# X CONGRÉS ISACA BARCELONA 2021

## UNA DÈCADA DE REPTES. UNA NOVA ÈPOCA PER L'AUDITORIA, SEGURETAT I PRIVACITAT

ISACA®
Barcelona Chapter

X CONGRÉS
ISACA **BARCELONA**
**2021**

UNA DÈCADA DE REPTES.
UNA NOVA ÈPOCA PER
L'AUDITORIA, SEGURETAT
I PRIVACITAT

# Don’t Trust anyone, Don’t Trust anything

## Ponent: Jordi Batlle

Enginyer en informàtica, Màster en auditoria i protecció de dades
GSEC, CCSP, CIPP/E

ISACA
Barcelona Chapter

# What is Zero Trust

Zero trust is based on the principle of “never trust, always verify”

Nist 800-207: Zero trust goal is to “prevent unauthorized access to data and services coupled with making the access control enforcement as granular as possible”

Zero Trust is a security concept centered on not automatically trust anything inside or outside company perimeter and instead verify anything and everything trying to connect to its systems before granting access

# What is NOT Zero Trust

A product or platform

Network segmentation

A firewall

A VPN

Multifactor Authentication

Install antimalware in your endpoint

# Paradigm shift

From the trusted network perimeter to work from everywhere

From corporate device to BYOD

From network-based trust to resource-based trust (users, applications,…)

From coarse-grained to fine-grained trust (subnet to session), no traffic should be unknown

From static policy to dynamic policy evaluated at the time of session establishment

# Sources of trust

User:
Who am I?

Device:
Is device
trusted?

Location:
Am I in a
“known”
location?

Time:
Is this a
usual time
for me?

Resource:
Is this an
applicatio
n
that I’m
authorized
to access?

Data:
Which
datasets I’m
authorized
to access?

# Trust components

## Identity

- User lifecycle
- Validate identity
- Multifactor
- Trust groups
- Least privilege

## Device

- Use trusted devices
- Enforce endpoint security and policies
- Health check

## Network

- Use trusted network
- Segment as needed
- Allow authorized users only
- Allow authorized devices only

