Making your networks future-proof

Post-quantum cryptography and virtualization

January 2024, Thomas Schneider and Tobias Fehenberger

Network access requirements

Security

IT-SiG 2.0, emerging EU NIS-2 directive: encryption, attack detection, assured supply chain

Scale

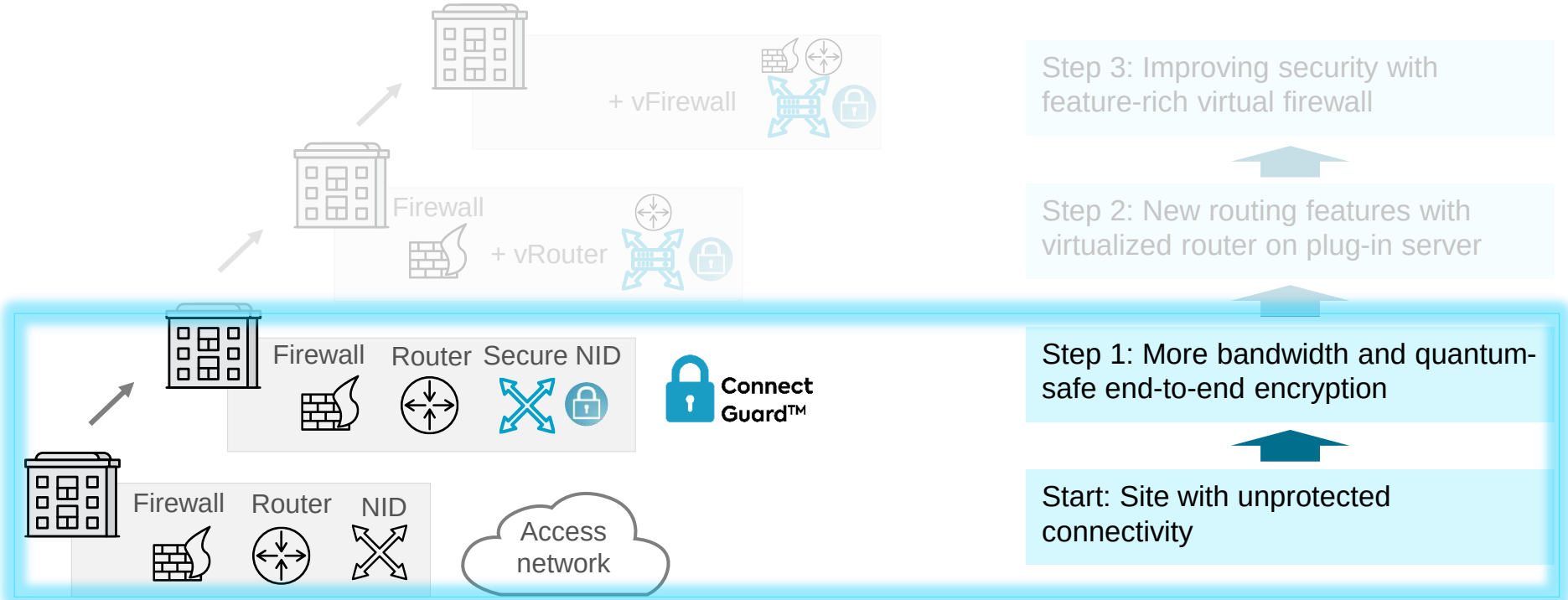
Applications and data in the cloud result in higher bandwidth on the access links

Sustainability

Single hardware for demarcation, security, sync and multiple virtualized applications

