Open Source Security Appliance
analisi di tre piattaforme e applicazioni realizzate

Gianluca Peco

INFN CCR Workshop

INDICE

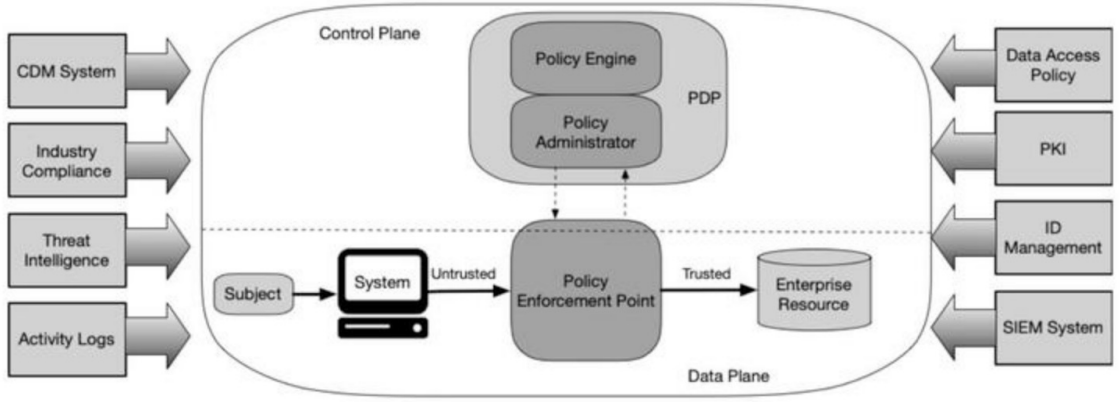
Introduzione

- L’ evoluzione delle applicazioni e dei sistemi, insieme all’introduzione delle tecnologie di virtualizzazione, container, etc. spingono verso le tecnologie che portano alla distribuzione e delocalizzazione delle rirorse.
- IoT, diffusione dei sistemi mobili e delle tecnologie wifi e xG frammentano il perimetro tradizionale luogo deputato al controllo di sicurezza
- Nasce l’esigenza di portare nella periferia dell’impero attività tipicamente svolte nelle province interne o nella capitale

