodan.io” one can find huge number of accessible CCTVs:

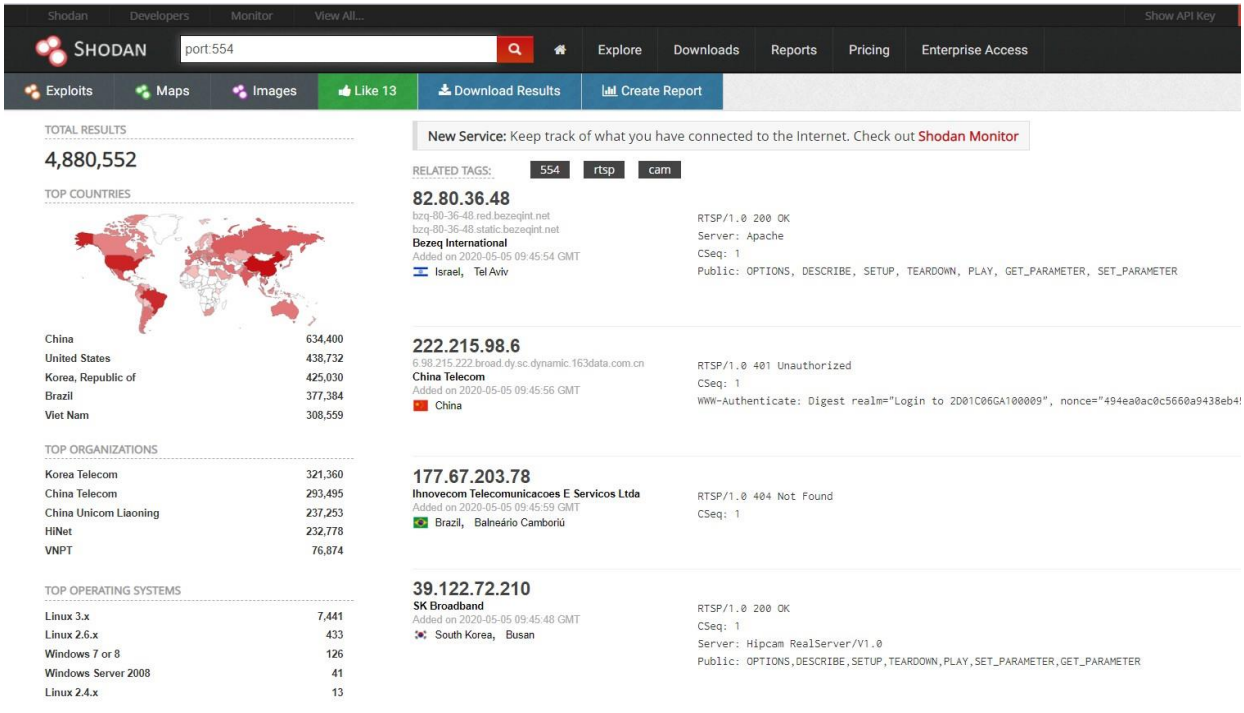


Figure 3 – Shodan.io – Search for directly accessible CCTV camera

It this only in theory?

No, it is not. It is a cold and harsh reality that hackers make use of corporate CCTV infrastructure sometimes, at will.

Here are a few real incidents as publicly published:

Source:	Description:	Link:
csoonline.com	Thousands of hacked CCTV devices used in DDoS attacks, Researchers found a botnet of over 25,000 CCTV cameras and digital video recorders	click here
esecurityplanet.com	Hackers Use 900 CCTV Cameras to Launch DDoS Attacks	click here
nakedsecurity.sophos.com	Woman hijacked CCTV cameras days before Trump inauguration	click here
www.vice.com	How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.	click here
washingtonpost.com	She installed a Ring camera in her children's room for 'peace of mind.' A hacker accessed it and harassed her 8-year-old daughter	click here
PrivSec Report 2020	5 million cyber-attacks on IP cameras blocked, research reveals	click here
ibtimes.co.uk	Hackers turning millions of smart CCTV cameras into botnets for DDoS attacks	click here
newsweek.com	Thousands of CCTV cameras hijacked by hackers to attack bank websites	click here
newindianexpress.com	Robbers use CCTV footage to plan break-ins	click here
cybersecurity-insiders.com	CCTV systems installed in Toilets of British Schools hacked!	click here