Multiple pain points to be addressed

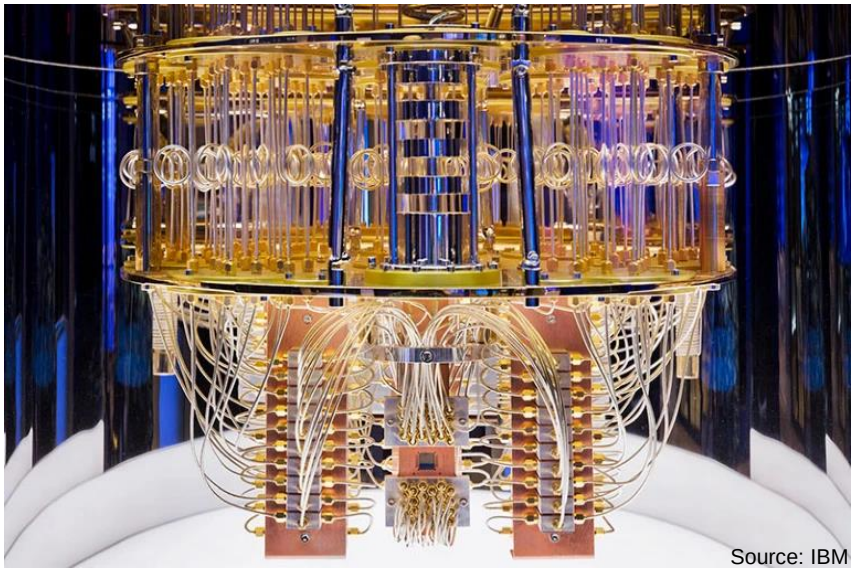
Creating more value at the network edge



Improving scale, security and flexibility

Quantum computers as attack tools

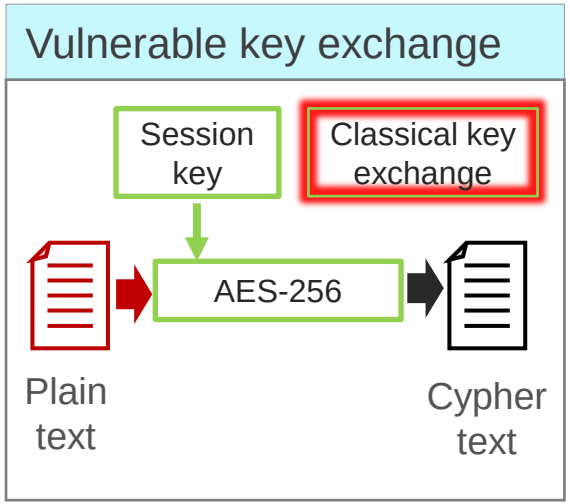
- Quantum computers are capable of breaking classical encryption
- Vulnerable asymmetric key protocols are used widely
- Migration to quantum-safe controls is a complex and time-consuming process
- “Store-now decrypt-later” attacks pose a significant threat – even today



Source: IBM

The danger is very serious and we need to act quickly

Making encryption quantum-safe and future-proof



Mitigation

Post-quantum cryptography (PQC)

Session key ← Quantum-safe algorithms — Secure key exchange

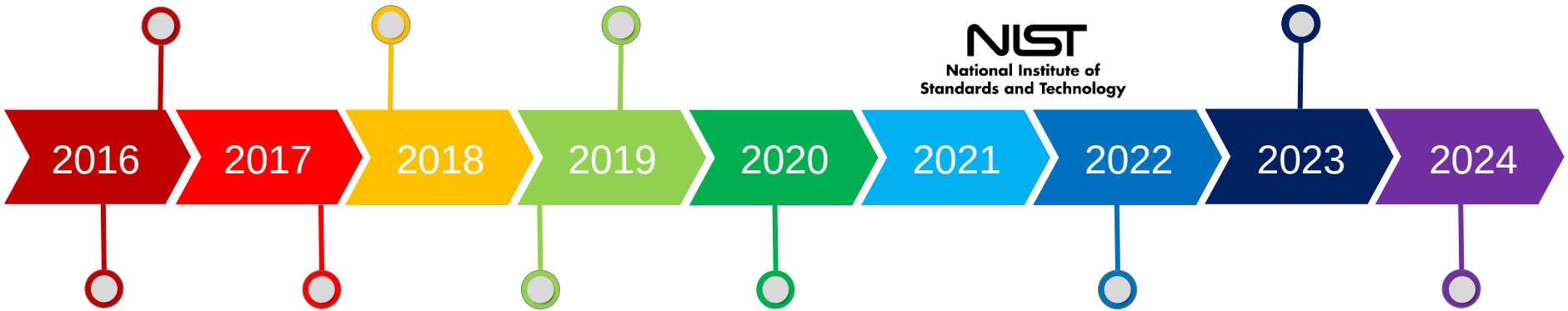
Applying quantum-resistant key exchange protocols using classical computers

Quantum key distribution (QKD)

Session key ← Quantum physics — Secure key exchange

Using quantum physics for secure key exchange

NIST Post-Quantum Cryptography Project



Dec 2016
Final requirements and criteria

April 2018
1st NIST PQC workshop

Aug 2019
2nd NIST PQC workshop

2020-2021
Round 3 seminars

NIST
National Institute of Standards and Technology

2023
Standards drafts released

Aug 2016
Draft submission requirements evaluation criteria

Nov 2017
DL for submissions

Jan 2019
2nd round started

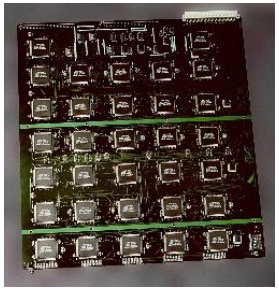
July 2020
Selected finalists and alternate candidates

July 2022
Announced finalists to be standardized and candidates for 4th round

~ Mid 2024
Final standards ready

Learning from the crypto-past

Brute-force attacks



“Deep Crack”
breaks DES (1998)

