TECNOLOGI@ do mês

WAGO

TECNOLOGI@ do mês - SEGURANÇA CIBERNÉTICA

Horário	Assuntos
16:00h	E-Safer – Segurança no setor Industrial
17:00h	WAGO – Segurança cibernética
18:00h	Happy hour

SEGURANÇA CIBERNÉTICA

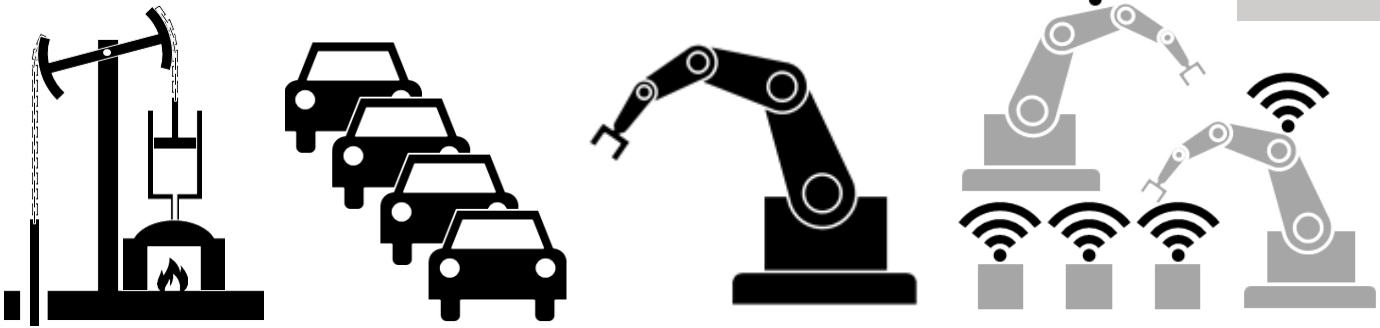
Evolução, Ameaças , Normas, PFCs

WAGO

EVOLUÇÃO DAS INDÚSTRIAS E REDES

Saímos de sistemas isolados e estamos indo para sistemas totalmente conectados

O número de dispositivos conectados na Internet no setor de automação industrial irá aumentar em mais de 50% de 2012 a 2025



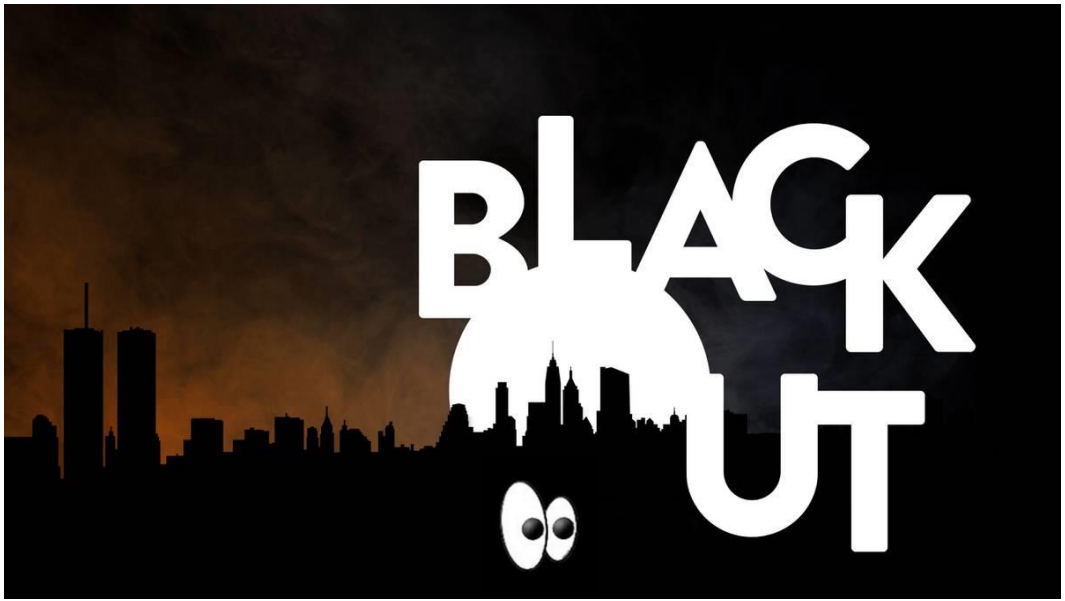
Indústria 1.0 **Indústria 2.0** **Indústria 3.0** **Indústria 4.0**

ATAQUE NA UCRÂNIA 2015

Apagão geral.

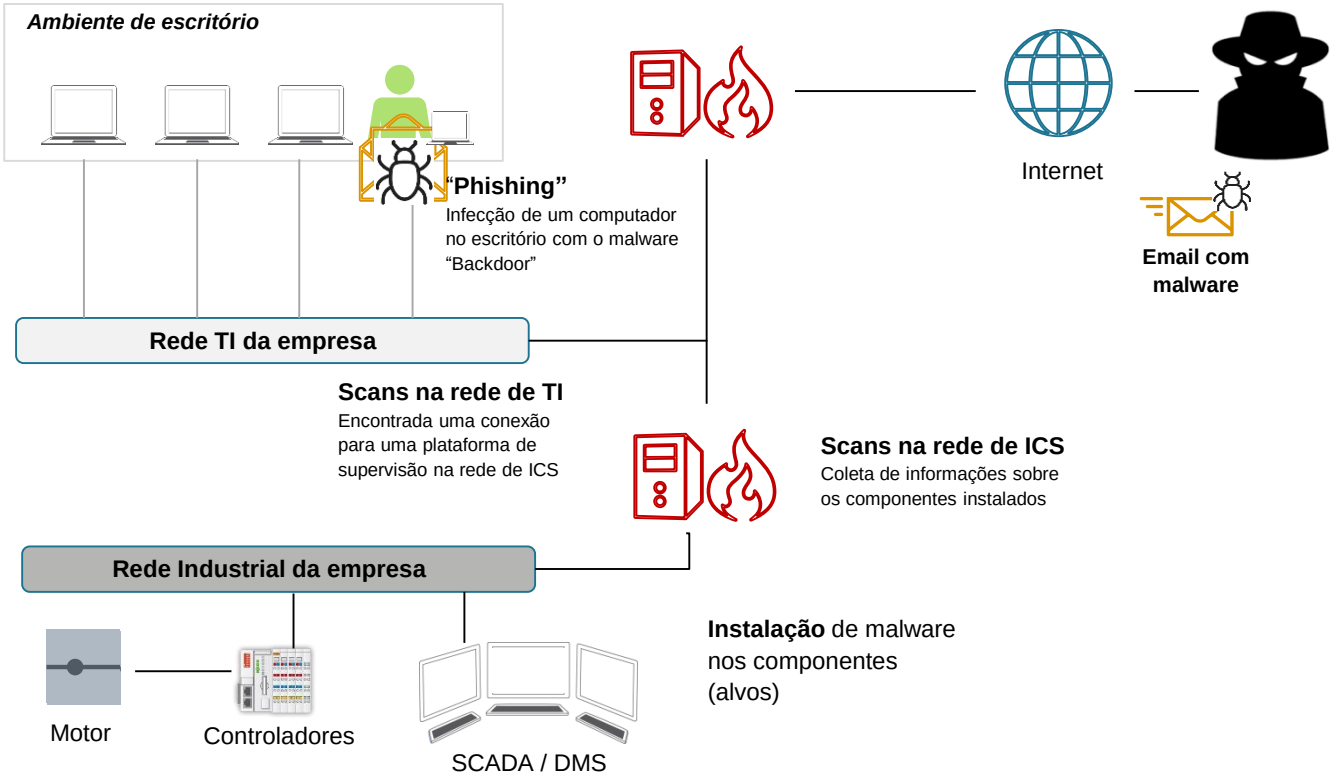
230.000
consumidores ficaram sem energia por um período de 1 a 6 horas

