Architecture Zero Trust

Simon Bellemare

Victor De Luca

24 novembre 2022

Agenda

1. À propos de Simon et Victor (10 min each)
2. L’architecture d’entreprise (15 min)
3. L’architecture Zero Trust (25 min)
4. Ce que l’avenir nous réserve (5 min)
5. Questions (15 min)

1. À propos de Simon et Victor

Simon

- Baccalauréat en génie électrique à Polytechnique Montréal. Promotion 139.
  - Concentration en aérospatial (aucunement reliée à ce que je fais aujourd'hui)
- Team Lead de l'équipe électrique de la Formule SAE électrique
- Stages chez Bombardier Transport et Nova Bus
- Premier emploi : ingénieur de réseaux chez Cisco à Toronto
  - Programme de formation CSAP
- Deuxième emploi : ingénieur en cybersécurité chez Zscaler
- Ingénieur de ventes → vente technique
  - Beaucoup de préjugés initialement
  - Rôle mariant business et technique

https://www.linkedin.com/in/simonbellemare/

Victor

- Joined the CAF 9 years ago and started my career in security.
  - Gained interest in cyber security during the 2015 conflict in Ukraine.
- B.Sc. en Cybersecurité à Polytechnique
- M.Eng in Information Systems Security.
- Cybersecurity for a bank, a consulting firm and now, Zscaler.
- Primarily focused on helping organizations protect critical systems and sensitive information from attackers.
- Fan of MITRE ATT&CK & Zero Trust Architecture.

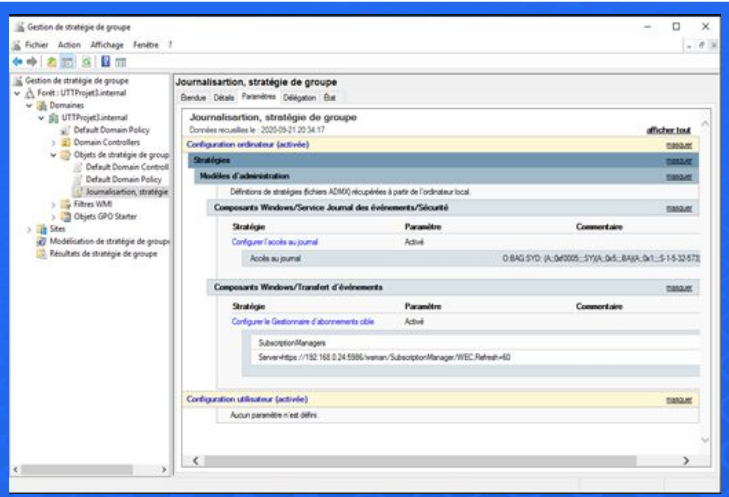
https://www.linkedin.com/in/victordeluca/

2. L’architecture d’entreprise

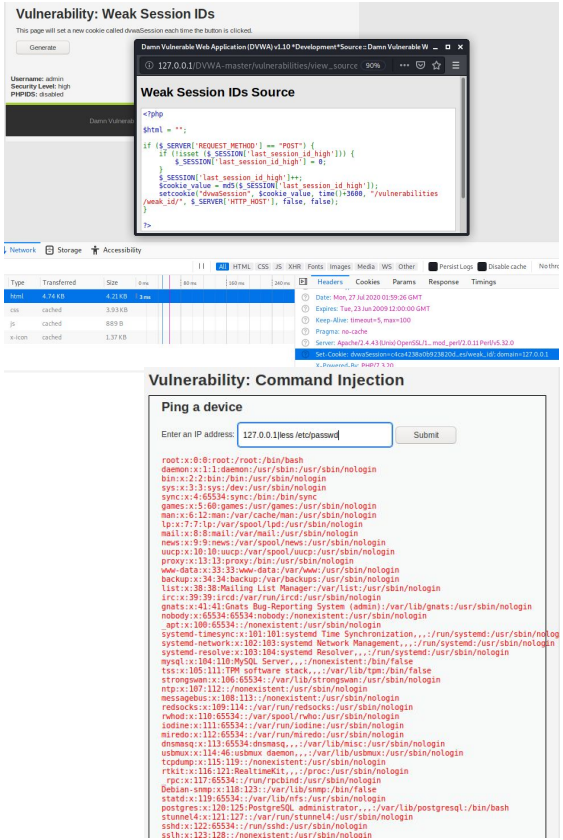
Ce que vous voyez (ou pas) dans vos classes (selon notre mémoire)