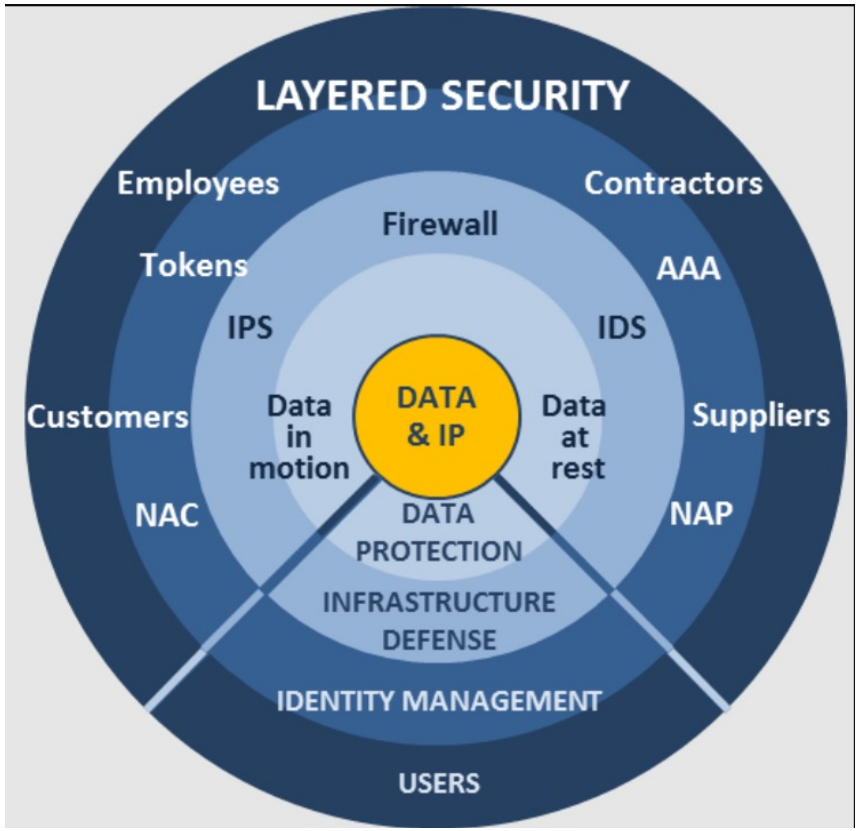
Evoluzione del perimetro

Zero trust architecture

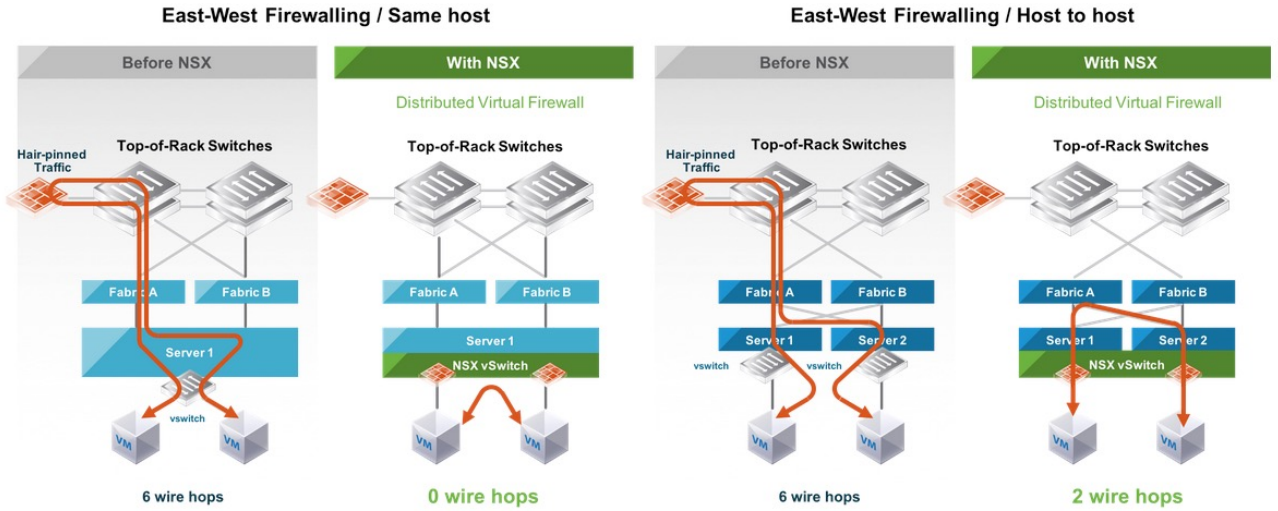
Layered security

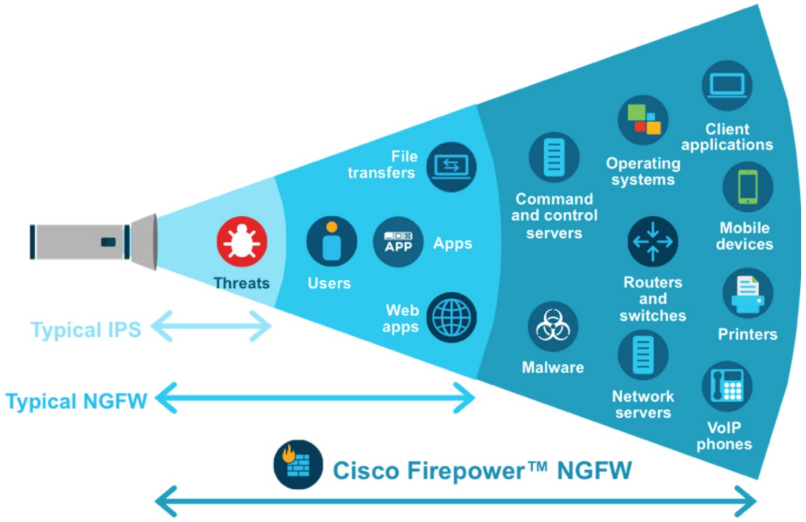


An example of zero trust architecture
Image: NIST

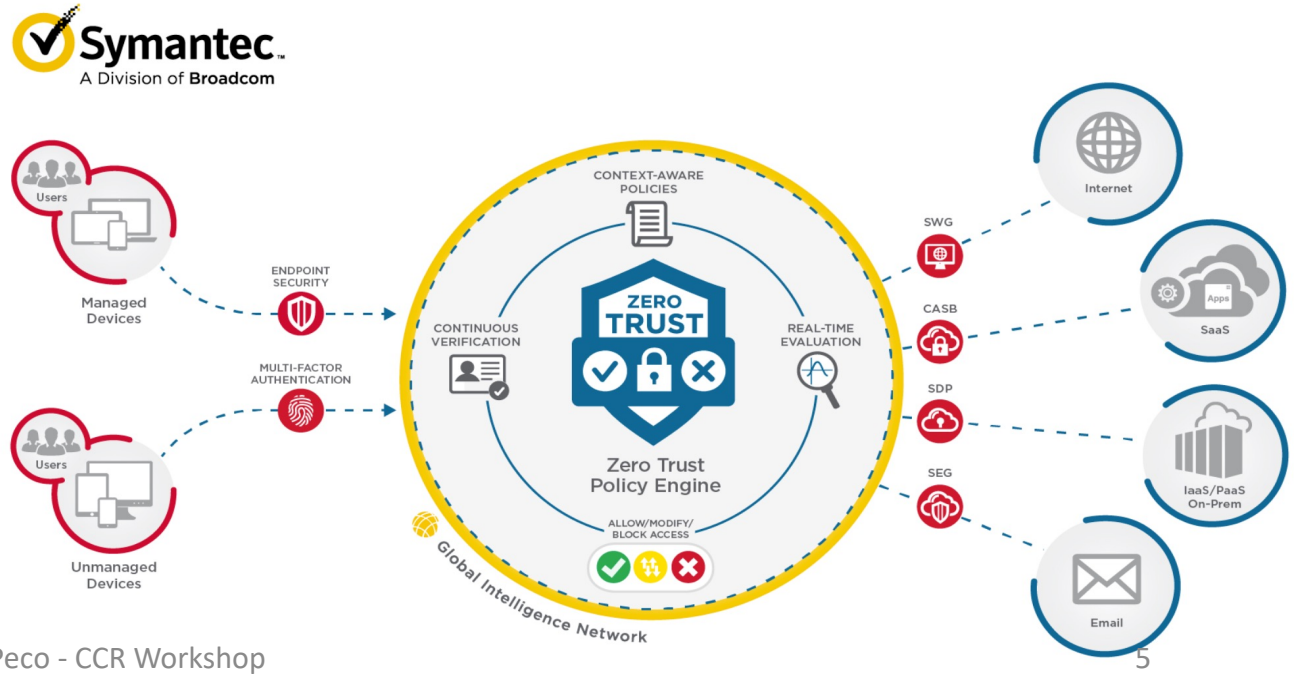


Evoluzione del perimetro Punto di vista di alcuni vendor





Security Visibility Comparison: Cisco Firepower vs. Traditional Firewalls

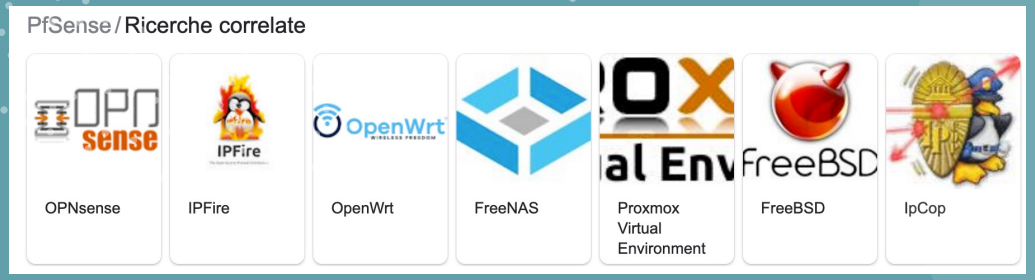


NGFW Opensource: perchè potrebbero essere utili?

