

STORMSHIELD

Trusted SD-WAN: combining performance and security

2022

Contents

04

Why is **SD-WAN implementation** necessary?

07

The cyber threat from NATION STATES

11

SD-WAN: **improving** the application experience

14

SD-WAN: **adaptability** for different uses

17

The need for secure communications

20

Effective SD-WAN management

23

Trusted SD-WAN:
the choice that offers peace of mind

27

Trusted SD-WAN by Stormshield:
all-in-one trust and security

Organisations have embarked on structural and digital changes offering a better experience for their employees and customers as well as improvements in their IT processes.

For this reason, the Software Defined Wide Area Network (SD-WAN) has a role to play in the required digital transformation of companies, because this technology simplifies the task of managing networks on different sites while streamlining costs.

This approach is an innovative way of improving performance and unifying connectivity across different networks, including the hybrid cloud. SD-WAN allows companies to **dynamically adapt Internet traffic** according to their priority and bandwidth quality needs at each location.

However, to better protect your infrastructure, **SD-WAN technology needs to be secure and trusted** in order to address cyber threats and geopolitical situations.

In a crowded market, it is no longer enough to manage reliable interconnections; you also need protection elements (flow filtering, VPN tunnels, URL filtering, intrusion detection, etc.) for the different networks. This ensures that WAN access can be secured and users protected under all circumstances. In order to make a wise choice, the following four aspects should be taken into consideration *at a minimum*: performance, cost, security and trust.

This white paper describes **the different aspects that an organisation should consider when implementing a Trusted SD-WAN approach**: in other words, a secure and trusted technology approach. This document is intended for consultants and IT security managers to help them understand the challenges of Trusted SD-WAN today.

Why **is SD-WAN implementation** necessary?

#1

The digital transformation that companies have undergone has changed user practices for applications that were once *on-premises* and used by employees working from the company's offices. Now, inter-site communications can still be carried out using MPLS[1] connections to link the various sites of the organisation, but the cost is often significant.

Similarly, the use of cloud-based applications (Microsoft 365, Salesforce etc.) has been identified as a second important aspect:

this business transformation is contributing to increased demands on WANs in both of these situations.

As a result, the way in which data flows has evolved, and companies are gradually turning to SD-WAN as they seek to remain competitive and meet the various technological challenges.

SD-WAN is an architecture paradigm that enables the **creation of a multi-site wide area network, and ensures high-quality, high-availability access to SaaS / Web applications, all managed from a central point**.

This technology is proving to be an attractive approach[2] for cost optimisation. As the name implies, it is *software-defined*

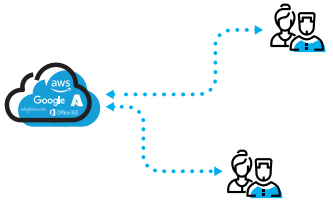
WHY IS SD-WAN ESSENTIAL?

because it allows automatic control of data through software to achieve **better application performance and resilience**.

It can manage network traffic from centralized policies based on different criteria such as application, user, time of day, etc. This results in a faster and more reliable WAN.



Secure inter-site communications



Quality connections to web applications
(AWS, Salesforce, Microsoft 365, etc.)

1 Created in the 1990s, MultiProtocol Label Switching is a private network that does not transit via the Internet. This is a technology that is being used less and less.
2 SaaS: Software as a Service. Source

AN ABUNDANT SERVICE OFFERING

> *As IT companies expand their business operations globally and move to cloud platforms, market demand* ***for a robust and secure WAN architecture*** *to achieve high connectivity and improve network performance is increasing.*
>
> **— Global Market Insights**

Changing usage practices have contributed to the growth of SD-WAN, which allows better management of inter-site communications and access to Web / SaaS services. This change in SD-WAN requirements is shaping the market, which is built around many players.

Between the historical players in the network and cybersecurity sector and cloud service providers, a plethora of options is available. The choice here is based on the value proposition across several criteria: streamlining of WAN links, simplicity of deployment, ease of management and monitoring, security of communications, etc.

Therefore, **the choice of SD-WAN solution is essentially based on the use cases to be implemented**, as well as on the structure of the company and its sensitivity to cyber threats.

For example, a company that uses SaaS solutions for its critical business applications will tend to opt for a cloud player. A multi-site organisation will look for easy deployment, especially for its smaller branches. And a company that is sensitive to cybersecurity, because of its field of activity or its skills, will turn to a cybersecurity solutions provider.

The cyber threat from NATION STATES

#2

More than ever, international and European geopolitics are making cybersecurity into a strategic issue:

the geopolitical environment is strained and cyber attacks are becoming more and more organised, characterised by the following elements[1]: speed, scalability, replicability and complexity, giving the attacker a structural advantage. As Philippe Piron, President of GE Power Conversion & Grid Solutions[2] points out, *"attackers are everywhere, difficult to detect and authenticate, creative, and quick to develop new attacks [...] "*.

Faced with this challenge, national governments are not sitting on their hands, but are arming themselves with cyber tools – either directly, or with help from organised groups.