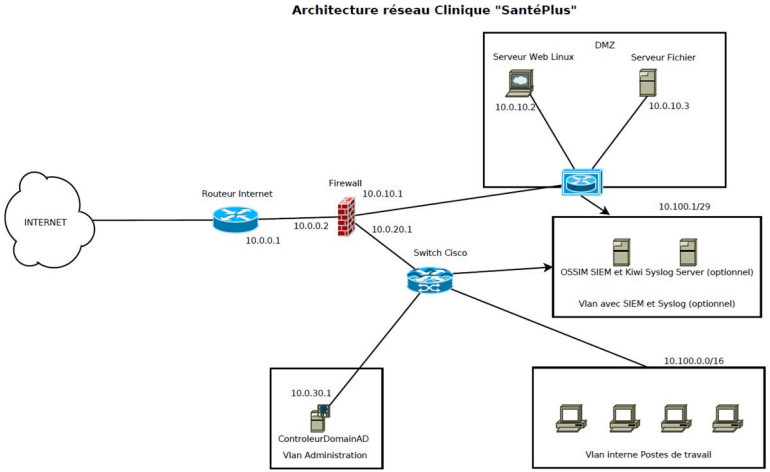
- Iptables
- Serveur syslog
- Switch Cisco
- Configuration manuelle des serveurs
- Peu de SaaS
- Identité locale
- Les standards de sécurité
- Gouvernance, risques et contrôles

```
# Generated by iptables-save v1.8.4 on Sun Sep 20 14:04:18 2020
*filter
:INPUT ACCEPT [4871:7976755]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [4435:536985]
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 443 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 389 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 636 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 7777 -j ACCEPT
-A INPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 3389 -j ACCEPT
-A INPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 3389 -j ACCEPT
-A OUTPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -s 192.168.0.0/24 -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 53 -j ACCEPT
-A OUTPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 389 -j ACCEPT
-A OUTPUT -s 192.168.0.0/24 -p tcp -m tcp --dport 636 -j ACCEPT
-A OUTPUT -d 192.168.0.0/24 -p tcp -m tcp --dport 636 -j ACCEPT
```



Ce que vous voyez (ou pas) dans vos classes (selon notre mémoire)



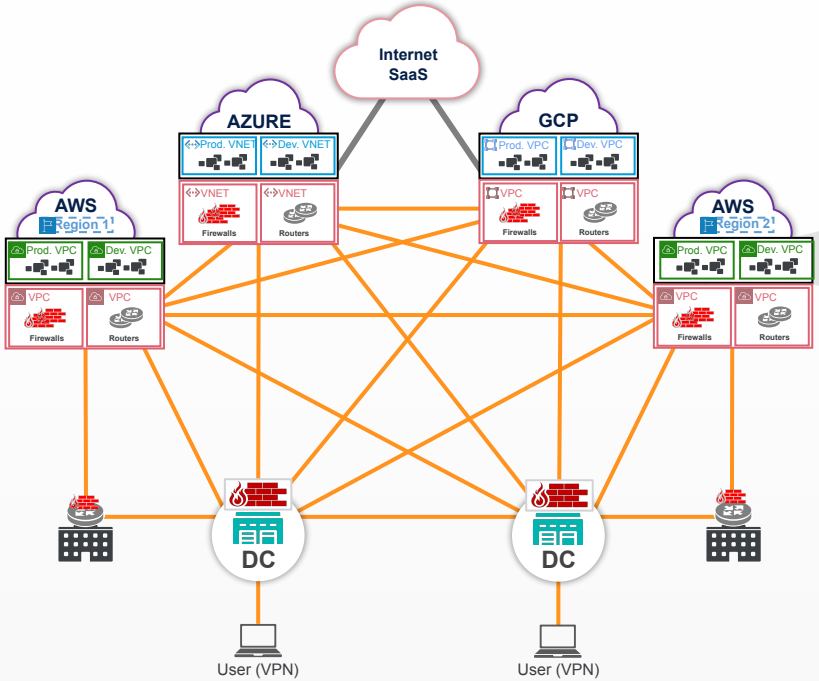



```
String identifiant = request.getParameter("identifiant");
String motDePasse = request.getParameter("motDePasse");
Class.forName("com.mysql.jdbc.Driver");
Connection con = (Connection)
```

```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#################
#### MODULES ####
#################

module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

###########################
#### GLOBAL DIRECTIVES ####
###########################

#
# Use traditional timestamp format.
# To enable high precision timestamps, comment out the following line.
#
$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat

# Filter duplicated messages
$RepeatedMsgReduction on

#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
#
#regle pour forward vers OSSIM
#
*.* @@192.168.0.35:514
#
$IncludeConfig /etc/rsyslog.d/*.conf
```

