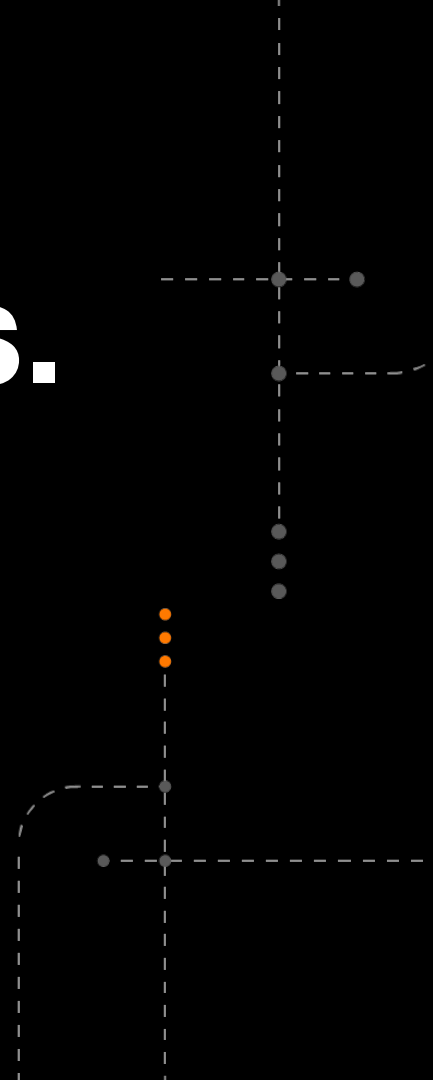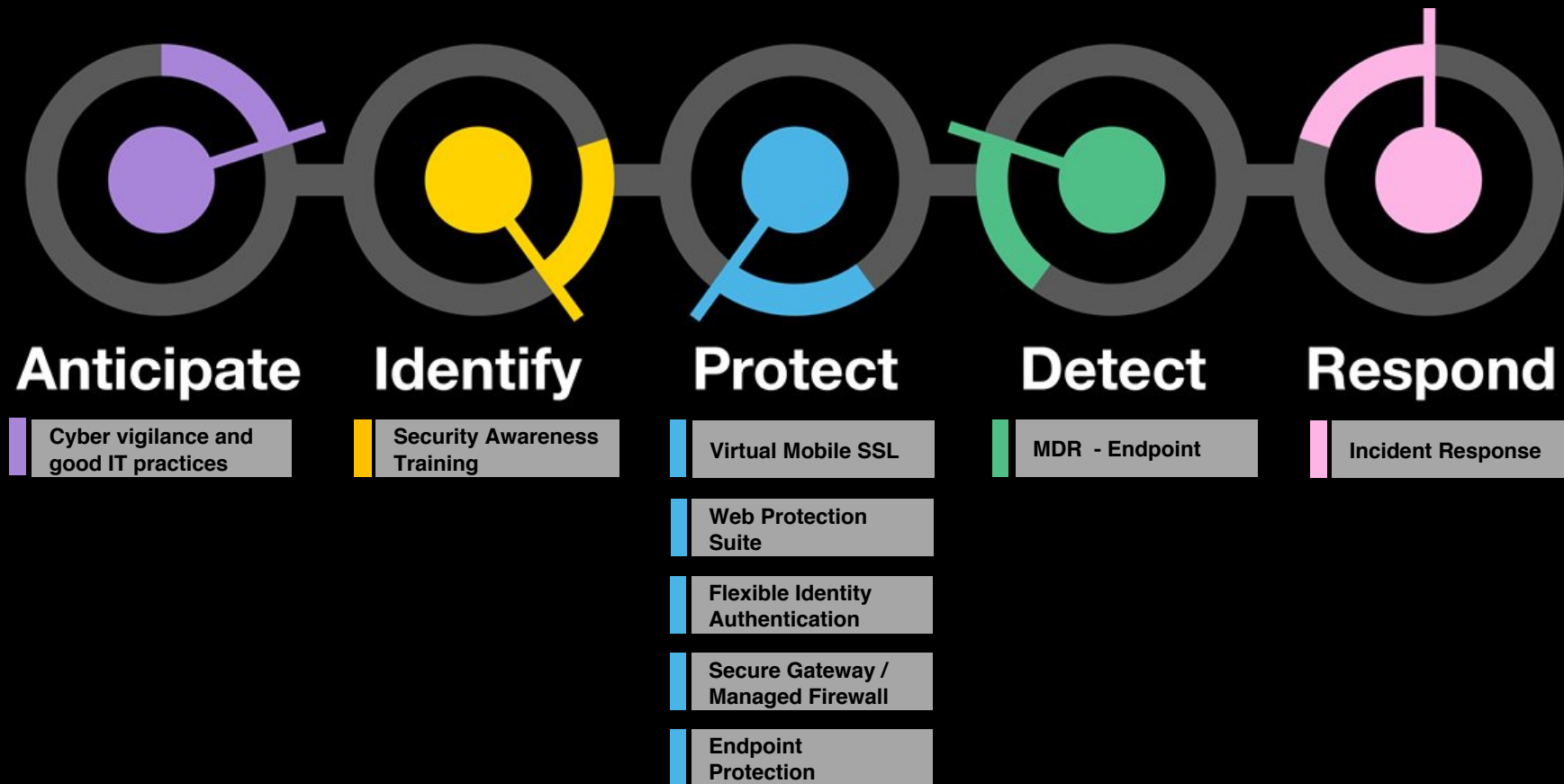# Our solutions adapted to this crisis.