As Professor Mike McGuire3, Senior Lecturer in Criminology at the University of Surrey in the UK, points out, nation-states are increasingly investing *"time and resources into obtaining strategic cyber advantages to advance their national interests, intelligence gathering capabilities, and military power through espionage and theft"*.

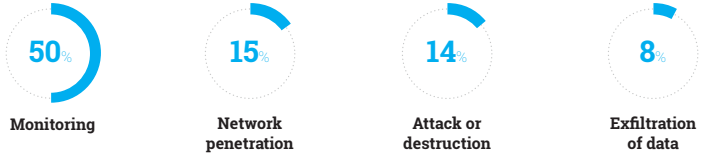
High value-added companies (industrial, pharmaceutical, etc.) are the first in the firing line; yet more generally, 82%[4] of organisations believe that geopolitics and cybersecurity are closely linked.

Therefore, a frequent assessment **of the risks from nation-state attacks should be a consideration** in every organisation's **protection strategy**. As Kevin Bocek[5], Vice President of Security Strategy and Threat Intelligence at Venafi, points out: *"All organisations need to strengthen measures to manage their critical security assets."*

The main targets of cyberattacks



The main cyber-weapons used



1 Philippe Piron in *Cyber defence: the new geopolitical weapon*. Source
2 *Ibid.*
3 Usine digitale. Source
4 Global Security Mag. Source
5 *Ibid.*

SD-WAN AND CYBERSECURITY

SD-WAN ensures high-availability, high-quality connections between sites and to cloud applications in an efficient and flexible manner.

However, the proliferation of new Web / SaaS user practices leads to an increase in risks (dependence on the Internet, third-party applications, etc.).

As a result, additional security layers must be applied within the SD-WAN architecture to reduce the significant danger of intrusions and monitoring of your sensitive communications.

In summary, the connectivity and criticality of WAN communications that are central to all exchanges within an organisation require a **layer of security and trust to ensure data confidentiality once the SD-WAN has been deployed**.

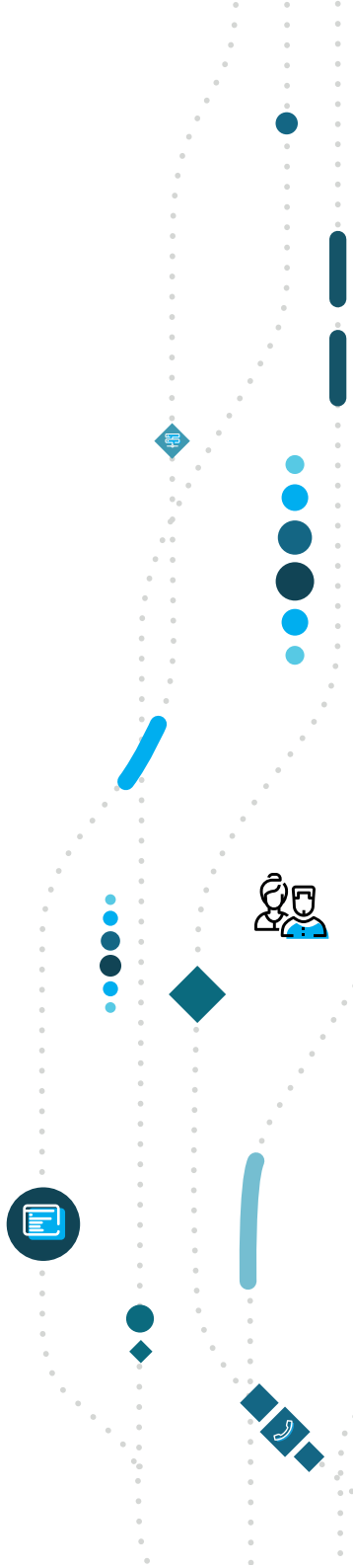
80%

of SD-WAN deployments will incorporate security services requirements in the coming years, according to Gartner.

> *Some actors remain reluctant to set the rules of the game for confrontations in cyberspace.* ***We could therefore be faced with rapid and uncontrolled escalation,*** *leading to unprecedented crises and unanticipated cascade effects.*

— Florence Parly
French Minister for the Armed Forces

Declaration on Cyber Security and Cyber Defence, Lille, 8 September 2021



SD-WAN: **improving the** application experience

#3

As mentioned earlier, SD-WAN implementations have adapted to the new user practices and digital transformation that organisations are undergoing. As IDC reports, 70% of applications will be cloud native by 2024.

And this calls for a high-quality connection. However, it can be unstable (packet loss and/or delays in reception). As a result, legitimate questions may arise: how can you ensure stable quality for critical business applications? What video and audio quality do users need? For how many sites?

SD-WAN optimises bandwidth, improving performance for different needs (VoIP, video, print streams, file transfers, SaaS applications etc.). This ensures continuity of service and an optimal experience for all employees.