30
Subestações foram desligadas



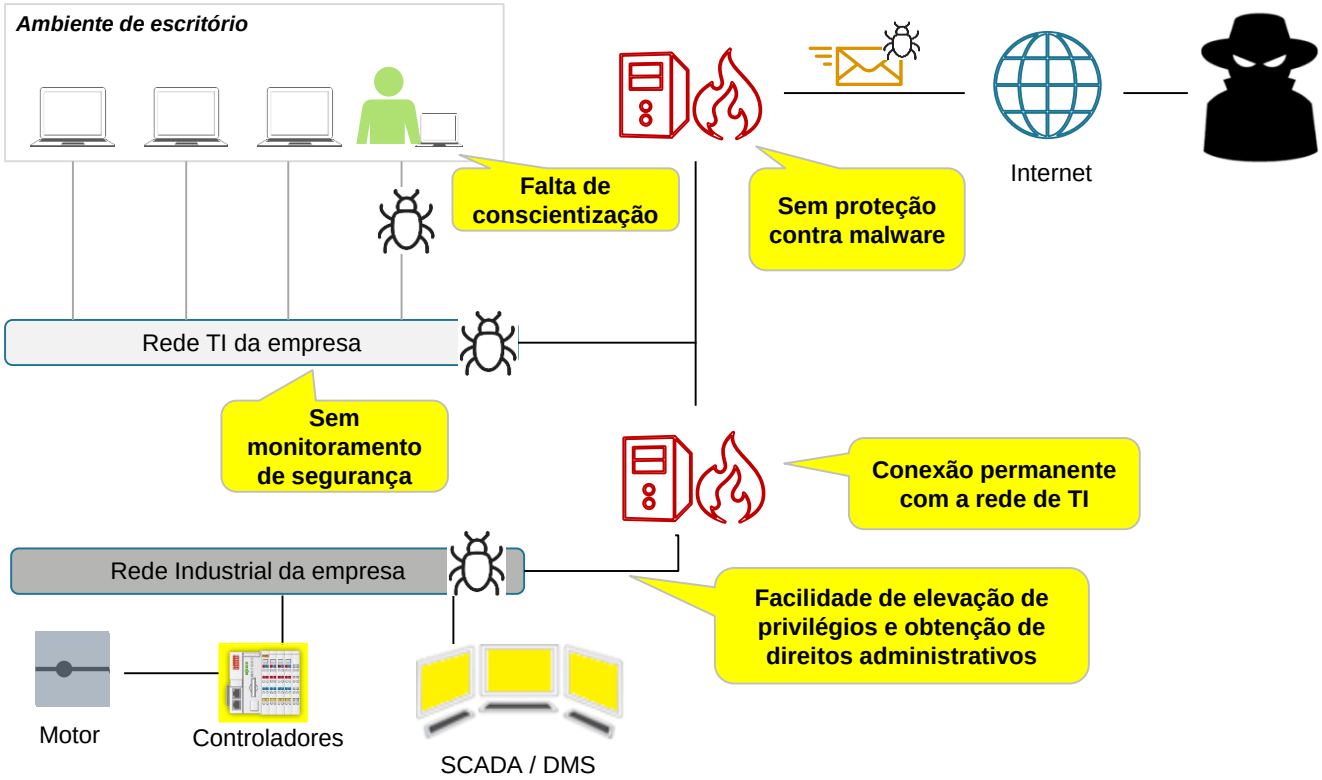
PASSO A PASSO DO ATAQUE

ICS – Industry control system possui várias vulnerabilidades



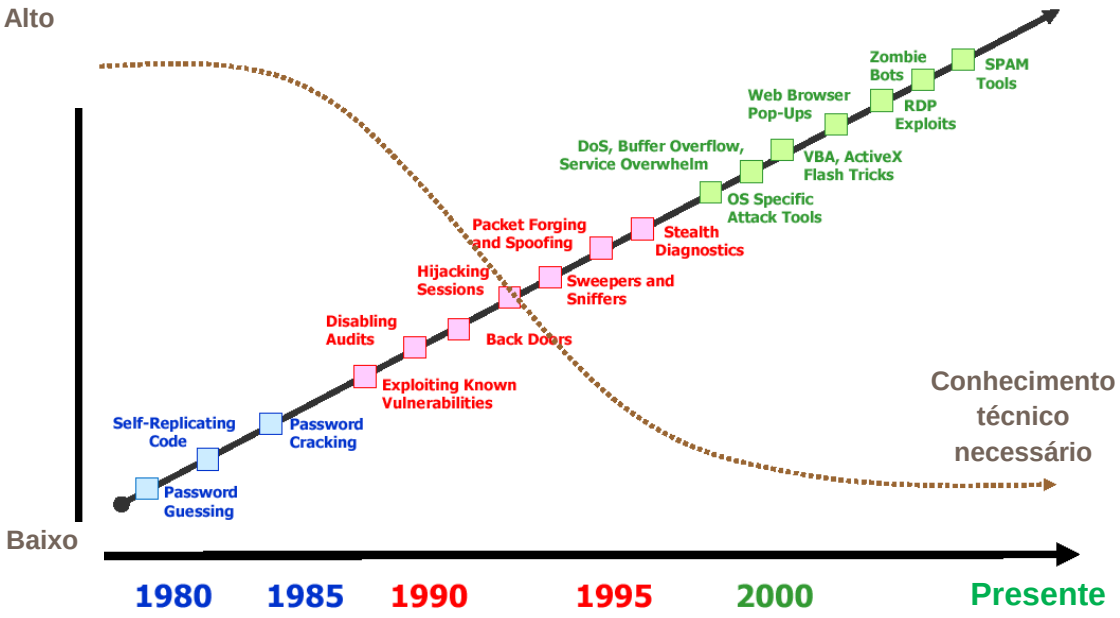
PRINCIPAIS VULNERABILIDADES

ICS – Industry control system possui várias vulnerabilidades



SOFISTICAÇÃO DAS FERRAMENTAS HARCKER

Conhecimento técnico necessário cada vez menor



Com **toolkits** baixados da internet o hacker precisa de muito pouco conhecimento técnico para lançar um ataque!

Exemplos:

SHODAN
Computer Search Engine

metasploit

KALI LINUX

BOAS PRÁTICAS, NORMAS E REGULATÓRIOS

IEC 62443 ou ISA 99

NIST

ISA™

Bundesamt
für Sicherheit in der
Informationstechnik

bdew
Energie. Wasser. Leben.

Information Security Management System
ISO 27001
Certified

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

TECNOLOGIA DA INFORMAÇÃO E AUTOMAÇÃO

Diferentes objetivos e prioridades de segurança

TECNOLOGIA DA INFORMAÇÃO E AUTOMAÇÃO

Diferentes objetivos e prioridades de segurança

TI : Proteger informações críticas do negócio

TA: Proteger recursos críticos à segurança e a produtividade

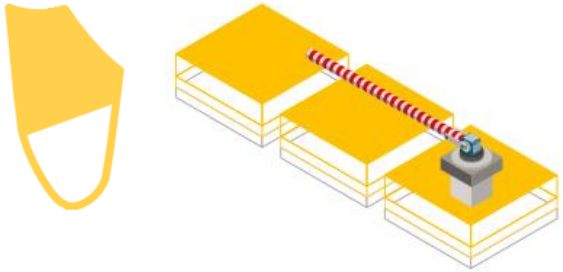
Segurança de TI
Confidencialidade
Integridade
Disponibilidade

Segurança de TA
Disponibilidade
Integridade
Confidencialidade

DEFENSE IN DEPTH – DEFESA EM PROFUNDIDADE

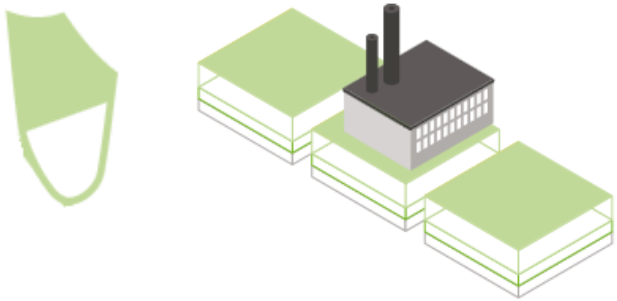
Nada é 100 % seguro – Precisamos mitigar as vulnerabilidades

DEFENSE IN DEPTH – DEFESA EM PROFUNDIDADE



ORGANIZAÇÃO IT

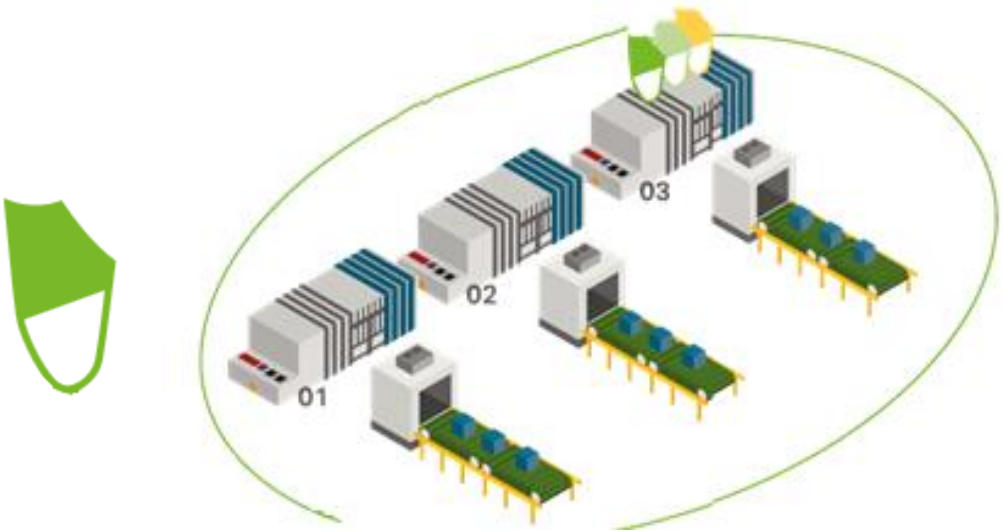
- Catraca ou similar * Firewall
- Controle de Identificação * Router
- Paredes , cercas



ORGANIZAÇÃO IT

- Controle de acesso * Segmentação Física de redes / VLAN
- Proibido entrada USB * Switches/ Router / Firewall
- Politicas de Senhas * WLAN, WPA encryption

DEFENSE IN DEPTH – DEFESA EM PROFUNDIDADE



ORGANIZAÇÃO

* Acessos baseados em função

  Acesso pessoal à máquina

IT

Segmentação usando VLAN

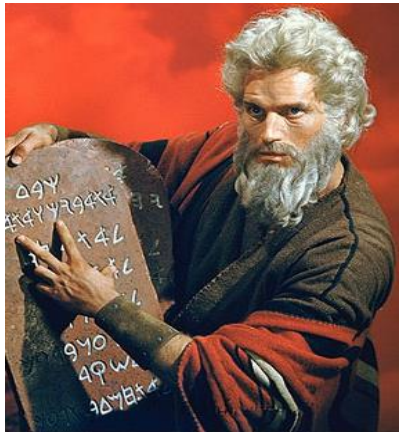
Switches/ Router / Firewall

Radius Server (Serviço de autenticação de usuários)

Controlador Firewall , VPN incorporado

OS DEZ MANDAMENTOS

Mandamentos	
1. Seja único	Somente use acesso individual (password, login), proibido o uso de senhas padrões
2. Crie zonas de riscos e isole!	Crie segmentação na rede de dados para minimizar o range de acesso remoto
3. Esteja fechado!	Permita sair somente conexões criptografadas como VPN
4. Não deixei estranhos entrar!	Use firewalls e filtros
5. Não deixe que alguem te tire da casinha !	Não click em web link (como e-mails)
6. Pergunte qual é a senha!	Permita que a conexão seja estabelicida somente sob autenticação.
7. Controle as entradas!	Configure acesso para prestadores de serviço.
8. Deixe um quarto de lama !	Estabeleça uma zona desmilitarizada (DMZ)
9. Dê uma olhada periodicamente nas crianças!	Monitore os seus equipamentos constantemente.
10. Limpe as mãos!	Mantenha os equipamentos de campo sempre atualizados (firmware)



CONTROLADORES PFC

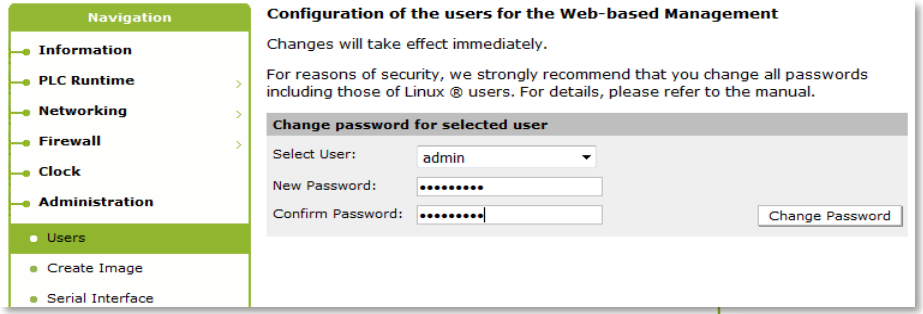
ALTO PROCESSAMENTO – RÁPIDO – INTELIGENTE – SEGURO

IoT READY

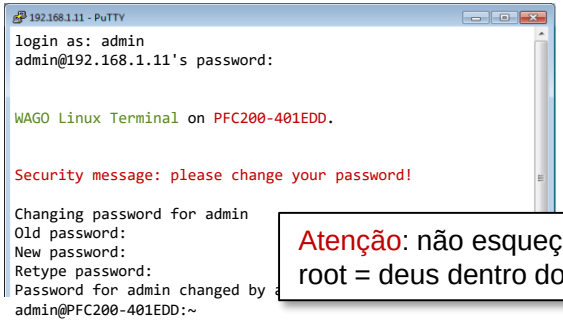
1. SEJA ÚNICO

Mude todos as senhas padrões
Use senhas diferentes e fortes.

1) Na WBM: Administration -> Users

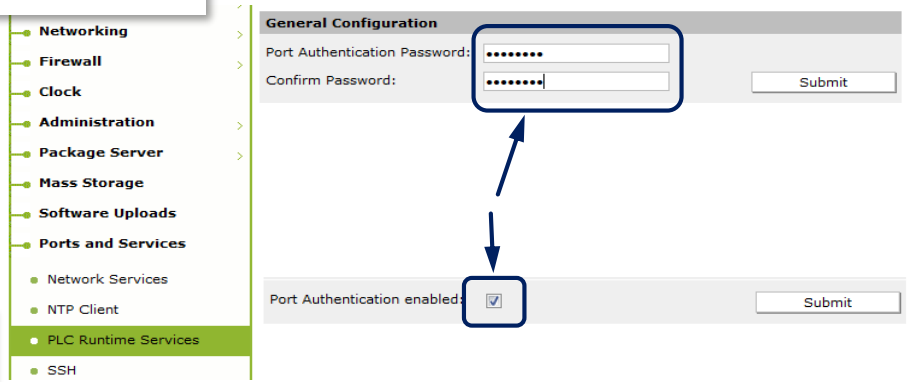


2) Com o console login (mude usuário admin e root)



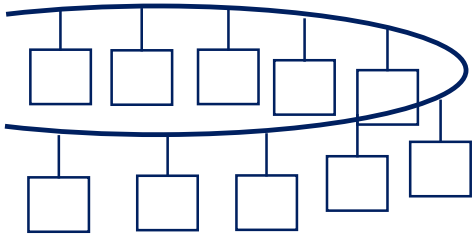
Atenção: não esqueça a conta root
root = deus dentro do WAGO!!