Orange Cyberdefense Global Portfolio Specific Solutions for the Crisis

Anticipate
- Cyber vigilance and good IT practices

Identify
- Security Awareness Training

Protect
- Virtual Mobile SSL
- Web Protection Suite
- Flexible Identity Authentication
- Secure Gateway / Managed Firewall
- Endpoint Protection

Detect
- MDR - Endpoint

Respond
- Incident Response

Anticipate

Strengthen good IT hygiene practices

Strengthen good IT hygiene practices

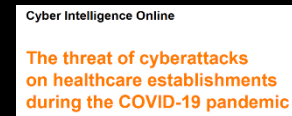**The advice from the National Cyber Security Centre**

Click on the image to open the link

Orange Cyberdefense's COVID 19 Advisory Paper

Click on the image to open the link

Threat intelligence: the report of our Epidemiology Lab

Click on the image to open the link

For more personalized support in the context of your business, please contact your OCD business contact.

Identify

Ensuring that my staff are well informed on Security Best Practices in the Crisis

Security Awareness Training

COVID-19 crisis

Customer Challenge

- What do my staff need to be more aware of during the Crisis and whilst typically working remotely from our offices?

Security Awareness Training at a glance

- Increasing awareness and improving the behavior of employees as a continuous process
- An effective security awareness program helps to reduce the risks within an organization by increasing awareness and securing cyber behavior from different interactive perspectives.

Specific measures set up during the Covid-19 crisis

- Employees are the 'human endpoint' of the IT environment and are vulnerable to malicious attacks, especially in the crisis.
- Organizations must mitigate risks by promoting awareness and safe behavior among employees.
- Insight into results, and progress of awareness and behavior, is necessary to be in control.

Raise the Security Awareness of your employees

Highly experienced Advisory Services and Training team

Can be delivered remotely online

Protect

Protect the information system, remote access, emails

Virtual Mobile SSL

Customer Challenge

▪ Requirement for additional remote access capabilities

Virtual Mobile SSL at a glance

Virtual Mobile SSL is a bespoke solution for remote access via virtual platforms installed inside the customer's Azure cloud environment (AWS and Flexible Engine coming soon). These virtual platforms are connected to the customer BVPN via Galerie and/or Expressroute or to a third-party MPLS via Expressroute. The customer manages the Expressroute junction.