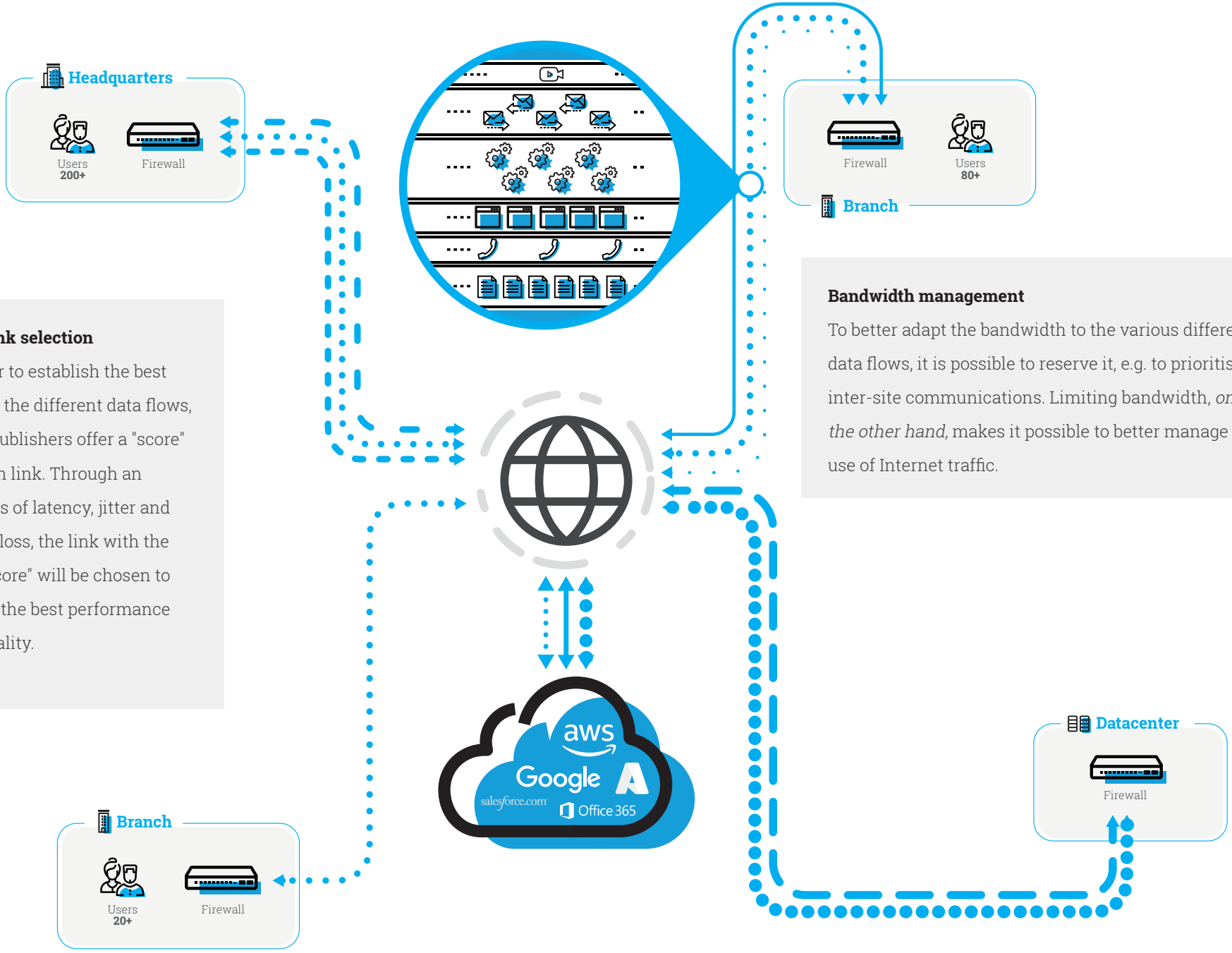
More than **214** **billion dollars** spent on public cloud services in 2019[1]

1 Stéphane Chmielewski, *Why is SD-WAN one of the pillars of digital transformation?* Source

BEST LINK SELECTION AND BANDWIDTH MANAGEMENT

With multiple WAN accesses (Internet, branch offices, etc.) and the emergence of the cloud, **SD-WAN delivers a real advantage, with higher speeds and an attractive cost ratio**, avoiding the need to invest in expensive links. This ensures reliable connectivity and performance at all times.

To best manage bandwidth and achieve the right level of service, it is important to look for solutions that improve response times on applications and/or streams used from different sites for better quality of service.



Best-link selection

In order to establish the best link for the different data flows, some publishers offer a "score" for each link. Through an analysis of latency, jitter and packet loss, the link with the best "score" will be chosen to ensure the best performance and quality.

Bandwidth management

To better adapt the bandwidth to the various different data flows, it is possible to reserve it, e.g. to prioritise inter-site communications. Limiting bandwidth, *on the other hand,* makes it possible to better manage the use of Internet traffic.

SD-WAN: **adaptability** for different use cases

#4

APPLICATION RECOGNITION

The SD-WAN approach is increasingly focused on optimising infrastructure to reduce costs and improve access to applications delivered in the cloud.