3) Para fazer downloading ao projeto plc

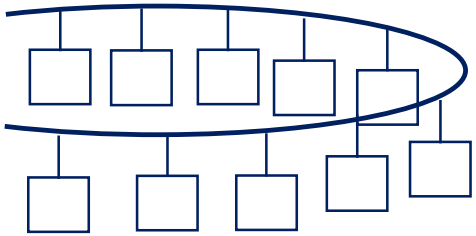


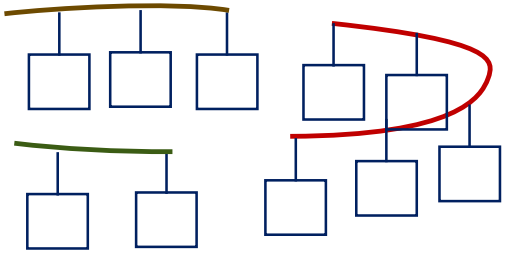
2. CRIE ZONAS DE RISCO E ISOLE

Use redes separadas entre TI e componentes de automação



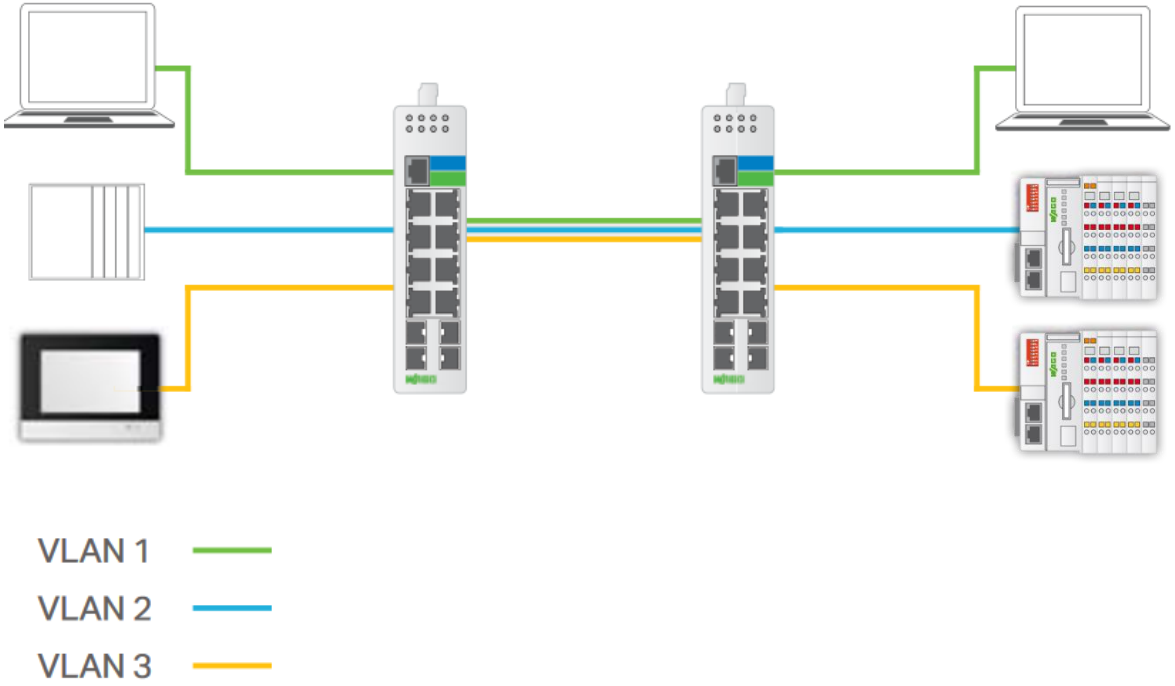
Crie segmentação de dados da rede para minimizar o range para acesso remoto