- Molte funzioni devono essere “delocalizzate”
  - quelle classiche tradizionalmente centralizzate: Routing, Firewall, Proxy, Nat
  - altre più specifiche: Load Balancer, NIDS, IPS, Logging, Monitor, Flow analysis
- Tali funzioni sono confluite nei NGFW, basati su HW dedicato e dotati di intelligenza fino al livello 7
- La virtualizzazione delle funzionalità di rete (NFV), i costi impegnativi dei NGFW commerciali e relativo corretto dimensionamento in funzione dei flussi di traffico rendono le soluzioni opensource sempre più appetibili

Panorama

- Il Panorama dei sistemi per la network security è ormai ampio anche nel mondo opensource
- Non abbiamo effettuato un'analisi approfondita di quanto disponibile ma ci siamo orientati verso due (tre) oggetti largamente diffusi e con un'ampia comunità di supporto
- PfSense/OPNSense e OpenWrt



Confronto Funzionalità di base OpenWrt PfSense OPNSense

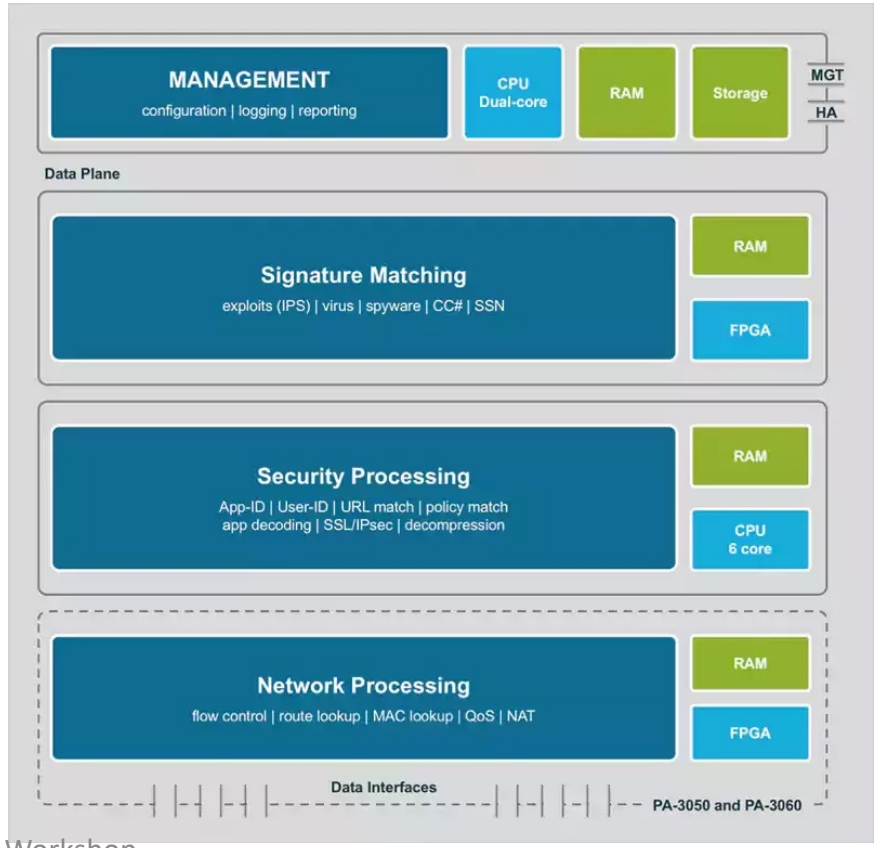
	OpenWRT	PfSense	OPNSenese
Ad blocker	yes	yes	yes
Captive Portal	no	yes	yes
CARP / HA	no	yes	yes
DNS Server	yes	yes	yes
DHCP Server	yes	yes	yes
HTTP Transparent / Web / Reverse Proxy (Squid)	yes	yes	yes
IP / Country block list	yes	yes	no
IDS / IPS	Yes (snort)	yes	yes
Packet Capture / Inspection	no	yes	yes
Port Forwarding	yes	yes	yes
QoS / Rate Limiting	yes	yes	yes
Software Load Balancer (HA Proxy)	no	yes	yes
Traffic Monitoring	Yes (partial)	yes	yes
Traffic Logging, Statistics, and Graphs	Yes (partial)	yes	yes
Traffic Shaping	yes	yes	yes
MultiFactorAuth	no	no	yes
SignatureAV (ClamAV)	yes	yes	yes
App-ID	no	no	yes
VLAN	yes	yes	yes
Wake-on-LAN (WOL)	yes	yes	yes
Website Blocker	no	yes	Yes