Mathematical attacks

Two hot PQC contenders
broken in 2022

Implementation attacks

2016

CacheBleed: A Timing Attack on OpenSSL Constant Time RSA

The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli

2017

2017

Dec 2023(!)
KyberSlash

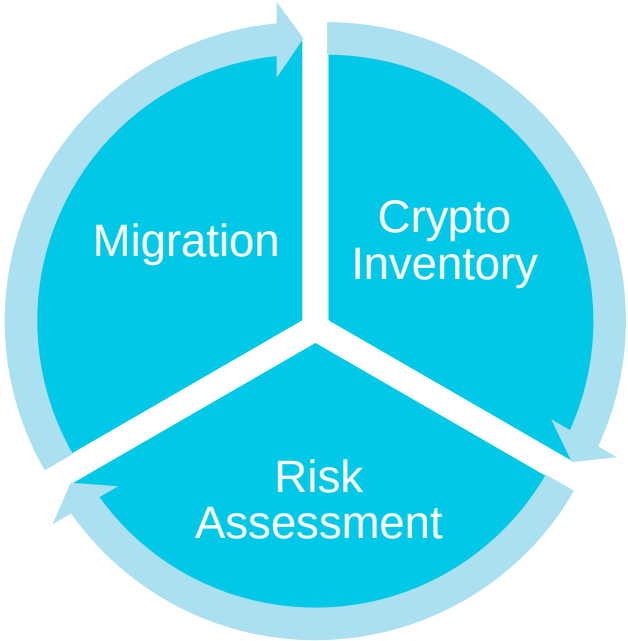
Never-ending
side-channel attacks

Highly complex and dynamic environment

Crypto Agility

Working group “Kryptoagilität“ at TeleTrusT just launched!

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.



Principal approaches

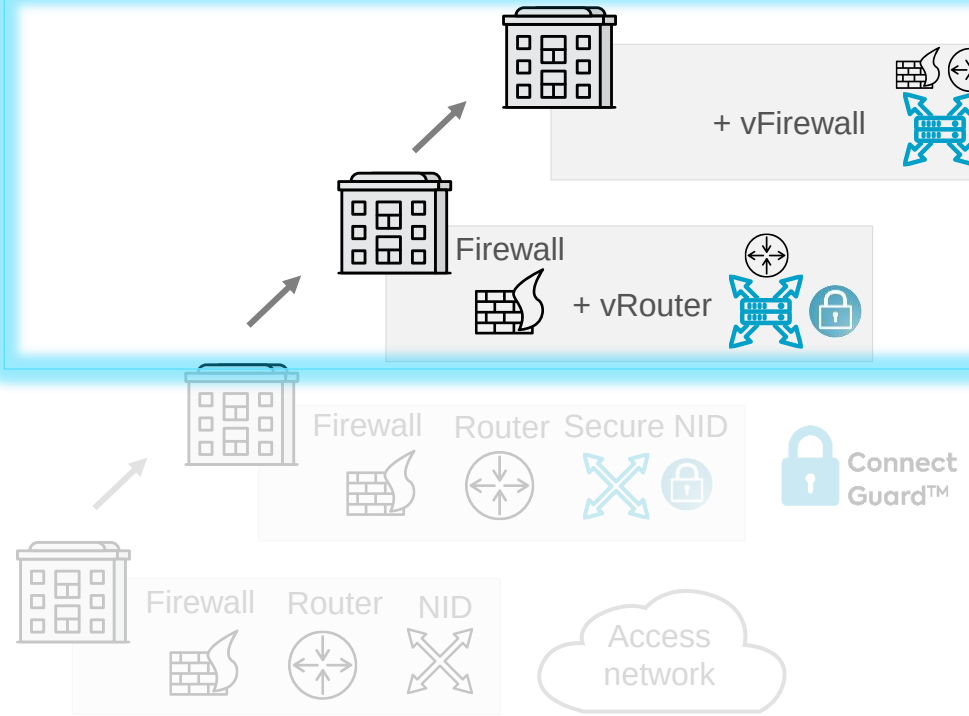
- Substitute vulnerable algorithms with quantum-safe ciphers (upgrade, replacement)
- Combine different crypto schemes
- Apply across several layers

