USING THE FESTO IoT GATEWAY IN ENTERPRISE NETWORKS

FESTO

Author:
Thomas Ruschival

Abstract - The purpose of the Festo IoT Gateway device is to allow for a communication between the factory floor and the cloud. Traditionally production networks are completely separated from the Internet. This application note describes a solution using Debian GNU/Linux in a virtual machine to connect the IoT Gateway to the Festo Cloud while complying with state of the art security recommendations. We propose micro-segmentation using tagged VLAN to separate the IoT Gateway 'Cloud' port from the enterprise network. In this document we show how to set up a separate network with firewall rules to control all communication to and from the IoT Gateway. This application note is intended to provide a low cost approach for small companies but the concepts also apply to more complex enterprise networks with hardware firewalls.

I. INTRODUCTION

Network security is a vital part of protecting the confidentiality, availability and integrity of companies assets. Information technology (IT) security has long been a concern for IT systems in the office. Firewalls separating networks from each other are common place. User and host authentication with elaborate authorization mechanisms are widespread and provide safeguards against adversaries.

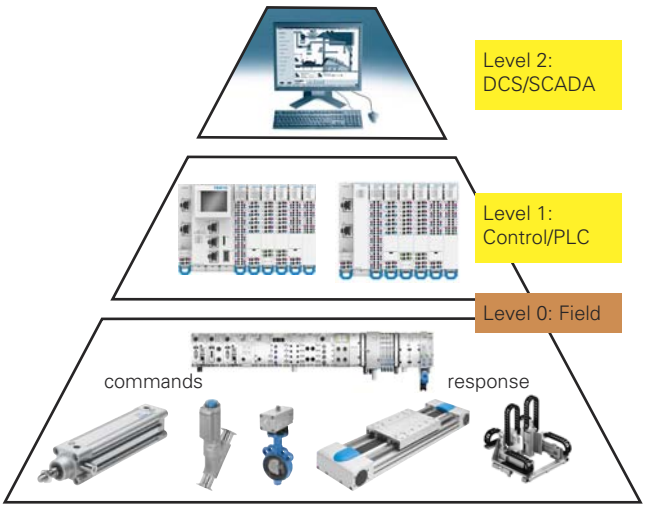

Fig. 1. Bottom part of the process control/automation pyramid

Traditionally, Industrial Control Systems were isolated systems with proprietary software and communication protocols. The communication architecture of the process control zone was strictly hierarchical in the sense that communication is always initiated from top to bottom and only occurs between adjacent layers. In this architecture lower layers respond to requests or commands from the next higher layer. **Figure 1** shows the classical process pyramid architecture.

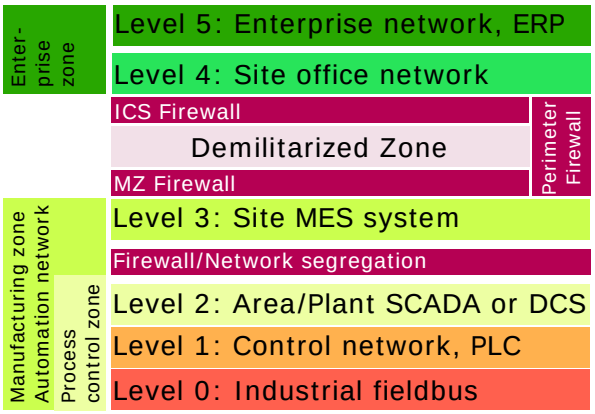

Fig. 2. Control hierarchy zones adapted from ISA99

Figure 2 formalizes this common approach and give security recommendations published in ISA99 "Industrial Automation and Control Systems Security" by the International Society of Automation (ISA) and later harmonized as international standard IEC62443 [1]. The architecture is conceptually separated into levels and zones. This is a theoretical approach, in concrete setups the layers may blur. Firewalls between the zones provide fine granular control over which hosts are allowed to communicate over which protocol with hosts in another network.

The enterprise zone comprises global enterprise resource planning (ERP) on level 5 and site local office networks on level 4. The office network includes file servers and office workstations and wireless devices. The hosts in the office network usually have outbound Internet access using common protocols like HTTP, HTTPS or others. The traffic is routed through The Internet Connection Sharing (ICS) firewall and the perimeter firewall. Proxy servers or stateful packet inspection can be used in the ICS firewall to monitor communication content or encapsulated protocols.