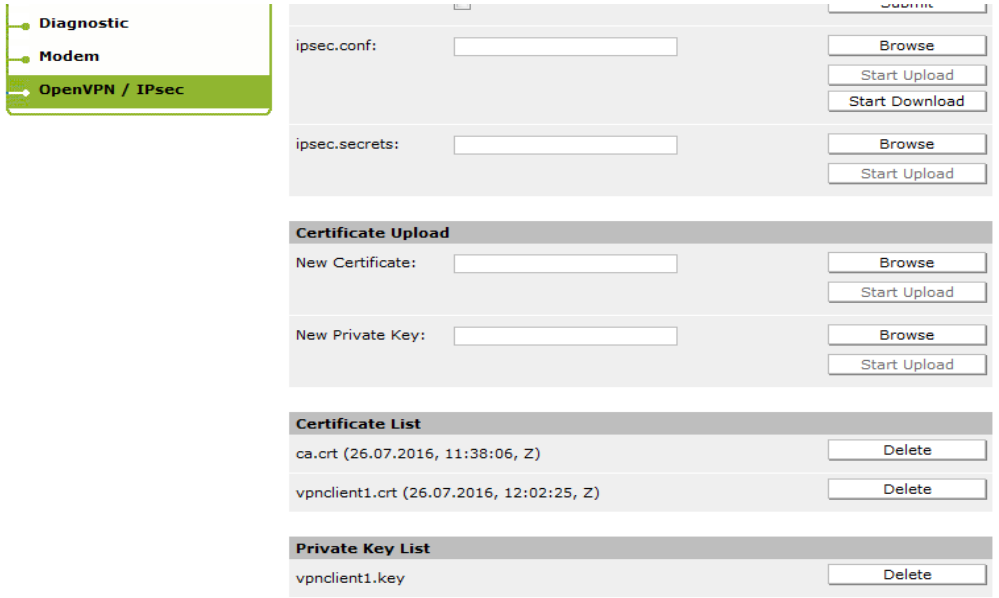
2. CRIE ZONAS DE RISCO E ISOLE

Use segmentações por VLANs

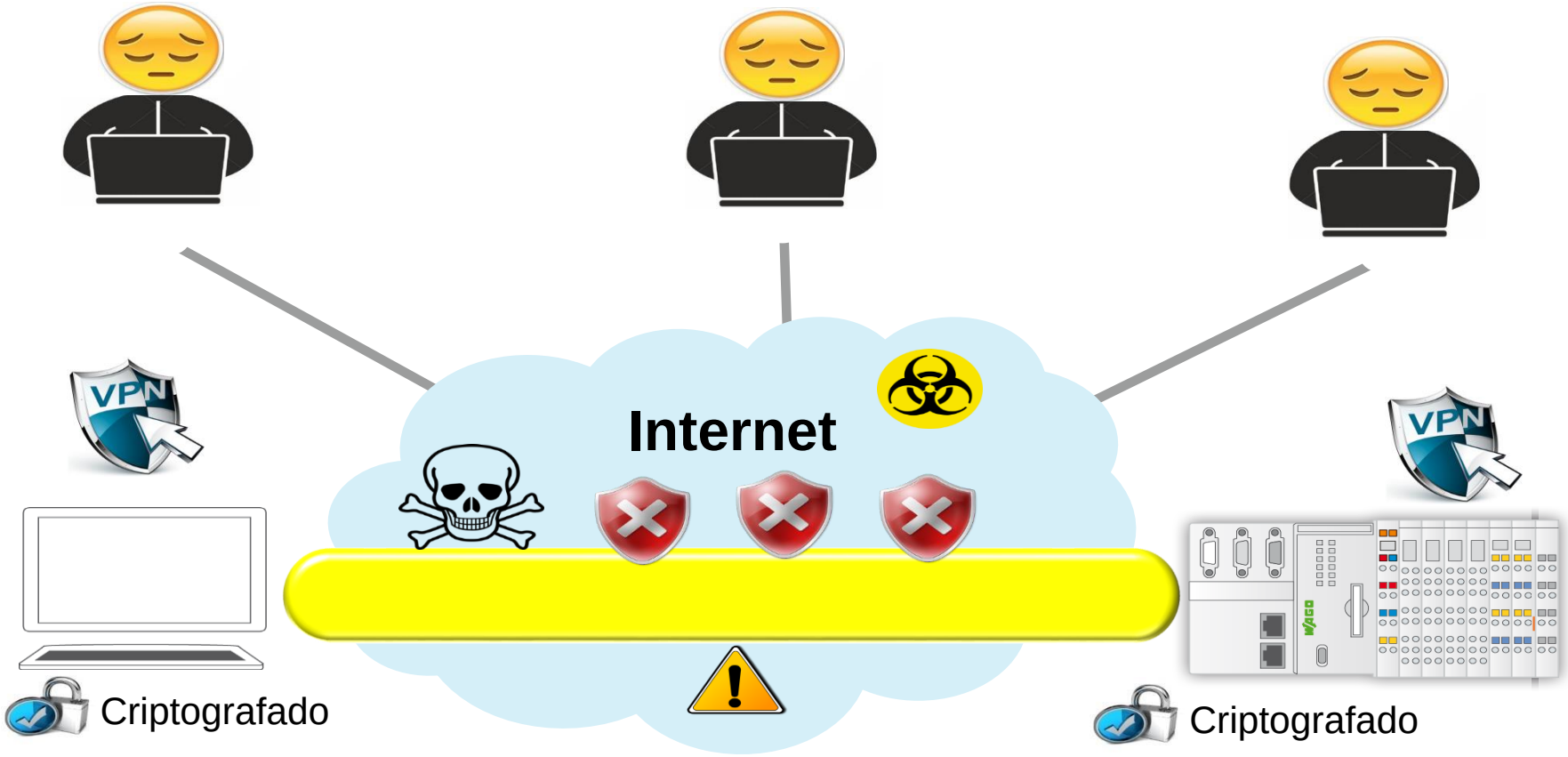


3. ESTEJA FECHADO

Permita apenas conexões de saída criptografadas, como a VPN

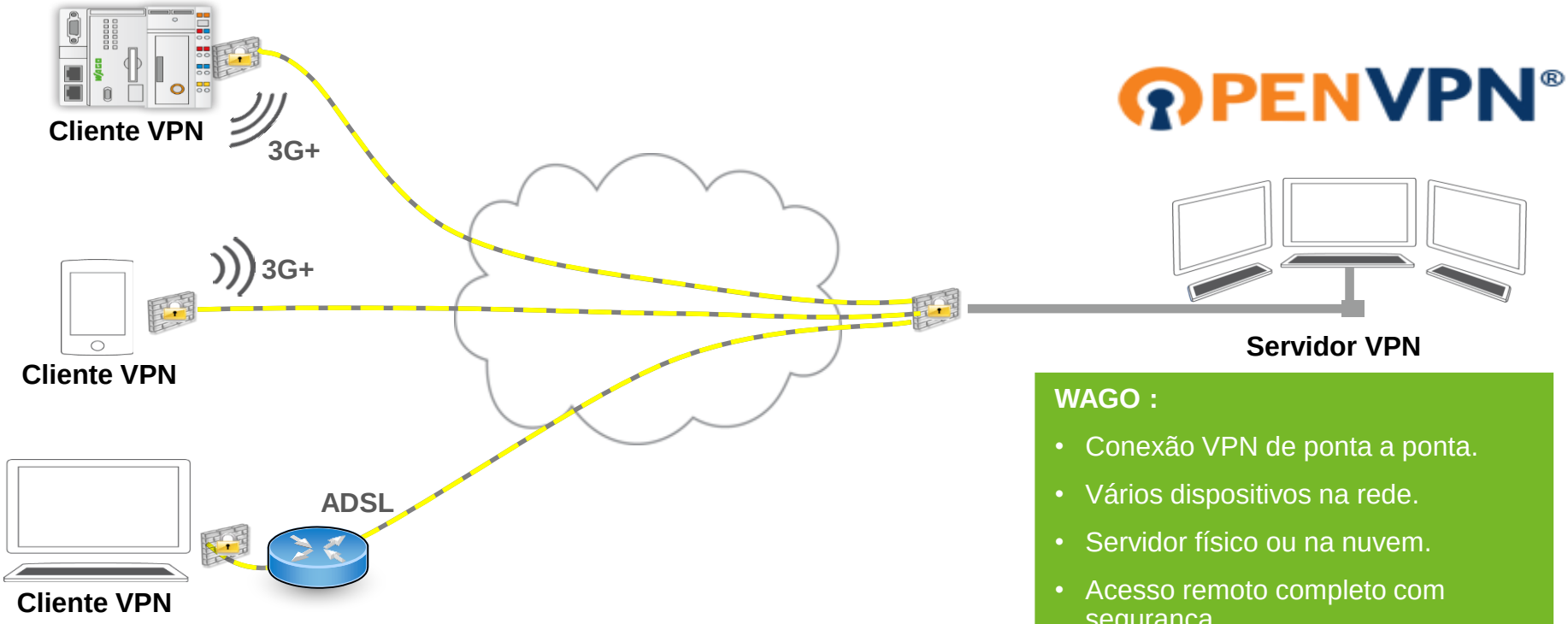


O QUE É VPN (VIRTUAL PRIVATE NETWORK)?



3. ESTEJA FECHADO

Solução com PFC WAGO e outros dispositivos

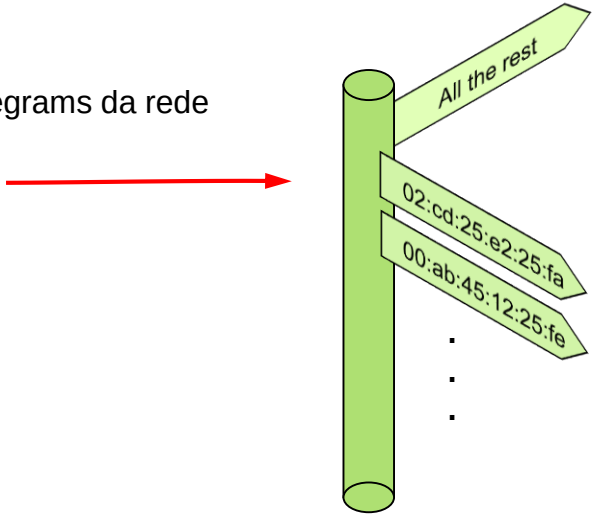


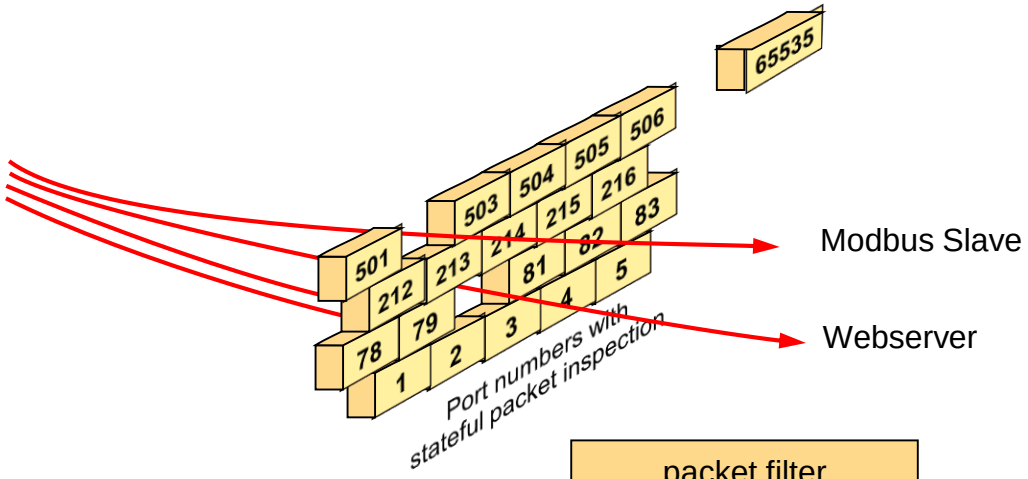
WAGO :

- Conexão VPN de ponta a ponta.
- Vários dispositivos na rede.
- Servidor físico ou na nuvem.
- Acesso remoto completo com segurança.

4. NÃO DEIXE ESTRANHOS ENTRAR

telegrams da rede





MAC address filter

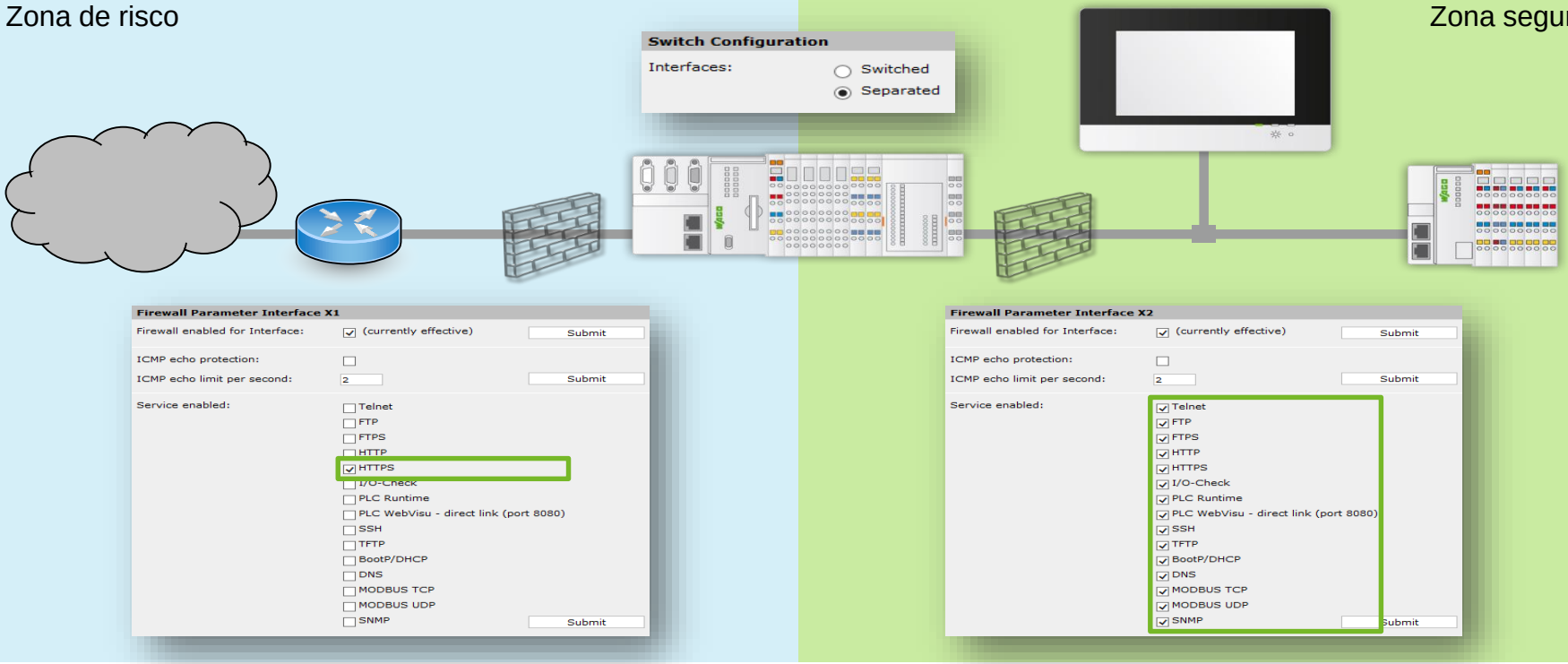
packet filter

4. NÃO DEIXE ESTRANHOS ENTRAR

PFCs - Firewall configurável por porta

Zona de risco

Zona segura



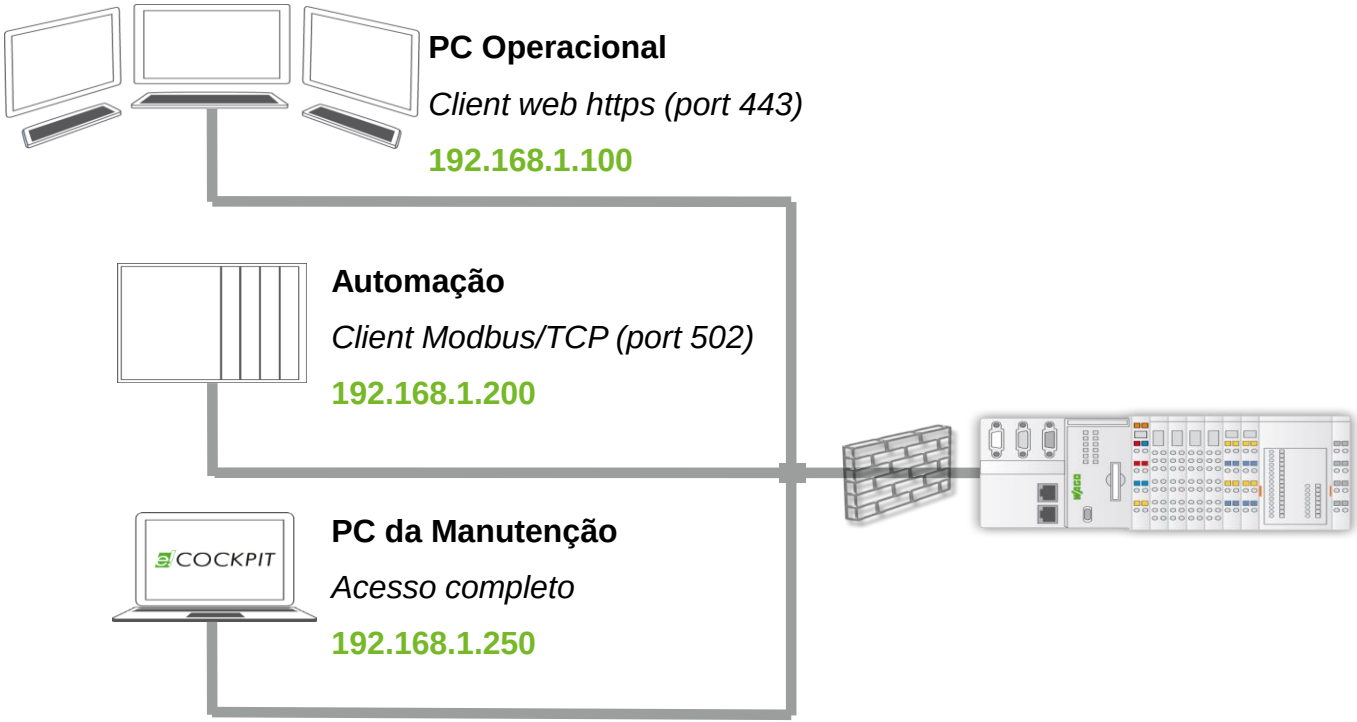
4. NÃO DEIXE ESTRANHOS ENTRAR

PFCs – Firewall com filtro de MAC address

Permitir apenas endereços específicos ou intervalos de endereços

4. NÃO DEIXE ESTRANHOS ENTRAR

PFCs – Firewall e regras personalizadas



User filter	
Count:	3

User filter 1	
Source IP address:	192.168.1.100
Destination port:	443
Protocol:	TCP
Input interface:	X1

