



**Business  
Services**

# Security White paper

Cloud Avenue

Version: 1.1

Date: 01/03/2022

---

**Orange unrestricted**

---

## Document description

### Properties

Document title	Security White paper – Cloud Avenue		
Version	1.1		
Author	Orange Business Services		
Status	<input type="checkbox"/> In progress	<input type="checkbox"/> Reviewed	<input checked="" type="checkbox"/> Validated
	<input type="checkbox"/> Approved		
Date	1 <sup>st</sup> of March 2022		

## Document classification

### Classification

Confidentiality	Orange Unrestricted
-----------------	---------------------

## Version history

Version	Operation	Name	Date
1.0	Initial Release	Orange Cloud for Business Security	05 2021
1.1	Update for Cloud Avenue	Orange Cloud for Business Security	03 2022

## Notice

All the information in this document is provided to the customer for informational purpose only. It represents Orange Business Services current and future product offers as of the date of issue of this document, which are subject to change. This document does not create any warranties, representations, contractual commitments, conditions or assurances from Orange Business Services, its affiliates, suppliers or licensors.

© Copyright 2021– Orange Business Services All rights reserved

# Content

Document description.....	2
Content.....	3
1. Introduction.....	6
1.1 Purpose of the document.....	6
1.2 Document organization.....	6
2. The security strengths of Orange’s Cloud services.....	7
3. Shared responsibility model.....	8
3.1 Cloud Avenue Responsibilities.....	9
3.2 Tenant Security Responsibilities.....	9
4. Common Security Measures.....	10
4.1 Security Policy.....	11
4.2 Organization of Security.....	12
4.3 Human resource-related security.....	14
4.3.1 Personal listing.....	14
4.3.2 Awareness.....	14
4.3.3 Writing undertaking of staff.....	14
4.4 Assets Management.....	15
4.4.1 Asset Inventory.....	15
4.4.1 Protective measures for support assets.....	15
4.4.2 Data deletion.....	16
4.5 Access Control.....	16
4.5.1 Access control for Orange operators.....	16
4.5.2 Access control for Orange customers.....	18
4.6 Cryptography.....	19
4.7 Physical and environmental security.....	19
4.8 Operational Security.....	21
4.8.1 Management of Operational Procedures.....	21
4.8.2 Protection against harmful codes.....	22
4.8.3 Backup Management.....	23
4.8.4 Security Logging and Supervision.....	23
4.8.5 Management of technical vulnerabilities.....	24

4.8.6 Security of administratives workstations within Orange ..... 26

4.8.7 Secure administration portal..... 27

4.9 Communications security ..... 27

4.9.1 Orange Cloud architecture policy..... 27

4.9.2 Security of exchange ..... 29

4.10 Acquisition, development and maintenance of information systems ..... 29

4.10.1 Risk analysis ..... 29

4.10.2 Good development and integration practice ..... 30

4.10.3 Security acceptance..... 30

4.11 Subcontractor management ..... 31

4.11.1 Security in contract with our subcontractors..... 31

4.12.2 Security monitoring of services provided by our subcontractors ..... 31

4.12 Management of security incidents..... 31

4.13 Security in the management of business continuity ..... 33

4.14 Conformity..... 33

4.14.1 Compliance with legal and contractual requirements ..... 33

4.14.2 Monitoring compliance with security policy ..... 34

4.14.3 Security related certifications ..... 35

5 Specific security measure ..... 36

5.1 Compute service..... 36

5.1.1 Virtual machine ..... 36

5.1.2 Auto scaling ..... 37

5.1.3 Image management service ..... 37

5.1.4 Dedicated cloud..... 37

5.2 Storage, Backup and Disaster recovery service..... 38

5.2.1 Datastore storage ..... 38

5.2.2 Network storage..... 38

5.2.3 Backup ..... 38

5.2.4 Disaster recovery service..... 39

5.3 Network services ..... 40

5.3.1 Edge gateway ..... 40

5.3.2 NAT Gateway..... 41

5.3.3 Distributed firewall..... 41

5.4 Security and Identity Service .....	42
5.4.1 Anti DOS/DDOS.....	42
5.4.2 IPS probe and WAF .....	42
A. TIER Classification of a datacenter .....	43

## 1. Introduction

### 1.1 Purpose of the document

This document is the security white paper of the Cloud Computing services of “Cloud Avenue” operated by Orange Business Services. It describes the main technical and organizational security measures applied by Orange Business Services to guarantee the security of Cloud Avenue services and the protection of customers’ data.

### 1.2 Document organization

This document is organized into the following chapters:

- Chapter 1 is the document introduction
- Chapter 2 is a summary of the benefits of Cloud Orange in matters of security
- Chapter 3 explains the Shared Responsibility Model for Cloud Avenue (as Cloud Service provider) and the customers (tenant owners)
- Chapter 4 lists the security measures used, organized according to the section ISO 27002
- Chapter 5 details the extra security measures specific to Cloud Avenue
- Appendix A describes the tier classification of a datacenter

## 2. The security strengths of Orange's Cloud services

This chapter lists the main security benefits of Orange Business Services' Cloud services:

- **A trusted partner:** Orange Business Services is certified ISO 9001, ISO27001<sup>1</sup> and ISAE 3402<sup>2</sup> type II (SOC1 report, former SAS70) and MTCS<sup>3</sup> level 3. These certifications provide cloud customers with assurance from 3rd party auditors that relevant cloud computing security practices and controls are in place and demonstrated
- **Data location:** Orange Business Services guarantees the location of customers' data and backups in one or more given countries.
- **Physical security of datacenters:** The security of all datacenters is periodically assessed to comply with Orange security and availability requirements. All datacenters used for Cloud Avenue are certified ISO27001, ISAE 3402 Type II (ex-SAS 70) and comply with TIER III or TIER IV requirements.
- **Operator experience:** The Cloud services have been designed on the basis of Orange's experience as a critical infrastructure operator and as one of the French leaders in security integration and consulting with Orange Cyberdefense.
- **Support and maintenance operation security:** The operating centers are located in France and abroad and have ISO 27001 security certification, ensuring the confidentiality of Orange customers' information. Administration hosts allow to strictly secure and control the administration rights, privileges and actions.
- **Administration portal security:** Customers are provided with portals allowing them to manage their Cloud services. Access to these portals is realized through personal accounts, actions are logged and data flows are protected and encrypted. Portal security is regularly checked with intrusion tests.
- **Connectivity with company VPNs:** Cloud customers' virtual environments can be securely interconnected with a Business VPN MPLS, providing greater end-to-end network isolation, together with a bandwidth and network service quality that the Internet cannot steadily provide.
- **Protection against intrusion and denial of service:** The infrastructure used to operate Cloud Avenue cloud services is protected against intrusions and DoS attacks. Customers can also be provided additional security protection on their virtual infrastructure or application (WAF, IDS and DDoS).
- **Service continuity of Orange Cloud services:** All Orange Cloud services come with high service availability rates (described in the service descriptions of each offer). Furthermore, all our Cloud services benefit from entirely redundant infrastructure, with high-availability mechanisms. Any local interruption is consequently transparent: network (Internet access, VPN access and firewall), administration portal, virtualization, storage, etc.

These measures are detailed in the rest of this document.

---

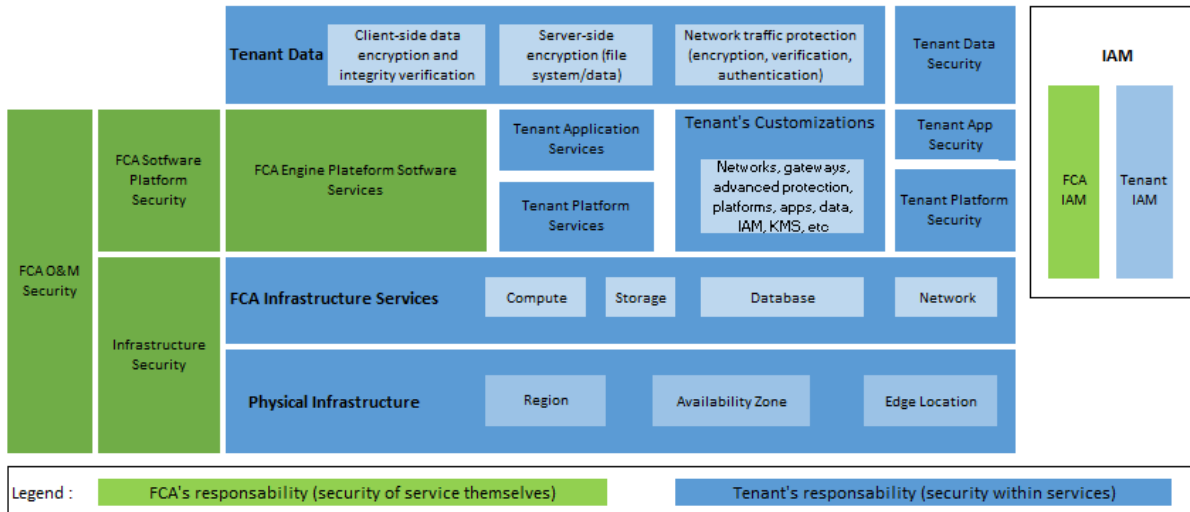
<sup>1</sup> Associated certificate: <https://certificats-attestations.afnor.org/certification=335181233155>

<sup>2</sup> ISAE 3402: standard ensuring customers of externalized services of the reliability of the internal control mechanism of their service provision. In particular, the standard covers the physical security of datacenters.

<sup>3</sup> Associated certificate : <https://www2.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/ComplianceAndCertification>

### 3. Shared responsibility model

In three primary cloud service delivery mechanisms defined by NIST<sup>4</sup>, as infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS), the tenants maintain complete control over their content, services, data location, encryption as well as access control. As a CSP (Cloud Service Provider), Orange Business Services is responsible for maintaining the security of applications, platform and infrastructure to ensure confidentiality, integrity and availability of Cloud Avenue. This shared responsibility model is fundamental to understand the respective roles of the tenants and Cloud Avenue in the context of cloud security principles.