Decision criteria

- Cost
- Time to secure
- Assurance level
- Long-term security

Continuous activity on governance and technical level

Creating more value at the network edge



Step 3: Improving security with feature-rich virtual firewall

Step 2: New routing features with virtualized router on plug-in server

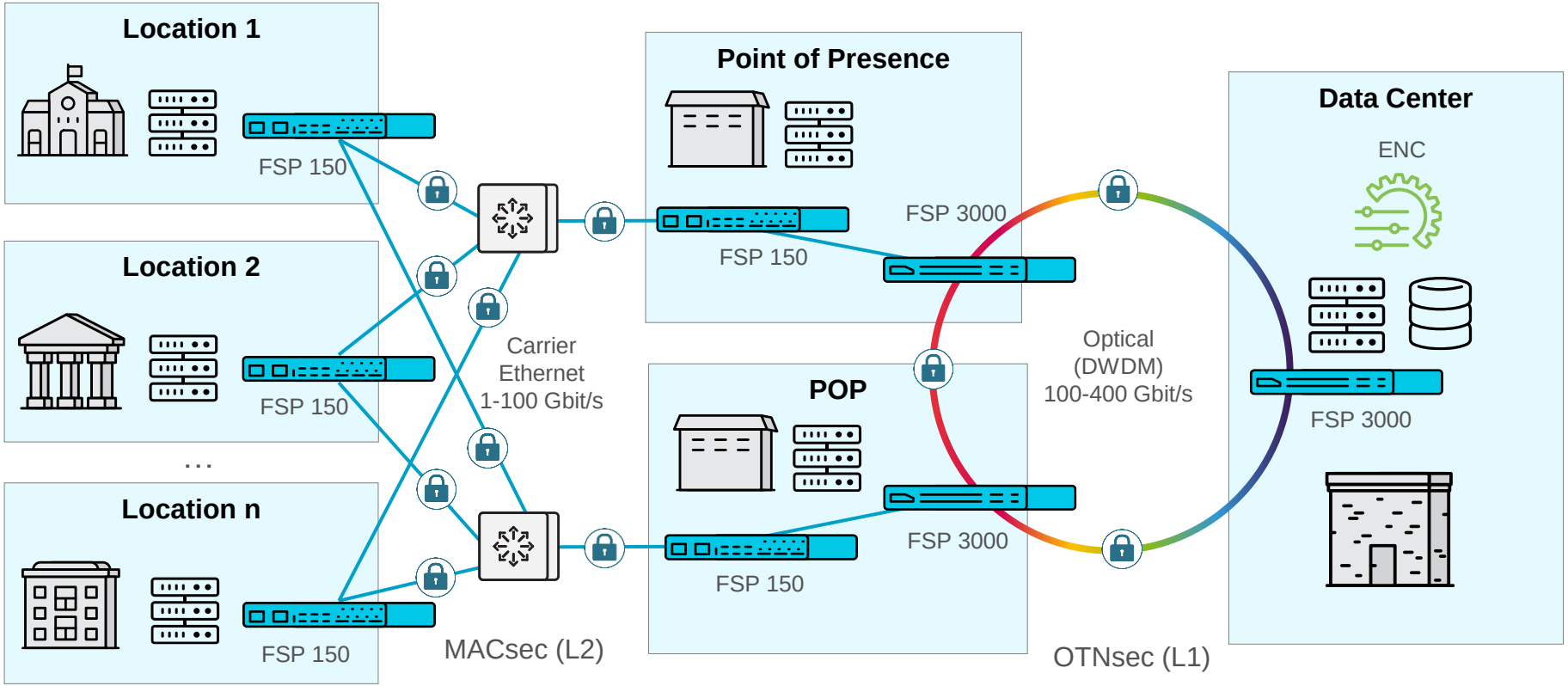
Step 1: More bandwidth and quantum-safe end-to-end encryption

Start: Site with unprotected connectivity

Improving scale, security and flexibility

THE BIG PICTURE

Secure connectivity across multiple network layers



LAYER 2 MACSEC ENCRYPTION WITH BSI VS-NFD APPROVAL

Network access device FSP 150-XG118Pro (CSH)

Network access

1G/10Gbit/s demarcation and aggregation

Sophisticated performance monitoring and resilience

Layer 2

Active support of
- Virtual LAN (VLAN)
- Quality of Service (QOS)
- Link Aggregation (LAG)

MACsec + Security

Hardware-based Ethernet encryption

Approved by German BSI for VS-NfD

Connect Guard™

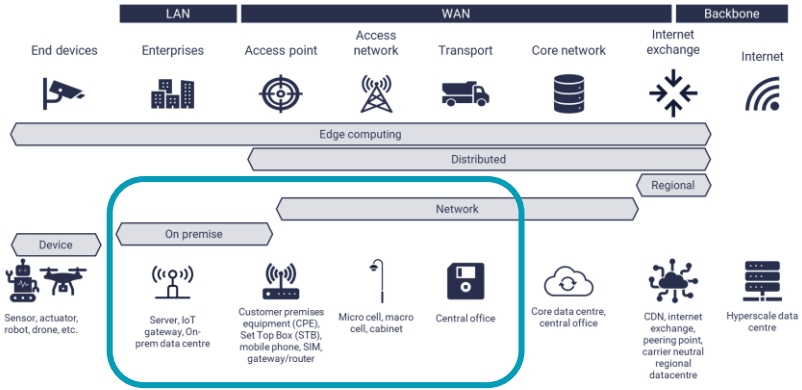
Virtualization

Pluggable server module

Hosting of virtualized network functions such as firewall, IDS/IPS (optional)