Confronto – Data plane/Control plane

Problema delle performace legate al data plane

Commodity HW: control plane e data plane condividono le stesse risorse

Dedicated HW: control plane e data plane utilizzano risorse ad alte prestazioni dedicate (FPGA o ASIC)



Confronto costi commodity HW (dati di targa)

Confronto tra alcuni sistemi commerciali e opensource appliance con taglio privo di FPGA nel data plane e OpenWrt su SoC hardware commodity

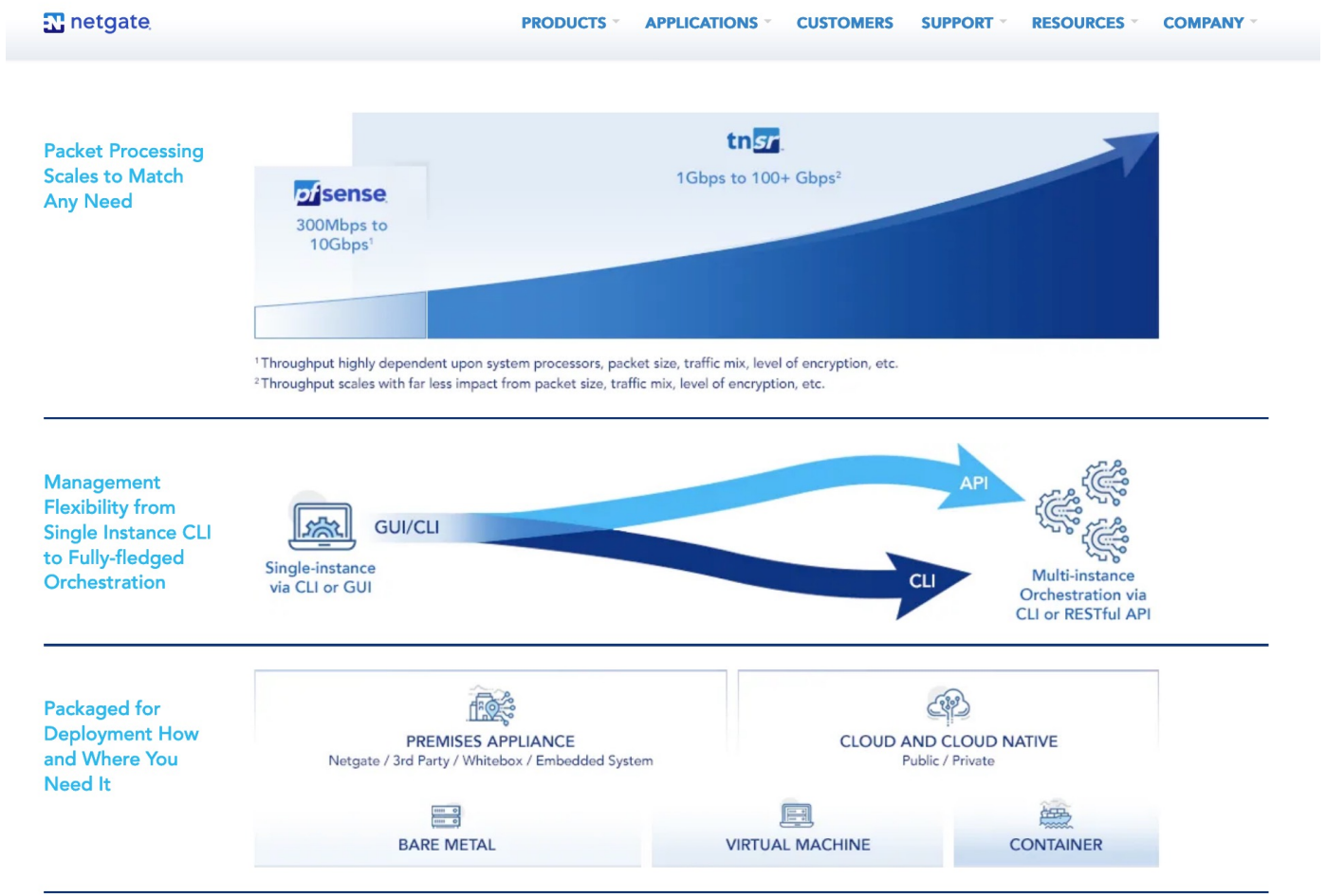
Tipologia	Max Troughput VPN (Gbit/s)	Max Troughput Threath (Gbit/s)	Max Troughput Fw (Gbit/s)	Costo Threath x Gbit/s	Costo Annuale x Gbit/s signature	Costo totale annuo su 5 anni
Free SW su VM	0.3	1	3			
Free SW su bare metal	0.3	1	3			
NGFW 0 HW OpenSource	1	1	10	$1,199	$0	$240
NGFW vendor-1 HW	0.4	0.8	4	$3,750	$1,625	$2,375
NGFW vendor-2 HW	1.3	0.9	3	$4,992	$3,333	$4,332
NGFW vendor-3 HW	1	1	10	$2,940	$3,575	$4,163
NGFW (OpenWrt) su Linksys AC1900	0.1	0.1	1	$1,500	$0	$300

Altre considerazioni su costi e performance

- Ovviamente quando si passa alla NFV i vantaggi dei processori hw dedicati vengono meno rendendo le prestazioni paragonabili
- Incidono maggiormente:
  - le integrazioni con i vari control plane dei sistemi di virtualizzazione o dei cloud provider
  - l'utilizzo di signature e regole free o community based
  - la rapidita' nell'identificare zero day attack

Funzionalità PfSense

- PfSense (Netgate) identifica la sua nuova piattaforma denominata Plus come possible concorrente anche nella fascia Nx10Gb con la disponibiltà di orchestrazione e gestibile su VM e container



OPNSense

- Fork di PfSense a sua volta fork di M0n0wall derivato da FreeBSD
- Basato su distro ISO con aggiornamenti trimestrali
- Ricche funzionalità di base
- Plugin community disponibili
- Possibilità di crearsi plugin personalizzati

OpenWrt

https://en.wikipedia.org/wiki/OpenWrt

- OpenWrt (from open wireless router) is an open-source project for embedded operating systems based on Linux, primarily used on embedded devices to route network traffic. The main components are Linux, util-linux, musl, and BusyBox. All components have been optimized to be small enough to fit into the limited storage and memory available in home routers.
- OpenWrt is configured using a command-line interface (ash shell) or a web interface (LuCI). There are about 3500 optional software packages available for installation via the opkg package management system.
- OpenWrt can run on various types of devices, including CPE routers, residential gateways, smartphones, pocket computers (e.g. Ben NanoNote). It is also possible to run OpenWrt on personal computers and laptops, which are most commonly based on the x86 architecture.