User filter 2	
Source IP address:	192.168.1.200
Destination port:	502
Protocol:	TCP
Input interface:	X1

User filter 3	
Source IP address:	192.168.1.250
Protocol:	TCP/UDP

5. NÃO DEIXE QUE ALGUEM TE TIRE DA CASINHA !

Não click em link web que não conheça (como em e-mails)
Não interaja com nenhuma comunicação que não conheça o participante
Mantenha os programas de seu computador atualizados

Estatística de phishing por ano *

Year	Campaigns
2005	173,063
2006	268,126
2007	327,814
2008	335,965
2009	412,392
2010	313,517
2011	284,445
2012	320,081
2013	491,399
2014	704,178
2015	1,413,978

* Source: Wikipedia

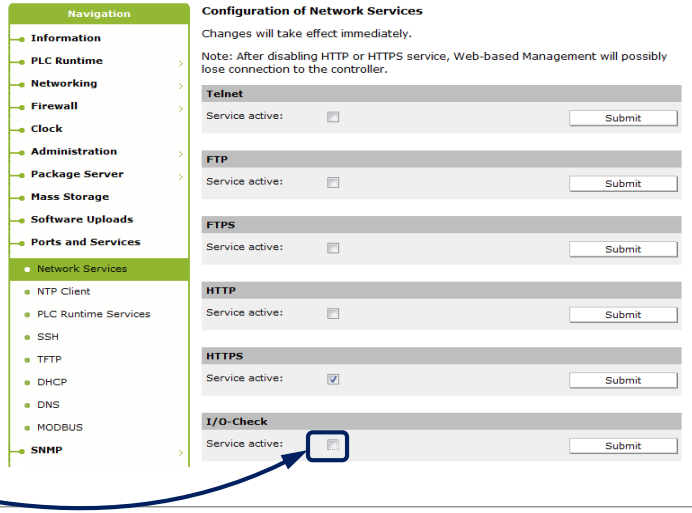
6. PERGUNTE O PASSWORD

Permita que conexões sejam estebelecidas somente com autenticação

Deixe a autenticação da porta ativa.
Limite o acesso do download Codesys e e!COCKPIT somente com senha

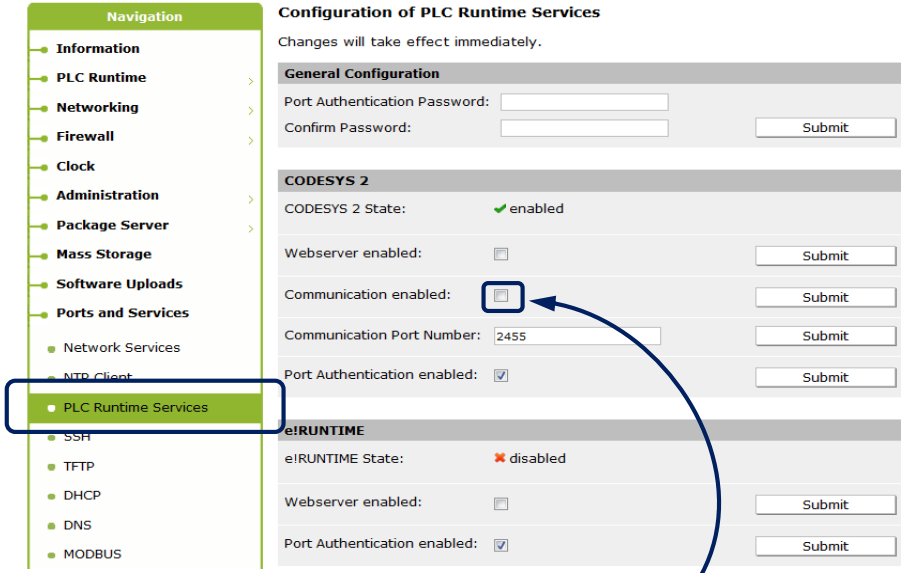
Desabilite o acesso do Ethernet settings e I/O-Check
(Eles não tem autenticação)

Acesso I/O-Check (port 6626)
no Ports and Services
-> Network Services
-> I/O-Check Service active



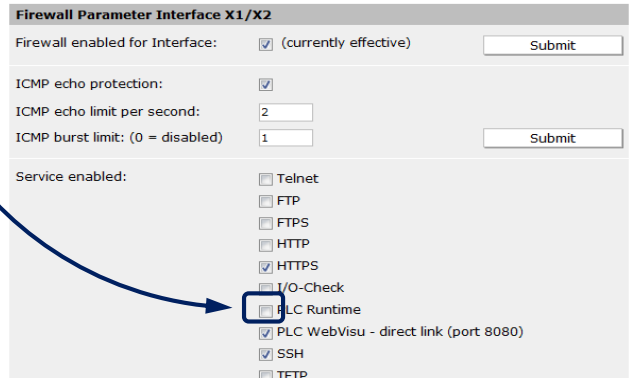
7. CONTROLE AS ENTRADAS

Desabilite a porta da ferramenta de programação, assim que finalizado.



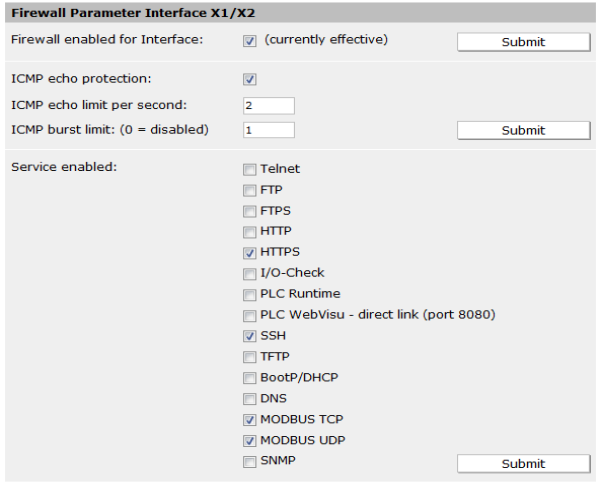
A porta do codesys permite várias coisas.
Feche para aumentar a segurança.

No e!COCKPIT o firewall pode bloquear a porta

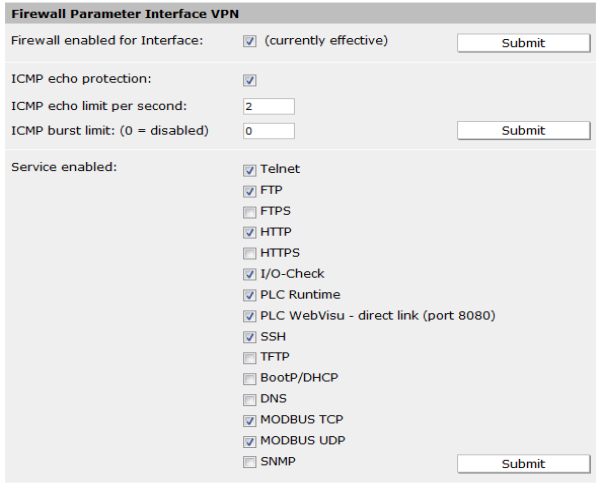


7. CONTROLE AS ENTRADAS

O acesso aos protocolos, por meio das portas fisícas, precisam ser bem restrito.



Mas caso tenha um acesso criptografado, podemos ser mais flexíveis.



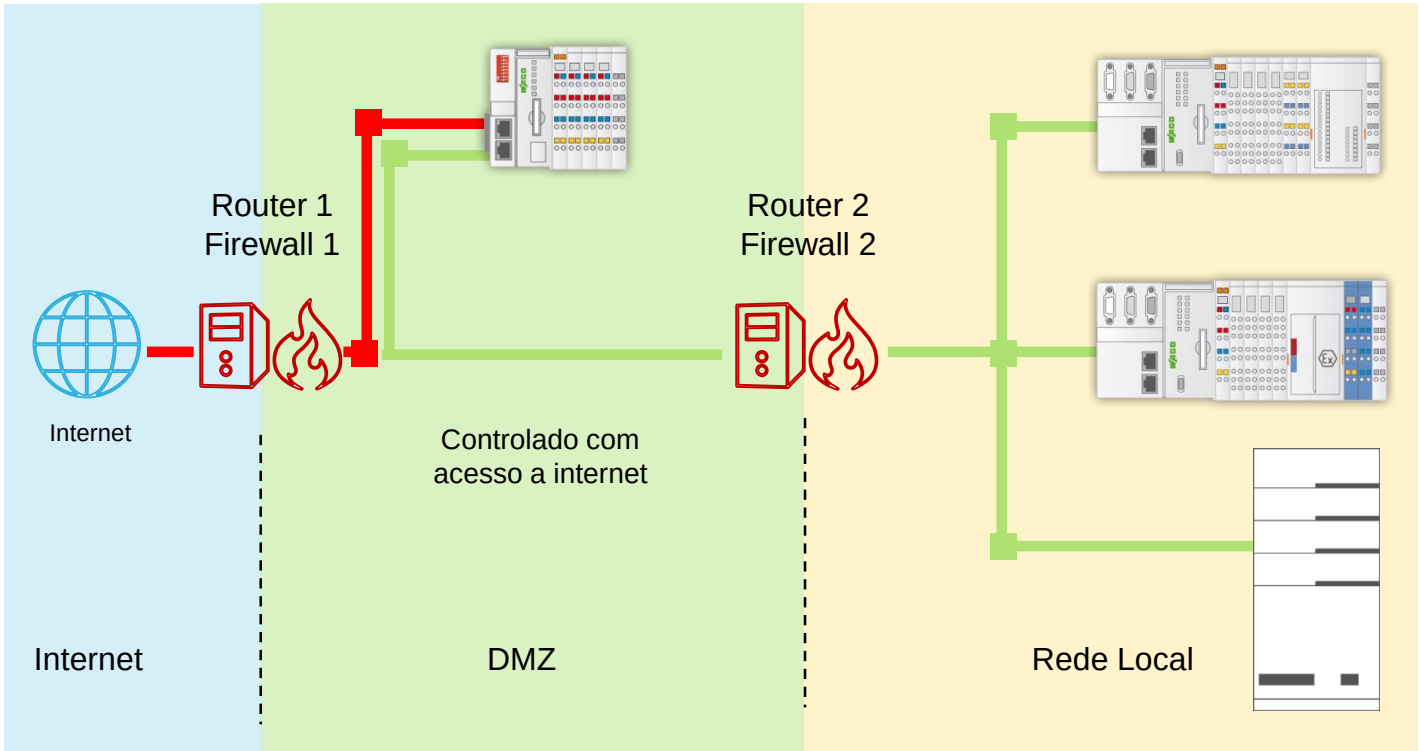
7. CONTROLE AS ENTRADAS

Limite o acesso físico aos painéis e ao componente também.