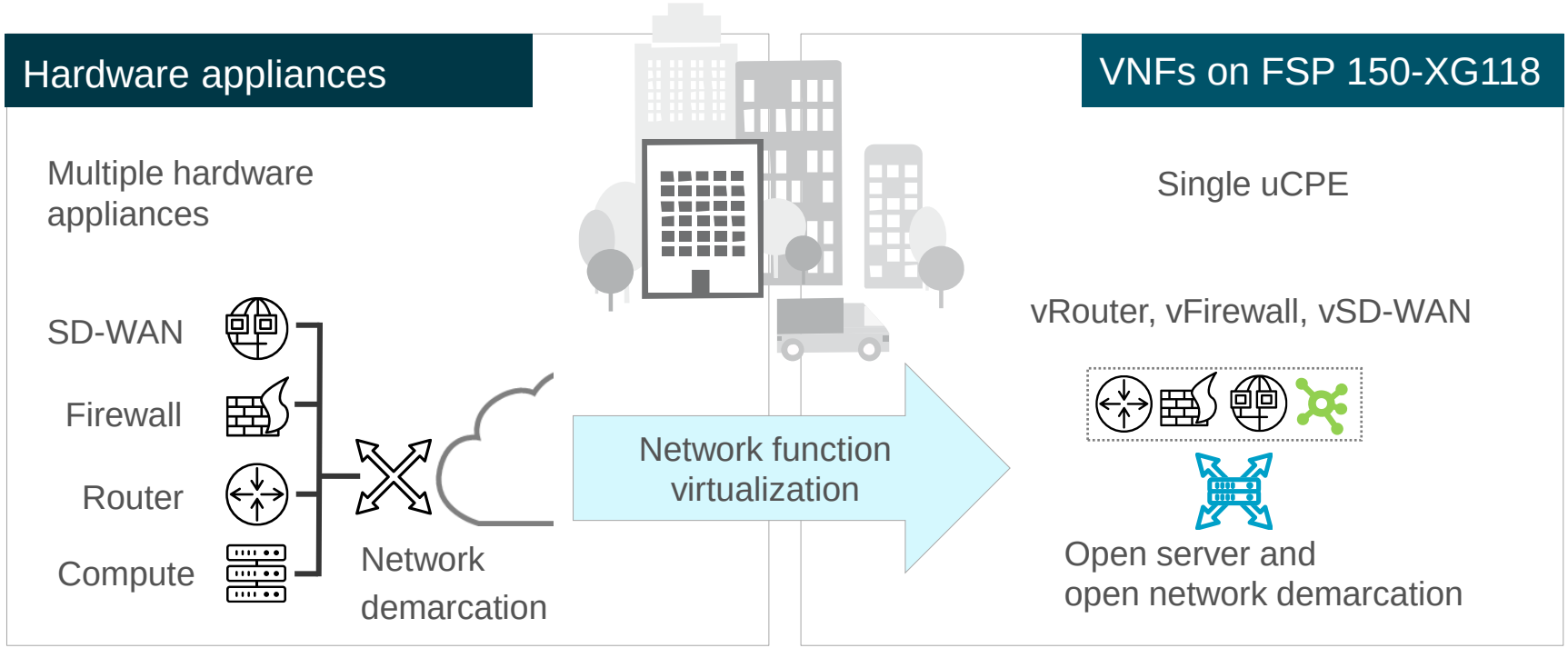
Verified VNFs

Edge cloud growth



Source: STL Partners

Simplify and operationalize with NFV



Ensemble enables choice

MANO

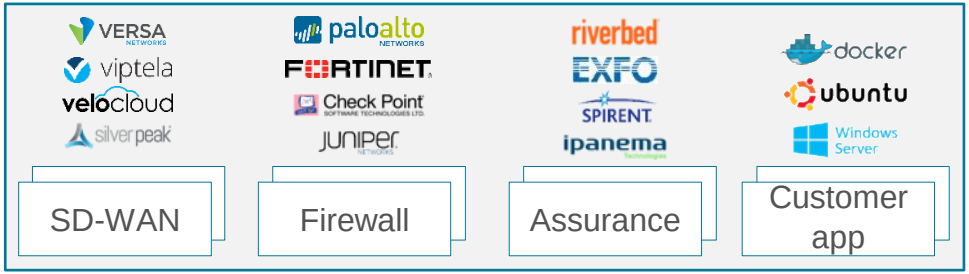
- Management and orchestration

Ensemble Director

Ensemble Orchestrator

VNFs / CNFs

- Customer choice per application Virtual network functions / containerized network functions
- sample of on-boarded VNFs, > 100 partners