Applicazioni realizzate

- OpenVPN concentrator (Presidenza) - OPNSense
  - User AuthN\AuthZ locale, Split Tunnel model, portale utente per la gestione delle credenziali e delle configurazioni del client, syslog e alert verso SIEM, VM
- Captive Portal (LNF-Presid-Bologna) - OPNSense
  - User AuthN\AuthZ remota, integrazione con infrastruttura wifi esistente basata su WAC e CAPWAP tunnel
- NGFW laboratorio (Bologna) - OPNSense
- Appliance remote office (Home – Road Warrior) - OpenWrt
  - Accesso ADSL , UPnP, Proxy direct e reverse, SyncThing USB disk, ToR network, VPN client, monitor della rete
- Nuovo TripKit con Hw dedicato (CNAF/Netgroup) - PfSense

To do

- Misure di prestazioni su hardware dedicato
- Misure di prestazioni su sistemi virtuali
- Confronto tra sistemi diversi a parità di funzionalità
- Integrazione con I sistemi di Virtualizzazione e Cloud

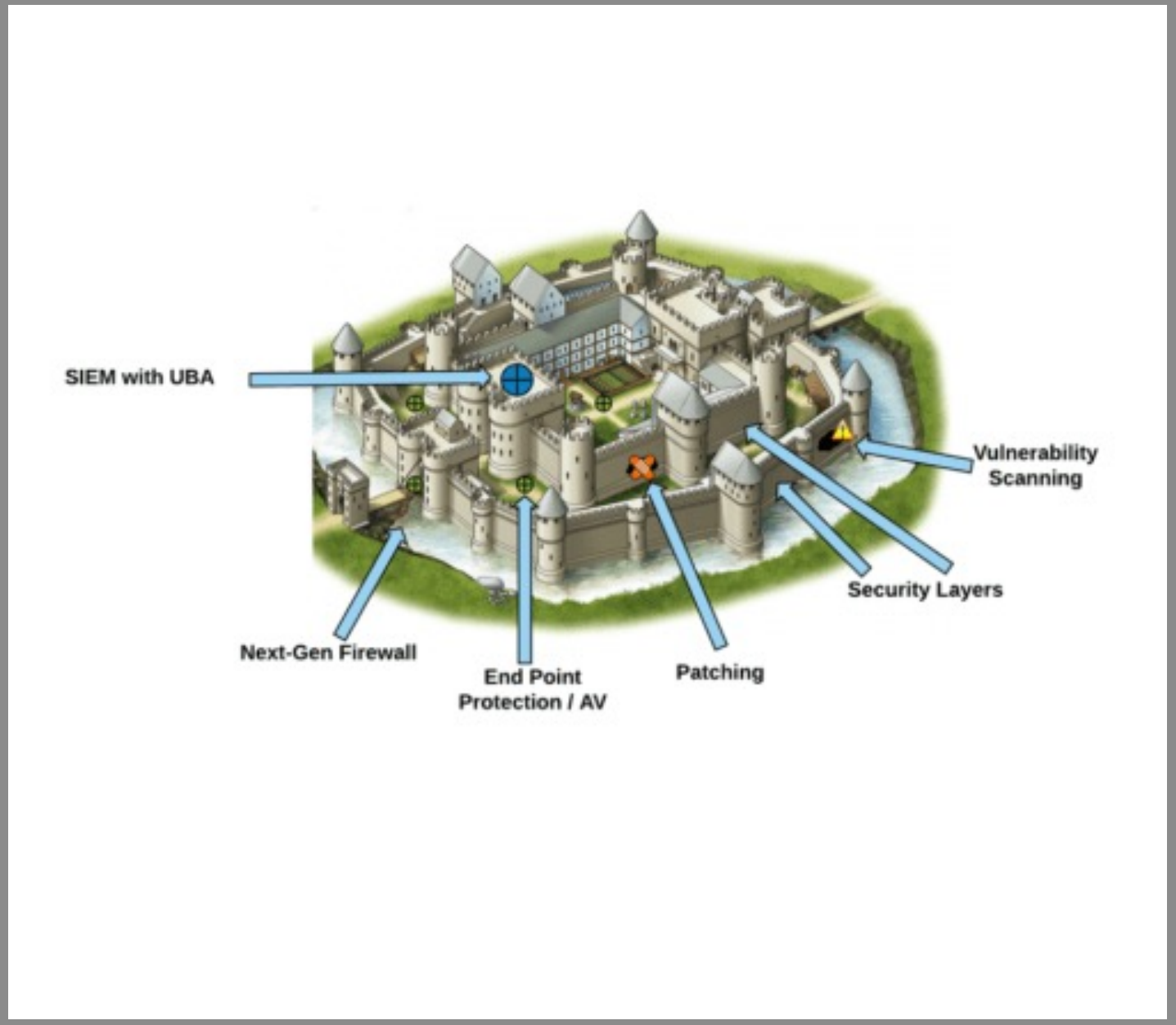
demo

OpenVPN

OpenWrt

The end

https://it.wikipedia.org/wiki/Palmanova



BUILDING A CYBERSECURITY KINGDOM

Cavalry = Endpoint Protection. Protects your local endpoints, such as computers and servers, with definition-based and behavior-based anti-virus, drive encryption, and device management. The cavalry protects the kingdom and its people from bad actors.

Drawbridge = VPN Connection. Allows off-network visitors to safely and securely access your business. Think of it as having a secret password for lowering the drawbridge to enter the castle.

Castle Wall = Firewall. Prevents incoming security threats with automatic remediation, sandboxing, anti-virus, intrusion prevention, and content filtering. The castle wall deters and catches threats.

Gatehouse = Multifactor Authentication. MFA provides an additional layer of security by verifying your identity using more than one method. For example, MFA prevents unwanted access to critical information by verifying usernames and passwords with an additional secret code, usually delivered through a mobile device or notification. The Gatehouse provides an extra layer of security when accessing assets (like files or software programs) that are on your network or in the cloud.