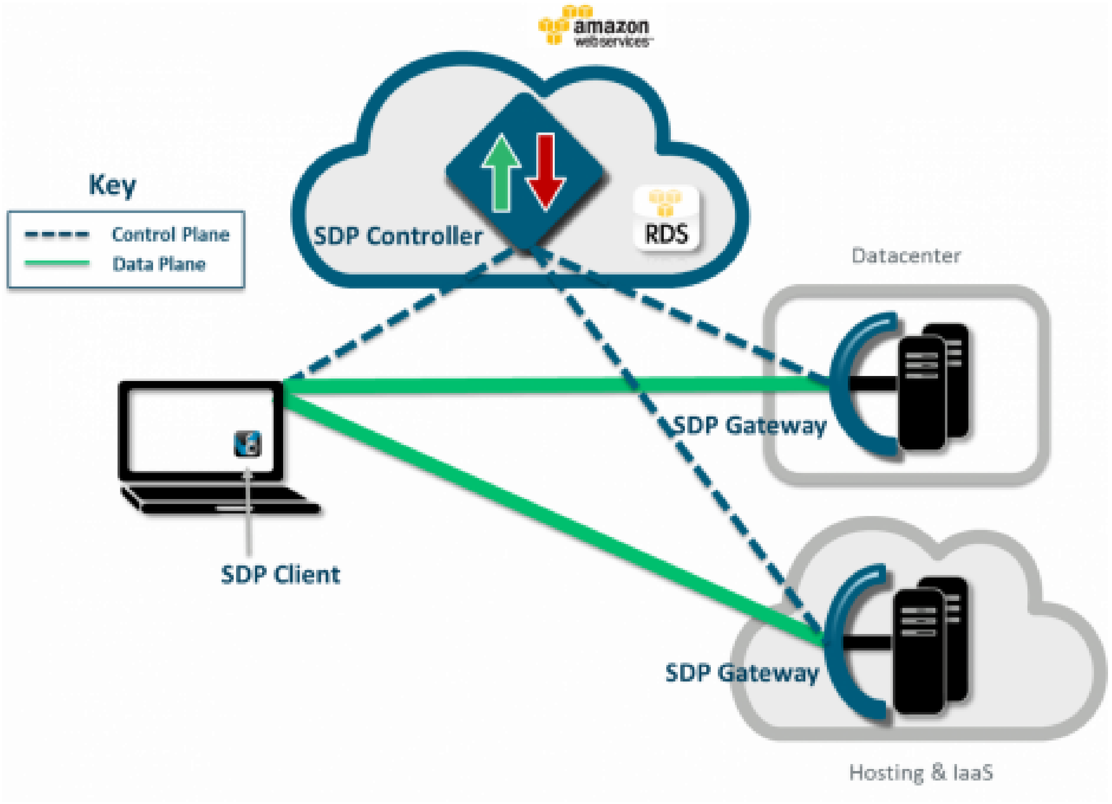
## Server environment

- Micro segmentation, avoid lateral movement
- Hardening
- Vulnerability management
- Privileged user management

## Application

- User authentication and authorization
- User privileges
- Data scope

# Zero Trust vs. SDP

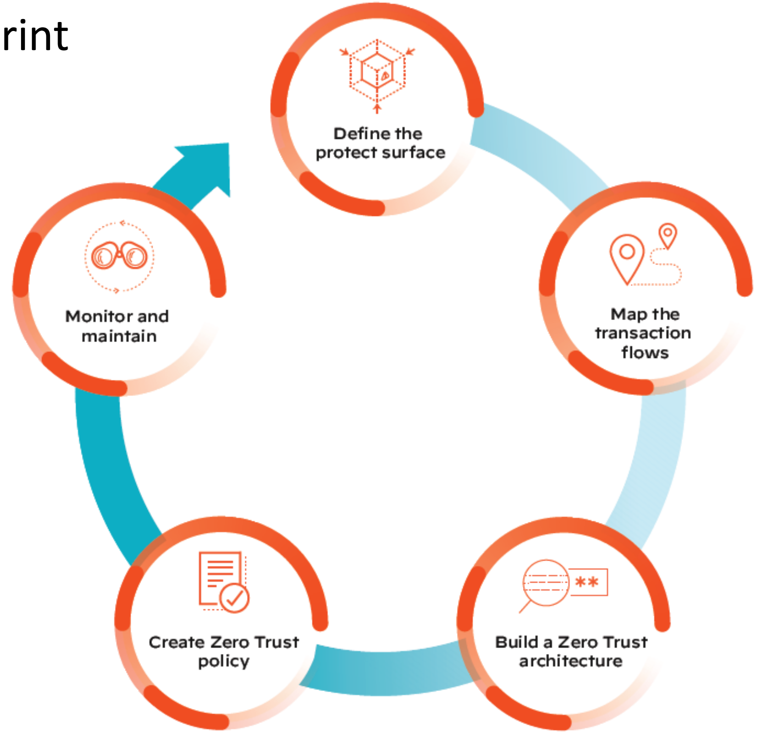


SDP « Software Defined Perimeter » is a SDN implementation of Zero Trust :

- The SDP client: an agent installed on end-points
- The SDP controler: the brain of the solution, where security policies are defined and pushed to the SDP components
- The SDP gateways: located at the server side, they proxified the traffic toward the applications, based on the security policies
- The communications are encrtypted between the SDP client, the Controler and the SDP gateway.

