NTT

CONSORCI ADMINISTRACIÓ OBERTA DE CATALUNYA (AOC)

NTT Access to the platform

September 2020

Contents

01

Introduction

- Introduction

02

AOC

- Requirements

03

NTT

- Concerns
- Proposal
- Diagram

04

AMZ

- What is it?
- Principles
- Diagram
- Security

NTT

Introduction

NTT values security as much as our customers, which is why we guarantee that our solutions are aligned to the industries best practices with a double objective:

- Address Security on NTT’s customers
- Address Security on NTT itself

This presentation has been made to show the current security measures as well as to provide AOC with the standard alternative that address the security requirements of our existing customers and allows NTT to deliver the services in a secure way.

AOC security requirements

NTT

Named accounts

NTT engineers must have unique named accounts in all production systems

Centralize access

Unify and centralize NTT engineers and AOC account accesses

Record activities

Log all user account activities

ENS

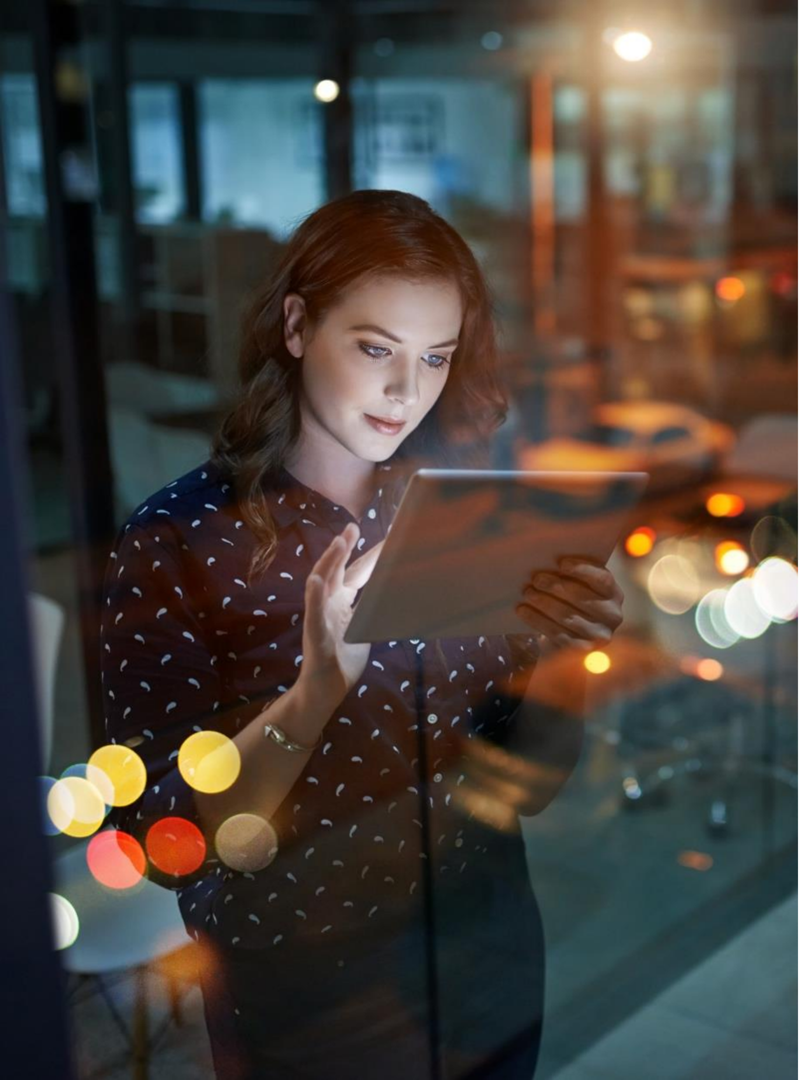
Meet National Security Scheme (Esquema Nacional de Seguridad – ENS) requirements for the CESICAT's security audit

NTT’s concerns

Potential facts:

- Access method deviated from NTT's access standard.
- Overhead in the service, Engineers must access using two PAM solutions.
- SLA can be affected, NTT will depend on a PAM managed by the customer.
- Lack in the admin passwords management can impact:
  - Automatization tasks cannot be done with the NTT tools.
  - Jobs cannot be scheduled or configured.
- Lack of control under administrator's passwords of the system managed.
- Potential security breach between the PAM connections.

This may lead to a major impact in the service that NTT can’t afford according to the contractual obligations and internal security policies.



