Network Security Overview

Lubos Kuzma
Blue Warden Consulting Ltd.

March 12, 2024

Agenda

- **Perimeter Security**
  - Network Segmentation
  - Encryption
  - Remote Access
  - Intrusion Detection/Prevention Systems (IDS/IPS)
  - Vulnerability Management
- **Zero Trust Security**
  - Principles
  - Zero Trust Network Access

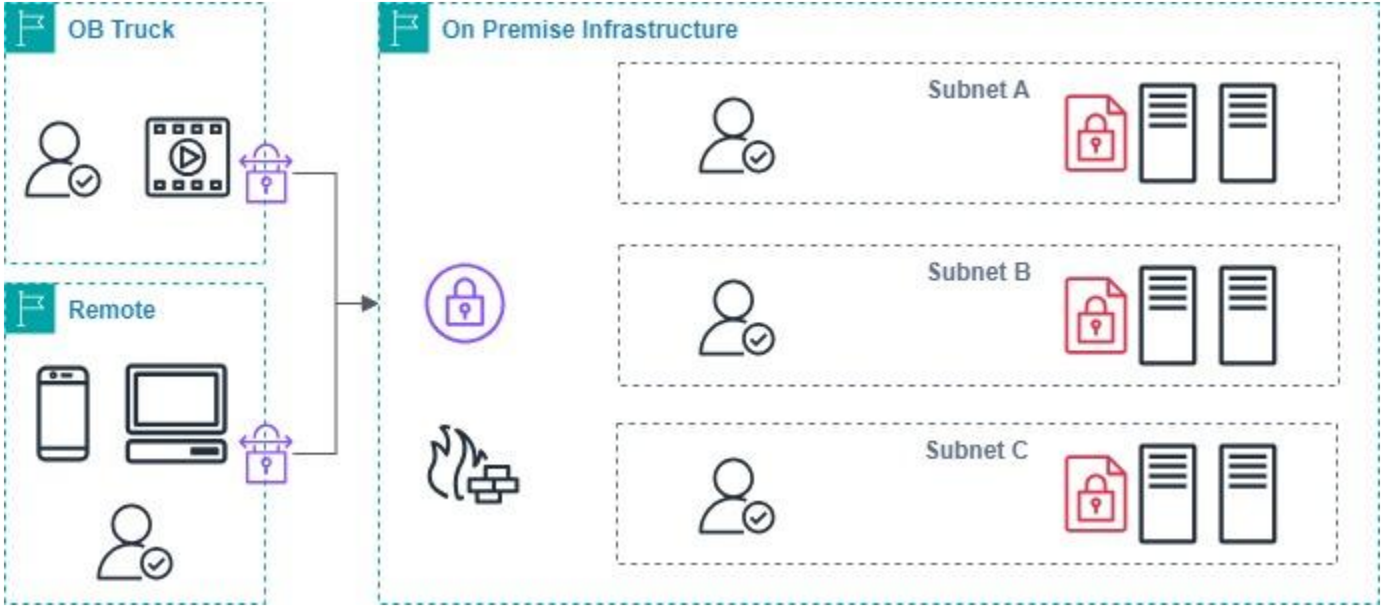
Perimeter Security

Traditional approach to security.