Guardian = EDR. Endpoint Detection and Response (EDR) monitors your entire business for suspicious behavior in real-time to detect cyberattacks, isolate infected machines, alert administrators, and remove cyberthreats. Like an omniscient guardian, EDR recognizes advanced, sneaky attacks and shuts them down before they attack your business, anywhere an asset is located.

Library = User Education. Teaches users about safe IT practices, such as internet, email, and peripheral device usage; password management; and data control. User educations also includes testing to ensure students retain what they have learned.

Clerks = Security Information and Event Management (SIEM). Records and stores your system's log files for use if a cyberattack occurs. Think of SIM like clerks recording a history of the castle's happenings for future scholars to reference.

Royal Archives = Data Backup. Whether you're on-premise or working from home, company files are stored, up-to-date, and protected.

Guards = Anti-Virus. Anti-virus keeps your business safe from known cybersecurity threats and bad actors. The guards need to be informed or see something illegal happening before responding.

Masons = Patching. Maintains your hardware, software, operating system, and security with regular code updates as new threats and vulnerabilities are detected. Patching works like masons who identify and repair cracks, holes, and other weak points in the castle's walls.

Moat = Email Security. Automatically scans email for spam, unlawful interception, phishing, malicious attachments. Encrypts outbound emails containing sensitive data and employs advanced threat protection (ATP) to identify bad actors based on their behavior. The moat ensures only safe traffic enters and exits the castle.

HIGHTOUCH TECHNOLOGIES