- O acesso ao Sdcard pode ser lacrado
- A extração do cartão SD pode ser detectado pelo programa para alarme

8. CRIE UM QUARTO DE LAMA PARA LIMPAR OS PÉS

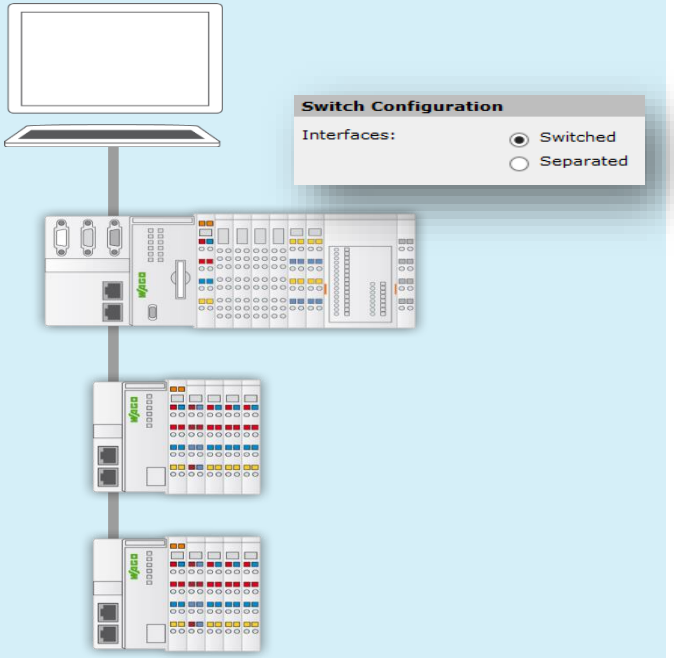
Crie uma zona desmilitarizada (DMZ)



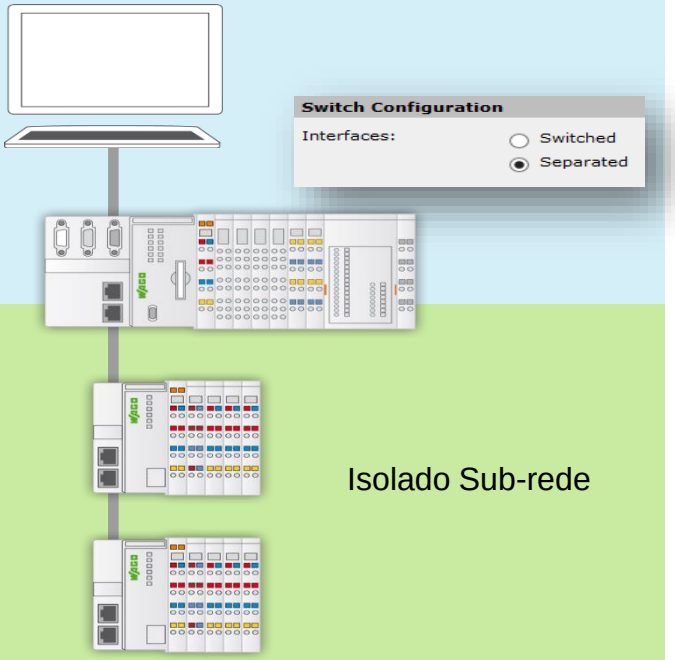
8. CRIE UM QUARTO DE LAMA PARA LIMPAR OS PÉS

Ip comuns ou separados

192.168.1.0



192.168.1.0



192.168.2.0

Isolado Sub-rede

9. DÊ UMA OLHADA PERIODICAMENTE

Não deixe o controlador exposto trabalhar por meses sem vigilância.
Verifique regularmente os estados dos controladores.

Existe algum comportamento não esperado ? CPU está sobrecarregada?
Verifique os arquivos de log files nos PFCx00.

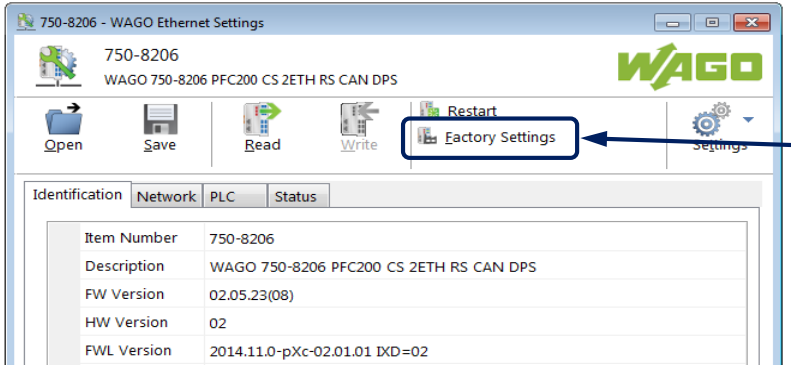
`/var/log/messages`
Muitas detalhes precisa até usar filtros

`/var/log/wago/wagolog.log`
Grava todas as mudança de Run para Stop

Se os filtros estão ativos:
`/var/log/lightpd/access.log`
Grava todos os acessos que passaram pelo filtro de usuário do firewall

10. LIMPE SUAS MÃOS

Mantenha os equipamentos atualizados através de firmware updates,
Habilite somente serviços necessários para a operação,
Se o hardware precisa ser trocado: limpe o PLC antes da reposição.



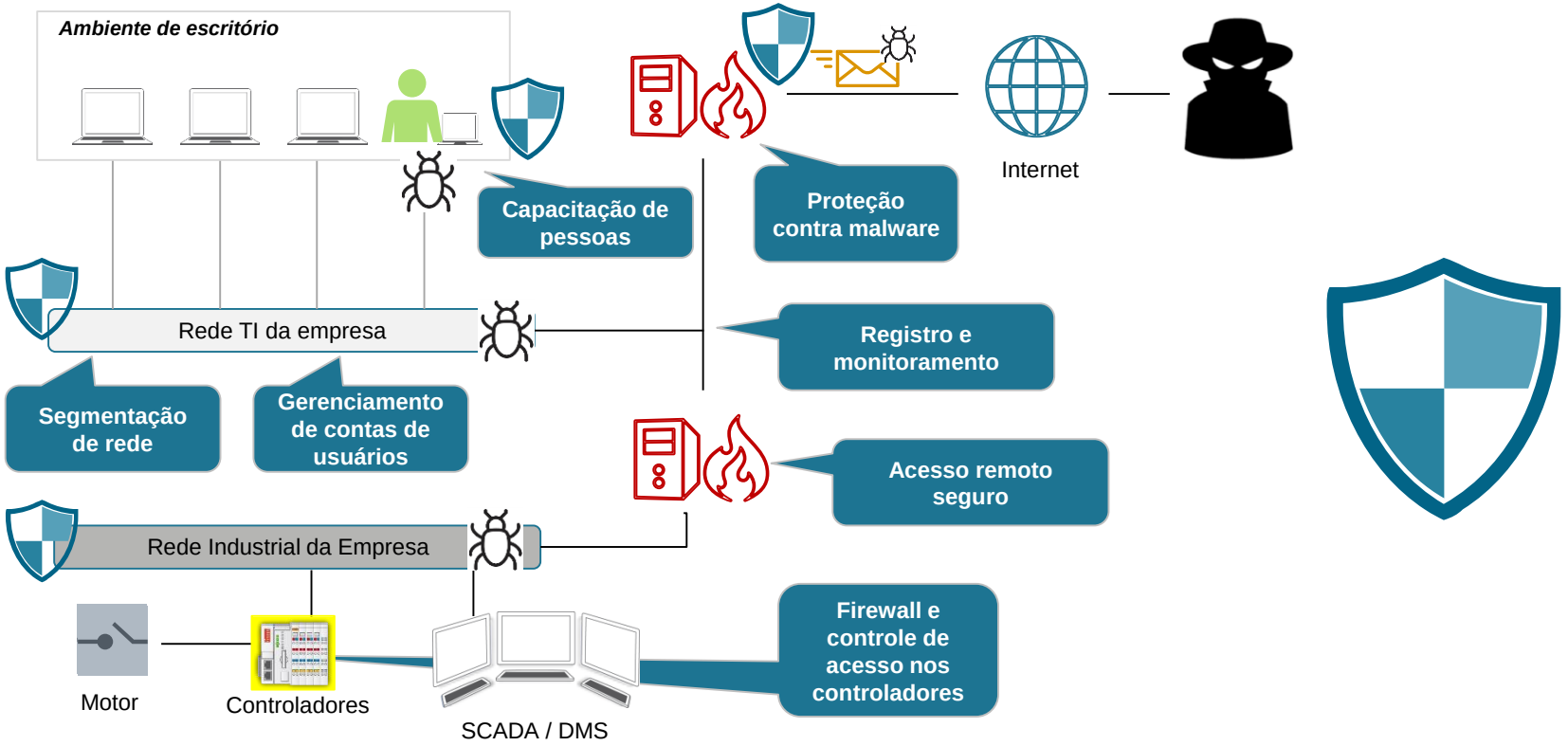
No 750-88x:
Limpa tudo Resets everything

Nos PFCs 750-8x00
Resets: Propriedade de rede (IP-adress, gateway, firewall, MAC filters, …), time zone, todos os passwords.