Network OS

- Convergence and abstraction layer

Ensemble Connector

Hardware

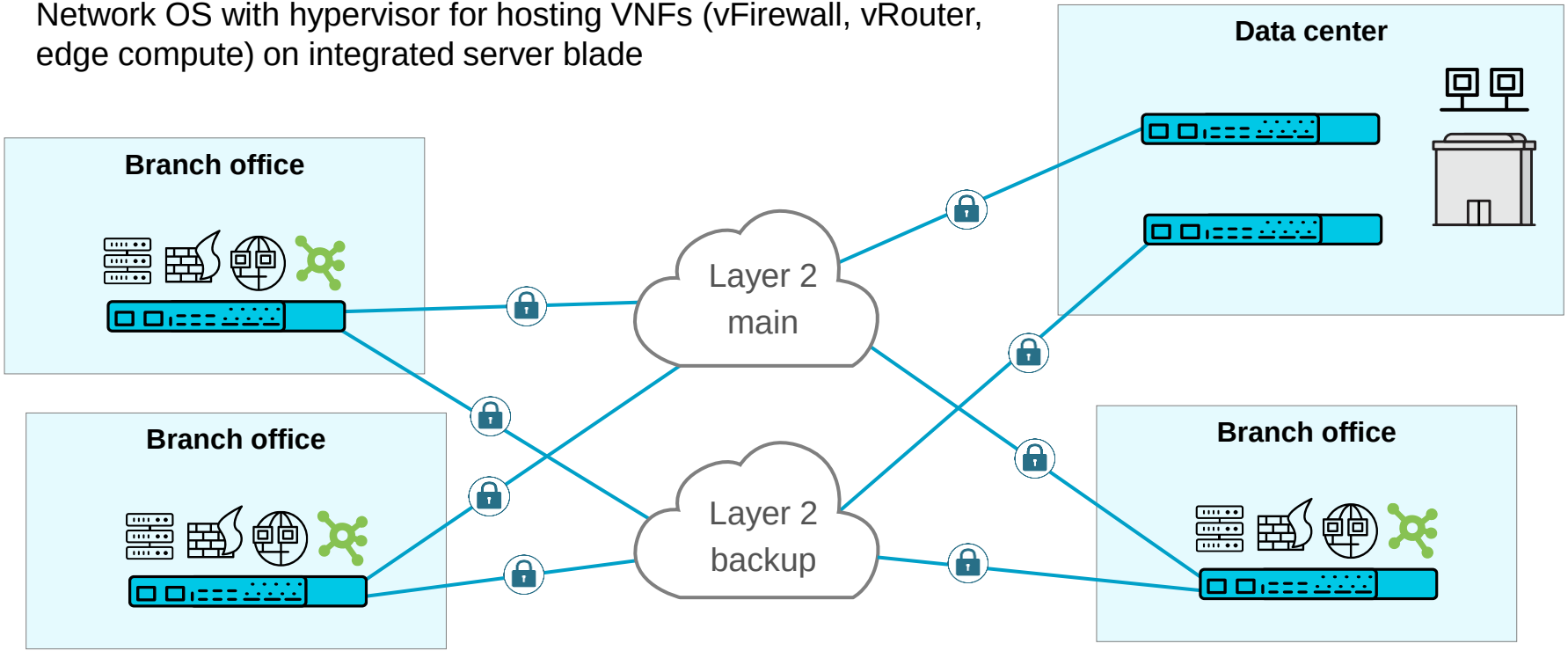
- Adva integrated server or white box

Adva NETWORK SECURITY · DELL · Hewlett Packard Enterprise · Lanner · ADVANTECH · SUPERMICRO · …others

USE CASE

Secure branch connectivity layer 2 + NFV

- Layer 2 MACsec encryption with FSP 150-XG118Pro (CSH)
- Network OS with hypervisor for hosting VNFs (vFirewall, vRouter, edge compute) on integrated server blade