BLUE WARDEN
CONSULTING

Network Security Overview

Infrastructure

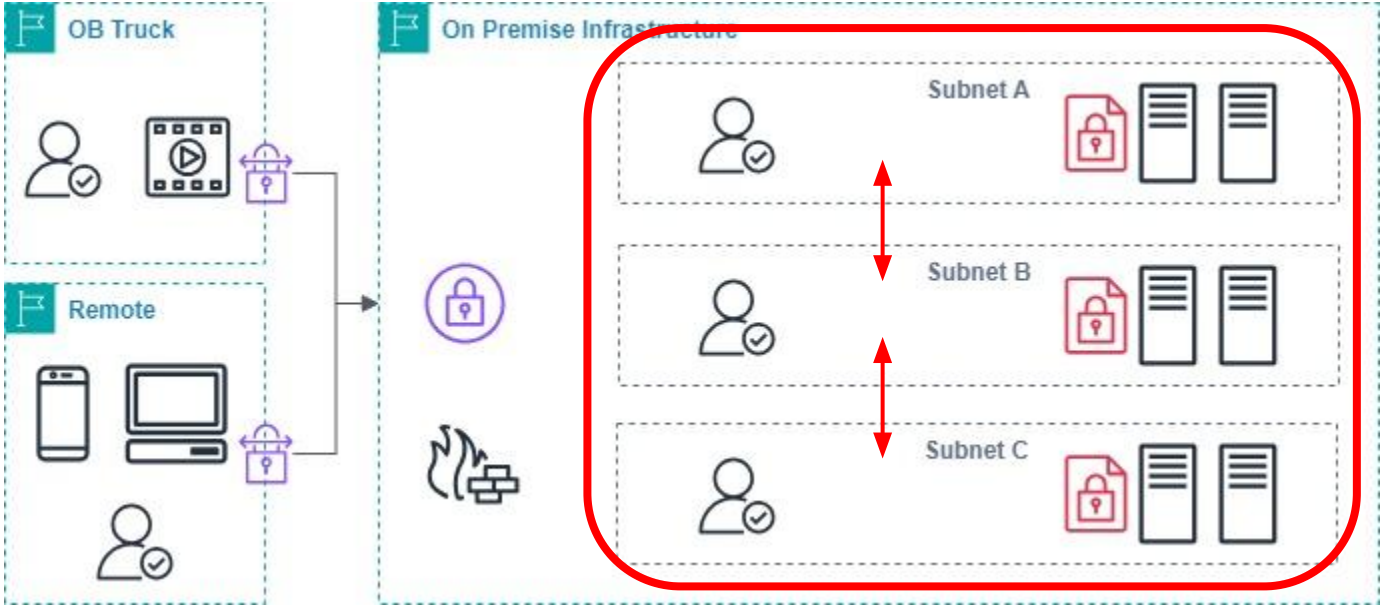


Network Segmentation

“Network Segmentation” is a specific network design based on separating large network into physical or logical units (Subnets and/or VLANs) that have limited, tightly controlled or no access between them.

Using:
- Subnetting
- VLANs
- Software Defined Networking (SDN)

Network Segmentation



Network Segmentation

Segmentation minimizes the security risk by creating multi-layer approach and making lateral movement harder (or ideally impossible) for attackers

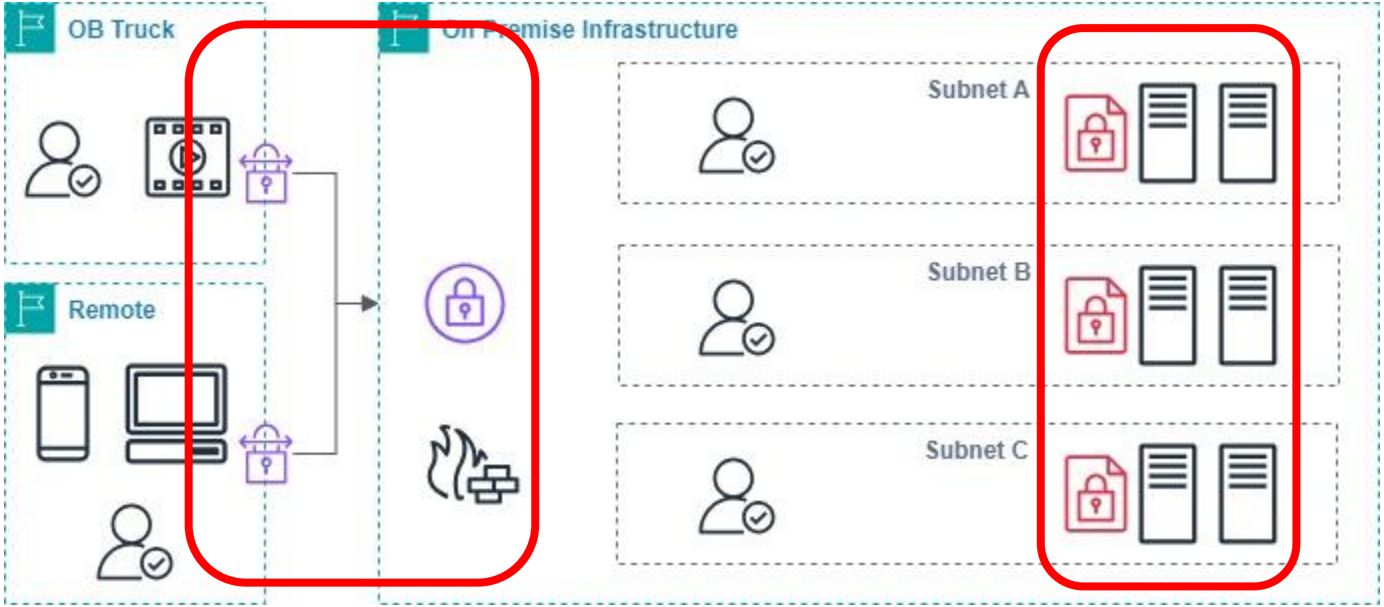
Segmented networks are easier to monitor and troubleshoot and typically show enhanced performance due to reduction of unwanted traffic