Home and virtual workers → **Virtual Mobile SSL** → **Enterprise IT**

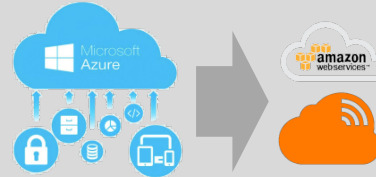**Multi-BU**

Offer packaged with:

▪ BVPN Galerie

▪ **Flexible Engine coming soon**

Prerequisites / Detail

10 to 5000 users per virtual platform

Customer has a public Azure cloud (soon AWS and FE)
Active Directory (AD, LDAP, RADIUS)

Web Protection Suite (WPS) – ZPA

COVID-19 crisis
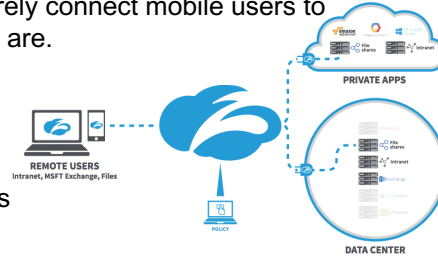
Customer Challenge

- Requirement to increase the number of remote access users

Web Protection Suite (WPS) at a glance

Fully managed cloud solution to securely connect mobile users to corporate applications, wherever they are.

Customer needs:
1. WPS subscription
2. Client on the terminals
3. VM connection to the data-centers

Service is based on an OPEX model, charged on a per user basis

Quickly answer to emergencies

**Prerequisites / Detail**

Fully Cloud-based,
No equipment to install

Flexible Identity Authentication (FIA)

COVID-19 crisis

Customer Challenge

▪ Improve the security of remote access

FIA at a glance

FIA protects the company's assets with single-use passwords, particularly for users connected remotely. A cloud-based solution that combines flexibility and agility

Authentication mode adapted to the user

Cloud Services

Enterprise IT
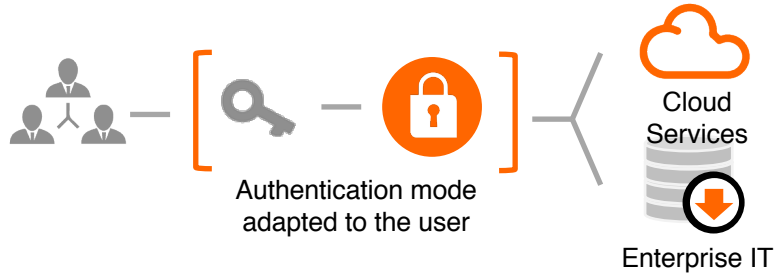
Offer benefits during the Covid-19 crisis

▪ Additional security of remote SSL VPN access, with a strong authentication process

Enhanced security

Secure Authentication
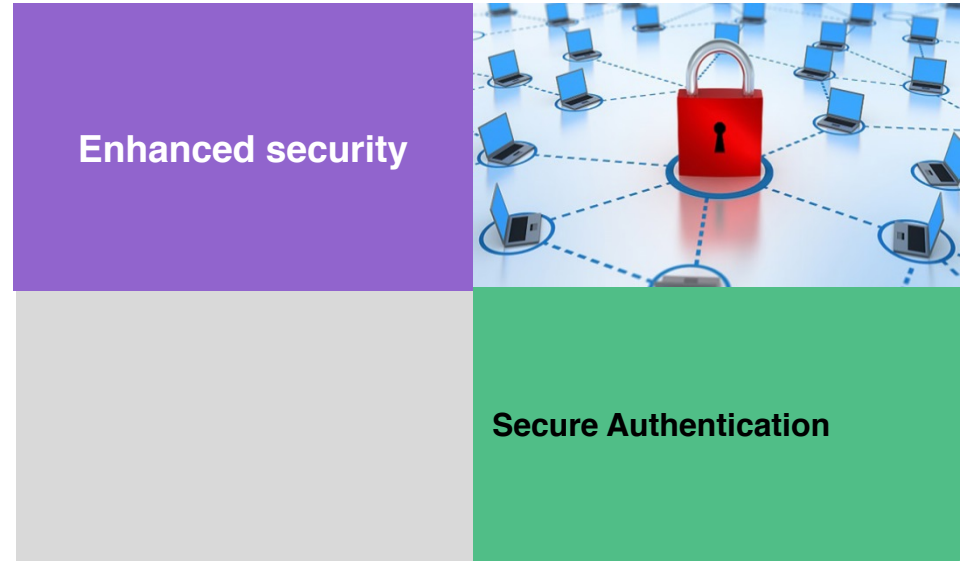
Secure Gateway / Managed Firewall

COVID-19 crisis

Customer Challenge

▪ Requirement to increase the number of remote access users

Managed Firewall at a glance

Managed Firewall is a fully managed security providing protection to companies' networks. The solution provides a secure internet connection and protects the internal network with a large range of appliances with various sizing.