USE CASE

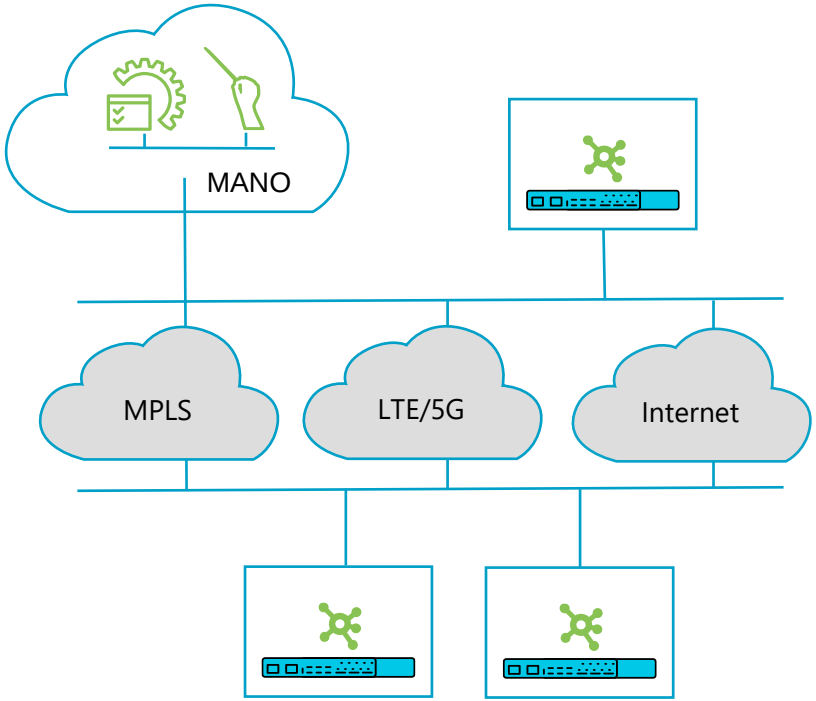
SD-WAN

Drivers

- Cost savings
- Multi-technology: MPLS, Ethernet, LTE/5G, Internet
- Business models e.g. managed service

Benefits

- Automation and zero touch provisioning
- Flexibility by VNFs
- Open, multi-vendor architecture
- Secure hosting with protected connectivity



USE CASE

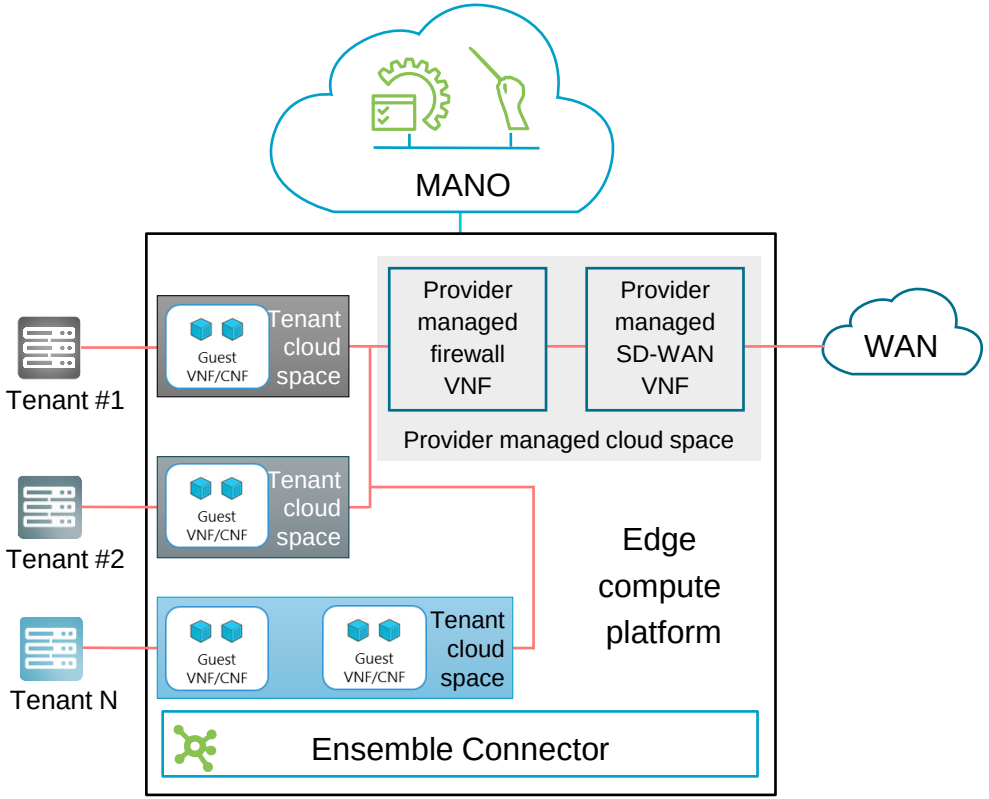
Edge compute

Drivers

- Customer applications use spare edge compute capacity
- Multi-tenant, self-managed private workloads in sandbox