As shown in the above figure, the primary responsibilities of Cloud Avenue are developing and operating the physical infrastructure of Cloud Avenue datacenters; the IaaS services provided by Cloud Avenue; and the built-in security functions of a variety of services. The primary responsibilities of the tenant are customizing the configuration and operating the virtual network, platform, application, data, management, security, and other cloud services to which a tenant subscribes on Cloud Avenue, including its customization of Cloud Avenue services according to its needs as well as the O&M of any platform, application, and IAM services that the tenant deploys on Cloud Avenue.

NIST<sup>4</sup>: National Institute of Standards and Technology



### 3.1 Cloud Avenue Responsibilities

Cloud Avenue is responsible for protecting the security of our IaaS services, as well as the physical environments of the Cloud Avenue global datacenters on which our cloud services operate. Cloud Avenue is not only responsible for the security, performance of the infrastructure, but also the overall security compliance of our infrastructure and services to respective standards and regulations.

In addition to protecting the global infrastructure, Cloud Avenue is also maintaining the products that are considered managed services, such as backup software, PRA solution etc. Following functions, but not limited to, are implemented fulfill the O&M security requirements of Cloud Avenue:

- Rapid security incident detection, isolation, and response to ensure fast recovery of cloud services.
- Vulnerability management mechanism to track, test, validate and implement across the platform.
- Secure configuration and version upkeep of cloud services.
- Basic security tasks like operating system update and middleware patching, firewall configuration and disaster recovery for managed services.

### 3.2 Tenant Security Responsibilities

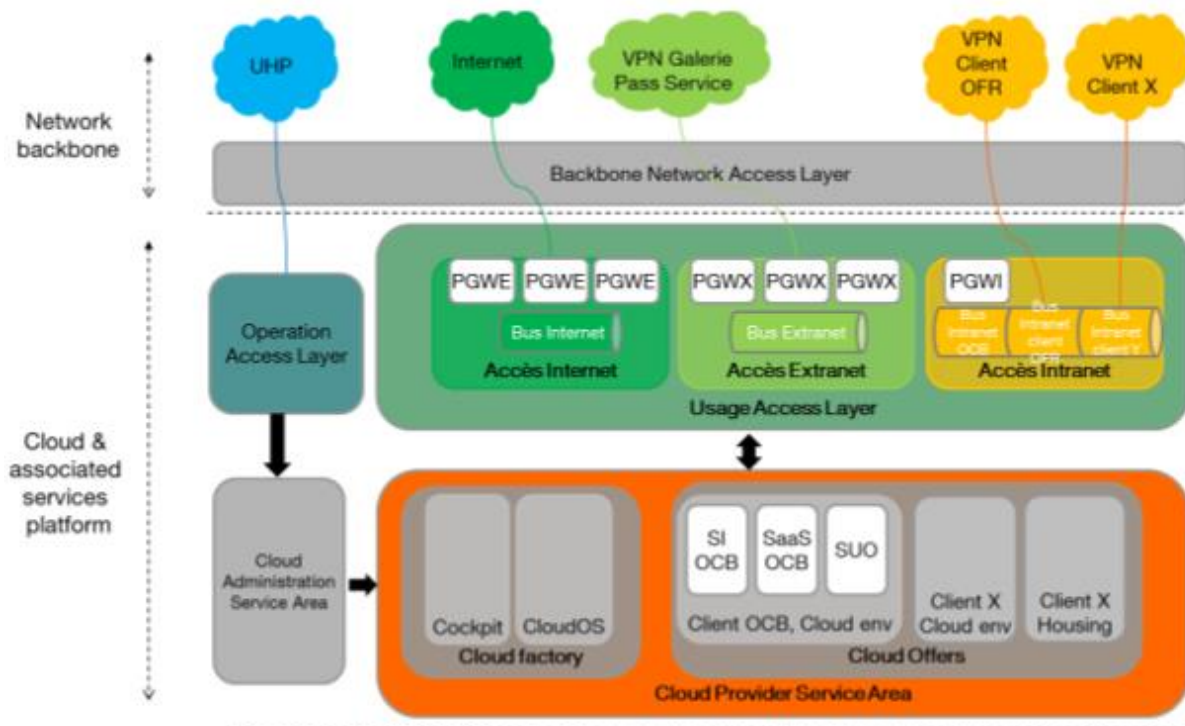
Within Cloud Avenue, tenants are responsible for security inside the IaaS cloud services which they subscribe and provision. This includes the security configurations and operations of the virtual machines, Virtual Datacenter (VDC), security groups, advanced security services, key and identity management. Tenants should pay attention to but not limited to following requirements when they are using Cloud Avenue services.

- Security configurations of organization-managed services, such as virtual firewalls, gateways, advanced security services, and security management tasks (patch management, hardening).
- Protection of Cloud Avenue account credentials and provision of individual user accounts with IAM and setting up multi-factor authentication, secure data transfer protocols in accordance with industry best practices.
- Adequate testing of cloud services that are deployed on Cloud Avenue to prevent adverse effects on applications and to minimize business impact.
- Creating user accounts based on least privilege principle and enforces segregation of duties, utilizing all available security features provided by Cloud Avenue such as logging, access control lists and permissions on applicable services.
- While Cloud Avenue strives to meet regulatory and industry security compliance as a Cloud Service Provider (CSP), organizations are responsible to comply any application and service that they deploys and operates on Cloud Avenue that is not part of our services.

## 4. Common Security Measures

Security measures are organized into 14 chapters, corresponding to the 14 sections in the ISO 27002 standard version in 2013.

Cloud Avenue provides services that allow a user to create a virtualized infrastructure over a shared physical infrastructure for all users. The virtualization mechanisms implemented ensure a strong logical partitioning of the client's virtualized resources (one per client). The access to the resources of a tenant is done through the CloudStore (login/password) with a TLS authentication.



### System Virtualization

The system virtualization is based on the proprietary solution VMware. The servers' simulation is made with vSphere<sup>5</sup> whereas networks' simulation is performed by NSX<sup>6</sup>. Plus the hypervisor has been hardened to strengthen its partitioning:

- Processing<sup>7</sup>: Different virtual server processors have no visibility on each other. There is a complete segregation between tenants.
- Persistent data: no local storage. The access to the virtual servers deployed in the holding

vSphere<sup>5</sup>: <https://www.vmware.com/products/vsphere.html>

NSX<sup>6</sup>: <https://www.vmware.com/products/nsx.html>

<sup>7</sup>: <https://download3.vmware.com/vcat/vmw-vcloud-architecture-toolkit-spv1-webworks/index.html#page/Core%20Platform/vCenter%20Server%20Cloud%20Provider%20Use%20Cases%20and%20Architectures/vCenter%20Server%20Use%20Cases%20and%20Architectures.2.04.html>

is established by means of a secure connection SSH or RDP.

- Memory: Tests conducted by Orange show that memory remnants from a previously allocated VM cannot be recovered

### Storage Virtualization

vCenter Server from vSphere suite provides the infrastructure for allocation and partitioning of compute and storage resources. This ensure a complete segregation between tenants which allows data access only to data owners or the corresponding storage. In addition, data written to the infrastructure is not recoverable once it is deleted by the customer (if no backup were implemented) or when the corresponding virtual infrastructure is terminated by the customer. These mechanisms are regularly tested. Finally, physical disks needing to be replaced are destroyed through a traceable and certified process.

### Network Virtualization

NSX carried by the vSphere suite component provides the network virtualization layer. The network virtualization layer is an abstraction between physical and virtual networks. NSX for vSphere provides logical switches, firewalls, load balancers, and VPNs. That means that the customer can decide which flows is allowed or not on the infrastructure and how to manage them in a secure way.

## 4.1 Security Policy

*This chapter corresponds to section 5 in ISO 27002 version 2013.*

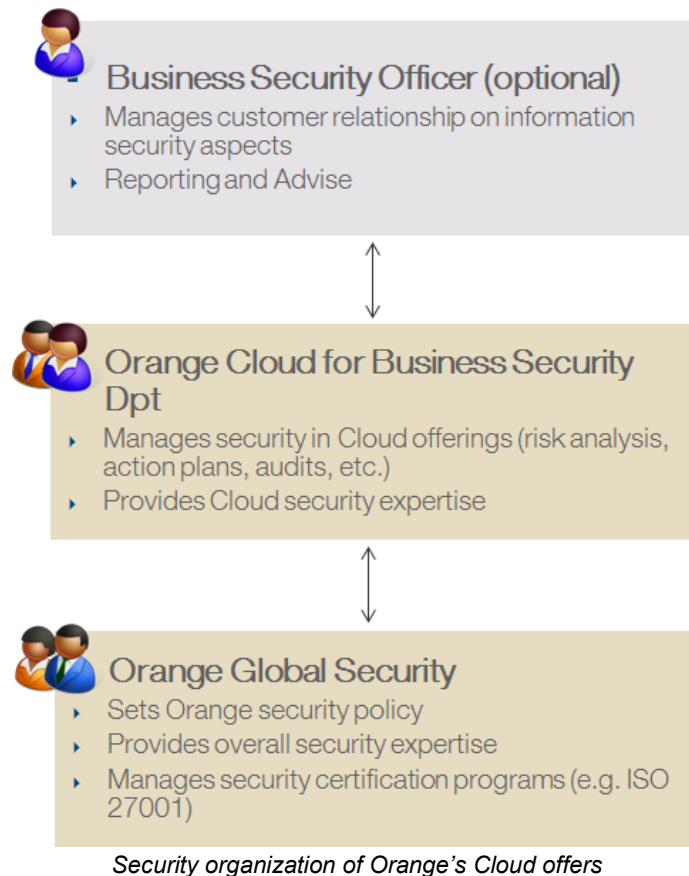
Orange Cloud services are subject to security policies from Orange group. The latter are aligned information system security standards: ISO 27001, ISO 27017, ISO 27018, ISO 9001, ISO 20000-1 and Service Organization Control (SOC).