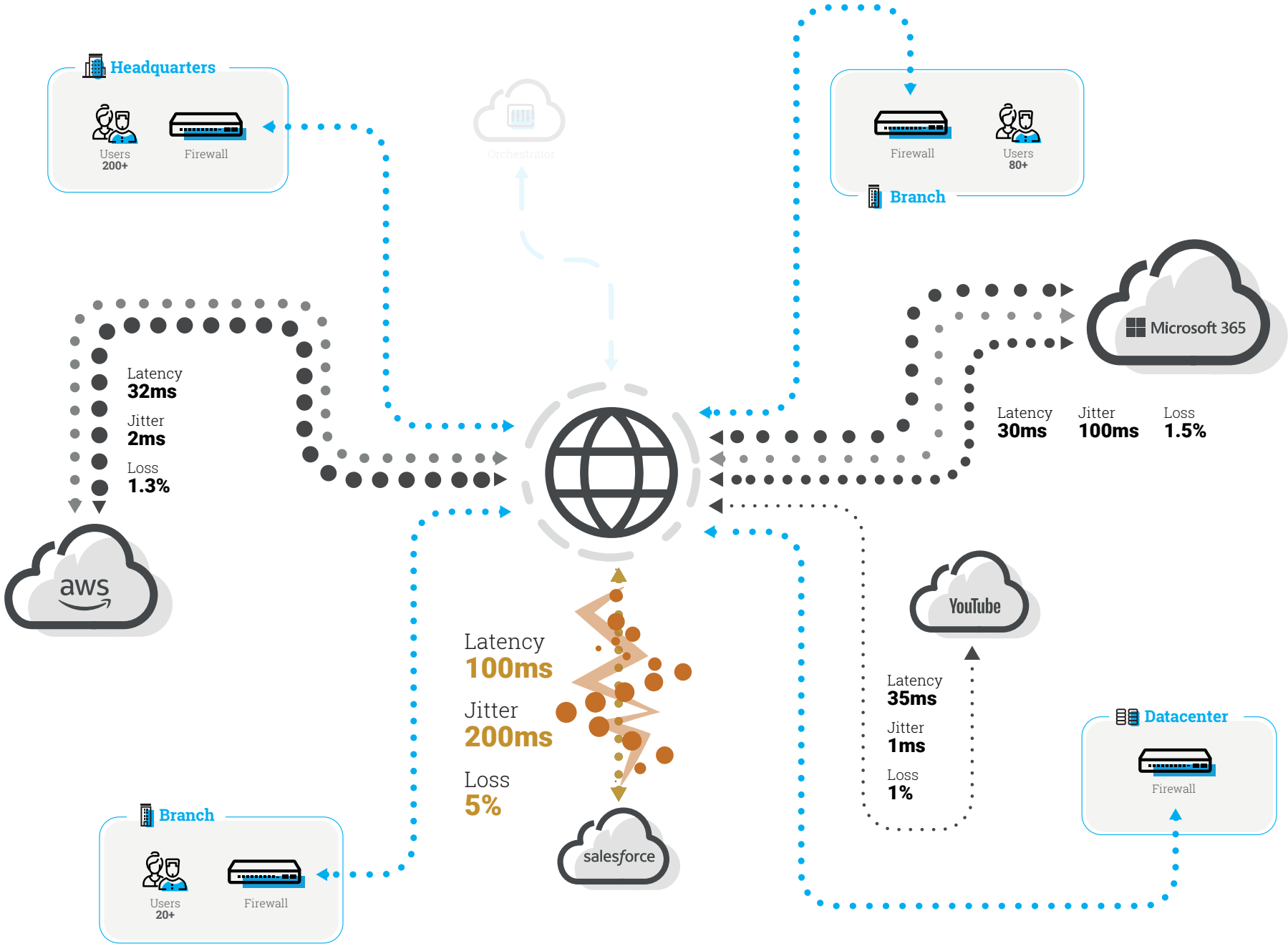
This transformation of SD-WAN architecture revolves around maintaining the quality of the user experience. As a result, most publishers are now opting for in-depth recognition of the data passing through the flows (e.g. HTTPS).

This makes it easier to distinguish between different cloud applications (standard or customised). **This identification improves visibility and ensures that specific Quality of Service (QoS) and *Service Level Agreement* (SLA) policies are set for each application**.

These solutions ensure high performance for the various SaaS applications used (Zoom, AWS, Salesforce, Google, etc.), as well as those in direct contact with customers.

For improved analysis of network traffic, it should not be forgotten that the security component must be present to ensure good protection for exchanges.

This includes comprehensive real-time web filtering of traffic, DPI IPS analysis to eliminate any risk of non-compliance of packets passing through the infrastructure, and SSL inspection of the various web protocols to ensure that usage practices are in accordance with the established security policy.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
Microsoft 365
Latency
32ms
Jitter
2ms
Loss
1.3%
Latency
30ms
Jitter
100ms
Loss
1.5%
aws
Latency
100ms
Jitter
200ms
Loss
5%
YouTube
Latency
35ms
Jitter
1ms
Loss
1%
Datacenter
Firewall
Branch
Users
20+
Firewall
salesforce

The **need for secure** communications

#5

SECURE COMMUNICATIONS

Data confidentiality and integrity, linked to the criticality of WAN communications within a company, is ensured by delivering secure inter-site communications. **Critical data must be encrypted to ensure that it cannot be used by anyone who does not have the right to access it**.