Extending legacy network and security to the public cloud

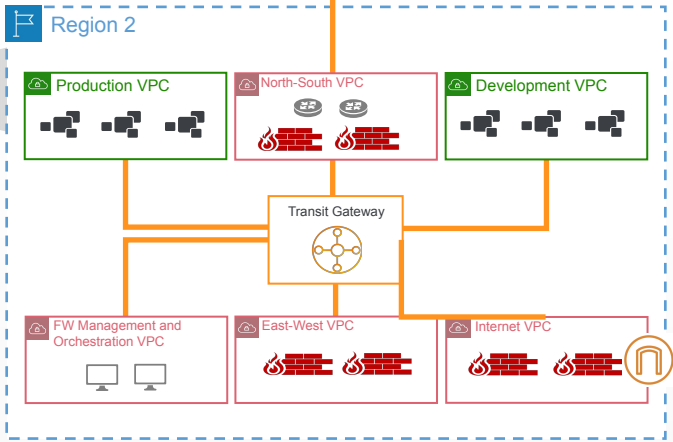
Extend the Corporate WAN to the Cloud
A mesh of site-to-site VPNs (Routable Network)



Increased the Risk of Lateral Threat Movement
A single infected workload can infect everything on the network

Increases the Internet Attack Surface
Every internet facing firewalls can be discovered and exploited

Workload Communications to other AWS Regions, Data Centers, IaaS, Paas(Azure, GCP)



East-West Workload to Workload Communication

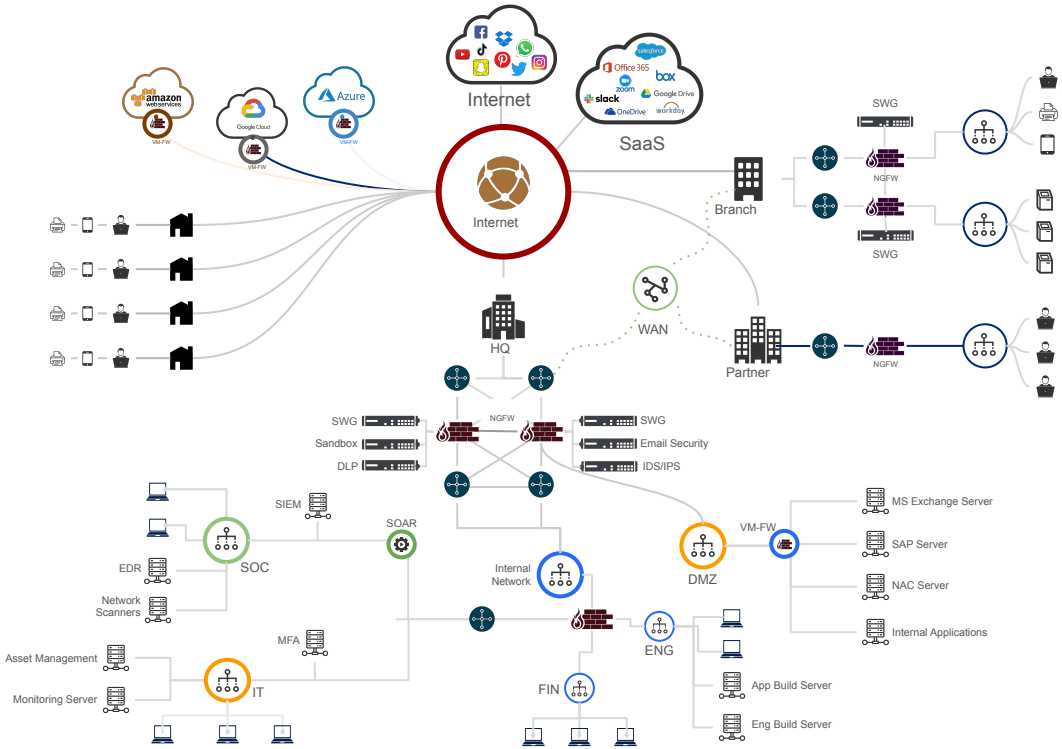
Workload to Internet Communication

FW VM bloat (+ squid proxies for cyber threat and data protection)

Routing complexity (IP overlap/conflict)

Unmanageably Complex and Expensive
Replicating DMZs across clouds, regions and zones
High cost of connecting everything with a mesh network