Managed NG Firewall **+** Or/And Proxy Anti-virus Web filtering Intrusion prevention

Offer benefits during the Covid-19 crisis

▪ The Managed Firewall offer includes a remote access option that can be enabled in such situations. Enabling the option for the first time requires a new order form.
▪ On Fortinet technology, the number of SSL VPN users can be increased temporarily above 30 users, during the crisis period. The maximum number of users has to be confirmed depending on the firewall capacity and utilization.

On Fortinet & Palo Alto managed firewalls, the number of concurrent SSL VPNs can be temporarily increased to help crisis period

Prerequisites / Detail

Internal IP address ranges for assignment to remotely connecting users.

Endpoint Protection Service

COVID-19 crisis

Customer Challenge

- Endpoint lacking proper protection from security attacks

Endpoint Protection at a glance

Traditional endpoint protection software is failing to detect and stop unknown attacks, due to their unique and constant changing signature and built-in evasion.

Orange Endpoint Protection Service leverages AI-based detection agents that effectively detects and stops threats never seen before

Offer benefits during the Covid-19 crisis

- Keep your employees productive when working from home.
  Due to the Covid-19 crisis it will be difficult for IT and CSIRT team to clean remote workers computers.

Enhanced Endpoint security

BlackBerry | CYLANCE

Prerequisites / Detail

Cloud Multi-tenant Management. Easy to spin up and deploy.
Pay-as-you-go option available

Detect

Detecting threats and protecting workplaces

Managed Threat Detection – Endpoint

COVID-19 crisis

Customer Challenge

- Many CyberSOC teams are losing a lot of visibility about what is happening on the workers' endpoint now when they are working remote. Is their existing endpoint protection working or not?

MTD Endpoint at a glance

MTD Endpoint leverages a small sensor that is deployed on all the endpoints that you want to monitor. It tracks all activities to be able to detect the threats that your endpoint protection could not stop.

Orange security analysts are monitoring indicators of threat 24x7 and will quickly respond to identified threats.

Offer benefits during the Covid-19 crisis

- Getting visibility about the security status of remote workers
- Being able to respond remotely if threats are detected
- Can be deployed across the company or only on employees with access to sensitive data.

Managed Threat Detection & Response

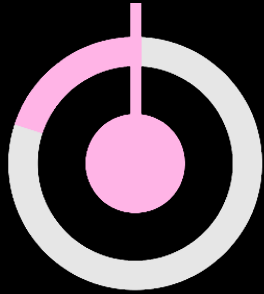Great compliment to any existing endpoint protection (ex: Microsoft, Symantec..)

cybereason®
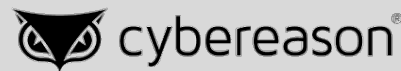
Prerequisites / Detail
Cloud Managed
Only sensors needs to be deployed by customer

Respond

How to react in the event of an attack:
Incident Response

Incident Response

Customer Challenge

▪ What do I do in case I have a serious breach?
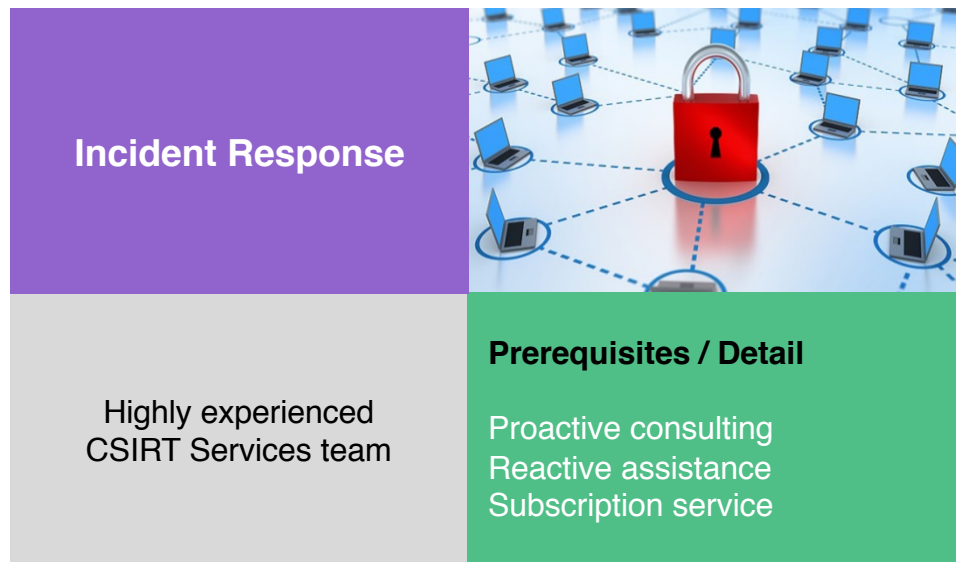
Incident Response at a glance