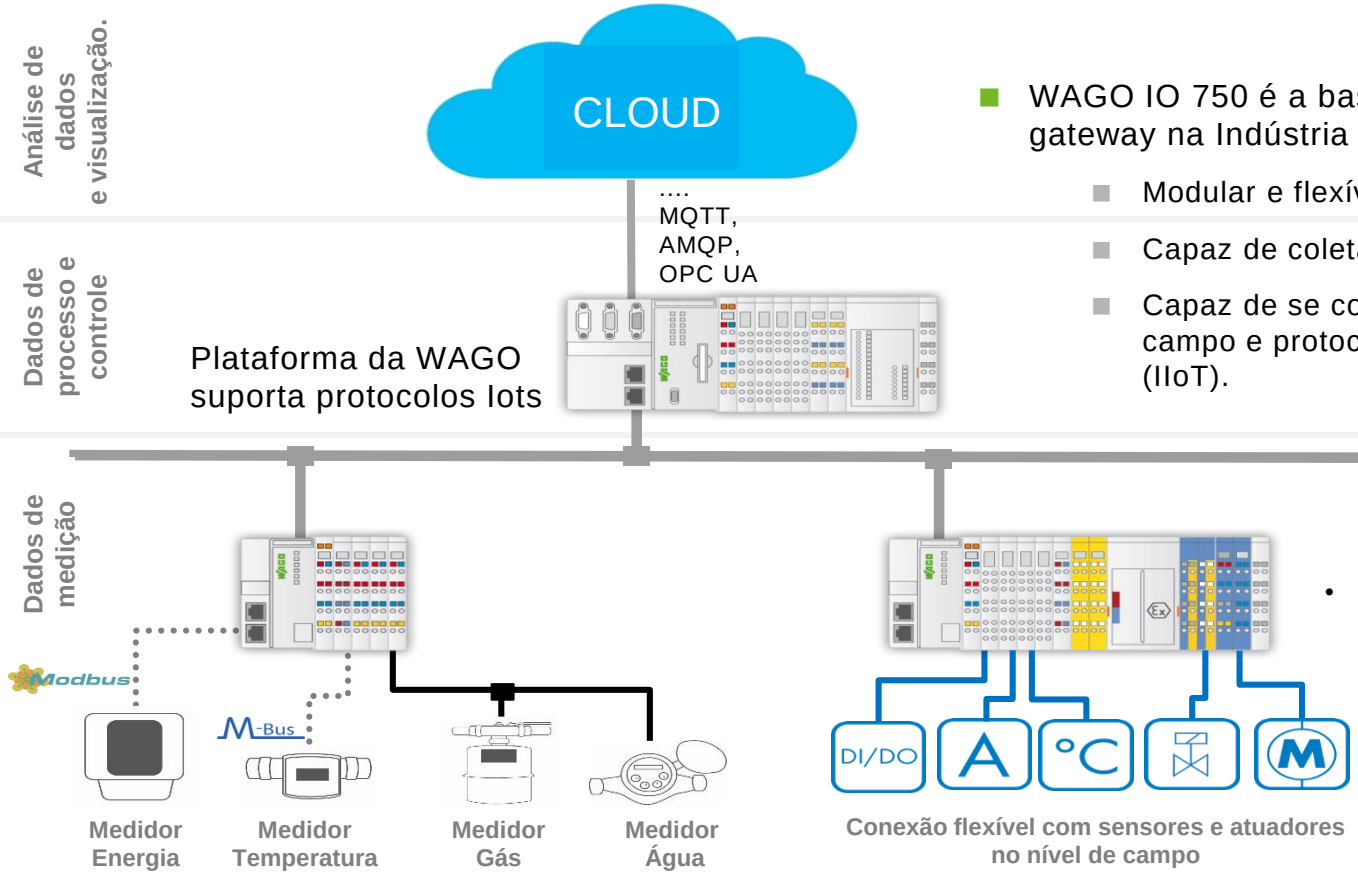
Lembre : DNS-Servers, figuras de usuários (do visu), arquivos de usuários (csv-files, logs gerados pelos users), bootproject, source code, webvisu, vpn certificados e chaves

PASSO A PASSO DO ATAQUE

Exemplo de como o ataque teria sido mitigado através da IEC 62443



PFC como Gateway para IIoT

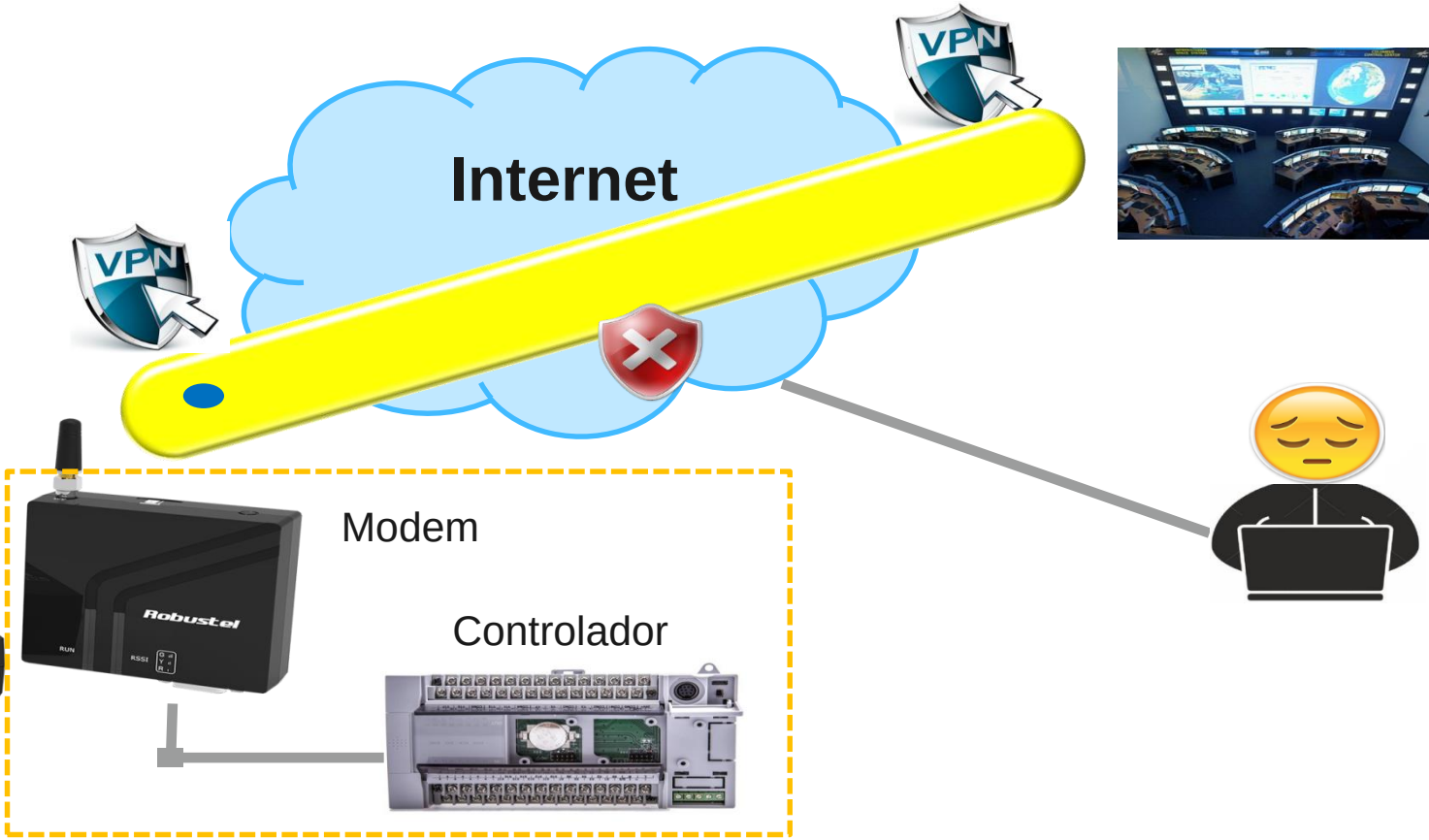


- WAGO IO 750 é a base perfeita p/ trabalhar como gateway na Indústria da Internet das coisas:
  - Modular e flexível
  - Capaz de coletar vários dados de campo
  - Capaz de se comunicar em diversos protocolos de campo e protocolos de Industry Internet of Thigs (IIoT).

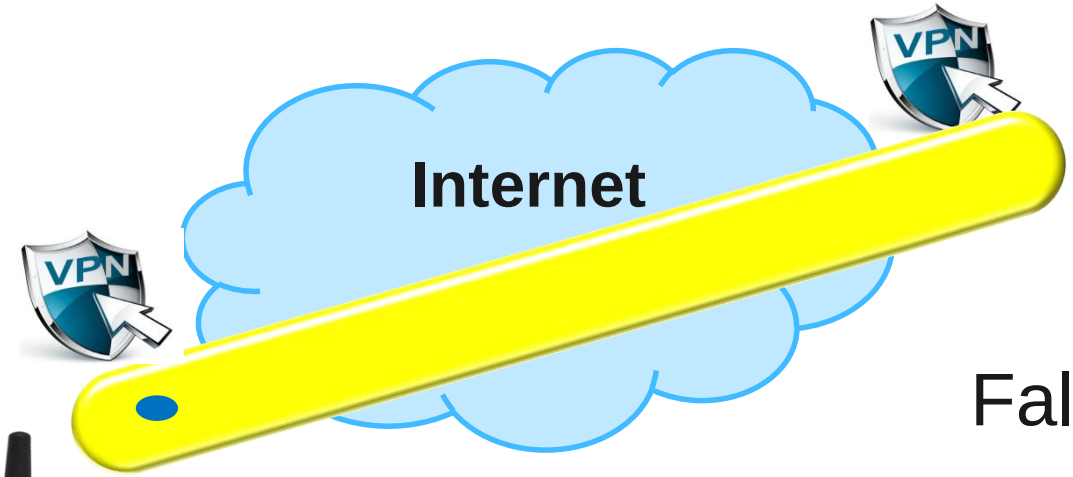
- Conetividade com nuvem para sensores/ atuadores que não tem acesso direto com a internet.

