Fijoport Zero Trust Architecture

Fergal Meath, Fijowave Ltd., January 2022

Abstract

There has been a recent explosion of IoT devices with varying levels of vulnerability to cyber attack. As we move to cloud applications to simplify connectivity, we may forget the importance of protecting our remote assets.

This white paper describes the challenges in this domain, provides some tips on how to respond to these challenges, and investigates the Zero Trust Security model.

The Environment

The internet of things refers to the interconnection of embedded computing devices, enabling them to send and receive data with other networks, devices and indeed people.

This interconnectedness presents a massive potential for good – remote working, health monitoring, personal security, energy management, industry 4.0, and other smart services that make our lives better. Unfortunately the potential for good is challenged by the potential for bad – data theft, espionage, ransomware, digital vandalism, and other cybercrimes.

In 2021 global losses from cybercrime have now exceeded $1 trillion[1].

The modern way of working has moved us to more cloud computing with SASE (Secure Access Service Edge) networking resulting in a widening of network perimeters to accommodate the distributed network endpoints of multiple remote satellite (home) offices.

Not only do we need to control the connectivity between devices and networks, we need to control the connectivity on a user level – limiting user access to particular applications and services on particular devices.

There has been a recent explosion of IoT devices with varying levels of vulnerability to cyber attack.

As we move to cloud applications to simplify connectivity, we may forget the importance of protecting our remote assets. IoT devices in the field collect sensitive data that needs to be kept confidential. IoT devices need to be configured remotely and even commanded to take actions. These devices present a massive attack surface for malicious actors to target.

Many see VPNs as the answer but VPNs alone simply create more network connections and can increase the attack surface.

The answer is to deploy a Zero Trust Architecture (ZTA) using VPN technology to encrypt the internetwork connections and centralised user access control to limit device access by application.

[1]Nord Layer (https://nordlayer.com/)

Cyber-security Challenges

There are three common cyber security challenges in the IoT world

Privacy: the data that you are monitoring is confidential. It is your duty to keep it private.
Data integrity: we need to be confident that the data has not been tampered with when transitioning the internet.
Legacy software: old technology and legacy computer systems cannot be connected to the internet any more because their security techniques have been found to be vulnerable.

Common cyber-attacks that we need to protect against

Malware: this term encompasses the following types of attacks...

- Viruses - these infect applications by attaching themselves to the initialization sequence. The virus replicates itself, infecting other code in the computer system.
- Trojans - a program hiding inside a useful program with malicious purposes. Unlike viruses, a trojan doesn't replicate itself and it is commonly used to establish a backdoor to be exploited by attackers.
- Worms—unlike viruses, they don't attack the host, being self-contained programs that propagate across networks and computers. Worms are often installed through email attachments, sending a copy of themselves to every contact in the infected computer email list. They are commonly used to overload an email server and achieve a denial-of-service attack.
- Ransomware—a type of malware that denies access to the victim's data, threatening to publish or delete it unless a ransom is paid. Advanced ransomware uses crypto-extortion, encrypting the victim's data so that it is impossible to decrypt without the decryption key.
- Spyware—a type of program installed to collect information about users, their systems or browsing habits, sending the data to a remote user. The attacker can then use the information for blackmailing purposes or download and install other malicious programs from the web.

Phishing: typically email or instant messages where the attacker masquerades as a reputable entity in order to coerce the victim into revealing private information.

Man-in-the-Middle (MitM) Attacks: the perpetrator secretly relays and potentially alters the communications between two parties who believe they are directly communicating with each other.

Denial-of-Service (DOS) Attack: the perpetrator aims to make a server or network unavailable to intended users, typically by flooding the target with superfluous requests in order to overload it.

SQL Injection: the attacker interferes with an application writing to it's database with the aim of getting to view that data, modify the data, or damage the database.

Zero-day Exploit: is an attack that exploits a vulnerability for which there is no software patch and that may be unknown to the software vendors and users.