The policies are at least yearly reviewed and regularly updated.

## 4.2 Organization of Security

This chapter corresponds to section 6 in ISO 27002 version 2013.

This part describes the security organization of Orange's Cloud offers.



### Business Security Officer (optional)

For customers with strong security requirements, a security expert (Business Security Officer) can be appointed to be the central point of contact of customer's CISO (Chief Information Security Officer) providing advice and detailed security reporting.






### Orange Business Services Offers Security Department

The Orange Cloud for Business Security department ensures that security is observed in all the Orange services. Its tasks are, for example:

- To define security policy and set the guidelines to be applied to Cloud services;
- To carry out and update security risk analyses (ISO 27005 type) for Cloud services;
- To manage the security action plans resulting from risk analysis;
- To guarantee the homogeneity of security solutions deployed in order to ensure their effectiveness and durability;

- To capitalize on Orange’s knowledge of Cloud security;
- To offer support and advice, to provide expertise in Cloud security issues;
- To train personnel and have them made aware of security procedures;
- To monitor the security level of services by conducting regular security audits (internal and/or external).

The Orange Business Services Security department is run by the Chief Security Officer. It is made up of security experts involved, and is organized as described below:

	Guarantee security of OCB organization	Reinforce Security Value of our services	Billable security services
	CSO/CISO role	Business Security Officer (BSO) for major services	Support to sales/presales Dedicated BSO
	Organisational certifications (ISO, ISAE, SOC)	Service certifications (ISO, SecNumCloud, MTCS)	Staff security certifications (CISSP, ISO27005...)
	Security policies Compliance (GDPR, NIS, SOX..)	Security White paper	Security Assurance Plan Security questionnaires
	Audit and Control Security Incident Mgt Vulnerability Mgt Access Control Mgt Security Risk Mgt Transversal Security projects	Security incident follow-up Vulnerability follow-up Security/InTTM process (risks) Penetration tests	Security incident follow-up Vulnerability follow-up On-demand audits and advice

### Orange Global Security

Orange Global Security (DSEC), attached to the General Secretary of the Group, initiates and coordinates security actions over the whole scope of the Orange Group. The department has the responsibility among other tasks:

- To define Security Policies (general, sectorial);
- To define the policies on personnel awareness and training in security and to promote security in the company strategy and culture;
- To interface with the main security and data protection entities:
  - French National Defense and Government authorities (SGDN<sup>8</sup>, ANSSI<sup>9</sup>, etc.);
  - French justice, police and gendarmerie authorities (in liaison with Orange Legal Management);
  - The CNIL<sup>10</sup> (French National Commission for Data Protection and Freedom, data protection regulator) (in liaison with Orange Legal Management and General Secretary);
  - Orange Risk Audit and Monitoring Management (DACR), the National Center for the Security of Information Systems (Orange entity);
  - The CERTs (Computer Emergency Response Teams), in particular the CERT-IST.
- To centralize security incident information and consolidate the dashboard;

SGDN<sup>8</sup>: <http://www.sgdsn.gouv.fr/>

ANSSI<sup>9</sup>: <https://www.ssi.gouv.fr/>

CNIL<sup>10</sup>: <https://www.cnil.fr/>

- To coordinate security certification programs such as ISMS ISO27001 certification;
- To conduct audits and assessments and to follow up on audits and assessments conducted on the initiative of the entities.

## 4.3 Human resource-related security

*This chapter corresponds to section 7 in ISO 27002 version 2013.*

### 4.3.1 Personal listing

A list of the staff contributing to the Cloud services build and operations is kept updated as part of the input/output management process. This list is used as a reference base when reviewing access authorizations personal's access rights are modified/removed whenever they change position or leave the company. A monthly review is performed to updates this list.

### 4.3.2 Awareness

Information System security awareness training is given to each new Orange staff member and all subcontractors joining the Orange teams. This training is regularly updated.

Each entity manager keeps their staff informed of security-related risks and of the legal and regulatory obligations. They are assisted by experts (inside or outside their entity).

Each entity manager has their staff made aware of, and ensures compliance with, ethical and responsible behaviour in various internal or external communication situations (emails, web, telephone, removable storage, seminars, travel, etc.).

Each entity manager makes sure that their internal staff is competent in matters of security, and if necessary arranges extra training.

### 4.3.3 Writing undertaking of staff

Employees have a general obligation of discretion written into their contract of employment and/or into their collective agreement.

For subcontractors, this undertaking is signed by the employee via their employer.

#### Acceptable use charter for computer resources

Similarly, each employee must, according to internal regulations, comply with the acceptable use charter for computer resources.

## 4.4 Assets Management

*This chapter corresponds to section 8 in ISO 27002 version 2013.*

### 4.4.1 Asset Inventory

The list of support assets (routers, switches, firewalls, storage bays, servers, virtual machines, etc.) in Cloud offers is kept in the Orange internal mapping tools. These tools trace both the components of the Orange Cloud infrastructure and the components of the customers' environments (e.g.: Virtual Machine, virtual firewalls, etc.)

These inventories are updated as part of the change management process.

#### 4.4.1 Protective measures for support assets

##### Classification of infrastructure resources

Infrastructure resources are classified on a 4-level scale, defined in the Orange Global Security Policy, and this qualifies the harm to Orange and its customers in the event of an incident involving the resource:

- Level 4: vital impact, very high (even vital) stakes corresponding to inadmissible risks;
- Level 3: critical impact, very high stakes corresponding to risks whose effects must be limited;
- Level 2: substantial impact, moderately high stakes and risks controlled with limited harm to the company;
- Level 1: no or practically no impact.

All shared Cloud infrastructure resources hosted in our datacenters (routers, switches, storage and backup bays, servers, etc.) are considered to be at least level 3 (i.e. level 3 or level 4). Measures for the protection of these critical resources are described throughout this document.

##### Classification, marking and protection of documentation

Documentation is classified and then marked in accordance with the Orange internal rules defined in the document "Document marking". Four levels are defined here: free circulation (unrestricted), Orange internal, **Orange confidential** and **Orange secret**.

Operational documents of Cloud projects / services are stored on file servers. Access is protected by personal access code and authorization management on a need-to-know basis.

##### Classification of customer information

The classification of customer information hosted on Orange's Cloud services is the customer's responsibility.

## 4.4.2 Data deletion

### Protection of de-allocated customer data

Customer data located on de-allocated resources cannot be accessed by another customer. This protection is provided by the internal mechanisms of VMware products used by Orange.

### Deletion of customer data at termination of contract

When the contract terminates, all the resources allocated to customers are de-allocated, and the customer data become unusable, as explained in the previous paragraph.

### Secure disposal or re-use of equipment

All items of equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal. Orange has established security policies detailing the sanitization and disposal procedures for handling storage devices.

### Deletion of hard drives

If for some reason, a hard drive needs to be erased, the following rules will be applied:

- All hard drives must be destroyed with the data inside;
- A hard drive can't be reused even if the data have been erased;
- It's prohibited to bring a hard drive outside the datacenter;
- All hard drives are destroyed within the datacenter;
- Before destruction hard drives are stored in a vault;
- Once a hard drive is destroyed, a document is written with several information (number of hard drive destroyed and the date). This document will be kept for legal obligation

## 4.5 Access Control

*This chapter corresponds to section 9 in ISO 27002 version 2013.*

Orange provides access control for the environments that are contractually its responsibility. Access control for systems and applications managed by the customer is the customer's responsibility.

### 4.5.1 Access control for Orange operators

#### Means of access

Orange operators manage the Cloud infrastructure (servers, storage bays, network equipment, security equipment, etc.) as follows:

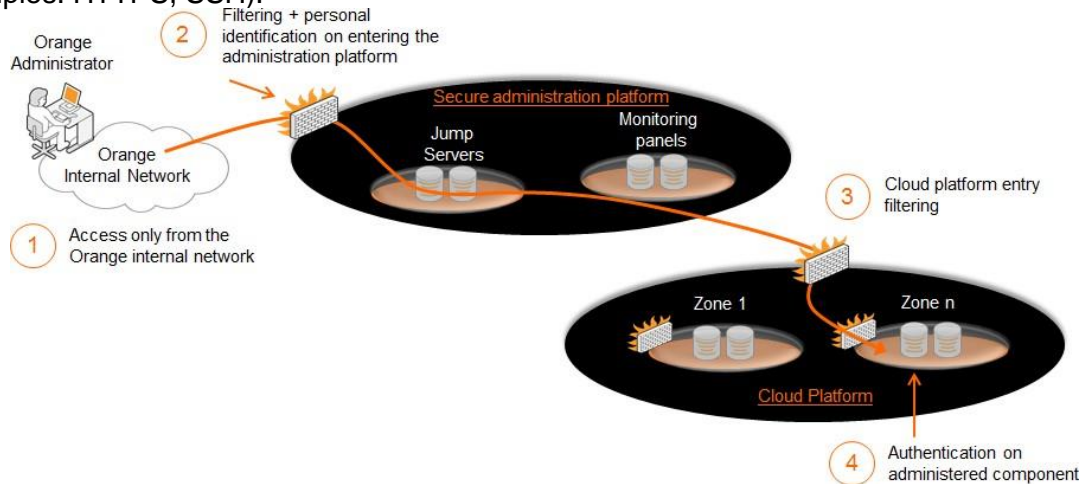
- 1 – Access from the Orange internal network. Cloud infrastructure administration is only possible from the Orange internal network.
- 2 – Filtering and personal authentication on entering the administration platform.