Encryption

- Encryption at ***rest*** and in ***transit***
- Only use modern and updated **cypher suites**
  - **AES-256** encryption for symmetric key (DES and 3DES are not recommended anymore)
  - **RSA-4096 or ECC-256** encryption for asymmetric keys (DH below Group 19 is not acceptable anymore)
  - **SHA-2** hashing (SHA-1 and MD5 are not acceptable anymore)
- Key management

Network Security Overview

Encryption

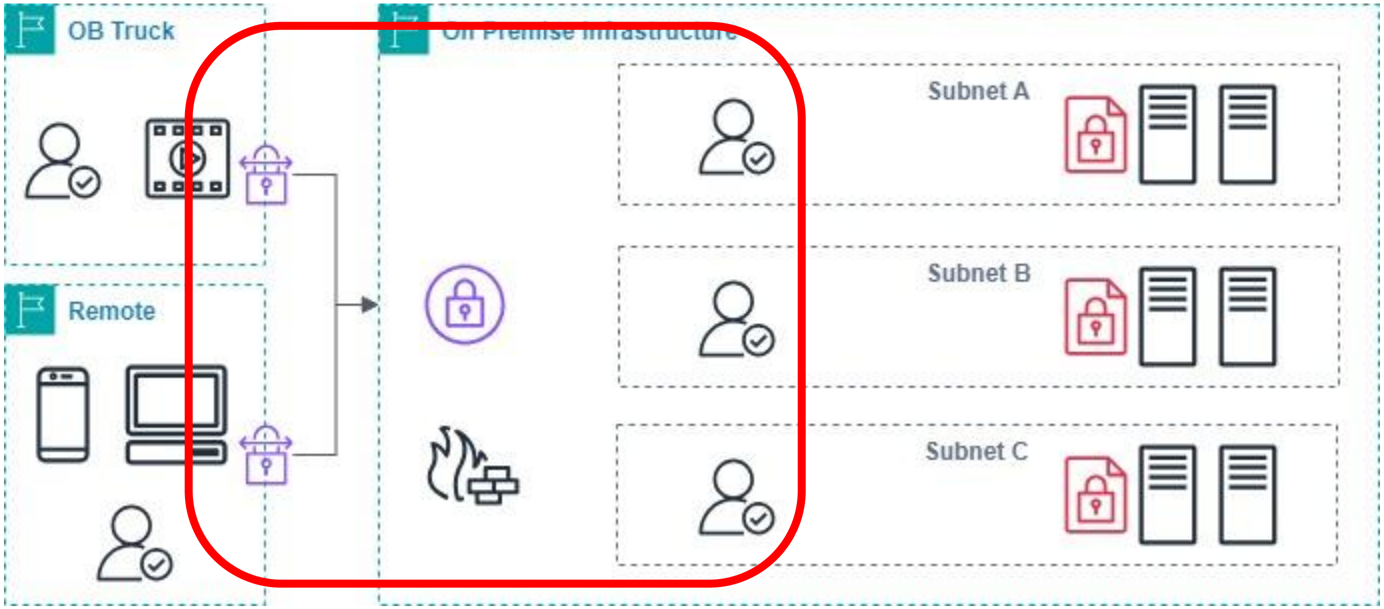


VPN and Remote Access

Remote Access:

- Only expose necessary services
  - RDP, FTP, Telnet, SSH, etc. - all can be potentially compromised
- Use certificates / identities for authentication where possible
- **Least privilege principles** is one of the most important concepts in security
- Use hardened VPN or IPSec gateways whenever possible

Remote Access



Intrusion Detection/Prevention System

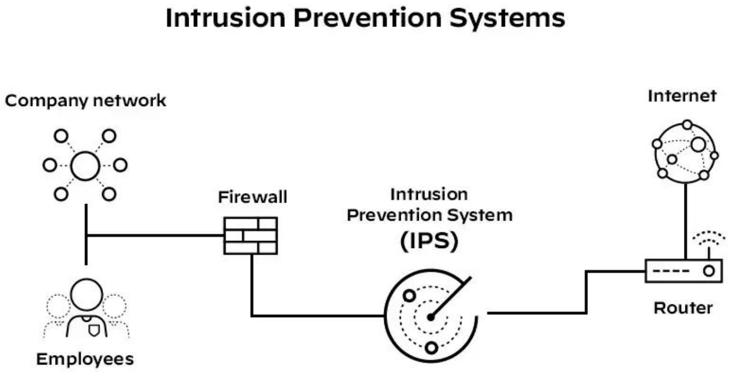
IPS and IDS systems are automatic or semi-automatic systems that monitor traffic for common vulnerability exploits.