Orange highly experienced incident responders can help you across the entire lifecycle of an incident. This includes services from proactive preparations to containment and eradication of threats.

The team has experiences ranging from digital forensics work, to responding to large scale ransomware attacks and advanced nation-state attacks.

Offer benefits during the Covid-19 crisis

▪ **Incident Response Workshop** – Proactive engagement to understand your current capabilities and help establish processes to be prepared

▪ **Incident Response Retaine**r – Subscription service that guarantees our help (with SLA) in case of an incident

▪ **Incident Response Emergency** – Reactive service without subscription where we will help customers based on available resources.

Incident Response

Highly experienced
CSIRT Services team

Prerequisites / Detail

Proactive consulting
Reactive assistance
Subscription service

Stakes

Work anywhere during a crisis

With self-isolation imposed by governments due to the coronavirus crisis, it is essential to allow my collaborators, safely access to the Information System, while working from home, with any equipment

Work anywhere as if in the office

Secure access to your Information System

- From anywhere
- With a computer, a tablet or a smartphone
- Encryption between the end-user device and Virtual Mobile SSL

Teleworkers and mobile workers

Virtual Mobile SSL

Public Cloud

Information System of the company
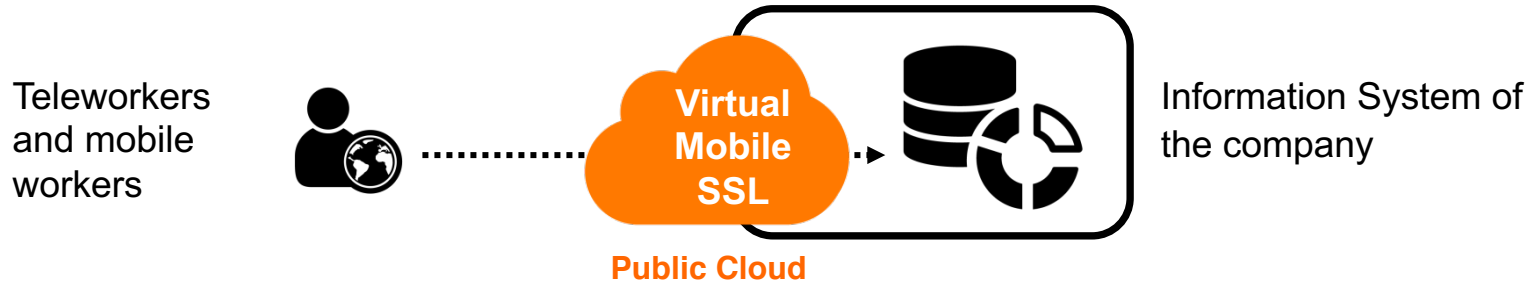
- Virtual Mobile SSL installed on Customer's Public Cloud tenant : Azure, AWS, Flexible Engine
- Service available independently of your Internet provider and type of Internet access: 5G, 4G, Wi-Fi, etc.