The Cloud platform is protected from the Orange internal network by an intermediate security zone called a bastion host. This step ensures:

- Network filtering;
  - Personal strong authentication;
  - Logging of sessions on a centralized log server;
  - Authorization: the administrator can only access resources authorized for their profile.
- 3 – Authentication and authorization on managed cloud environments. The he authorized administrator are given exactly the privileges necessary to their duties. All their actions are logged on a system ensuring non-repudiation.

Administration access is always done securely via the SSL/TLS protocol (workflow examples: HTTPS, SSH).



### Password authentication and management

Connections with operating accounts comply with the following password management policy:

- Complexity
  - The password must have at least 12 characters.
  - The password must contain at least one upper case letter, one lower case letter, one numerical digit and one special character;
  - A dictionary attack is done to ensure that the password could not be brute forced in case of compromise
- Renewal
  - The password must be renewed at least every 3 months;
  - The password must differ from the 5 previous passwords.
- Blocking
  - The account must be automatically blocked after 5 failed authentication attempts;
  - The account must be automatically blocked if the password expiry date has passed.
- Password protection
  - The login screens must be accessible only through encrypted and secure communications;

- The password entered must not be displayed in cleartext;
- The password must not be stored in clear text (e.g. only its hash must be stored).
- Session duration
  - Inactive sessions must be ended automatically after a period of time determined for each service.
- Logging
  - Authentication-related events must be noted in the log.

Strong authentication is ensured with an additional token either soft or hard.

### Review of rights for Orange operators

A review of authorizations and rights is carried out every semester. This activity consists in comparing the Human Resource file, describing the roles of each person, with the actual rights assigned in the systems. If non-legitimate rights are discovered, suitable measures are applied:

- Suspension of the account;
- Examination of traces of use to reveal any incidents;
- Corrective measures (updating procedures, having management made aware of the issue, etc.).

These reviews are the subject of a report and are audited yearly by external auditors.

### 4.5.2 Access control for Orange customers

Customers log in to cloud environments for the purpose of administration or access to application services. This access is via the Internet and/or private network (customer VPN) according to the services and options selected by the customer.

Customer access is always done securely via the TLS protocol.

- Server authentication (administration portals, application servers) is systematically done via an X.509 "server" certificate issued by a recognized certification authority.
- Customer authentication is based on a login/password previously sent securely to each customer. For certain services, strong authentication is possible (use of a software token generating a one-time password, use of the X.509 "customer" certificate).
- Network workflows are systematically encrypted.

The customer bears responsibility for the security of the authentication details sent to them by Orange. Within the possibilities offered by the tools, Orange sets a minimum complexity for all passwords handled by the customer.

The customer can then manage access accounts himself (creation/deletion, user profiles, administrator profiles). The associated logins and rights are the customer's responsibility.

## 4.6 Cryptography

*This chapter corresponds to section 10 in ISO 27002 version 2013.*

**Cryptographic sequences** - All cryptographic sequences used in Cloud services are based on market standards with a proven security level. Administration workflows are systematically encrypted using the SSL/TLS protocol.

**Certificate management** – Server authentication certificates are based on certification authorities (e.g.: VeriSign, Thawte, etc.) recognized by the main Web browsers. Authentication certificates for our internal administration services (accessible only by Orange operators) can be based on X.509 certificates generated by an Orange internal certification authority.

**Token** – Software tokens can be used by Orange Business Services operators. Certain Cloud services also allow the use of tokens to strengthen customer authentication.

**Encryption of hard drives of Orange operators** – To ensure the security of data and operations, all workstations (PC, laptops) hard disks are encrypted using McAfee Endpoint Encryption for PC solution. Sensitive data can also be encrypted using ZoneCentral encryption tool. ZoneCentral is a security product for encrypting the data on hard drives, emails, and containers with access reserved for authorized and identified users only. The ZoneCentral tool has been certified EAL3+ by ANSSI (ANSSI-CC-2012/07) issued on February 13<sup>th</sup>, 2012

## 4.7 Physical and environmental security

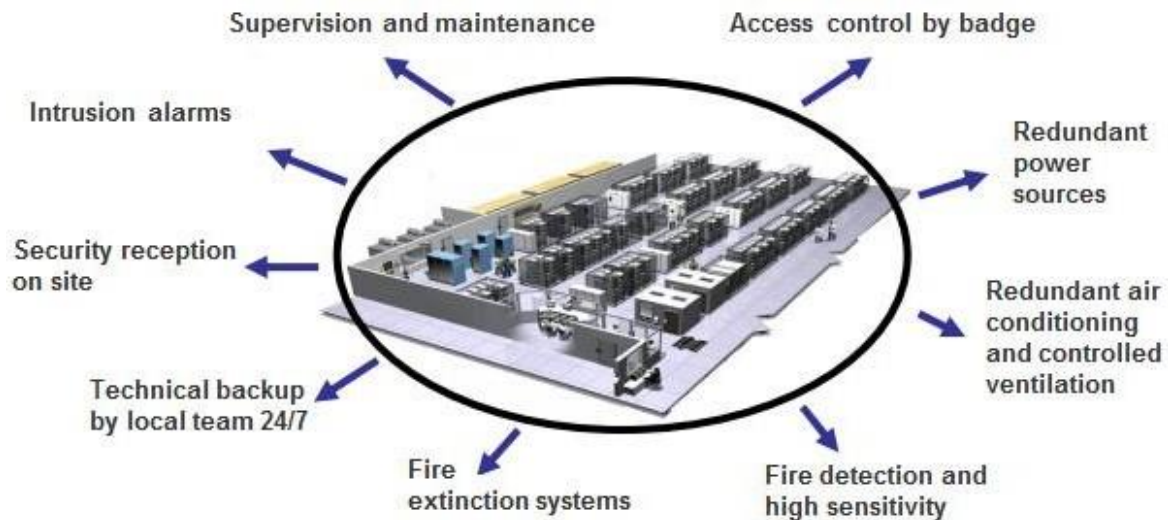
*This chapter corresponds to section 11 in ISO 27002 version 2013.*

The purpose of physical and environmental security is to protect the information system of Orange and its customers from:

- Environmental threats and harm: explosions, earthquakes, fire, water damage, electrical breakdown, air conditioning breakdown, telecommunication breakdown, etc.
- The threat of physical intrusions: access of non-authorized persons into the room, theft of hard drives containing sensitive information, etc.

### Physical and environmental security of our datacenters

Our Cloud services (infrastructures, backups, etc.) are hosted in several datacenters with following security measures:



ISAE 3402 - All datacenters are certified ISAE 3402 Type II (ex-SAS 70). ISAE 3402 is a standard giving customers of externalized services an assurance of the reliability of the internal control mechanism of their service provision. This independent audit report gives Orange Business Services customers the assurance that the services they benefit from meet the requirements of the Sarbanes-Oxley act in the USA and meet the key objectives of security, change management and service continuity.

ISO 27001: all datacenters used for Cloud Avenue are certified ISO27001. This is the most recognized security management standard. It provides customers with the assurance that the physical security of their data in datacenter is well managed.

TIER classification<sup>11</sup> - The datacenters for Cloud Avenue are built and operated to be compatible with TIER IV requirements.

### Physical and environmental security of our operating platforms

Operating platforms are places where Orange operates its Cloud services. The various platforms are:

- MSC (Major Service Centre) in Egypt: level 1 and level 2 support for infrastructures driving Cloud Avenue (firewall, servers, networks, etc.);
- MSC in France: Preproduction, level 3 support for Cloud services.

The following operating platforms have ISO 27001 security certification from AFNOR: the Cesson-Sévigné site, and the MSCs in Mauritius, India and Egypt. The functional scope of the certification is the deployment, supply and support of managed services and

TIER classification<sup>11</sup>: Definition in appendix A

communication solutions.

## 4.8 Operational Security

*This chapter corresponds to section 12 in ISO 27002 version 2013.*

### 4.8.1 Management of Operational Procedures

#### ISO 2000 and ISO Certification

The management of services by Orange Business Services is ISO 20000<sup>12</sup> certified. The requirements of ISO 20000 certification are aligned with the best practices in the latest version of ITIL (v3 2011) for processes such as service provision, relations management, problem- solving, testing and production launch, and stringent security requirements.

#### Change management

Change management is carried out according to the ITILv3 model; this concerns security-related changes in particular. For each service, change management is performed under the responsibility of a change manager.

- “Standard” changes, i.e. pre-identified in a catalog, follow a simplified process and do not require a prior study by a security expert. Operations’ team change meeting is held every week.
- Changes identified as “non-standard” (developments) are formalized in RFCs (Request For Change) and are discussed with the security team. RFCs are subject to a prior security study by a security expert from Orange Security Team, who gives their opinion. If it’s an important feature an HRLA<sup>13</sup> or an SRA<sup>14</sup> can be perform to evaluate the risks of the feature.

For every new features with public access, a penetration test is performed by Orange Security Team. All “high” and “critical” vulnerabilities have to be fixed before the release of the feature.

The change management implemented by Orange thus ensures:

- Minimal impact of change on operational services and users;
- Standardized methods, procedures and control mechanisms;
- Identification of personnel authorized to request a change;
- The control of change for compliance with security policy;
- Formalization of the correct assessment of the impact, priority, advantages and risks of a change;
- Definition of the change categories and associated implementation times;
- Management of the priorities of changes according to risks and impacts;
- Improvement in the quality of information and communication;
  - Ensuring that all the parties concerned have been involved to limit

ISO 20000<sup>12</sup> : Certificate link : <https://certificats-attestations.afnor.org/certification=335171233155>

HLRA<sup>13</sup> : High Level Risk Assessment

SRA<sup>14</sup> : Security Risk Assessment

- incidents related to the changes;
- The configuration database is supplied with correct information;
- Documentation of all changes;
- Proactive communication of scheduled outages to users/customers.

### Capacity management

Capacity management is carried out in accordance with the ITILv3 model under the responsibility of a “capacity manager”. The aim is to ensure a constant level of service for customers. Capacity management enables future requirements to be anticipated by analyzing the measurements and trends in the consumption of Cloud infrastructure resources.