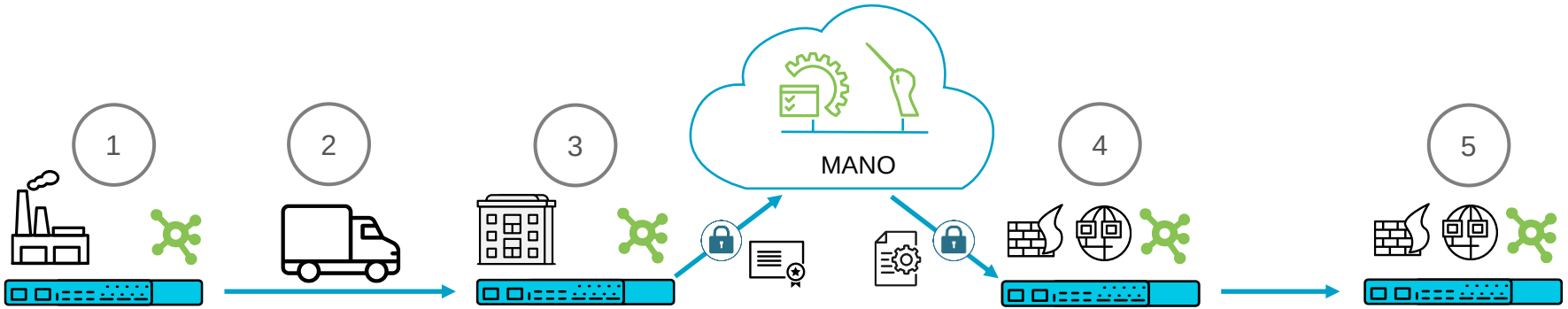
Benefits

- Enhancing services with SD-WAN, firewall, IDS/IPS, etc.
- Secure hosting with protected connectivity



USE CASE

Automated and secure service activation - ZTP



XG118 server is preinstalled with network OS

New service details are configured at MANO

Server sent to customer

Installation

L2 encrypted network connection

Authentication with MANO

Download site configuration data and VNF images from MANO

Initialization, automated testing, **service activation**

Ensemble Director | Ensemble Orchestrator

https://10.72.165.181/gui/smartwan/index.html#/

Ensemble Virtualization Director

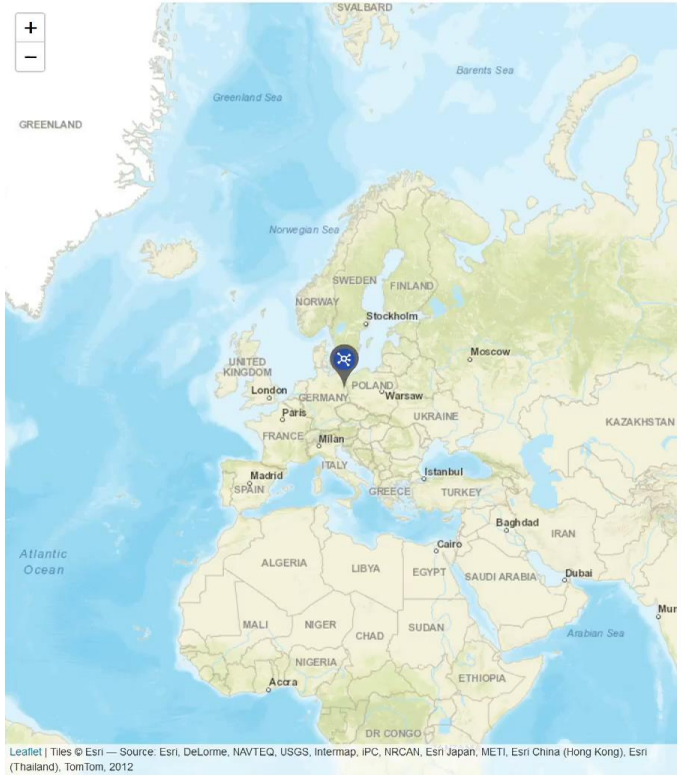
advasecurity.com

Inventory
Fault
Jobs
Orchestrator
Security
Configure
Settings

Network Map

Alarms: All

Host Name



Leaflet | Tiles © Esri — Source: Esri, DeLorme, NAVTEQ, USGS, Intermap, iPC, NRCAN, Esri Japan, METI, Esri China (Hong Kong), Esri (Thailand), TomTom, 2012

0	2	4
Alarms	Sessions	Connectors

ALARMS | EVENTS

REFRESH

No results found

Key take-aways

Quantum-safe encryption for long-term security at the network edge

Protected edge cloud for software-defined networking

Virtual network functions provide agility and the ability to react to future demands

Security solutions for the “Cybernation Deutschland”

Thank you

info@advasecurity.com