IPsec VPN has been an essential part of WANs for many years. It is a protocol with a set of standards that enables different sites on a WAN to be connected securely via the Internet. This interconnection method can be used for all purposes, to all destinations with almost no cost.

For this reason, **the SD-WAN must offer robust, end-to-end encryption**. As a result, the security of data transiting between a company's various sites must be ensured by the implementation of IPsec VPN tunnels.

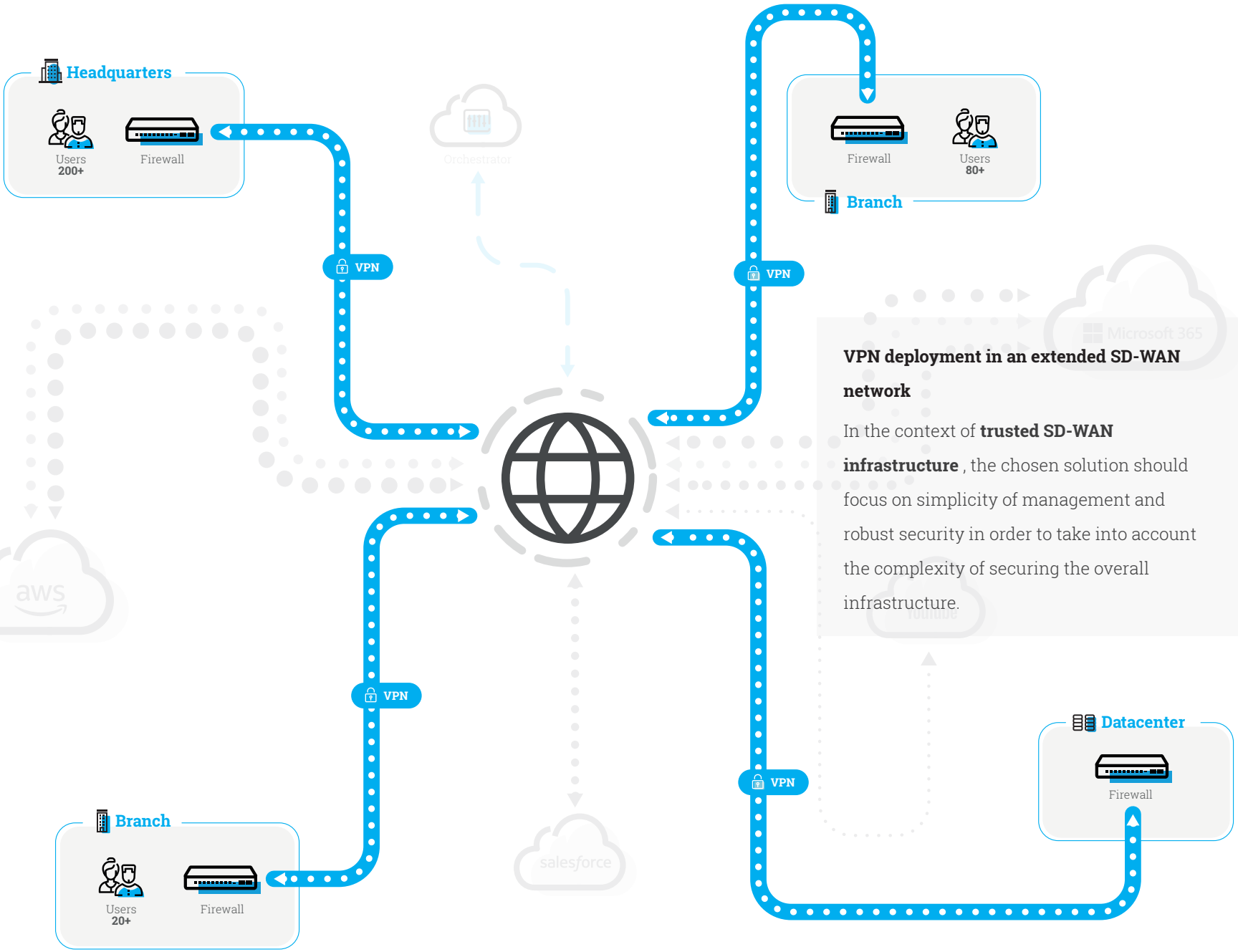


Did you know?

In order to increase the level of security effectively, IPsec VPN can be used as a complementary security measure to "encapsulate protocols that are already secured by other mechanisms[1]".

ANSSI-NT_ IPsec Guide Source





VPN deployment in an extended SD-WAN network

In the context of **trusted SD-WAN infrastructure** , the chosen solution should focus on simplicity of management and robust security in order to take into account the complexity of securing the overall infrastructure.

Effective SD-WAN **management**

#6

Implementing an SD-WAN architecture that relies on centralised management makes it easier to deploy and update the infrastructure while providing global visibility.

For example, from a single management console, security features and routing policies can be deployed or modified across multiple sites, instead of sending a technician to the site.