Capacity management oversees and acts mainly on:

- CPU/RAM resources;
- Network resources (bandwidth, address space);
- Storage and backup resources;
- Software licenses.

For each service, the “capacity manager” regularly compiles statistics with various indicators specific to each service (technical measurements, business forecasts).

## 4.8.2 Protection against harmful codes

### Customer environment

Certain Cloud services natively include a dedicated antivirus for customer environments. This service is used by Linux and Windows machine

The antivirus agent installed regularly updates its virus signature database (at least once a day) from a specific updating server located in a security zone dedicated to customer machine updates. This virus signature database server is itself updated in real time on public servers available on the Internet from the antivirus publisher.

### Orange infrastructure

All operating systems have antivirus; this concerns both the servers deployed within the infrastructures and administration machines.

The antivirus agent installed regularly updates its virus signature database (at least once a day) from a specific internal Orange updating server located in a security zone totally isolated from customer environments. This virus signature database server is updated in real time on public servers available on the Internet from the antivirus publisher.

Orange internal security zones are also protected by the use of Intrusion Prevention System (IPS) probes operated by a Security Operating Center (SOC).

### 4.8.3 Backup Management

#### Customer environment

The data in customer environments are backed up in accordance with a backup policy specific to each service and according to the customer's options. In general, customers' data are backed up automatically and periodically with a retention period.

The backups can be of different kinds according to the services and options. Example:

- File level backup, particularly for application data;
- Image level backup for virtual machines;
- Raw data backup (file server).

Recovery methods vary according to offerings:

- Recovery independently by the customer;
- Recovery by Orange in response to a request for change via the administration portal.

#### Orange infrastructure

All the configurations of cloud infrastructure equipment are regularly backed up. This concerns in particular:

- Servers: Windows, Linux, application data (databases in particular);
- Network equipment (routers, switches);
- Security equipment (UTM firewall, VPN appliance);
- Storage equipment.

Backups for static configurations are carried out on each configuration change. The backup operation is controlled by the change management process.

All configuration backups are stored on third party sites (distinct datacenters) to guarantee the availability of configuration data in case of a major incident on the production site. Configuration backups for new datacenters are carried out on the same production site but in different computer rooms. Backups are stored securely (virtual partitioning) on a need-to-know basis.

### 4.8.4 Security Logging and Supervision

Orange systematically oversees its Cloud infrastructures and services, particularly as regards security. Events are logged for all the components, including security components. The purposes of logging are:

- To detect and analyze security incidents;
- To meet legal obligations;
- Troubleshooting.

All components are supervised 24/7 and standby duties are arranged in case of critical incidents, especially when security is affected.

### Nature of security logs

Events that are logged are defined component by component according to two criteria:

- Legal requirements: In France, the LCEN<sup>15</sup>, CPCE<sup>16</sup> and GDPR<sup>17</sup> (European law)
- Security requirements:
  - Events related to administration for all the components,
  - Events affecting security components (e.g. Firewall logs).

Logging and log supervision are carried out in compliance with the General Data Protection Regulation (GDPR).

### Centralization of security logs

All the cloud infrastructure components feedback their logs periodically or in real time to collection servers located in specific security zones. The integrity of security logs is protected and the logs are only accessible by administrators in charge of security.

### Single time reference

Timestamping of Logs, including security logs, is done with reference to a single time for all components in the cloud infrastructures. The time service is provided by various NTP servers in specific security zones. The time reference is supplied by a dedicated physical server (root server with GPS antenna) installed in Orange Business Services' internal service zones.

### Customer consultation of logs

With certain services, the customer can access the Logs for their environment, including application and firewall logs. Access to logs is secure and restricted to each customer's environment.

## 4.8.5 Management of technical vulnerabilities

The main purpose of vulnerability management is to keep the Cloud infrastructures and services secure. Vulnerabilities are identified during a security watch and vulnerability scans. They are then qualified with a patch to be deployed in production.

The security watch, monitoring of patch deployment and reporting are the responsibility of "Security Operation Managers".

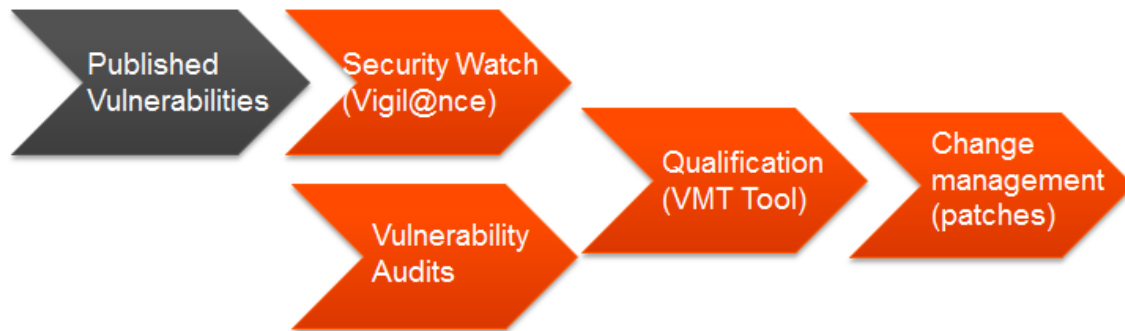
---

LCEN<sup>15</sup> : Law on Confidence in the Digital Economy

CPCE<sup>16</sup> : Post and Electronic Communications Code

GDPR<sup>17</sup> : General Data Protection Regulation





### Security watch

All components are subject to a permanent security watch aimed at identifying technical vulnerabilities that may affect the security of infrastructures and Cloud services.

The security watch is supplied with information from several channels:

- Security bulletins from product publishers (virtualization hypervisor, network and security equipment, OS, etc.);
- Watch reports: Vigil@nce, CVE, NIST NVD, CERT-FR etc.;
- Customer feedback;
- Feedback from our vulnerability audits and scans.

Vigil@nce is the security watch tool of the Orange group. It also provides an inventory of the various products (hardware and software versions) used within each service, based on the CMDB. Thus, the “Operations Security Managers” for the various services are alerted as soon as a vulnerability is likely to affect the services for which they are responsible.

### Vulnerability audits

Regular audits (or permanent ones on the most critical infrastructures) are launched on our production platforms both to measure the state of vulnerability of our platforms and to potentially identify vulnerabilities that have not been analyzed by the watch. To do this, Orange uses solutions from third party leaders in the vulnerability scan market (Qualys, Nessus). Moreover for any new feature, a technical audit is performed to make sure that this new feature match with our security standard before releasing it in production platforms.

### Vulnerability qualification

Security vulnerabilities and patches are qualified with the Orange internal “Vulnerability Management Tool (VMT)” under the responsibility of the “Operations Security Manager”. The Operations Security Manager decides the level of criticality of each vulnerability and the action plan to be followed (no action, change of configuration, installation of a security patch). They can optionally co-opt engineering teams or other security managers (e.g.: Engineering Security Manager, Chief security officer) to decide on the processing of a vulnerability.

### Application of security patches

All qualified security patches (change in configuration, security patch) are deployed in the production launch process (change management):

- Vulnerabilities with low/medium criticality are managed as minor or major production launches (CAB). The scheduling is adapted to Orange Business Services' operational constraints.
- Vulnerabilities with high/critical criticality are managed as urgent production launches (ECAB).

Equipment inventory files are updated after applying patches.

### Reporting

The Operations Security Manager prepares an internal monthly report on the security watch and vulnerabilities processed over the period. This report is produced using the Orange internal tools and for confidentiality reasons is not sent to customers.

In the case of a critical vulnerability likely to seriously affect its customers, Orange Business Services may communicate directly with its customers to inform them.

### 4.8.6 Security of administratives workstations within Orange

All Orange operator workstations used to administrate Cloud infrastructures and services are based on generic and secure configuration models:

- The configuration of workstations (operating system, middleware and applications, user rights) is stringent from a security point of view. (hardened master for internal purpose "E-buro");
- There is systematically an antivirus which is updated automatically and regularly;
- Policy of system updates with Orange patches validated internally before circulation.

All workstations hard disks are encrypted using McAfee Endpoint Encryption for PC (eePC) solution. Sensitive data can also be encrypted using ZoneCentral encryption tool. ZoneCentral is a security product for encrypting the data on hard drives, emails, and containers with access reserved for authorized and identified users only. The ZoneCentral tool has been certified EAL3+ by ANSSI (ANSSI-CC-2012/07) issued on February 13<sup>th</sup>, 2012.

All work to be done or executed are performed via jump servers that are under stricter and more secured environments. These jump boxes are then filtered and monitored by token based access platforms such as CyberArk that trace each activity and can be replayed for auditing.

### 4.8.7 Secure administration portal

An administration portal is available for each customer for managing the various services and users; it is accessible from the Internet and/or the Orange Business Services customer VPN. The administration portal is accessible in HTTPS (TLS) via a login/password. The administrators' user IDs (login/password) are previously sent by Orange Business Services to the customer following a secure procedure. Server authentication is performed with an X.509 certificate.

All these actions performed on the portal are logged.

## 4.9 Communications security

*This chapter corresponds to section 13 in ISO 27002 version 2013.*

### 4.9.1 Orange Cloud architecture policy

#### General principles

The architectures of the various Cloud services or templates of architectures for Cloud Avenue are validated by an engineering security manager under the governance of the Chief Security, Risk and Compliance Officer. The latter guarantees the coherence of the various architectures from a security point of view.

This approach based on a predefined architecture model offers several advantages:

- Simplifies deployment of new Cloud services;
- Makes practices and architectures homogeneous across the various services;
- Enables sharing of some equipment;
- Guarantees the security of services: the models are validated then their deployment is overseen by the Cloud Security Competence Center. The security level of each new service is also assessed by audits and intrusion tests before production launch. This also applies to all major changes. The results of internal audits and intrusion tests are not sent to customers for confidentiality reasons.
- Makes it easier to maintain secure conditions.