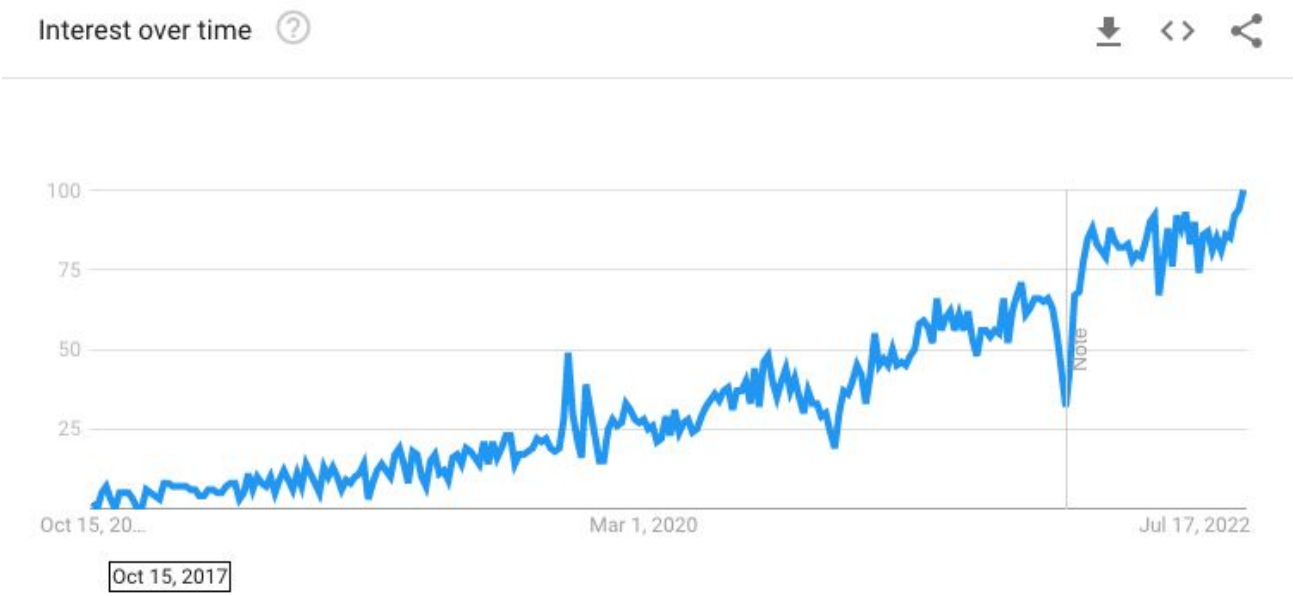
Architecture de sécurité d'entreprise



Hub & Spoke Networks + Castle & Moat Security

3. L’architecture Zero Trust

An Overview of Zero Trust



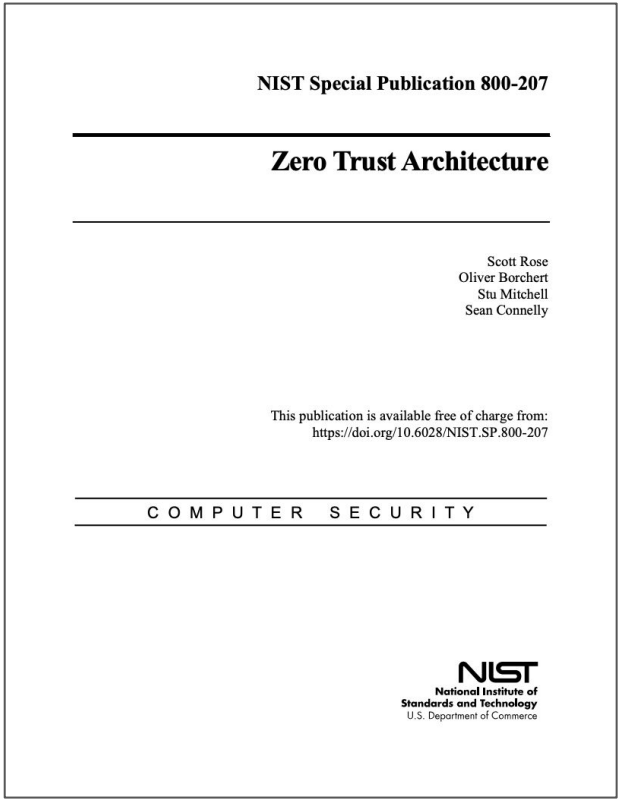
https://trends.google.com/trends/explore?date=today%205-y&q=%22zero%20trust%22

An Overview of Zero Trust

NIST defines the underlying principle of a zero trust architecture as

"**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)."

It's an overhaul of the old proverb "Never trust. Always verify."



NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

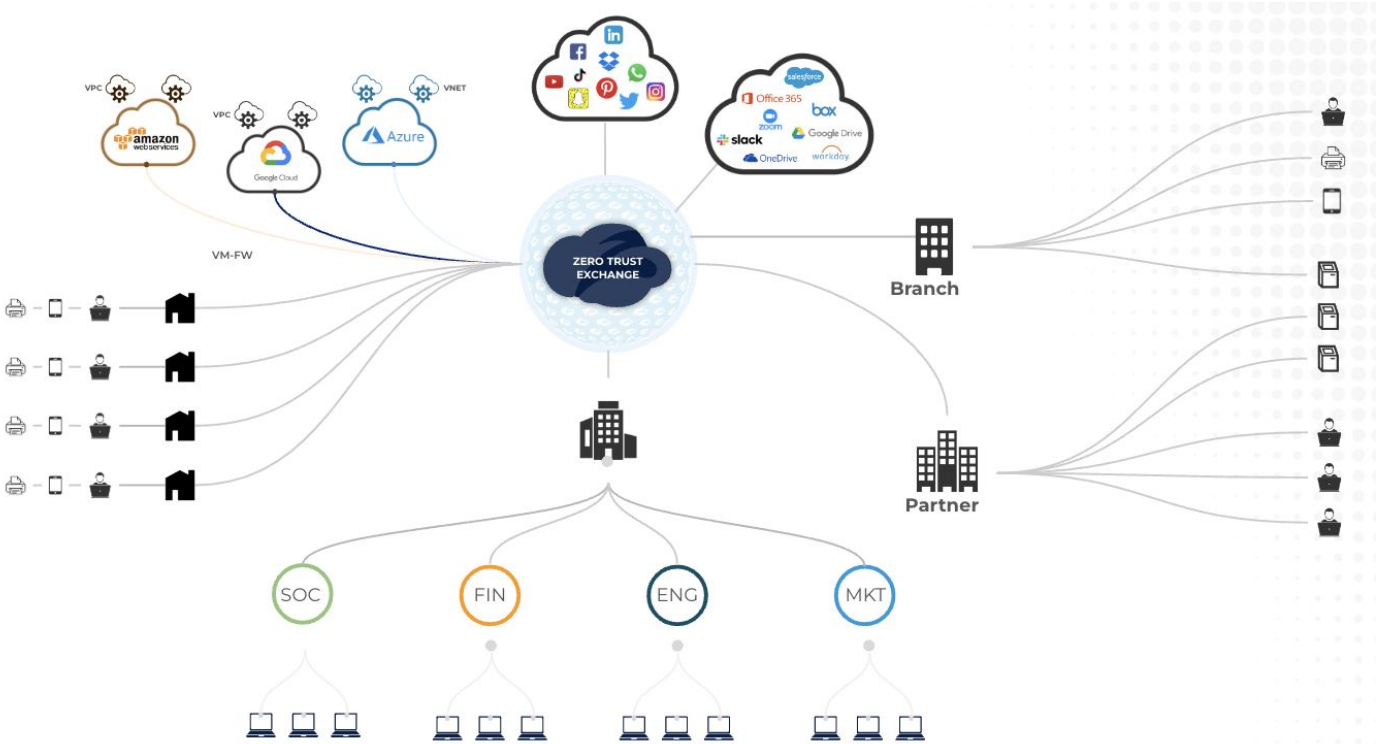
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

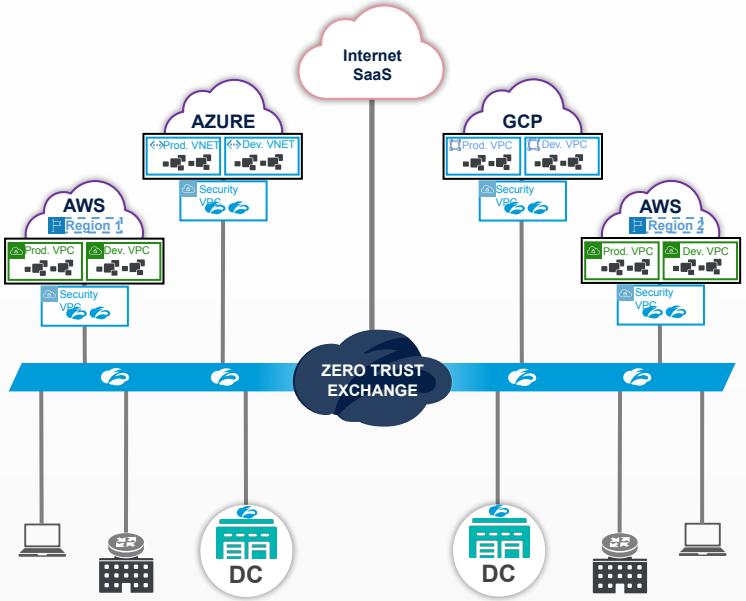
https://doi.org/10.6028/NIST.SP.800-207

Migration des applications vers le cloud - impact sur l'architecture



With Zero Trust Cloud Connectivity, you don't extend your WAN

Secure Workload-to-Workload Communications over any network (Non-Routable Network)



- **Eliminates the Risk of Lateral Threat Movement**
  Native workload to workload segmentation over any network
- **Eliminates the Internet Attack Surface**
  Apps are not discoverable on the internet
- **Eliminates VM bloat (FWs, squid proxies, routing)**
- **Eliminates routing complexity (no IP overlap issues)**
- **Reduces operational complexity and cost**
  Eliminates the need for virtual DMZs and a mesh of site-to-site VPNS

What are some of the principles of Zero Trust Network Architecture?

Designing an architecture with controls in mind is difficult.
Designing an architecture with a ZTNA mindset is easier.

Assume breach mentality

Always assume the attacker is in your network. Because it probably is.

Least privilege access

Provide access based on strong identity and security posture. Not on location.