Password Attack (brute force): the attacker submits many passwords or passphrases in the hope of eventually guessing correctly. A dictionary attack involves trying a calculated smart list of passwords.

Cross-site Scripting: the attacker injects client side scripts in vulnerable web applications – these scripts will be executed on other computers that use the exploited web application.

Significant Ransomware Attacks in 2021[2]

- A VPN password was compromised, leading to the US company Colonial Pipeline attack and resulted in a blockade of petroleum and diesel fuels on the East Coast of the US for 6 days, led to a 4% increase in fuel prices, and cost the company $3.8 million (paid in Bitcoin).

- Norwegian company "Volue" suffered a ransomware cyber-attack that blocked water and wastewater facilities serving 85% of the country.

- Norwegian company AKVA Group - fish farming control services were blocked, consequently they reported first quarter losses of $6 million.

- Criminals gained access to a water plant in Tampa, Florida, which serves about 15,000 people. They took advantage of the Team Viewer connection to access the system and modify the amount of sodium hydroxide (lye) to pour in a much higher amount than normally used (to control the acidity of the water). The case was brought to the attention of the FBI and the Secret Service.

- The Natantz nuclear power plant (Iran) suffered a cyber-attack that caused a blackout, 24 hours after it was commissioned. The Iranian government initially claimed it was an "accident", but

[2] Cyber Security Report 2021 H1, Telefonica Tech

after Israeli press reports claimed it was a cyber-attack they described it as "nuclear terrorism".

- A series of cyber-attacks brought down several Spanish national services, including the websites of several ministries and the INE (National Statistics Institute).

- Ireland's public health service, the HSE, was hit by a ransomware cyber-attack that forced the cancellation of appointments and diagnoses at several hospitals.

What should I do if I'm hacked?

- Shut down devices, servers, machine instances as quickly as you can.
- Contact your IT service provider. They can help you to analyse the problem and will guide you through the steps necessary to protect you and your organisation from further damage.
- Inform those whose information may have been compromised.
- Review your security policies and tools.

How do I Prevent a Cyber Attack?

- Do not connect your device directly to the internet – use a NAT or a firewall so that your device cannot be seen by hackers.

- Ensure your services are encrypted
  - web services should use HTTPS (HTTP + TLS).
  - file transfer services should use FTPS (FTP + TLS) or SFTP (SSH + FTP).

- Use Virtual Private Network (VPN) technology to connect your device to a remote network. Data sent from your device will be encrypted and may only be viewed by devices on the remote network.

- Avoid simple passwords (john123) as these may be easily “brute forced” – use complex passwords with at least 8 characters, including at least 1 uppercase, 1 number and 1 symbol. Keep your passwords private. Consider using a tool like Password Safe.