Articles were written to raise CCTV vulnerability awareness:

Source:	Description:	Link:
portnox.com	Why is It So Easy to Hack an IP Security Camera and Any IoT Device?	click here
networkmiddleeast.com	Cyber security and IP cameras: the threat is real	click here
darkreading.com	Internet-Connected CCTV Cameras Vulnerable to 'Peekaboo' Hack	click here
telegraph.co.uk	CCTV vulnerability could allow cyber criminals to hack video surveillance recordings	click here
tssbulletproof.com	Are Surveillance Cameras Vulnerable To Cyber Attacks?	click here
Security electronics and networks.com	Cyber Attacks On CCTV Systems: What Are The Risks?	click here

Just to name a few....

Terafence proposed solution

Nearly all articles suggest, among other measures, to strictly prohibit network access to the CCTV endpoints and devices, some go the distance and suggest network SEGMENTATION.

Terafence products are designed to provide CCTV IP-Based camera total Isolation and Segmentation, completely denying ICP/IP access to the CCTV camera.
By implementing SecureCAM unit between the IP camera and the network switch total access denial is achieved. SecureCAM can be installed to protect a group of CCTV cameras, isolating them from any threat, internal or external.
SecureCAM acquires CCTV video streams from the configured IP cameras and makes these streams available on its B side, facing the Network and the CCTV NVR, AI, video storage and alike. All RTSP requests are now handled by SecureCAM B side.

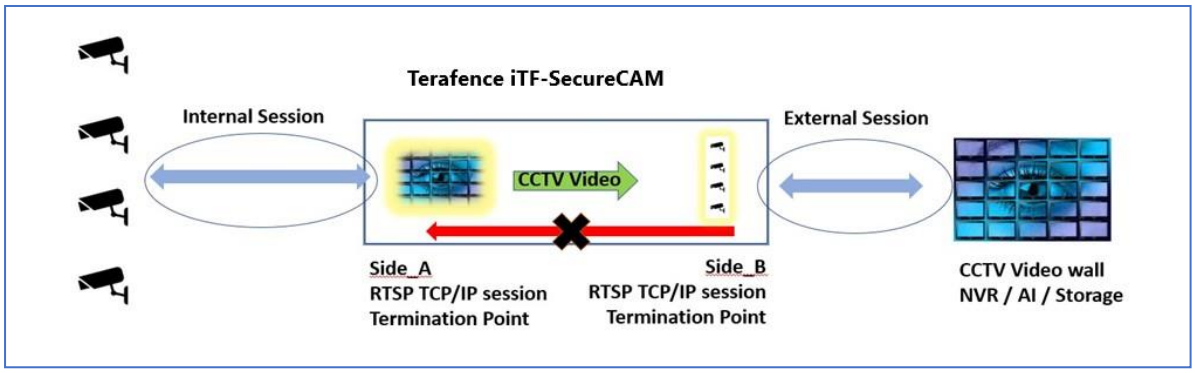


Figure 4 – SecureCAM CCTV segmentation – General Concept

Thus, total Isolation and Segmentation is achieved without compromising CCTV video performance or functionality.

SecureCAM can be configured to either allow or deny PTZ commands to selected CCTV cameras via a secure channel (out-of-band to the LAN network) maintaining PTZ functionality.