IoT READY

Modem + CLP – Segurança em Perigo



Modem + CLP – Segurança em Perigo

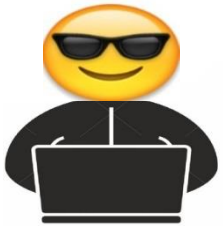


Centro de Controle

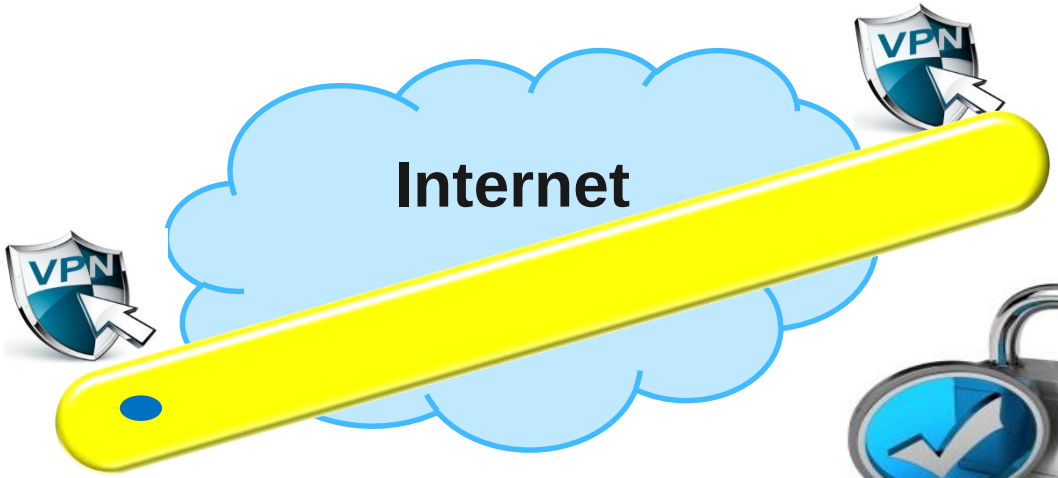
Falha de Segurança

Modem

Controlador

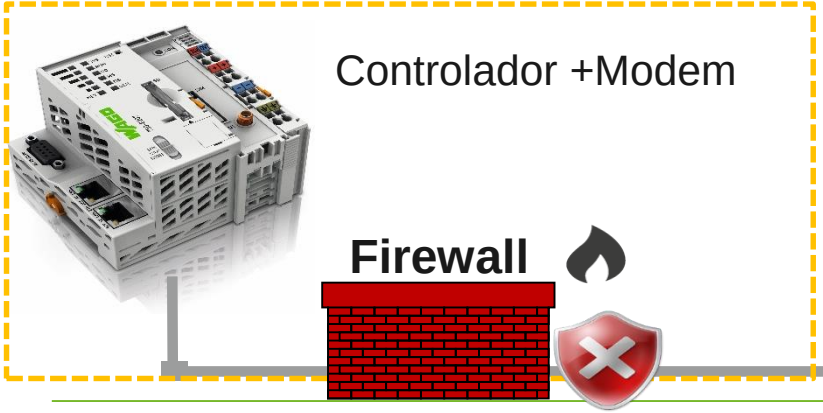


Modem + CLP – Segurança em Perigo



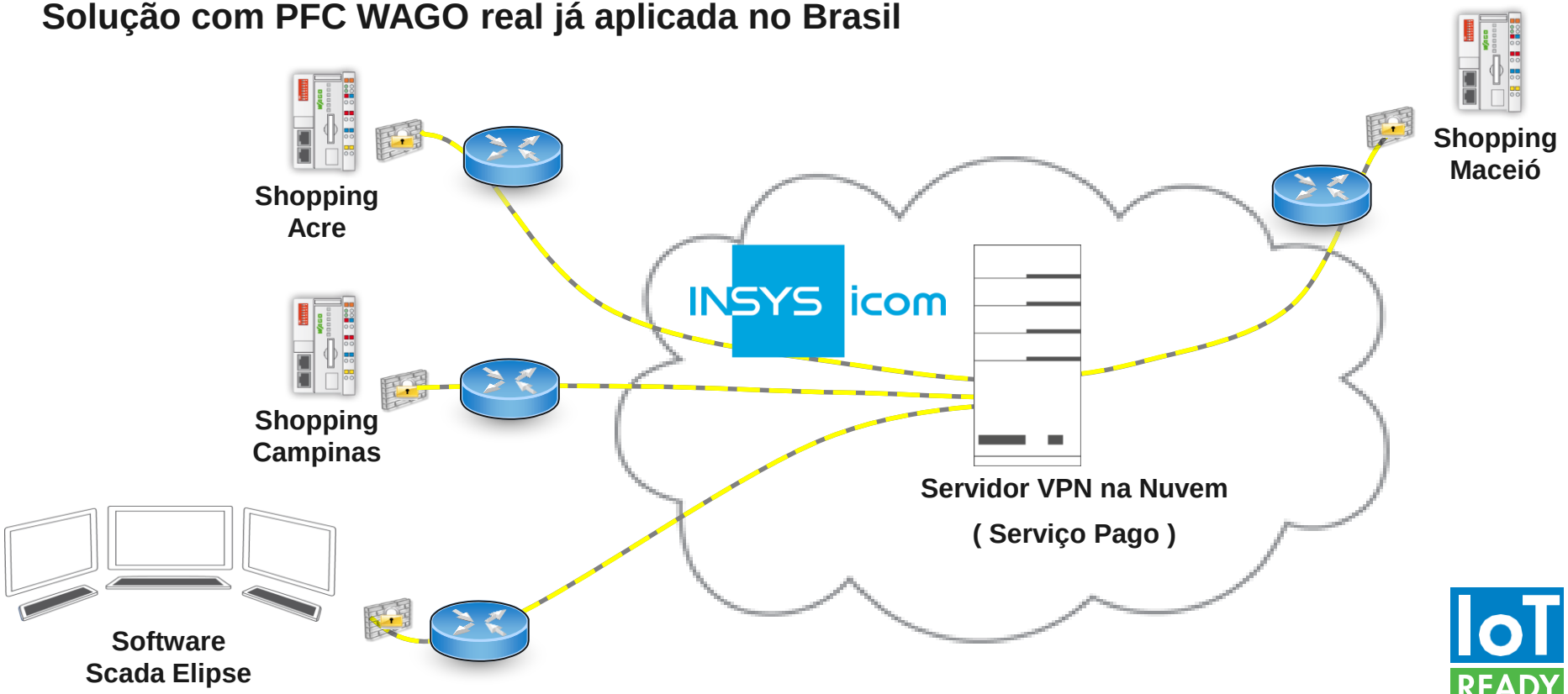
Centro de Controle

VPN e Firewall Integrado



VPN Estrutura – Exemplo de Aplicação

Solução com PFC WAGO real já aplicada no Brasil



IoT READY

AS TECNOLOGIAS

1 Software

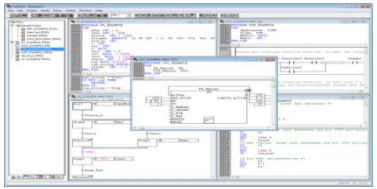



***e!*COCKPIT**

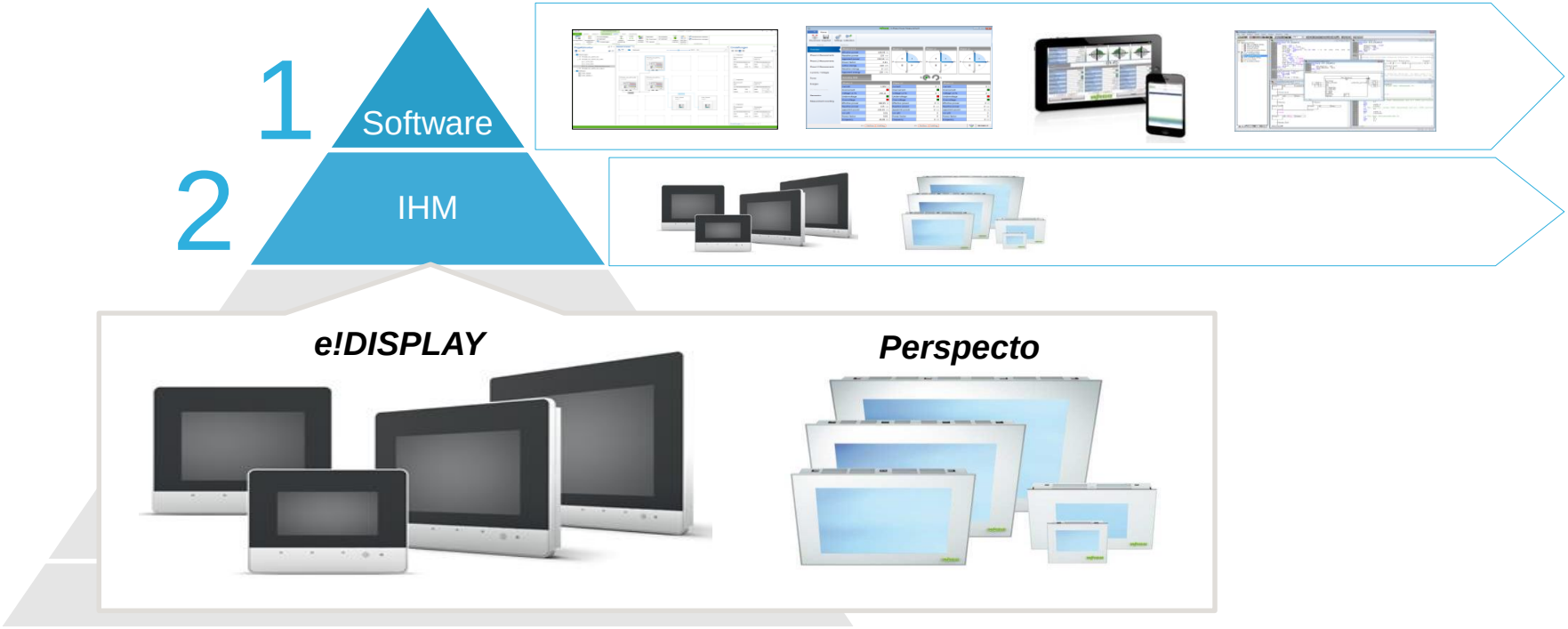
I/O Check

WebVisu app

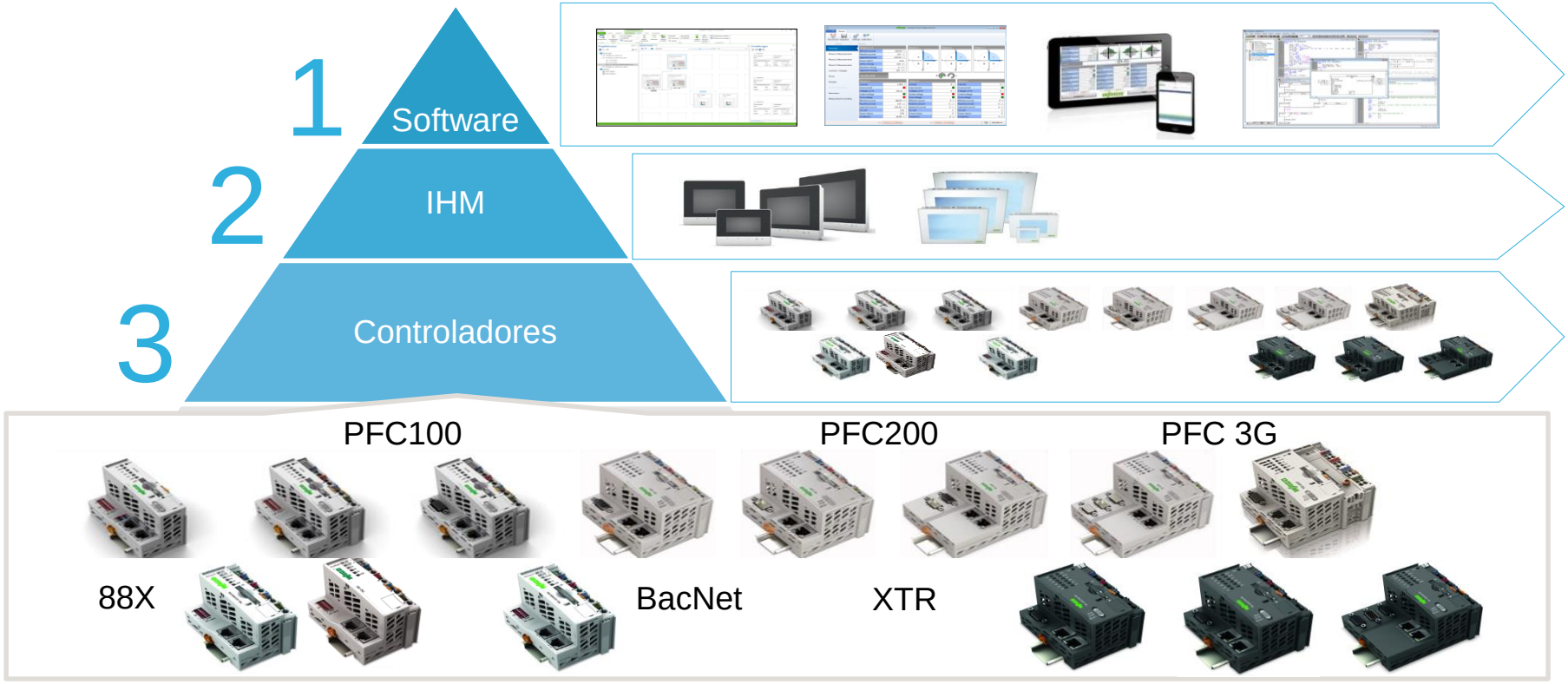
Codesys



AS TECNOLOGIAS



AS TECNOLOGIAS



AS TECNOLOGIAS

Acopladores

DI e DOs

AI e AOs

Safety

Especiais
Medição de Energia
Bluetooth
Célula de carga

EXi

XTR

4

I/O e Acopladores

Infraestrutura

AS TECNOLOGIAS

1 Software

Switches
Gerenciáveis, fontes,
disjuntores
eletrônicos, bornes

5 Infraestrutura

OBRIGADO!

Siga-nos no LinkedIn