Reduce attack surface

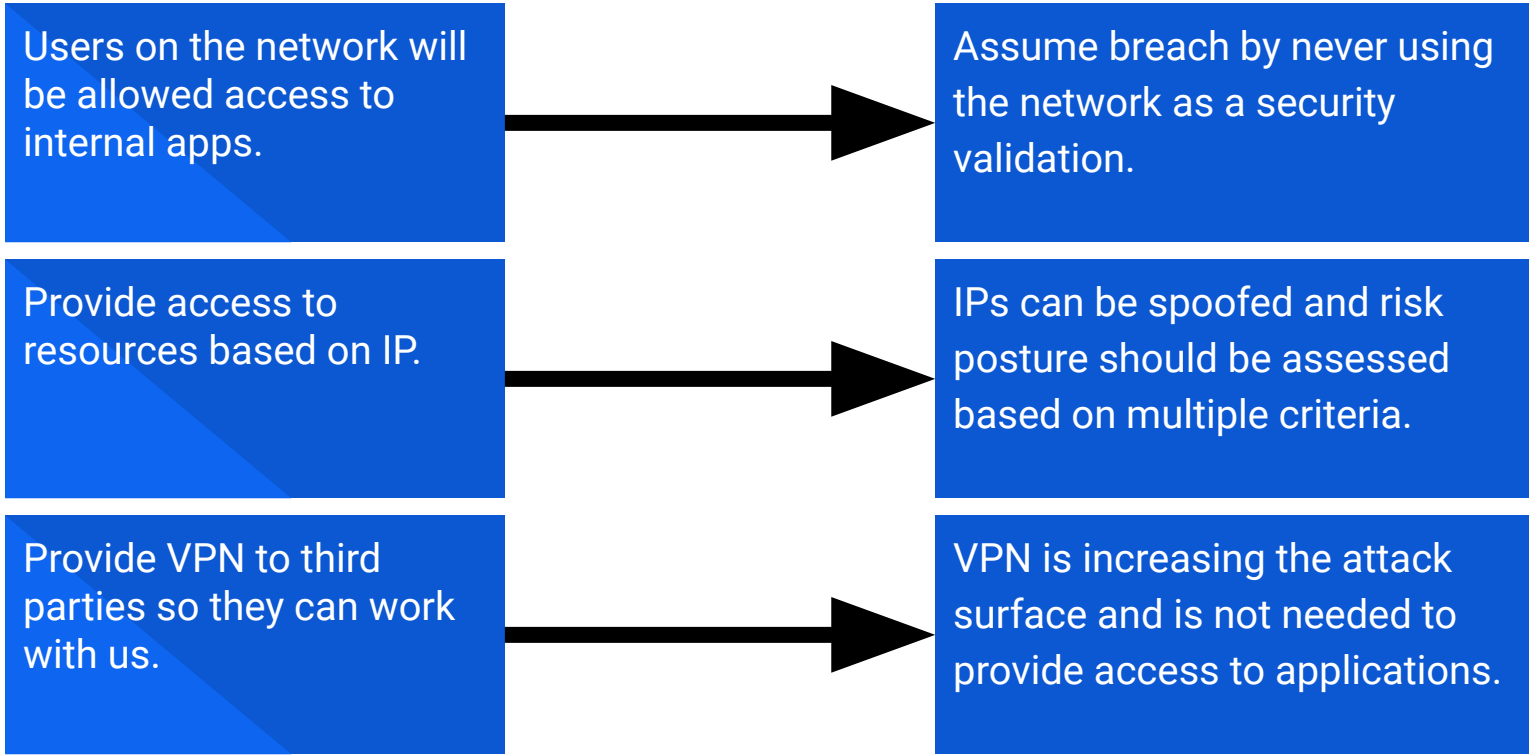
Hackers cannot attack what they cannot see. Reduce your digital footprint.

Assess risk continually

Risk is fluid. Phishing is normal. Users get compromised. Safe yesterday isn't safe today.

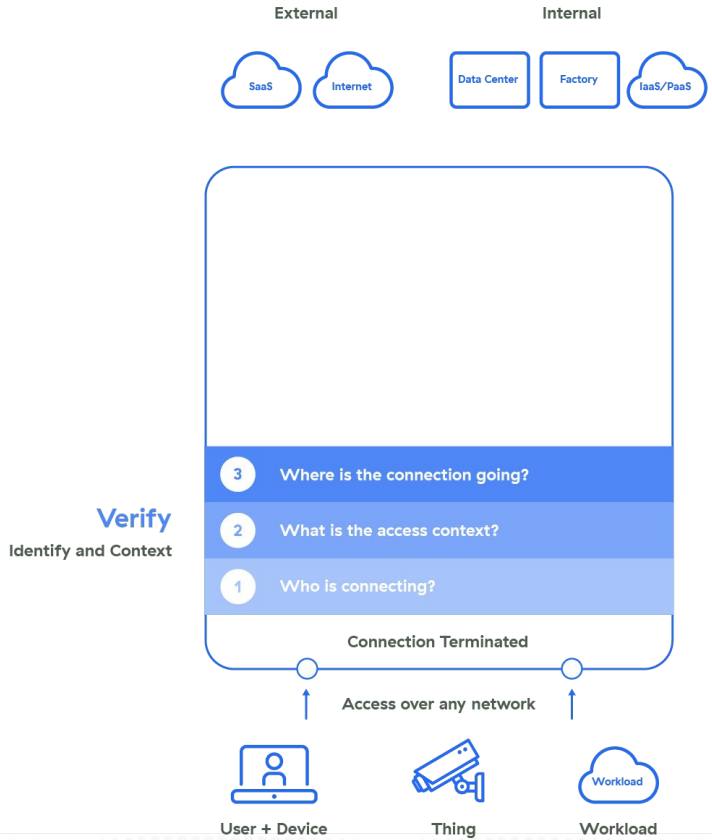
So can you give me a real life example?