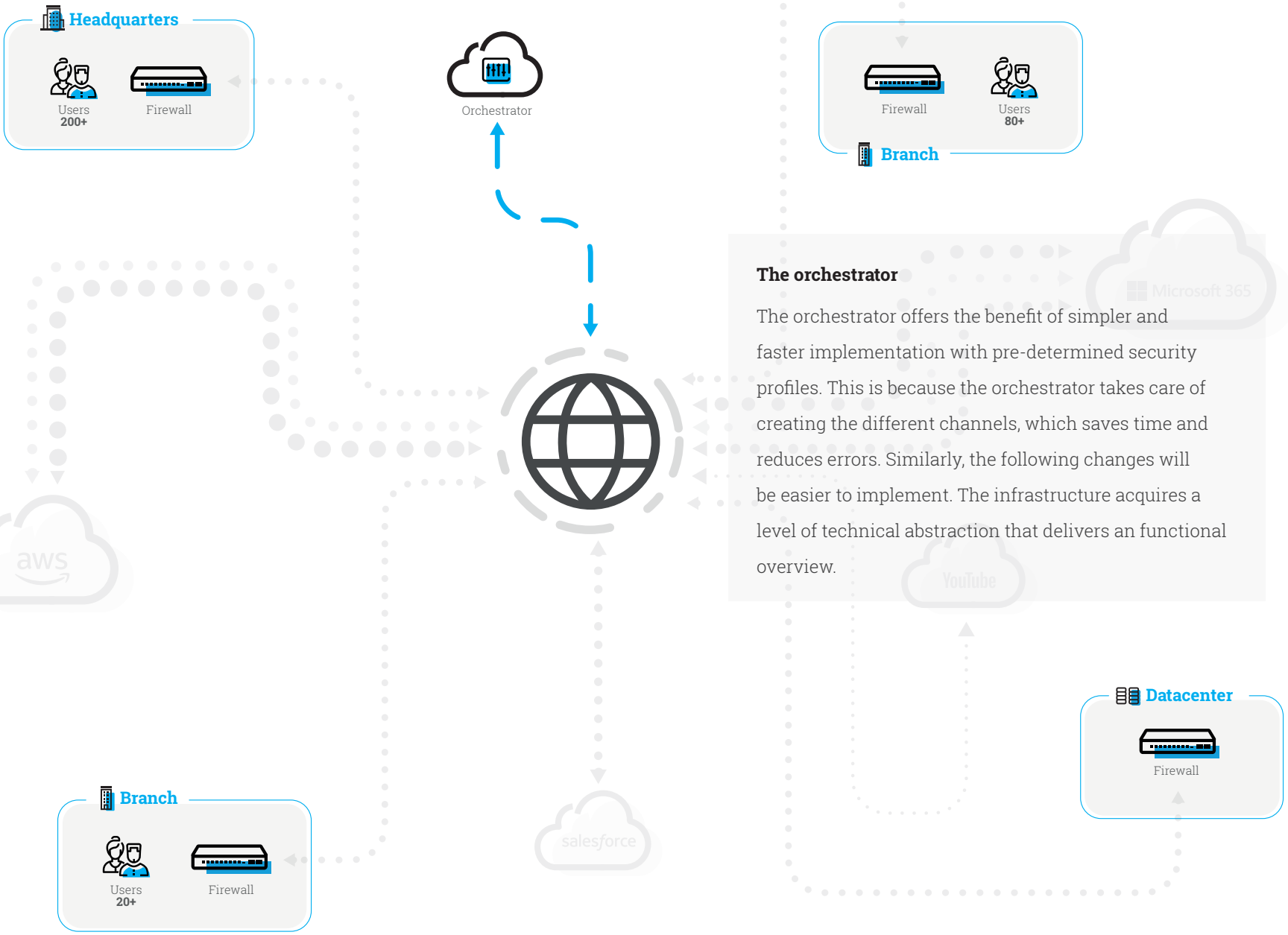
With just a few clicks, it is also possible to define the various interactions between the sites before the orchestrator takes care of configuring all the connection and security equipment.

ORCHESTRATION

In addition, the overview provided by orchestration solutions ensures **a 360° view of the state of the infrastructure and the performance of each application**. This monitoring also offers the possibility of reporting SLA indicators (latency, jitter, packet loss) on link quality.

This comprehensive overview allows an efficient bandwidth management policy (QoS) to be put in place to guarantee reliable connectivity at all times. Lastly, this overview provides a useful insight into shadow IT use.

In summary, the chosen orchestration solution must **provide the necessary layer of trust in network security while facilitating simplified configuration**. Its supervision functions can monitor link quality indicators while allowing the management of events (logs) and security incidents.



The orchestrator

The orchestrator offers the benefit of simpler and faster implementation with pre-determined security profiles. This is because the orchestrator takes care of creating the different channels, which saves time and reduces errors. Similarly, the following changes will be easier to implement. The infrastructure acquires a level of technical abstraction that delivers an functional overview.

Trusted SD-WAN: **the choice that offers peace of mind**

#7

TRUSTED SD-WAN

As mentioned earlier, SD-WAN streamlines remote communications and cloud access, but security must also be part of the equation. A legitimate question is: are there secure SD-WAN architectures that are certified and/or approved by an independent certification body?

As it stands, we find that there are no vendor-independent SD-WAN certifications or qualifications that promote this technological approach.