For each new service, the security validation of the architecture is completed with a systematic risk analysis. These 2 actions form the basis of the "SecurityInTTM" approach to guarantee that security is taken into account in the design of services.

#### Trusted domains and Security zones

The architectures of the various Cloud services all apply the same model consisting of separating trusted domains, including the Back-end (Orange internal) and Front End supporting the Cloud services seen by customers. Back-end / Front End partitioning is physical, i.e. there are servers dedicated to the back-end and others dedicated to the front-end. Within each trusted domain, security zones provide virtual partitioning by using functionalities such as:

- Virtualization (virtual machines, virtual firewalls, virtual load balancers,

- virtual routers);
- VLANs;
- Virtual networks VPN;
- Virtual storage.

Virtual partitioning guarantees the isolation of the various customer environments.

Communications (network flows) between the various security zones are systematically controlled by firewalls. The local configuration of the various components is also designed to strengthen partitioning and security.

### Orange infrastructure

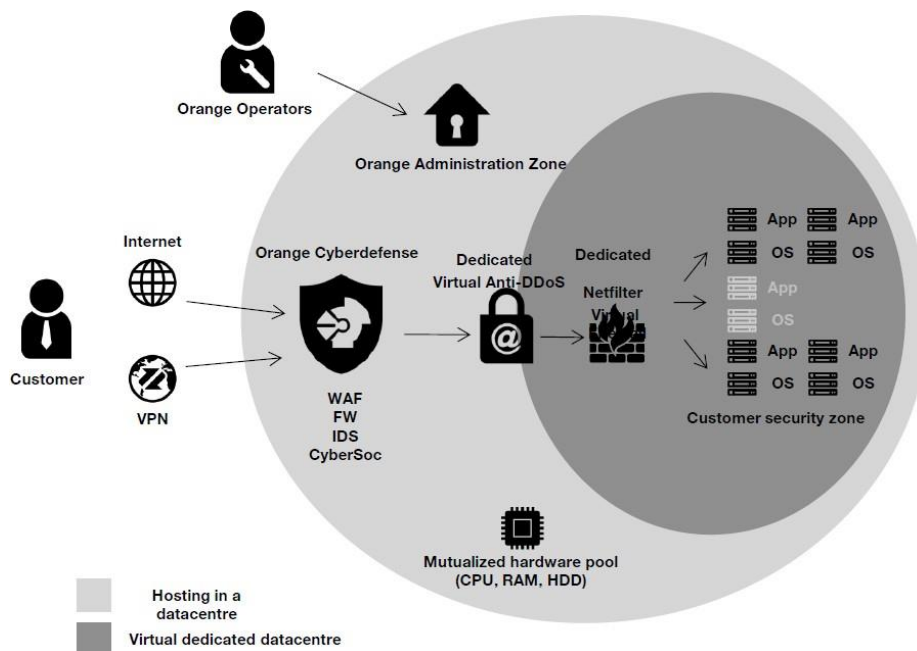
Infrastructure servers are clustered into security zones according to their function (administration server, front-end server used by customers), their nature (database, webservers) and their level of exposure (for example, whether or not they are accessible by customers). Thus, security zones are dedicated to the Orange operating tools.

In general, all the servers have an interface dedicated to data workflows and a technical interface dedicated to service workflows (including administration).

All cloud infrastructure components (servers, firewall, routers, storage bays, etc.) are configured based on secure configuration guidelines established by the various engineering departments with the assistance of Orange group security experts.

### Customer environments

Isolation between customer environments is based on the virtualization functions described above. Within an environment, the customer can manage security functions (including virtual firewalls). The functions supplied to customers vary according to the chosen services and options.



## 4.9.2 Security of exchange

### Security of Orange internal workflows

Orange internal exchanges are rendered secure by the following means:

- **Networks:** The interconnection networks between Cloud platforms and operating platforms are protected by encrypted tunnels (TLS 1.2)
- **Messaging:** At the customers' request, sensitive data exchanged by email between customers and Orange Business Services can be encrypted by a third party tool agreed with the customer (e.g.: Zed containers). Orange Business Services leverage PKI based email security across all departments and locations using smart cards or USB dongles.
- **Administration flows:** Administration workflows are given state of the art protection in accordance with SSL-type connections (SSH, HTTPS).

Exchanges between the various security zones are systematically controlled by firewalls applying the elementary principle, "anything not explicitly authorized is forbidden". Flows are logged.

### Customer flow security

Customers log in to cloud environments for the purpose of administration or access to services. Customers' administration flows are systematically rendered secure by protocols guaranteeing their authentication, confidentiality and integrity (TLSv1.2, AES256, etc.). Access methods vary according to the services and options chosen by the customer.

The security of service workflows depends on the service in question, but in general, exchanges are secured with a TLS connection.

## 4.10 Acquisition, development and maintenance of information systems

*This chapter corresponds to section 14 in ISO 27002 version 2013.*

### 4.10.1 Risk analysis

All changes (acquisitions, developments, etc.) are subject to security risk analysis carried out by the Orange Cloud for Business security team. Risk analyses enable security measures to be put into place to limit the risks identified. For confidentiality reasons these documents are not sent to customers.

## 4.10.2 Good development and integration practice

### Good development practices

The specific developments carried out by Orange or by a subcontractor comply with the internal Orange guide on best secure development practices described in our internal security policy.

### Good integration practices / strengthening of configuration security

Systems and software under Orange's responsibility are configured with a high level of security by applying a "hardening guide". For example, for VMware based environments like Cloud Avenue, Orange relies on the security guides established by VMware.

(<https://www.vmware.com/security/hardening-guides.html>)

## 4.10.3 Security acceptance

### Security validation of components

The most critical components on the Cloud platform are subject to security tests (configuration/code review and/or intrusion tests) to validate their security level.

As an example, the administration portals have already been subjected to several intrusion tests and a configuration/code review).

All the templates (OS or applications) supplied by Orange are also subject to validation and are regularly tested and updated to take account of the latest vulnerabilities.

### Non-production platform

Development/qualification/pre-production platforms are available, in particular to validate the security of changes or to conduct complete intrusion audits.

### Absence of customer data on non-production platforms

There are no customer data on non-production platforms, which are completely separate from production platforms.

## 4.11 Subcontractor management

*This chapter corresponds to section 15 in ISO 27002 version 2013.*

### 4.11.1 Security in contract with our subcontractors

In our contracts, our service providers/suppliers give an undertaking on the confidentiality and integrity of data to which they have access during the service.

Subcontractors integrated into internal Orange teams use the same tools and processes as Orange staff and therefore, by default, comply with best practice as set out in this document: awareness, physical and virtual access control, etc.

### 4.12.2 Security monitoring of services provided by our subcontractors

As part of sourcing process, Orange subcontractors are due to describe their security measures in a security assurance plan reviewed annually. Orange may also audit its subcontractors to verify that they are complying with the contractual security undertakings. These audits result in security action plans for improving the security level of subcontractors.

## 4.12 Management of security incidents

*This chapter corresponds to section 16 in ISO 27002 version 2013.*

The policy on managing security incidents is described in chapter 5 and annex A of "OCB security policy". It is set out in chapter "15.1 – Security Incident Management" in the incident management process. The present chapter explains the principles described in these documents.

### Preparation of operational teams

The purpose of this phase is to prepare each person for processing incidents: operational excellence (awareness, regular training in managing various types of incident, etc.) and quick access to up-to-date documentation (asset inventories, network diagrams, technical documentation, logs, etc.).

### Detection of security incidents

The means of detection deployed for detecting a security incident are:

- Supervision tools;
- SIEM<sup>18</sup> in charge of supervising logs (IPS, log FW, systems log, application logs, etc.);
- Watch cell;
- Security team and other personnel;
- Alerts from customers;
- Complaints from other providers via Abuse Desk.

This supervision is performed on components that are the direct responsibility of Orange (portals, hypervisors, customer environments with security managed by Orange, etc.).

Seriousness of the incident - The table below summarizes the levels of seriousness of incidents and the actions to be carried out:

Level	Description
High	Corrective action immediately
Medium	Action can be delayed, but a security maintenance operation must be scheduled now
Low	Action can be delayed until the next scheduled maintenance operation

The incident ticket is directed to the appropriate team including the Security Department.

### Response to security incidents

The following responses may be given:

- Emergency measures (quarantine, etc.);
- Crisis cell activation;
- Communication with customers, partners, operators, etc.
- Patch application;
- System recovery;

### Post-incident review and actions

Once the security incident has been dealt with, the Orange Business Services security team analyzes the nature of the incident and the quality of Orange's response. If necessary, the Orange Business Services security team updates the procedures for managing security incidents as part of the continuous improvement approach.

---

SIEM<sup>18</sup> : Security Information Event Management, a tool for correlating logs



## 4.13 Security in the management of business continuity

*This chapter corresponds to section 17 in ISO 27002 version 2013.*

The availability rates of each service are given in the service descriptions.

All our Cloud services have complete infrastructure redundancy over two sites (or, as a temporary exception, over several computer rooms), with high availability mechanisms so that local failures are made transparent: network (Internet access, VPN access, and firewall), administration portal, virtualization, storage, etc.

Backups are performed daily with an array snapshot for a 7 days retention. Depending on the service, a backup file save can be done with Netbackup or Flexible storage.

There are rollback clauses in the Cloud services contracts. If the Service is terminated, unless the termination is through a fault of the customer, the customer can ask Orange Business Services to trigger rollback. Orange Business Services will then deploy the means reasonably necessary to ensure continuity of the Service, so that at the end of the Rollback Period, the customer is afforded the capacities to continue to satisfy their requirements (cf. contract for more details).