Non-ZTNA VS ZTNA Mindset

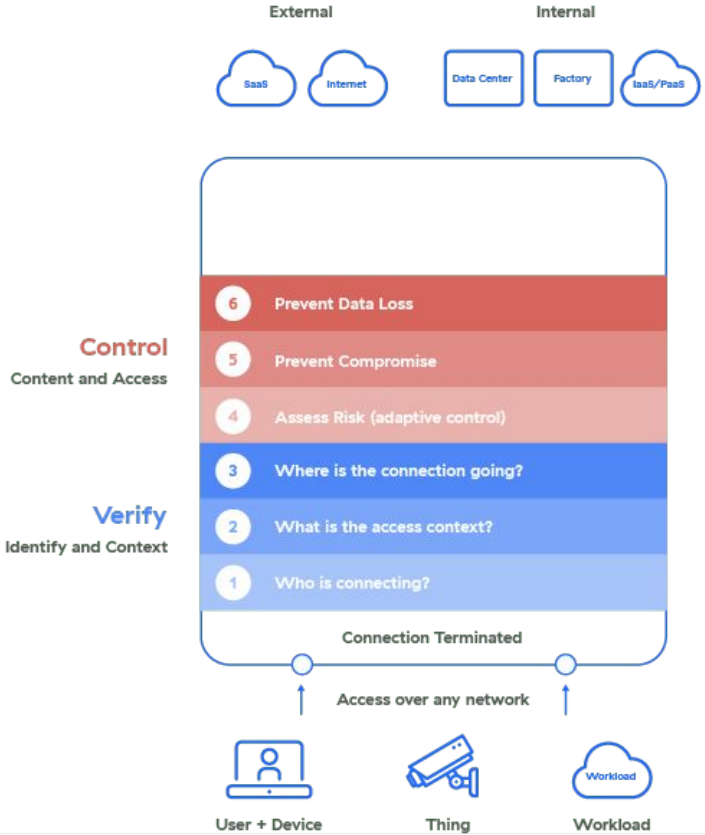


Seven Essentials Elements of a Zero Trust Architecture

Verify identity and context



Control Content and Access



Importance of SSL/TLS Inspection

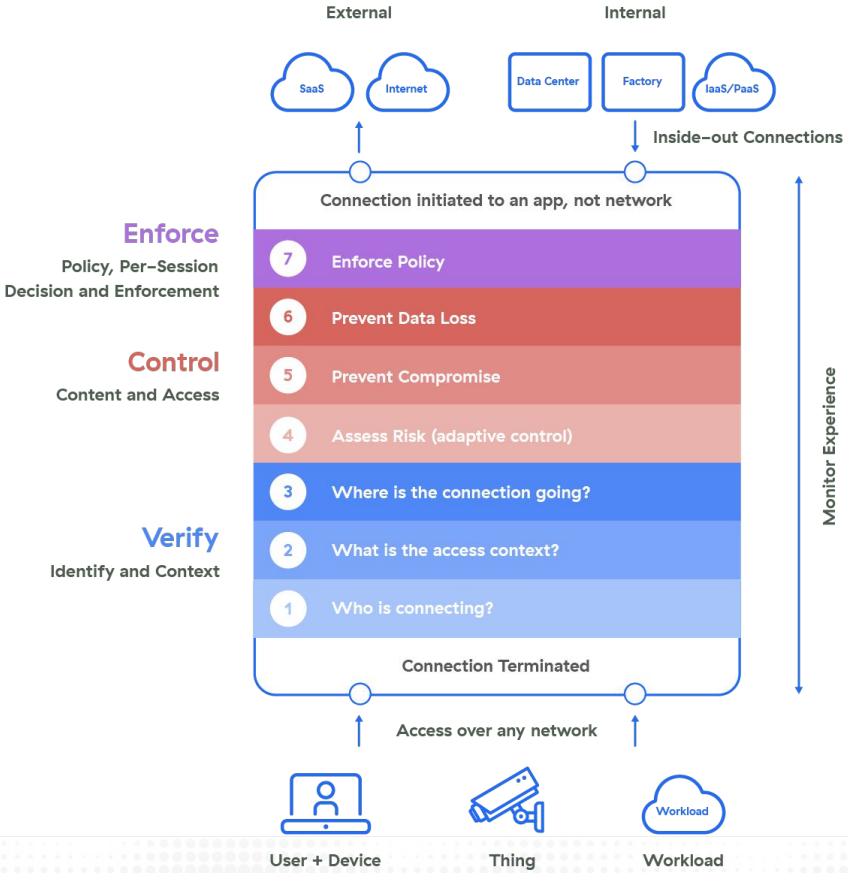
Before

Domain

After

Domain, URL, Req/Res Headers, Req/Res Payloads

Enforce – Policy, Per-Session Decision and Enforcement



Traditional Network Controls

Figure 60: Traditional network controls preserve visibility so anyone can see all of the houses and doors.

Zero Trust Network Access

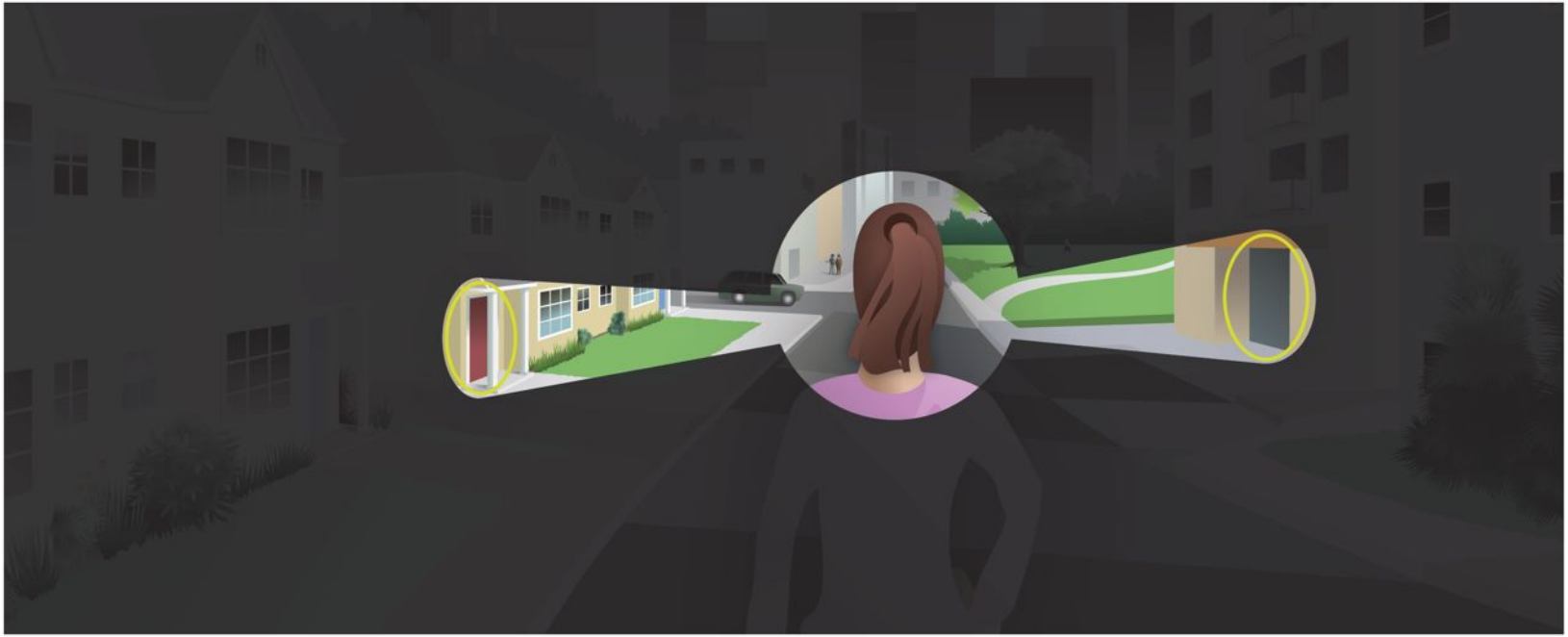


Figure 62: Ensuring users can access what they need and nothing more is key to zero trust.

4. Ce que l’avenir nous réserve

Les changements au niveau de la connectivité

Connectivité 5G+ sur chaque appareil

Disparition du Wi-Fi?

Disparition des commutateurs?

Disparition des routeurs?

Disparitions des coupe-feux?

Sources pour en lire d’avantage:

https://www.techtarget.com/searchnetworking/tip/How-5G-deployment-will-affect-enterprise-network-hardware-software

https://www.lightreading.com/mobile/5g/will-5g-kill-wifi-qualcomm-thinks-it-just-might/d/d-id/749618

5. Questions

Rejoignez le Discord de PolyCyber

Connectez-vous sur LinkedIn

https://www.linkedin.com/in/simonbellemare/

https://www.linkedin.com/in/victordeluca/