Therefore, it is important to have practical elements against which to objectively judge the chosen SD-WAN solution. WHEN selecting a vendor from among several hardware and software solutions, it is necessary to ask questions such as the robustness of the product and the trustworthiness with regard to geopolitical and economic issues.

Firstly, as the ANSSI[1] points out, **robustness** "*consists of testing their capacity to resist computer attacks according to a defined context of use and level of threat*".

Therefore, solutions that take this aspect into consideration for the overall security of the SD-WAN infrastructure should be preferred.

Secondly, it is important that the concept of **trust** is clearly included in the product strategy in order to adhere to the commitments made to an official certification/qualification body.

In summary, given the lack of official SD-WAN certification, it is necessary to rely on the various product certifications/qualifications and the various security standards provided by the government authorities in order to obtain a Trusted SD-WAN type architecture.



Did you know?

Hardening
is the process of making a system more secure.

This approach consists of **reducing the software components installed on the system, the tools, the users and the non-essential rights to the necessary minimum level** , while still offering the features necessary for proper operation.

1 ANSSI, Source

ENSURING SOFTWARE QUALITY

Remote site connections and cloud access via SD-WAN increase connectivity, but can also increase security risks if this component is not considered,

as the solutions that make up the SD-WAN represent a target for attack by cyber criminals. Moreover, as the ANSSI[1] points out, the software elements for a given infrastructure must be checked and their configuration hardened before they are used.

Also, as mentioned above, **priority** should **be given to trusted publishers who are able to offer products that are either qualified or certified** by legitimate third-party organisations such as the ANSSI in France, the CCN in Spain, the BSI in Germany and the ENISA at European level. This is because they guarantee compliance with regulatory, technical and safety requirements.

This ensures robust protection of the product, and as the ANSSI indicates [...] is a "*commitment by the solution provider to meet trust criteria*"[2]. In addition, to achieve a high level of robustness, products need to prove their resistance to cyberattacks according to a specific framework. This includes an audit of the source code for the product in question.

As we have just seen, there are no certified and/or qualified SD-WAN solutions on the market today. To fill this gap, you need to analyse the information independently beforehand in order to choose one or more suppliers offering robust and trusted products (preferably qualified), with SD-WAN functionalities (orchestration, QoS optimisation, etc.) and security options (firewalls, flow filtering, VPNs, etc.), ensuring an effective package that protects your infrastructure at all times.

VPN IPsec

DR

Securing interconnections

"DR IS interconnections must be secured using VPN tunnels that protect all exchanged flows (confidentiality, integrity, anti-replay, mutual authentication of endpoints). For this purpose, the organisation has defined a IPsec DR VPN protocol.

ANSSI, ANSSI-PG-075 Guide Source

1 ANSSI in *Guide offering recommendations for sensitive information architectures and systems.* Source
2 ANSSI. Source

The 4 key points
when choosing your Trusted SD-WAN

#1

Opt where possible for a supplier recognised by an official and independent body (ANSSI, CCN etc.)

#2

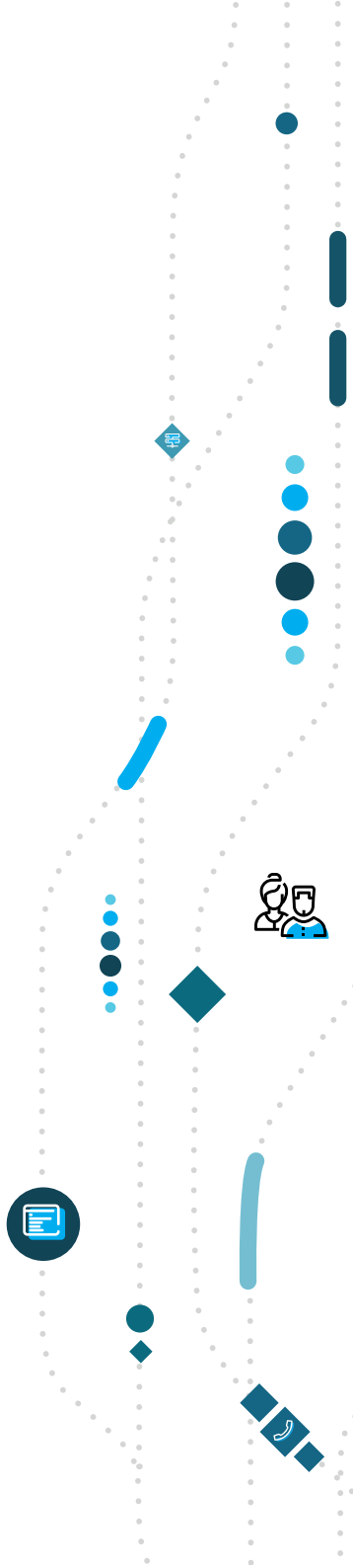
Make sure that the vendor has the SD-WAN and security elements required for better functional coverage. Secure all-in-one architecture: use of an appliance to provide unified SD-WAN, firewall and secure end-to-end connections, among others.

#3

Favour technologies that offer unified visibility. Optimised management and improved centralisation of different functions.

#4

Enjoy efficient management of cloud applications (Microsoft 365, Salesforce etc.)