## 4.14 Conformity

*This chapter corresponds to section 18 in ISO 27002 version 2013.*

### 4.14.1 Compliance with legal and contractual requirements

As part of the risk analysis attached to all Orange projects, a review of the legal and contractual obligations is conducted and an action plan is proposed. The resulting deliverable is called the LOA (Legal Obligation Assessment). The points covered are:

- Compliance with contractual clauses (licenses, industrial property, specific undertakings in the description of services, etc.).
- compliance with specific regulations arising from Orange's field of activity (LCEN<sup>19</sup> and CPCE<sup>20</sup>);
- Keeping a register of the processing of data of a personal nature, in conformity with the law of 6 January 1978 and General Data Protection Regulation (GDPR). Orange Business Services has nominated a Data Protection Officer (DPO) who keeps the register. The DPO is the contact specialized in the protection of personal

---

LCEN<sup>19</sup> : Law on Confidence in the Digital Economy

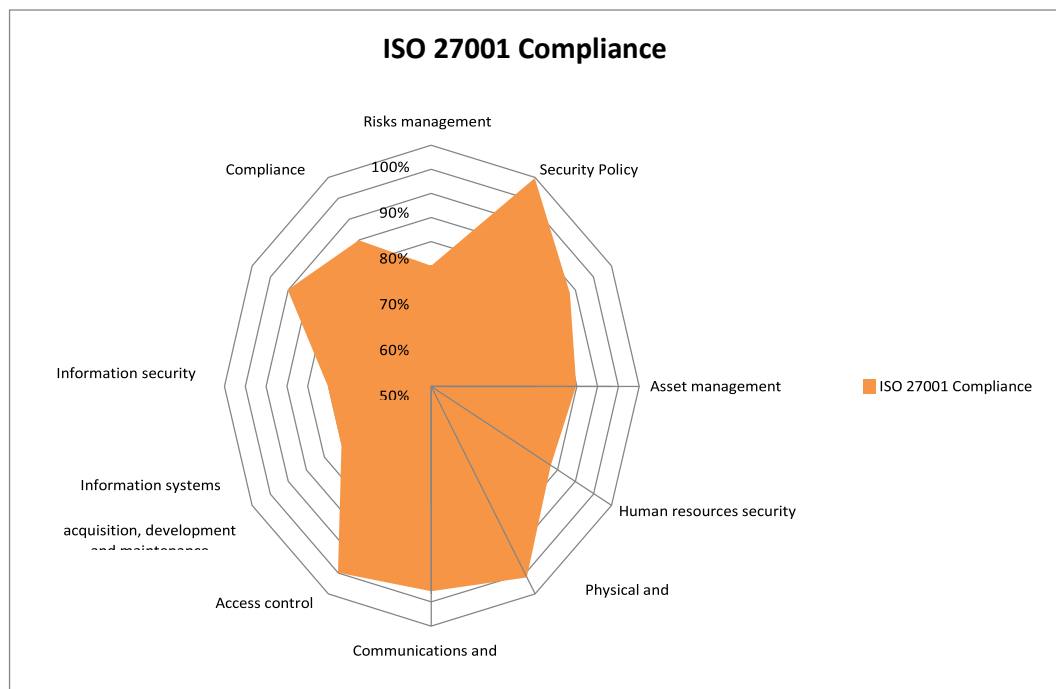
CPCE<sup>20</sup> : Post and Electronic Communications Code

data, both for the manager processing these data and in the relations between the latter and the CNIL (French National Commission for Data Protection and Freedom), the independent administrative authority charged with overseeing compliance with the freedom of information act. The DPO thus has a central role in the secure development of new information and communication technologies, and within the company disseminates the culture of freedom of information and the control of risks to personal data.

#### 4.14.2 Monitoring compliance with security policy

Orange Business Services is in charge of monitoring application of the Security Policy for each Cloud service. Thus it performs continuous monitoring and runs organizational and technical audits.

- Example of organizational audit: control of rights management
- Examples of technical audits: intrusion tests, Nessus or Qualys scans, configuration audit, etc.



Example of ISO 27001 maturity report (values given as examples)

In addition to this, Orange Business Services undergoes regular audits (AFNOR, ISAE 3402) conducted by external bodies and leading to security level checks.

### 4.14.3 Security related certifications

Orange<sup>21</sup> has the following certifications pertaining to the scope of Cloud services:

- **ISO 27001 security certification**
  - Orange Business Services has ISO 27001 security certification within the scope of the "deployment, supply and support of service management and communications solutions" for the sites in Cesson-Sévigné, Egypt, Mauritius.
- **ISO 27017 security certification**
  - Orange Business Services is one of the first French companies to be ISO 27017 certified, taking into account the entirety of the security recommendations specifically dedicated to cloud security (the highest security level).
- **ISO 27018 security certification**
  - Orange Business Services is one of the first French companies to be ISO 27018 certified, taking into account the entirety of the security recommendations specifically dedicated to the protection of personal data (the highest security level).

---

Orange<sup>21</sup> : List of certifications <https://cloud.orange-business.com/choisir-le-cloud-orange/certifications/certifications-des-offres-de-cloud/>

## 5 Specific security measure

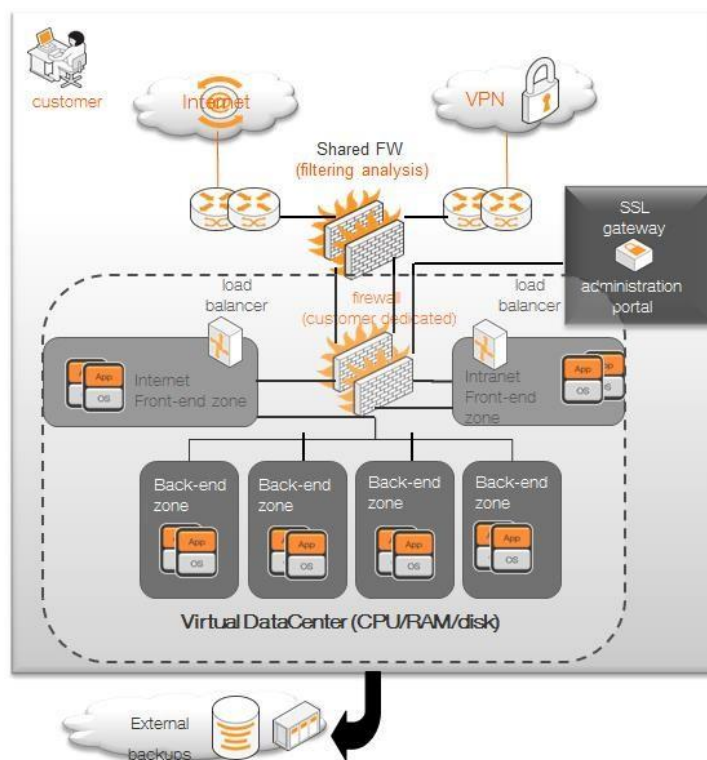
The purpose of this chapter is to present the security measures specific to each service. They are complementary to the common security measures presented in chapter 4.

### 5.1 Compute service

Orange Cloud Avenue provides wide range of cloud-based computing services with varying instance configurations that can scale up and down automatically depending on customer business requirements.

The following security measures are deployed in this service:

- Virtual firewall security zones;
- Virtual Load Balancing;
- Strong authentication by software authenticator.



#### 5.1.1 Virtual machine

A virtual machine is a computing server that consists of CPU, memory, image, storage disks and allows on-demand allocation and scaling.

A virtual machine integrates security group, and multi-data-copy capabilities to build up an efficient, secure, and reliable computing environment for users to ensure stable, continuous running of their services.

A virtual machine can be added to a Vapp which is a group of virtual machine dedicated for an application and a Vapp can be added to a Virtual Datacenter (VDC) to have an easy control on your infrastructure and platform.

### 5.1.2 Auto scaling

Customers can himself change the settings of his infrastructure with auto scaling to automatically scale service resources up and down based on service requirements. Auto scaling ensures that resource usage satisfies current service requirements without any manual intervention, scaling application systems out as service utilization grows with tenant business and scaling in as it declines.

Auto scaling helps avoid the impact of resource exhaustion-type attacks as well as security risks resulting from human errors during manual allocation of resources.

### 5.1.3 Image management service

An image is used to create a virtual machine with a preinstalled Operating System (OS). Image management service on Cloud Avenue is managed by VCD (VMware Cloud Director) to allow you to upload an ISO/OVA to a catalog. This allow a user to create, edit and delete images.

These images can be divided into 3 categories:

- Public images are standard operating system images provided by Cloud Avenue.
- Private images are created by users for their own used.
- Shared images are custom images created by any user, maintained on a voluntary basis by the user community and provided for all users to use.

VCD interface provides a simple and convenient self-service management functions for images. Customers can manage their images through VCD. Cloud Avenue staff update and maintain public images, which includes performing security hardening and applying security patches on them as required. The staff also provide security-related information for users to reference in deployment testing, troubleshooting, and other O&M activities. Users can deploy their virtual machine by selecting one of the public images provided, creating a private image from an existing cloud server deployment or an external image file, or using a shared image and participating in its development and maintenance.

### 5.1.4 Dedicated cloud

By default (standard mode) all the resources are shared between customers. If a customer has strong requirements, Cloud Avenue can offer a dedicated cloud. A dedicated cloud provides an isolated virtual computing resource pool in the Public Cloud, in which a Tenant can apply for dedicated physical servers to build their own computing resources pool and use highly reliable distributed storage resources and isolated networks.

A dedicated cloud is very suitable for scenarios which customers have very critical requirements about security isolation, high performance and high reliability, such as financial and government organizations etc.

## 5.2 Storage, Backup and Disaster recovery service

### 5.2.1 Datastore storage

Datastore storage is a scalable virtual block storage service based on the distributed architecture. The method for using a datastore is the same as that for using hard disks on traditional servers. Maximum file size for a VDMK file is 2 To. If a virtual machine should have a storage up to 2 To, customers need to add multiple VDMK file to reach the wanted storage for the virtual machine.