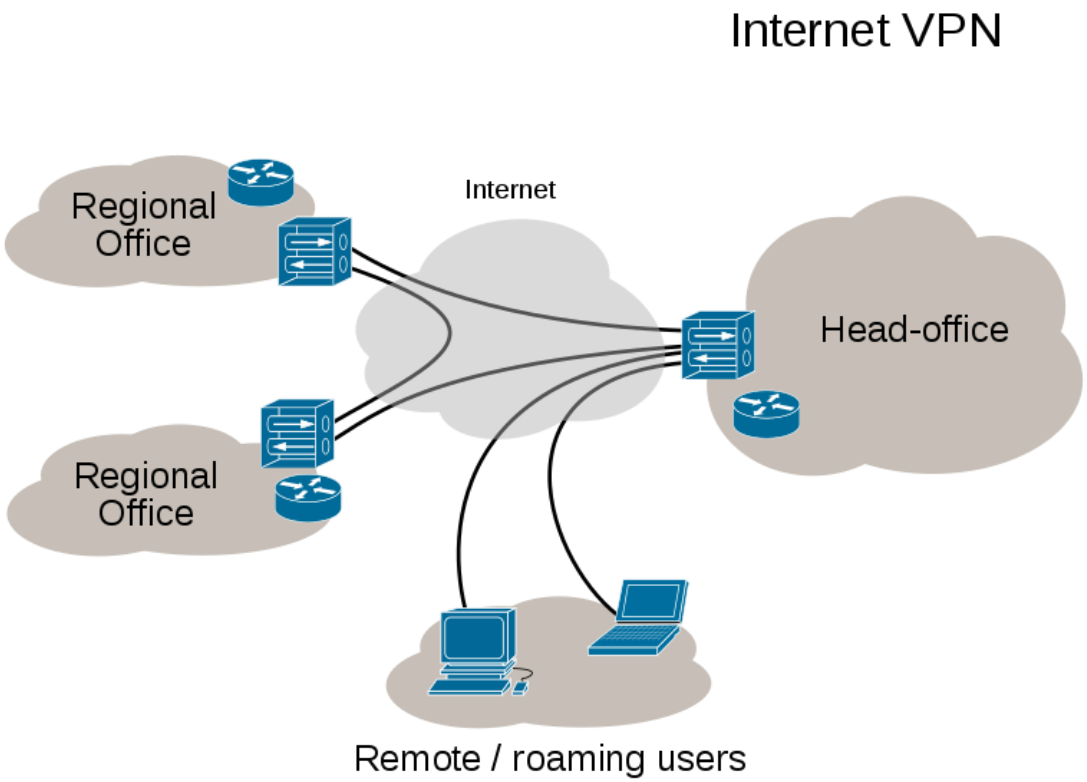
- Do not click on internet links received by text or email from unknown senders.

- Never share your credentials by voice call, email or text messaging with unknown parties.

Problem with VPNs

Businesses employ Virtual Private Network VPN technology in order to route their traffic safely through the internet between head office and regional offices and remote or roaming users.

Whilst VPN technology is an essential part of any secure networking solution it is also not without risks.



- With the evolution of work practices towards mobility and cloud there has been an increase in VPN targeted attacks[3].
- A VPN is only as strong as its weakest component. If one branch office has a compromised VPN (compromised key or exploited computer) then the entire corporate network may be vulnerable.
- By implement VPNs with centralised administration and secure access service edge (SASE) we are effectively widening network perimeters to accommodate the distributed network endpoints of multiple remote sites.
- We can mitigate these risks by employing a Zero Trust Architecture (ZTA).