Targets **and prerequisites**

International businesses of any sector and size

Must have:

- A tenant in Public Cloud : Azure, AWS or Flexible Engine

- A directory: AD, LDAP, Radius

- A secured link between his MPLS network and his Public Cloud tenant

How **it works**

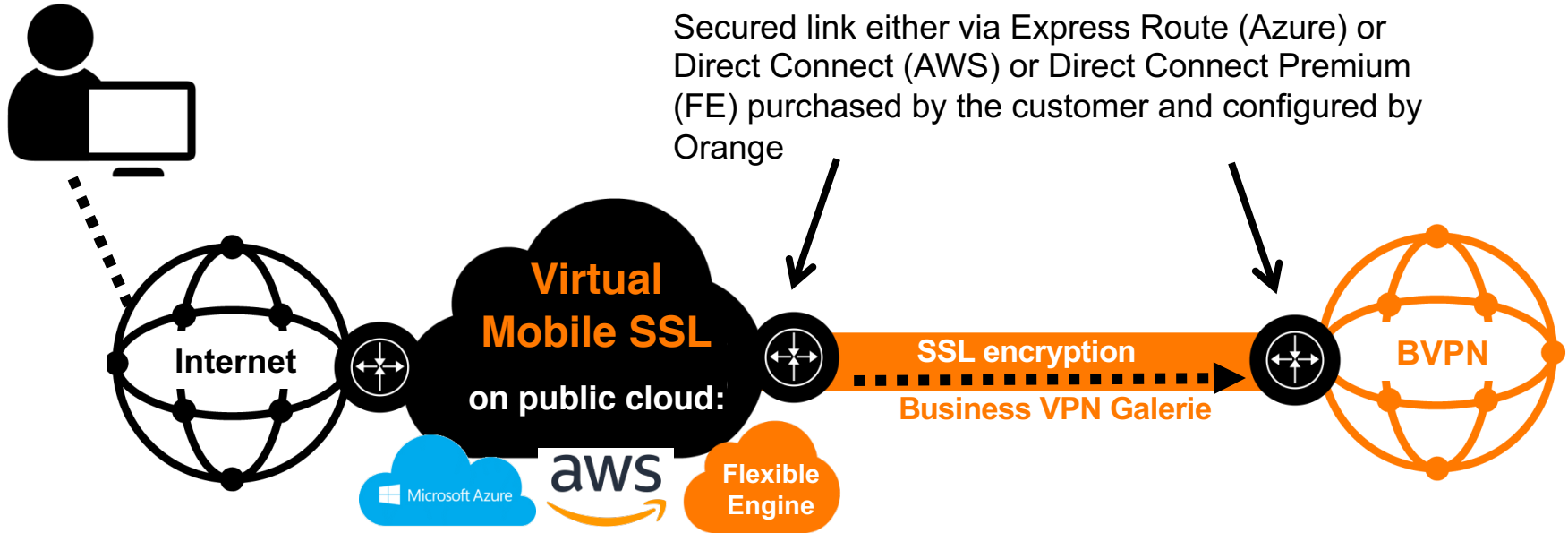A software from the user device, creates an encrypted tunnel with Virtual Mobile SSL

The user accesses the IS, using his usual business software

The user's computer is checked: anti-virus up-to-date, etc.

BVPN customer: access to the IS via BVPN Galerie

Secured link either via Express Route (Azure) or Direct Connect (AWS) or Direct Connect Premium (FE) purchased by the customer and configured by Orange

Internet

Virtual Mobile SSL

on public cloud:

Microsoft Azure

aws

Flexible Engine

SSL encryption

Business VPN Galerie

BVPN

BVPN customer: access to the IS via BVPN Galerie

Secured link via Express Route (Azure) or Direct Connect (AWS) or Direct Connect Premium (FE) purchased and **configured by the customer**

Internet

Virtual Mobile SSL

on public cloud:

Microsoft Azure

aws

Flexible Engine

SSL encryption

BVPN

Client **MPLS tiers**

Secured link via Express Route (Azure) or Direct Connect (AWS) or Direct Connect Premium (FE) purchased and **configured by the customer**

Internet

Virtual Mobile SSL

on public cloud:

Microsoft Azure

aws

Flexible Engine

SSL encryption

MPLS

Service **Levels**

Service level = 1 Virtual Machine with a number of simultaneous users

3 levels of service

- Small Site: 10 – 25 – 50 – 100 simultaneous accesses

- Medium Site: 250 – 500 – 1000 simultaneous accesses

- Large Site: 2500 – 5000 simultaneous accesses

Several virtual machines can be set up to increase the capacity