Trusted SD-WAN by Stormshield: **all-in-one trust and security**

#8

Stormshield supports you **in the integration of the Trusted SD-WAN** into your infrastructure, **securely and efficiently**



Easily manage your extended network

With Stormshield's SD-WAN capabilities, **centralise and control your cross-site connections and cloud access** for your extended infrastructure.



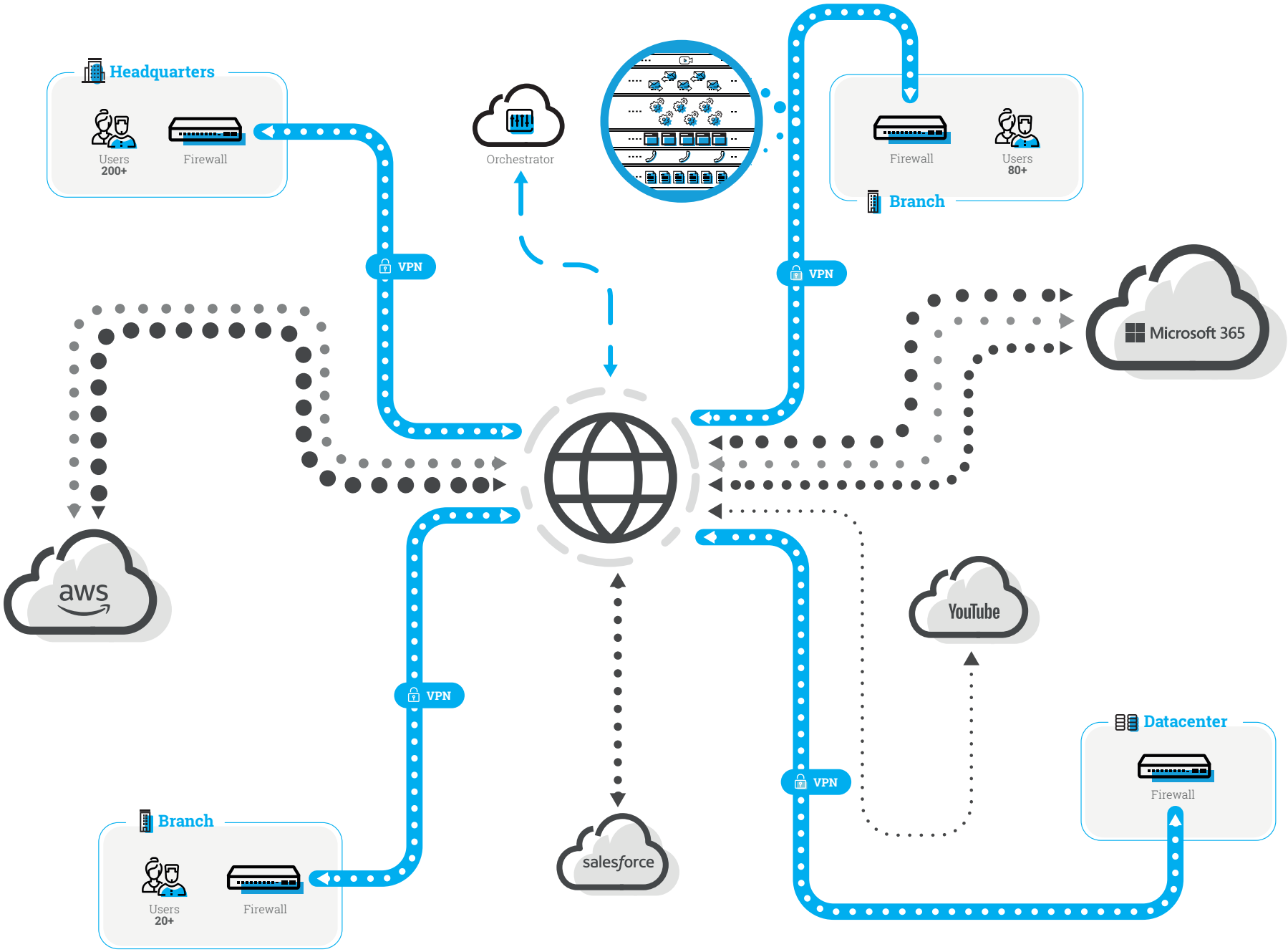
Secure your SD-WAN at all times

Gain peace of mind with Stormshield's secure SD-WAN technology **for unparalleled protection of all your connections**. Your employees have secure access to company resources, wherever they are, and from any device.



Choose your trusted SD-WAN

Based on technology certified to the highest European standards, Stormshield's SD-WAN gives you the confidence to ensure the cyber-serenity of your infrastructure.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
VPN
VPN
Microsoft 365
aws
VPN
YouTube
Datacenter
Firewall
VPN
salesforce
Branch
Users
20+
Firewall

THE **EUROPEAN CHOICE** FOR **CYBERSECURITY**

www.stormshield.com

All distribution, reproduction or representation, even in part, of this white paper, for any purposes other than private use, regardless of the medium, is prohibited, and may engage the civil and criminal liability of any person failing to comply with this prohibition.

Copyright © 2022 Stormshield