Positive:

- Part of more comprehensive Incident response system

Negative:

- Not a 100% prevention
- Can potentially degrade performance


Intrusion Prevention Systems
Company network
Internet
Firewall
Intrusion Prevention System (IPS)
Router
Employees

https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

Vulnerability Management and Patching

- Dedicated person or automatic systems
- Automatic Systems:
    - Dedicated software that scans whole network for vulnerabilities
    - Frequent scans (every 3 months or more often)
- Dedicated Person:
    - Maintains extensive database of assets
    - Manually monitors for new vulnerabilities
    - Patches the systems with newest updates

Zero Trust Security

Modern approach to security.

Zero Trust Security

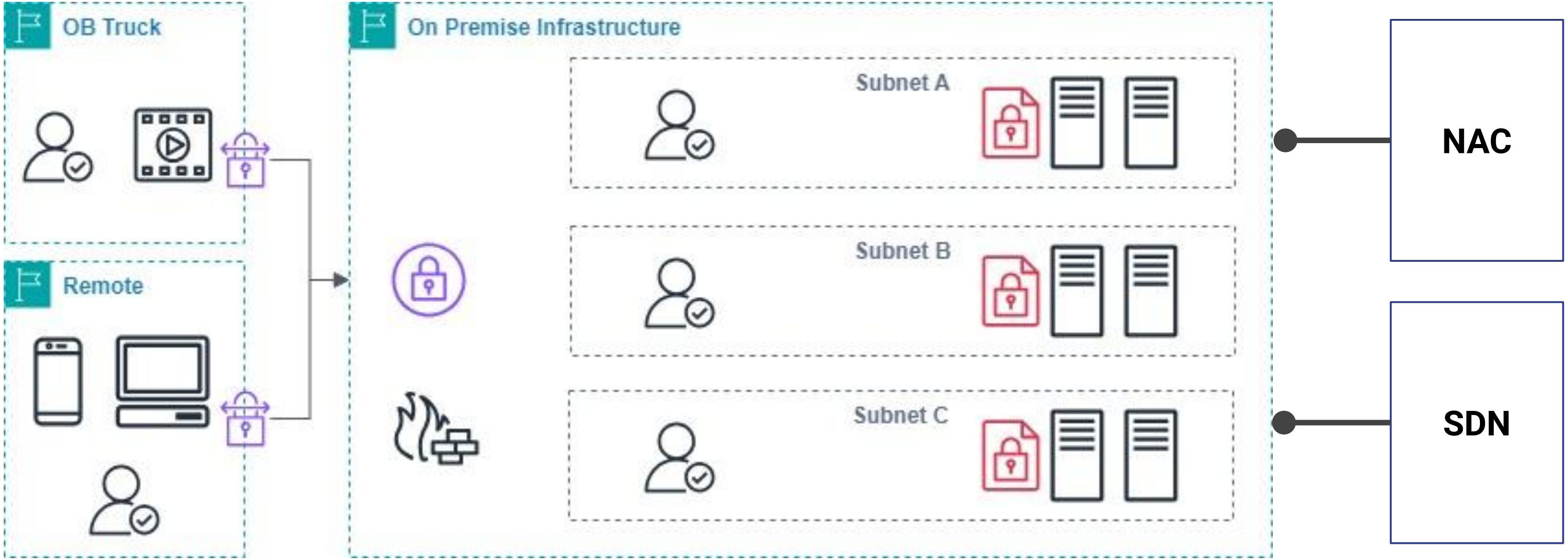
- Zero Trust Security is a set of principles and methodologies rather than specific technology or implementation.
- Inherently **not** trusting any traffic (including internal)
- 3 Principles of Zero Trust:

Verify All Traffic

Least Privilege Access

Comprehensive Monitoring

Infrastructure



Verify All Traffic

In Perimeter Security, internal traffic is automatically trusted.
This is different in ZTS, where all traffic is inherently untrusted and must authenticate.

- Every client/service (internal or external) must be authenticated every time it interacts with other clients/service and must have authorization to do so.
- Network Access Controller manages **policy-based** access through **authentication, authorization and scheduling.**

Least Privilege Access

Least Privilege Access principles expand on previous principle.