SecureCAM layout example

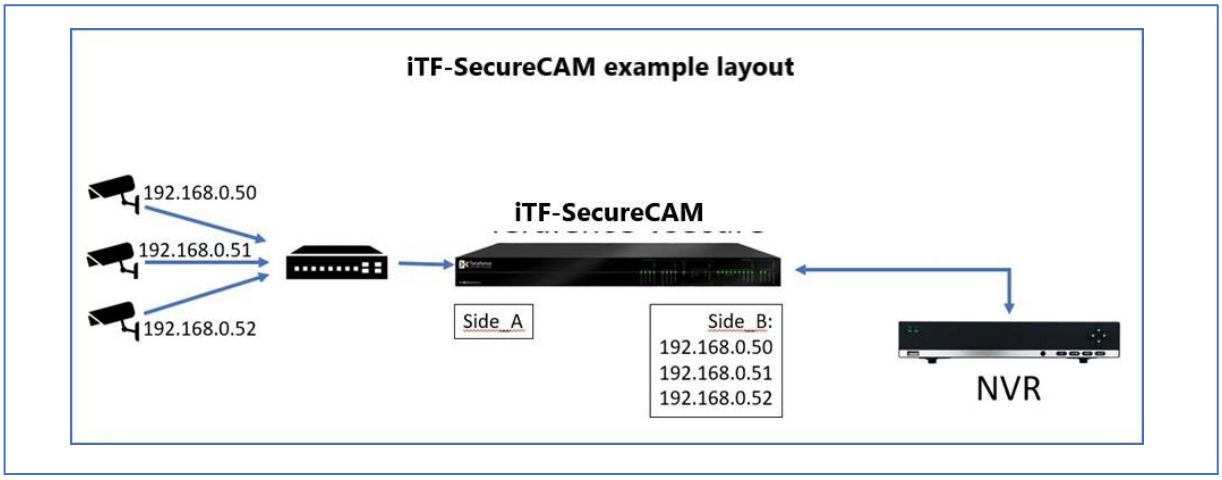


Figure 5 –SecureCAM Typical Layout for CCTV camera

SecureCAM is to be implemented in-line between the protected segment and all other enterprise assets, servers, and internet connection. SecureCAM Side-B mimics the (video over RTSP) functionality of Side-A CCTV IP cameras.

Terafence Advanced Cyber Security Features:

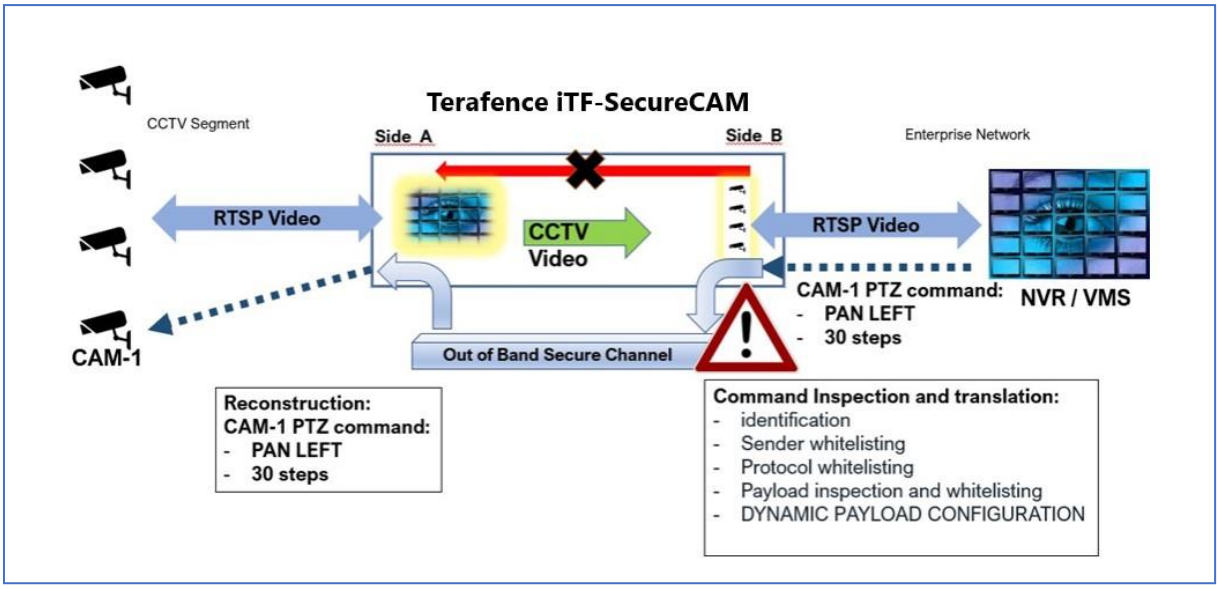
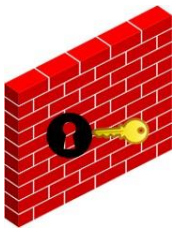