The companies network is separated from the internet by the 'perimeter firewall'. Only a well-known set of protocols is allowed to connect from the hosts enterprise network to the Internet. Request from the Internet on specific ports are forwarded to hosts located in the demilitarized zone (DMZ). A typical example of a host in the DMZ is the company web server that responds to HTTP(S) requests from the Internet. Additionally intrusion protection systems (IPS) can be deployed on the perimeter firewall to detect abnormal communication patterns. The manufacturing zone comprises all IT systems for plant operations on the site. A manufacturing zone firewall (MZ) may be deployed to separate access to and from the demilitarized zone.

The Manufacturing zone often maintains a separate network infrastructure with dedicated DHCP, DNS and file servers. Typical level 3 systems are manufacturing execution systems, plant historian servers, and engineering systems [2].

The systems in the process control zone control one specific manufacturing process or cell. SCADA or DCS systems are found in level 2. Level 1 contains programmable logic controllers (PLC) or application specific controllers. Level 0 comprises sensors and actuators connected to the PLCs via field buses, industrial Ethernet or directly wired.

The hosts on the manufacturing zone are critical assets for the company. Compromised participants may affect production, product quality and company trade secrets. As additional challenge the hosts in the manufacturing zone run out dated versions of operating systems and cannot be easily upgraded due to functional restrictions.

According to the strictly hierarchical approach host on the automation network usually have no Internet connection. It is not advised to grant direct access from the Internet or the enterprise zone to the manufacturing zone.

A. New challenges and architectural changes

Many existing communication architectures where planned according to **Figure 2**. However, following this architecture some use-cases are difficult to implement. For instance synchronization of the MES system with ERP systems require access from the enterprise network. Remote monitoring for service companies or manufacturers to devices introduce direct channels from field devices to Internet sites. For instance remote monitoring services of assets using GSM communication. Other companies offer remote service for equipment and systems [3]. However these accesses are conducted through a specifically designed manner. Any of these scenarios must guarantee the strict separation of production control and secondary functions like predictive maintenance. This holds in particular for safety related systems.

NAMUR, the association of process automation operators has launched the project "NAMUR Open Architecture (NOA)" [4]. The goal of the project is to develop architectures that allow a second communication channel for read-only access to information in field devices while leaving the hierarchy for control intact.

The Festo IoT Gateway is designed to accommodate these bypass channels for accessing data generated in the field.

B. The Festo IoT Gateway

The Festo IoT Gateway allows to connect to the Festo Cloud running on Microsoft Azure infrastructure. TCP ports for cloud applications cannot be easily changed since the same software is shared by all customers.

To keep the IoT gateway deployment and configuration as simple as possible the device relies on a DHCP server for network configuration. Only in rare cases manual configuration using the Festo Automation Suite is required.

As basic device security design consideration all communication is established from the IoT Gateway. The device does not respond to any incoming packets on the 'Cloud' Port, including ICMP packets such as ping.

For confidentiality and authentication device and cloud communicate over TLS 1.2 channels. During production the IoT gateway generates a unique public key certificate. The public key is distributed and the private key securely stored in the device. All IoT gateways also have public keys of the Festo Cloud application. Together these certificates grant secure authentication of both communication partners.

II. CHALLENGES

Large scale remote access facilities do not attend the requirements of small machine operators or equipment manufacturers selling applications to a large variety of customers. For one these systems require trained personnel for installation and operation and are often considered too expensive to deploy 'just' for predictive maintenance. Enterprise IT has to guarantee network security and availability. Strict and sometimes complex policies regulate installation and network access of devices. These policies do not yet cover use-cases of new device like the Festo IoT Gateway. In this application note we suggest at cost efficient solution to provide field level information in the cloud without circumvention of established security design principles in the network.

III. PROPOSED SOLUTION

A common approach to providing network security by limiting visibility and the effect of rogue or compromised devices is microsegmentation using virtual LAN. This allows for sharing a common network infrastructure yet separating the devices connected to that switch. VLANs guarantee that communication complies with broadcast and multi-cast bound-aries.

The solution is deployed using a standard Debian 9.1 GNU/Linux [5] distribution running on a Virtual Machine, or real host, with two network interfaces. The proposed VM uses layer 3 NAT network interfaces. This avoids negative effects on the exiting layer 2 network infrastructure like layer 2 loops which may occur with bridged interfaces.