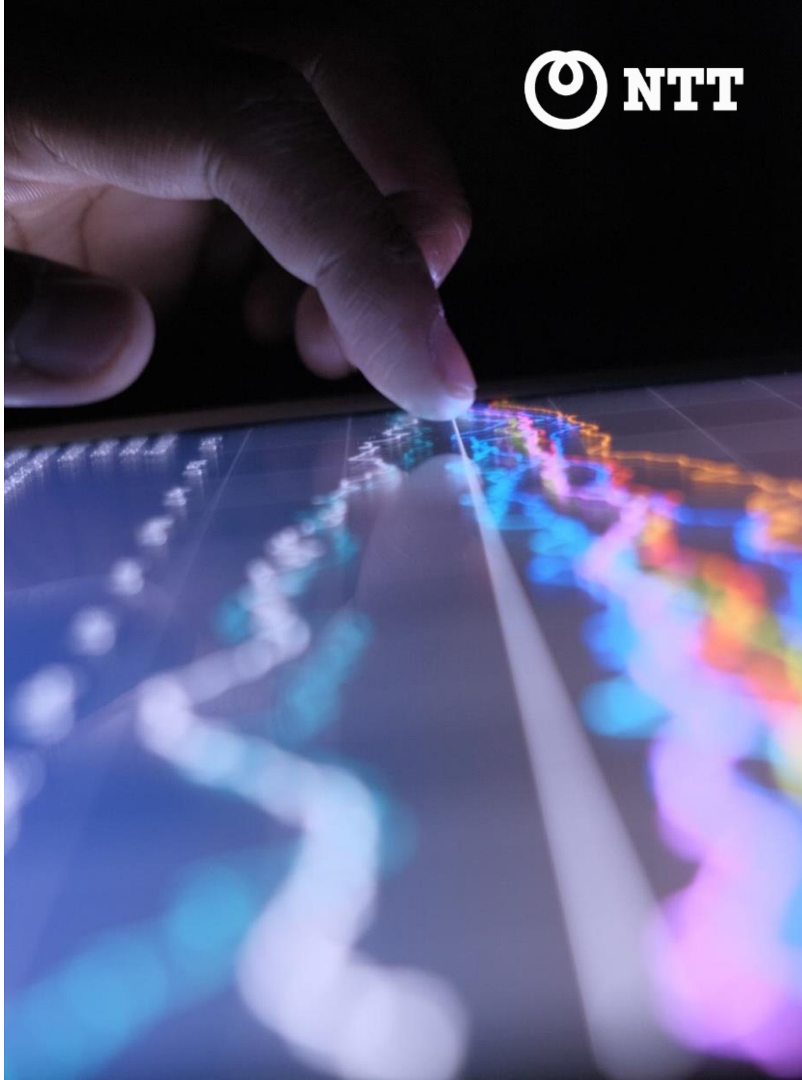
NTT's Access Management Zone (AMZ)

NTT infrastructure (AMZ) is used to securely access all of NTT customers. The AMZ is a PCI-DSS certified platform which has the security controls to ensure that all access is secure and traceable.

This platform provides NTT with the possibility of providing the services in a standard approach taking advantage of the shared service model and existing operational efficiencies

AMZ Principles

- **Highly Available** - Across multiple regions
- **Scalable** - Accommodates many internal users, NTT affiliates and contractors.
- **Secure** - PCI compliant enforcing unique user ID's, MFA and session recording
- **Multi-tenant** - One solution that is able to accommodate many support teams.
- **Agile** - Users can work efficiently, with an intuitive interface and standard tools.



AMZ Security Controls

01 **Secure builds**

Hardening based on CIS and enforced with GPOs and Puppet

02 **Secure Access**

RBAC SSO Terminal Server (Fortigate), MFA (OKTA and Radius) and Session recording (ObserveIT)

03 **Server Protection**

Antivirus and antimalware (Falcon CrowdStrike) and Host-based IDS (AlertLogic)

04 **Network protection**

Network segmentation, Firewall IDS (Fortigate), Web filtering (Fortigate) and DNS based Content filtering (Cisco Umbrella)

05 **Monitoring**

Active Directory account auditing, SIEM and SOC (AlertLogic) and File Integrity Monitoring (Azure FIM & Azure Security Center)