[3]2021 VPN Risk Report, Cybersecurity Insiders

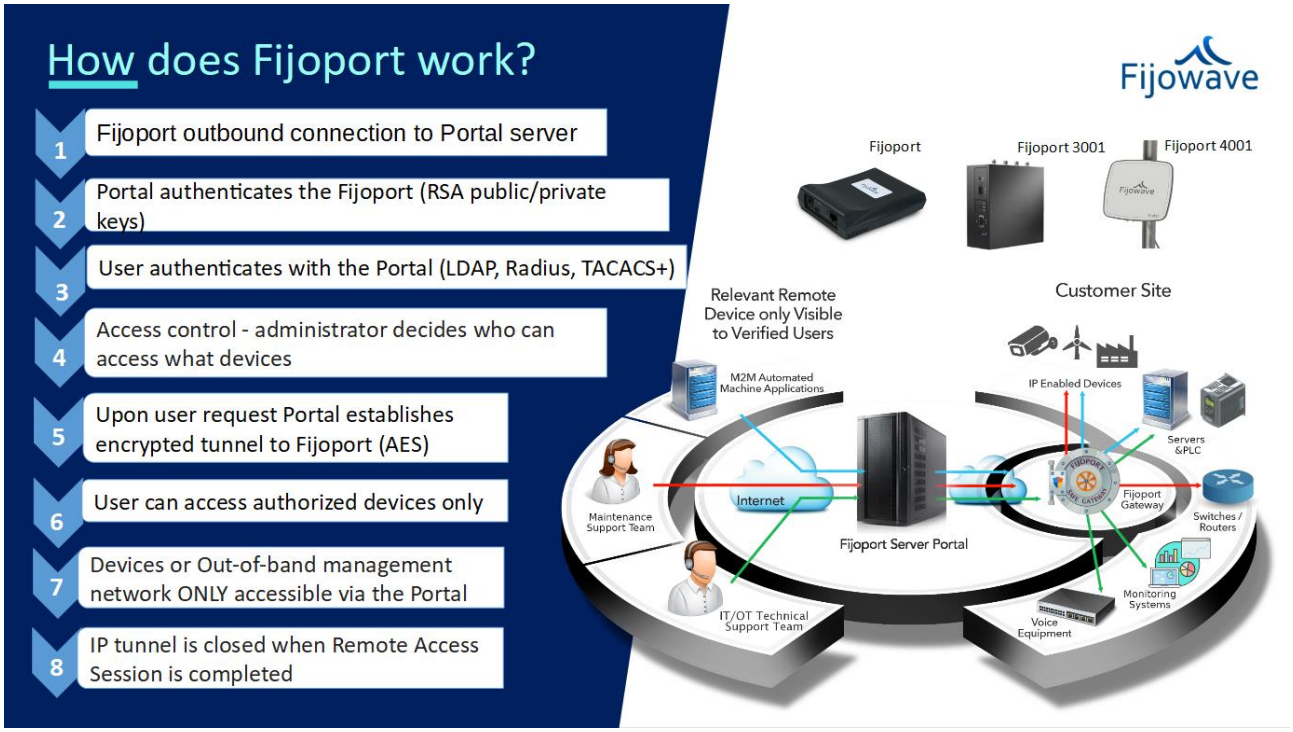
Zero Trust Architecture (ZTA)

Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defences from static, network-based perimeters to a focus on users, assets, and resources. A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows.

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e. local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Zero trust focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource.[4]

[4]NIST Special Publication 800-207

Fijoport ZTA



- The Policy Engine is implemented centrally in the Server Portal.
- Fijoport provides a Secure Access Service Edge (SASE).
- Remote devices need not have any connection to the internet whatsoever.
- Fijoport is granted access to the device.
- Fijoport is only accessible via the Portal.
- Users must authenticate with the Portal.
- Users have no automatic access rights to any Fijoport or any remote devices.
- Centralised administration of remote access policies can place users in groups that have access to individual device resources (e.g. switch support users can access switch serial console and switch SSH console, and voice equipment support can only access web interface of voice equipment).
- A compromised device cannot send unsolicited data via the Zero Trust Network.

Key Take Aways from Fijoport White Paper

- There is an explosion of IoT devices with varying levels of vulnerability to cyber attack.

- As we move to the cloud to simplify connectivity from our personal devices are we forgetting to protect our remote assets. IoT devices in the field collect sensitive data that needs to be kept confidential. IoT devices need to be configured remotely and even commanded to take actions. These devices present a massive attack surface for malicious actors to target.

- While the IoT industry is contemplating the widespread implementation of VPN technology to secure the OT (Operational Technology) network, we should not ignore the fact that the IT (Information Technology) world has started to replace traditional VPNs with Zero Trust Networks. Why not skip straight to the zero security trust model in this brave new IoT world?

- Zero trust model - secure edge gateway (Fijoport) connects to a centralised Cloud Portal - all remote access decisions are made in the Cloud Portal by the administrator only - zero trust by default = zero remote access - administrator can create remote access policies that may be applied to different users (and removed) (e.g. use case: control of third party suppliers), users access may be limited to individual devices and applications running on those devices (e.g. http interface, serial interface, ssh console interface).

Fijowave
Cyber Security

Fijowave Limited,

3015 Lake Drive,

Citywest Business Park,

Dublin, D24 DKP4, Ireland.

Web: https://www.fijowave.com/

Email: sales@fijowave.com