The first interface connects to the office network that allows Internet access through the perimeter firewall. A second net-work interface connects to the VLAN shared with the 'Cloud' port of the IoT Gateway. We suggest that the network interface of the host connected to the VLAN is used exclusively by this VM to avoid possible interference with other VMs on the host.

Figure 3 shows the proposed network architecture. We deploy a stateful iptables firewall on Linux for fine granular control over the communication. The firewall allows outbound connections for HTTPS (port 443), AMQP (port 5671) and AMQP over TLS (port 5672).

On the VLAN no other devices are connected. This means, the VM must provide DHCP service and acts as a router for the IoT Gateway. The IoT Gateway needs to resolve the IP address of the

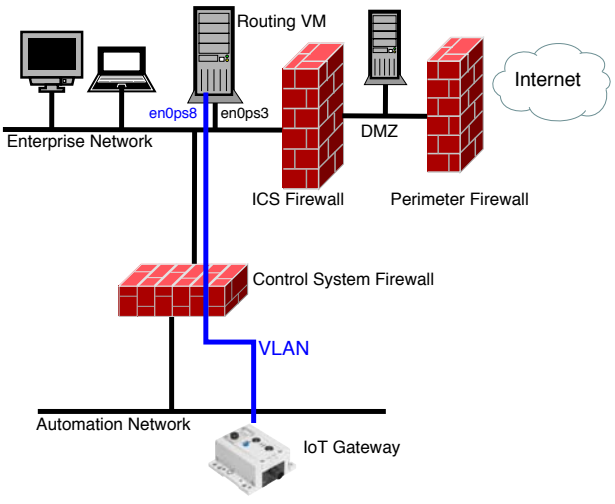

Fig. 3. Proposed Network Architecture

Festo Cloud services. In the proposed solution the VM does not run a Domain Name System (DNS) server, hence we additionally allow DNS requests (port 53) to be forwarded to the enterprise or public DNS server.

For this solution to work the perimeter firewall must allow outbound HTTPS (port 443) and AMQP over TLS connections on TCP port 5671 and 5672.

A. IP configuration

We use the Debian package net-tools to configure the network using listing 1 in /etc/network/interfaces. The interface enp0s3 is connected to the office network. It expects to receive IP configuration from the company DHCP server. The second interface enp0s8, connected to the VLAN is configured with a static IP address. For details see [6].

```
1   #/etc/network/interfaces
2
3   source /etc/network/interfaces.d/*
4
5   # The loopback network interface
6   auto lo
7   iface lo inet loopback
8
9   # The primary network interface
10  allow-hotplug enp0s3
11  iface enp0s3 inet dhcp
12  allow-hotplug enp0s8
13  iface enp0s8 inet static
14  address 192.168.133.254/24
```

Listing 1. /etc/network/interfaces

B. DHCP configuration

DHCP server is provided by the package isc-dhcp-server which uses the configuration listing 2 in /etc/default/isc-dhcp-server and listing 3 in /etc/dhcp/dhcpd.conf. To avoid interference with the company DHCP-server on the office-network we configure the server to only listen on en0ps8 i.e. the network interfaces connected to the IoT Gateway.

```
1   #/etc/default/isc-dhcp-server
2
3   INTERFACESv4="enp0s8"
4   INTERFACESv6=""
```

Listing 2. /etc/default/isc-dhcp-server

In the minimal setup in listing 3, we provide the IoT Gatway with a valid IP address, routing information and the company nameserver, here ns1.company.com. For details see [7].

```
#/etc/dhcp/dhcpd.conf

default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
subnet 192.168.133.0 netmask 255.255.255.0 {
range 192.168.133.1 192.168.133.2;
option domain-name-servers ns1.company.com ;
option domain-name "gateway.iot";
option routers 192.168.133.254;
option broadcast-address 192.168.133.255;
default-lease-time 600;
max-lease-time 7200;
}
```