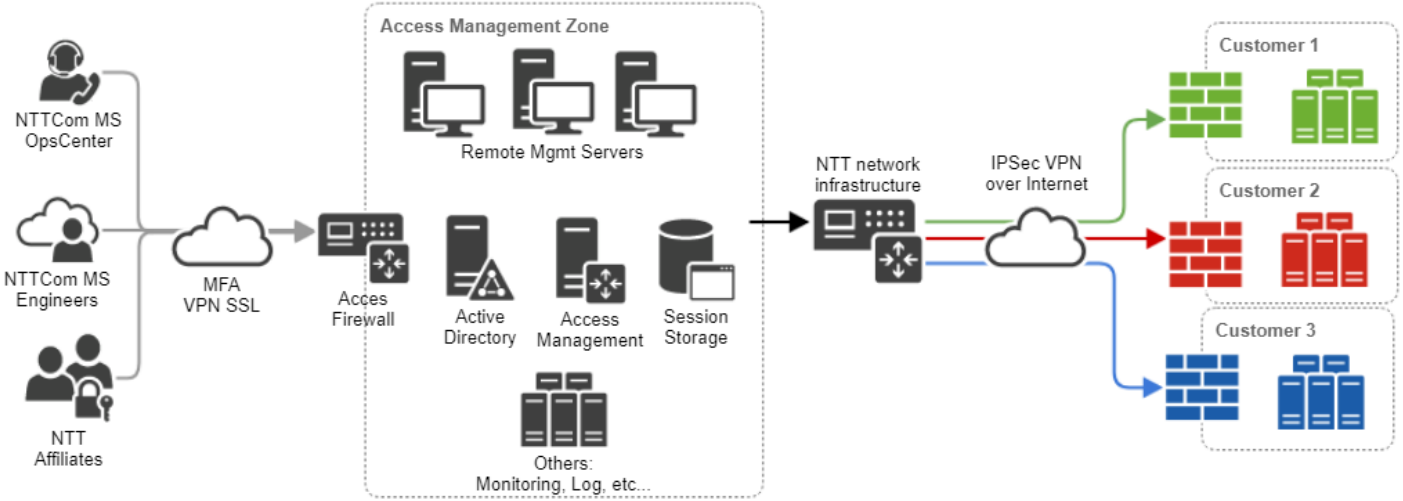
06 **Vulnerability**

Internal vulnerability Scans (Qualys), Annual pentest done by approved ASV and subscribed to multiple vulnerability notification feeds

07 **Compliance**

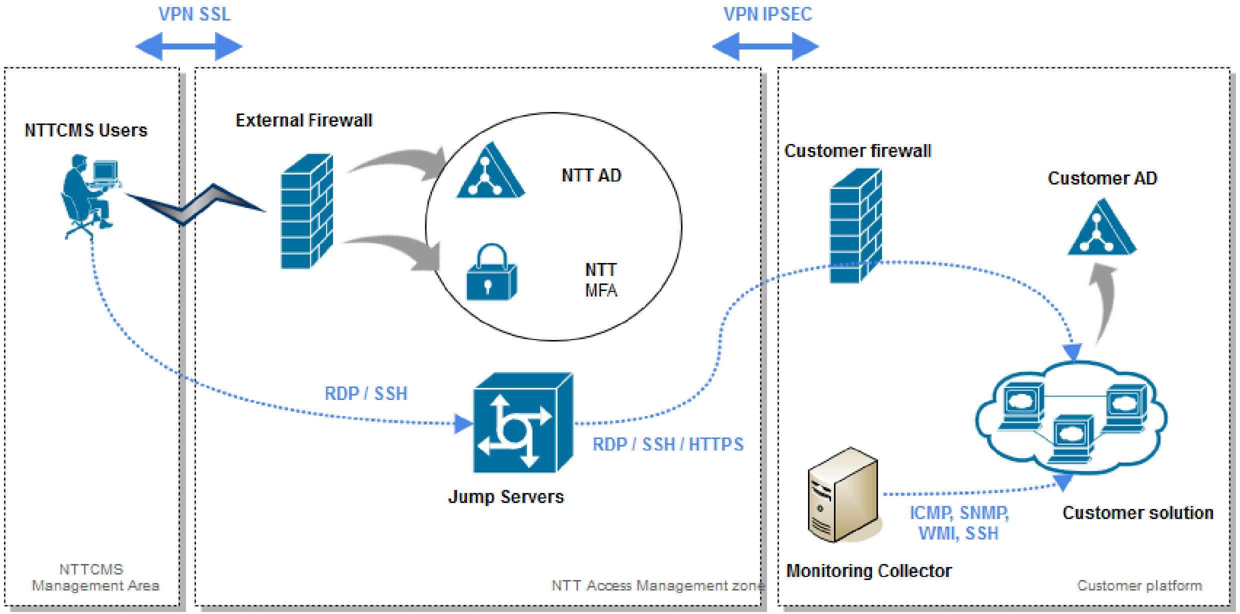
Compliance Scans on servers (Qualys) and annual certification audit (Approved QSA)