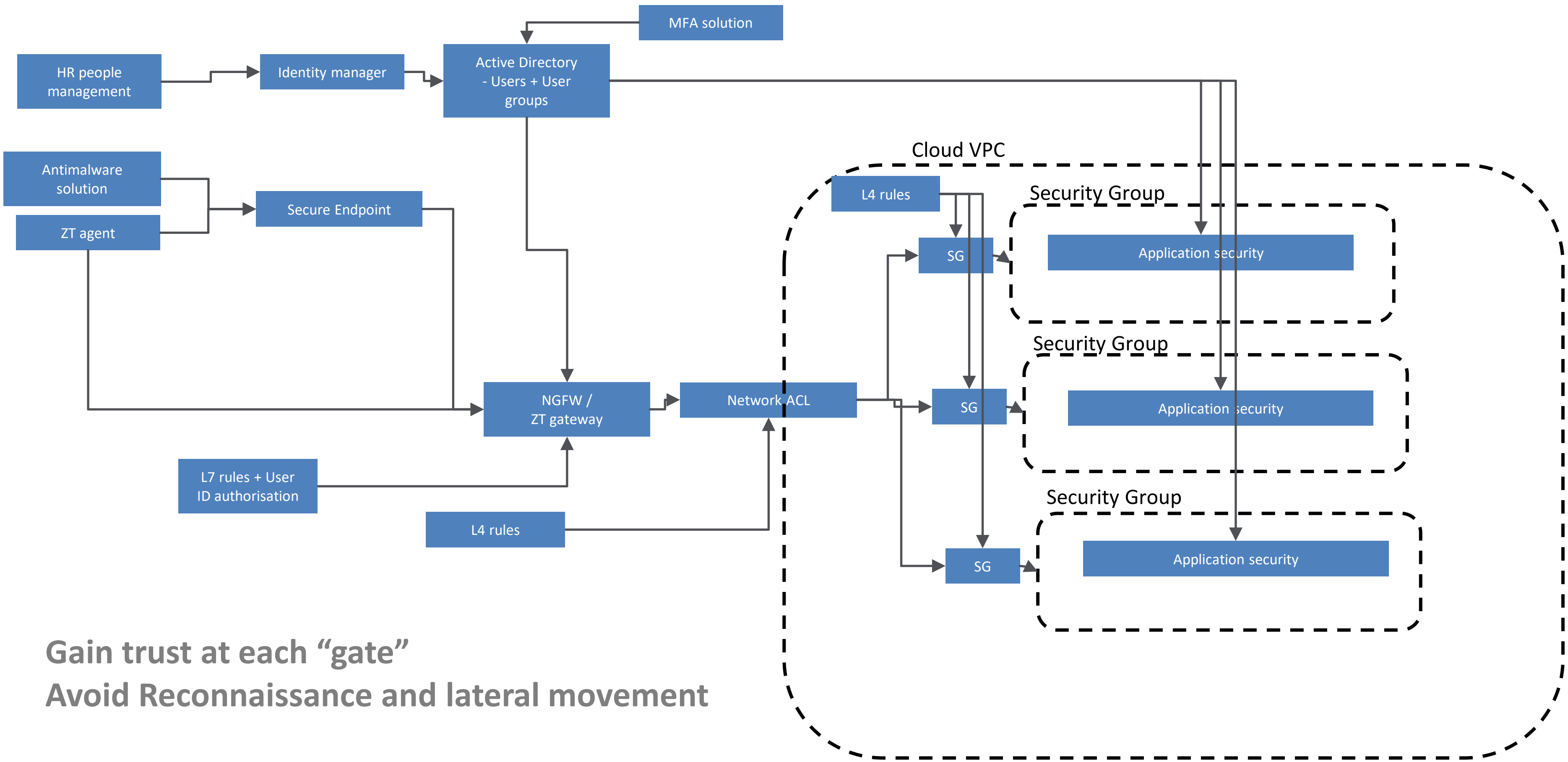
# Zero Trust five step methodology for implementation

It’s a journey not a sprint


Define the protect surface
Map the transaction flows
Build a Zero Trust architecture
Create Zero Trust policy
Monitor and maintain

*Palo Alto five step methodology

# Zero Trust E2E control points



**Gain trust at each "gate"**
**Avoid Reconnaissance and lateral movement**

# Some references

NIST Special Publication 800-207 – Zero Trust Architecture

Forrester - A Practical Guide To A Zero Trust Implementation

Palo Alto Networks - Simplify Zero Trust Implementation with A Five-Step Methodology

# Thank you!

Jordi Batlle
https://www.linkedin.com/in/jbatllec