Figure 6 –SecureCAM Advanced Cyber Protection of CCTV Systems

CCTV Side:	**NVR/VMS Side:**
SecureCAM will offer protection to the Enterprise Network from the CCTV Segment as well securing the Enterprise from malware infected cameras or any attempt to gain access via the CCTV segment switches. SecureCAM will intercept IP Camera traffic and whitelist, and inspect the following: • Camera IP • Camera MAC • Protocol Restriction • FIRMWARE Ver/SIGNATURE/DATE SecureCAM can identify Camera Firmware alteration and send an alarm to operators and/or block the camera traffic to the Enterprise Network as suspected to be infected by malware. Any breach of the above inspections will generate a Cyber Alarm sent to the NRV/VMS on Side B.	SecureCAM will intercept VMS commands and will whitelist and inspect: • Identification • Sender IP / MAC • Protocol • Payload • Dynamic Payload Configuration SecureCAM will block all and any TCP/IP traffic to the CCTV protected segment BUT will intercept NVR/VMS commands (like PTZ) to the CCTV camera. The command will be whitelisted, payload inspected and compared to configured thresholds. Once cleared, the command will be internally translated and sent over an out-of-band secure channel and not via the (deactivated) LAN channels to eliminate any security risk by opening the LAN channels even momentarily. Any breach will be sent to the VMS as a Cyber Threat.

Security– FireWall including IDS/IPS vs. Terafence Technology

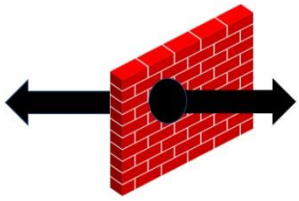
“I can do this with a FireWall… Can I?"



Yes, you can configure a FireWall to allow unidirectional data flow… but,
Your CCTV system will no longer work.

A firewall is a mainly system that provides network security by filtering incoming and outgoing network traffic based on a set of user-defined rules / keys.

In general, the purpose of a firewall is to reduce or eliminate the occurrence of unwanted network communications while allowing all legitimate (with the correct key) communication to flow freely.



A FireWall will, eventually, will grant access to an entity that fits the FireWall rule (key) configuration, the problem is that once access is granted, that entity gains full access to the end-device and the FireWall is no longer in effect (unless it’s a Layer_7 firewall). In other words, the FireWall will grant a live session between the end-device and the someone.

This is exactly what a hacker needs to gain access and manipulate the end-device.

Still, preventing all inbound traffic will make the FireWall “a unidirectional” device but this will prevent the protocol continuity and functionality between the CCTV device and the NVR/VMS. These two need to communicate to properly work, the NVR/VMS sends RTSP request command to obtain video stream, the IP Camera will transmit the video in respond. Without a mediator, this will not work, and no FireWall will mediate such protocols as they are not designed to do so.

With Terafence, no entity will gain full access to the end-device. Terafence will take an active (Internal Session) role as a mediator between the CCTV and NVR/VMS, unlike any FireWall.

In special applications, Terafence may allow a heavily filtered commands (only) to be accepted, filtered, disassembled, and coded and then forwarded to the end-device via a secure, out-of-band channel. The actual TCP/IP session will terminate on the Terafence side next to the sending device (External Session).

At no time live sessions will become available, thus manipulation avoided.

SecureCAM Technical Information

Hardware Specifications:

19” half-size rack-mount

Power supply: 1x12VDC, 8AMP

2xRJ-45 Gigabit Ethernet CAT-7 ports

Front Panel indication LEDs

20, 50 and 100 Video Channels support (according to the model)

Total bandwidth – 1Gbps

Video Stream forwarding up to 25/30 fps

Features supported:

Out-of-Band Secure channel for NVR/VMS commands.

Advanced filtering and payload inspection of NVR/VMS commands

Complete TCP/IP sessions denial end to end

RTSP over TCP/IP

Video compression – H.264 / H.265

Unit Management:

WEB based GUI for unit setup (on A side)

WEB based operational monitoring and statistics (on B side)

Clustered configuration control and management

High availability – Full unit redundancy *

Contact Information:

info@terafence.in