Datastore storage can divided into 2 modes:

- Mutualized storage (by default). Even if the storage is mutualized, a strong segregation is present. This means customer' storage is only readable by the customer and nobody else.
- Dedicated storage, with guaranteed performance (with One room, Dual room or HA Dual room. Encryption is an option as well to securely store customers' data).

### 5.2.2 Network storage

Network storage supports CIFS and NFS protocol. For a security concern this kind of storage has to be dedicated to prevent other customers to access it.

On this case, customer can himself decide the snapshot policy for the network storage.

### 5.2.3 Backup

Backup option is a self-service option offers by the software NetBackup Self-Service. This feature allow the customers to have a secure and efficient way to backup your virtual machine.

The provided features are:

- Access to a portal to manage your backup called NSS<sup>22</sup> (NetBackup Service) portal
- Save virtual machine on pre-defined policy. This save is local that's mean the data are saved on the same datacenter that the virtual machine.
- Restore a virtual machine through NSS portal
- Save through replication to another physical location

---

<sup>22</sup> NSS : <https://www.veritas.com/fr/fr/protection/netbackup/self-service>

- Daily report as a “weather” to have a quick look of the status.

### Backup and restore a virtual machine

NSS portal offers a complete control to manage your backup policy according to customers' recommendation. The options to backup or restore a virtual machine are:

- Visualize which virtual machine has a backup policy or not
- Apply a backup policy to your virtual machine(s)
- Restore (completely or partially) a virtual machine
- Perform an immediate backup of a virtual machine
- Visualize backup storage per virtual machine and the global volume storage used by backups

A backup policy is defined by a local backup frequency, a local retention period, a backup range and a remote location backup (optional).

For customers with high requirement it's possible to encrypt the backup to improve the overall security of the backups.

## 5.2.4 Disaster recovery service

### Virtual machine replication to a remote site

This feature provided by Cloud Avenue offers disaster recovery plan to securely replicate virtual machine from the main Cloud Avenue site to the backup site. This solution is based on the Zerto<sup>23</sup> software (Zerto Virtual Replication). A portal is provided by Orange to his customer to manage these backups. With this solution you can:

- Protect some or all your virtual machine
- Manage the failover and the restoration between the main Cloud Avenue site and the backup site

This solution offers more advantages for the customers including security advantages because the customer can himself manage his infrastructure according to his planning and provide an application data protection as well as the infrastructure itself.

Cloud Avenue is compatible at least with TIER III+, with a minimal theoretical availability of 99,90%. The combination of Cloud Avenue availability and the offered solutions for backup allow a high resilience on customer's infrastructure.

---

<sup>23</sup> Zerto : <https://www.zerto.com/>

## 5.3 Network services

### 5.3.1 Edge gateway

This network and security layer of Cloud Avenue is managed by VMware solution named NSX. It is performed on 2 different levels to have a better security segregation:

- A “Provider Edge Service Gateway” level, in which the NSX gateways connected to the various external networks (internet, VPN Gallery, others) are located; at this level, the gateways are managed by Orange Business Services. A separate gateway is deployed for each external network.
- An "Edge Gateway vDC" level, in which there are the Edge gateways connected to the vDCs and carrying the various organizational networks; at this level, the gateways are managed by the Customer directly in the VCD portal.

A vDC Edge Gateway is used to create Organization networks that can be shared among all of the Organization's vDCs. Each vDC Edge Gateway can be attached to a single Provider Edge tier gateway.

Two levels of vDC Edge Gateway resiliency are available:

- "Standalone" mode: its resilience is ensured by the VMware HA option, which allows you to restart a VM in less than a minute.
- HA mode (High Availability): activates a 2nd gateway, the two work in a cluster, with a switchover in 9s maximum in the event of a problem.

Two levels of vDC Edge Gateway management interface are available:

- Standard (default) - configuration of the following functionalities: Router, Firewall, NAT, DHCP, Load Balancer and IP-Sec Tunnel (point to point).
- Advanced - access to all the network functions of VCD: Firewall, NAT, DHCP, Routing (dynamic), Load Balancer, VPN IPSec, VPN-Plus SSL (nomadic access) and SSL Certificates (can be implemented in the Load Balancer), as well as :
  - A distributed firewall, which makes it possible to implement the micro-segmentation mechanisms specific to VMware NSX
  - A complete Load Balancer based on the HA proxy software, capable among other things of doing SSL offload.



### 5.3.2 NAT Gateway

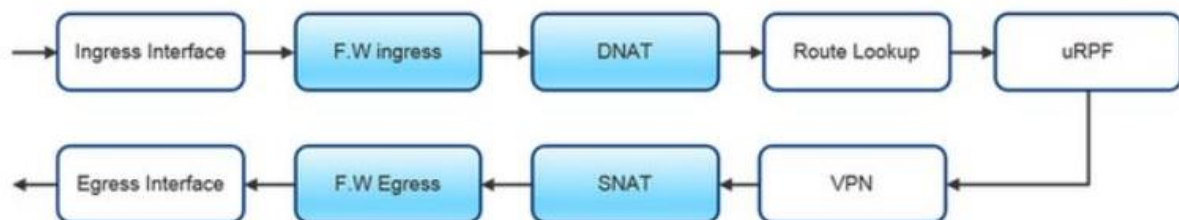
The NAT Gateway service offers the Network Address Translation (NAT) function for your organizations. This feature is managed by the Edge gateway (description in 5.3.1).

The NAT Gateway service provides different types for different application scenarios. These scenarios are explained in the tab below:

Rule	Common name	Description
DNAT	Destination NAT	A DNAT rule is an ingress rule. It is used to forward an incoming packet on a public interface to a virtual machine on a private network  To make it clear it's a communication <b>from</b> a public network <b>to</b> a private network
SNAT	Source NAT	A SNAT rule is an egress rule. It is used to forward a packet from a private interface to an external network (public)  To make it clear it's a communication <b>from</b> a private network <b>to</b> a public network

With DNAT you can only translate one IP address to one “natted” IP address (1:1). On the contrary with SNAT you can translate one or more (a subnet for example) IP address to one “natted” IP address (we can configure 1:1 or n:1).

Firewall and NAT rules can be mixed. The picture below summarizes when we have mixed rules between NAT and firewall



NAT and firewall rules mixed

### 5.3.3 Distributed firewall

The Customer has the option of configuring firewall rules directly at the Virtual Machines level. This is called micro segmentation. Unlike a perimeter firewall, which defines trust zones and filters the flows between these trust zones, the distributed firewall implements filtering rules directly at the level of the “VM Kernel” of the Virtual Machines, which makes it possible to build zones of virtual trust, although the VMs are on the same network (same “subnet”).

These filtering rules are configured via the VCD portal, via the context menu of a vDC.

The advantages of using the distributed firewall:

- Security rules remain valid after moving the VM to another vDC
- The protection is valid in the "east-west" direction; even if a machine on the network located after the perimeter FW is compromised, security rules continue to protect other machines on the network.

## 5.4 Security and Identity Service

### 5.4.1 Anti DOS/DDOS

The anti-distributed denial of service (Anti-DDoS) aims to provide precise capabilities for defending DDoS attacks.

Anti-DDoS provides the following functions in Cloud Avenue environment:

- A free protection against denial of service (DOS or DDOS) named "black hole". This mechanism protect the mutualized customers against an attacker by redirecting the flows to a network black hole. This makes the service not available anymore.
- As an option, a solution called "clean pipe". This mechanism is based on the fact to know which resource we want to protect and clean the illegitimate flows to keep the service available from the legitimate flows.

### 5.4.2 IPS probe and WAF

With the accurate certificate, Cloud Avenue has an IPS (Intrusion Preventive System) probe deployed in the infrastructure to detect any malicious activity on the platform. This allow our operational team to have more reactivity in case of attack and quickly respond to an accurate actions in order to block the malicious traffic from layer 3 and 4 from the OSI model<sup>24</sup>.

We have the same security with a WAF for the Web Application Firewall (WAF) to block unwanted traffic/requests for layer 7 from the OSI model which is the application level (HTTP and HTTPS).

---

<sup>24</sup> OSI model : [https://en.wikipedia.org/wiki/OSI\\_model](https://en.wikipedia.org/wiki/OSI_model)

## A. TIER Classification of a datacenter

Datacenter classification by the Uptime Institute is currently the only world-recognized reference base: it defines performance in terms of the continuity of services and technical infrastructure of a datacenter. This classification is deliberately simplified into five main levels (called tiers), shown in the following table, corresponding to the main infrastructure categories, the initial deployment phases and the handling capacities in terms of electrical load (W/m<sup>2</sup>). Each level is assigned a statistical availability index based on the functioning history of dozens of major datacenters and on reliability studies carried out using expert software.

	Tier I	Tier II	Tier III	Tier III+	Tier IV
Source of replacement	1 generator	1 generator	1 generator	1 generator	2 or (N+1) generators
Primary energy	1 active line	1 active line	1 active line and 1 passive line	Rated power after a major fault	Rated power after a major fault
High Quality energy	1 active line	1 active line	1 active line and 1 passive line	2 active lines	2 active lines
High Quality redundancy	N	N+1	N+1	2N or 2(N+1)	2N or 2(N+1)
Maintainable without operation shut-down	No	No	Yes	Yes	Yes
Maximum charge level (Watt/m <sup>2</sup> )	250 W/m <sup>2</sup>	500 W/m <sup>2</sup>	1000 W/m <sup>2</sup>	>1000 W/m <sup>2</sup>	>1000 W/m <sup>2</sup>
Theoretical availability rate	99.671%	99.749%	99.982%	99.990%	99.995%
Maximum number of hours of service down time per year averaged over several years and several datacenters	28.82 h/year	21.98 h/year	1.58 h/year	0.87 h/year	0.44 h/year

The infrastructures set up by Orange in its generation 2004-2010 datacenters are classified at TIER III+ level. The latest generation datacenters, built after 2010, are in tier IV. In some of them, the air conditioning installations are equipped with the free-cooling function.