Listing 3. /etc/dhcp/dhcpd.conf

C. Iptables firewall configuration

Netfilter iptables is the most common firewall tech-nology on linux and enabled in the default Debian Linux kernel configuration. Listing 4 shows an executable shellscript to setup the firewall. The rules use a white-listing approach denying all traffic that is not explicitly allowed. For details on the syntax see [8].

```
#!/bin/bash

#nterface to Festo Device
INIF="enp0s8"
# Interface to Customer
OUTIF="enp0s3"

# set chain policy of each chain to ACCEPT
iptables -P INPUT DROP
iptables -P FORWARD ACCEPT
iptables -P OUTPUT DROP

# flush all rules
iptables -F
iptables -F -t nat
# delete user-defined chains
iptables -X
# set packet counter to zero
iptables -Z

# accept established incoming connections
iptables -A INPUT -i $INIF -m conntrack \
--ctstate ESTABLISHED,RELATED -j ACCEPT
# accept outgoing DNS-traffic
iptables -A INPUT -i $INIF -p udp \
--sport 53 -j ACCEPT
# accept DHCP Requests
iptables -A INPUT -i $INIF -p udp \
--dport 67 -j ACCEPT
#
iptables -A OUTPUT -o $OUTIF -p udp \
```

```
--dport 53 -m conntrack \
--ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
# accept outgoing HTTPS traffic
iptables -A OUTPUT -o $OUTIF -p tcp \
--dport 443 -m conntrack \
--ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
# accept outgoing AMQP traffic
iptables -A OUTPUT -o $OUTIF -p tcp \
--sport 5671 -m conntrack \
--ctstate NEW,ESTABLISHED,RELATED -j ACCEPT
# accept outgoing AMQP traffic
iptables -A OUTPUT -o $OUTIF -p tcp \
--sport 5672 -m conntrack \
--ctstate NEW,ESTABLISHED,RELATED -j ACCEPT

# NAT of connections
iptables -t nat -I POSTROUTING \
-o $OUTIF -j MASQUERADE

#enable IP-forwarding in the kernel
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Listing 4. /usr/sbin/firewall.sh

D. Port based authentication

At the moment the IoT gateway does not support IEEE 802.1X port based authentication [9]. MAC Address Bypass (MAB) can be implemented to use the Festo IoT Gateway in a IEEE 802.1X enabled network. This has been successfully tested in the Festo IT.

IV. CONCLUSION

Publishing information from manufacturing devices to the Internet is a sensitive undertaking and requires thorough planning. This application note shows how to connect the Festo IoT Gateway to the Internet while maintaining the network architecture for all other network hosts. The current proposed setup shows only one easy low cost implementation while maintaining a high standard for the security of the customer enterprise network. The IoT gateway will also work with other enterprise grade firewall vendors like Cisco, Fortinet, or SonicWall. The IoT Gateway has been integrated and tested at Festo in a Cisco CPwE [10] certified network.

FESTO

REFERENCES

[1] IEC, "Industrial automation and control systems security," International Electrotechnical Commission, Geneva, CH, Standard 62443-1, 2009.
[2] "Secure architecture for industrial control systems," SANS, 2015.[Online]. Available: https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327
[3] "Siemens - SIMATIC Remote Services," https://support.industry. siemens.com/cs/sc/2281/simatic-remote-services, accessed: 2018-01-11.
[4] C. K. und Thomas Tauchnitz und Ulrich Epple und Lars Nothdurft und Christian Diedrich und Tizian Schroder und Daniel Grossmann und Suprateek Banerjee und Michael Krau und Chris Iatrou und Leon Urbas, "Namur open architecture," atp edition, vol. 59, no. 01-02, pp. 20–37, 2017. [Online]. Available: http://ojs.di-verlag.de/index.php/atp edition/article/view/620
[5] "Osboxes - debian 9.1 virtual box images," https://www.osboxes.org/debian/, accessed: 2018-01-22.
[6] "Debian - /etc/network/interfaces, man (5) interfaces," https://manpages.debian.org/jessie/ifupdown/interfaces.5.en.html, accessed: 2018-01-19.
[7] "Isc - dhcp server configuration, man (5) dhcpd.conf," https: //linux.die.net/man/5/dhcpd.conf.
[8] "netfilter iptables /etc/network/interfaces, man (8) iptables," https://linux.die.net/man/8/iptables, accessed: 2018-01-19.
[9] "Ieee standard for local and metropolitan area networks–port-based network access control," IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004), pp. 1–205, Feb 2010.
[10] "Cisco - cpwe converged plantwide ethernet (cpwe) design and implementation," accessed: 2018-01-29. [Online]. Avail-able: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE DIG/CPwE chapter1.html