- Every authenticated user (this can be a client, service or device) will have **role** attached to it.
- The role will only have as much access as necessary to perform its duties, but not more
- Authorization of roles is granular and refined on ongoing basis

Comprehensive Monitoring

Comprehensive Monitoring principle **always assumes breach**.

- The monitoring of the systems are constantly monitored for unusual activity
- Extensive logging is employed
- Logs are often reviewed

Zero Trust Network Access

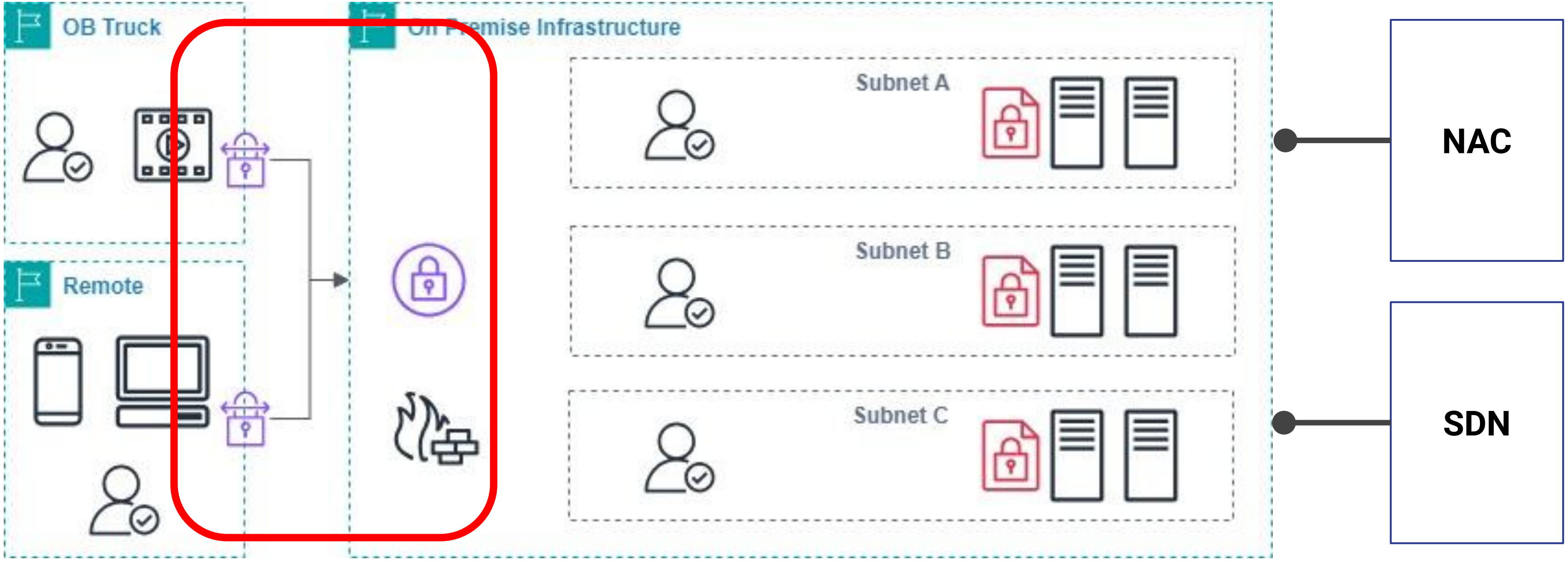
- ZTNA is thought of as an addition to VPN
- **Trust Broker** is added in line with the Firewall
    - Can be built into the Firewall or can be cloud-based
    - Manages the trust relationships for all external connections

Verify All Traffic

Least Privilege Access

Comprehensive Monitoring

Zero Trust Network Access



Actionable Items

- ☑ Enforce strong password policies and MFA
- ☑ Try to get away from usernames and passwords (using certificates instead)
- ☑ Follow Least Privilege principles for user management
- ☑ Check the route tables and firewall rules
- ☑ Check and update cypher suites / turn on encryption

Actionable Items

- ☑ Use VPN for any remote connection and only allow specific traffic (white lists)
- ☑ Close all unused ports and block them in firewall
- ☑ Suggest IDS or IPS for your facility (if feasible)
- ☑ Start vulnerability and patching management system (even if it is manual)

Questions & Answers

BLUE WARDEN
CONSULTING

Lubos Kuzma

Book free discovery session: https://calendly.com/bluewardenconsulting
Email: lubos.kuzma@bluewardenconsulting.com