AMZ access diagram



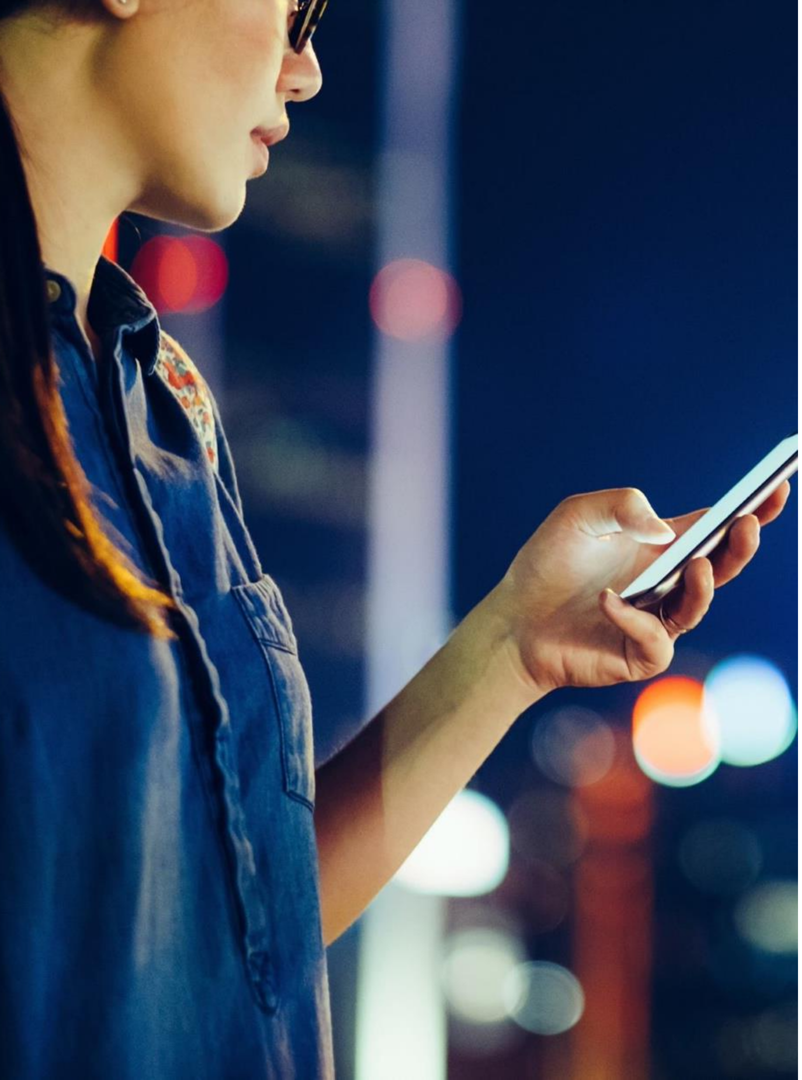
1. User establishes the VPN SSL (Forticlient) using his AD account and Okta Multi Factor.
2. Once connected the user can login by Remote Desktop to a Staging Server with his AD named account.
3. Once logged, the user can open an RDP / SSH connection to a customer device, using local accounts or named accounts in the customer AD

NTT proposal diagram



NTT access flows would be as follows:

1. NTT configures IPSEC tunnels between the NTT infrastructure firewalls and AOC firewalls
2. NTT engineers connect using the standard NTT VPN client to the AMZ platform, using NTT Active Directory and NTT MFA.
3. NTT engineers, login to the AMZ JumpServers, using NTT AD
4. NTT engineers connect from AMZ JumpServers to client managed servers (RDP, SSH), directly or using a Bastion Host.



NTT PAM

- NTT is currently deploying XTAM (https://www.xtontech.com) as a PAM solution at NTT
- XTAM will be deployed in AMZ as an additional security layer to the existing management tools
- Some features are:
  - Password vault
  - Use of standard RDP/SSH clients
  - Enforced RBAC and workflow policies
  - Automatic password rotation
  - Session recording
  - Remote isolated PAM nodes in customer infrastructure

NTT

Thank you