

STORMSHIELD

Vertrauenswürdiges SD-WAN: Leistung und Sicherheit in Einem

2022

Inhalt

04

Warum ist die Einführung von SD-WAN unverzichtbar?

07

Cyberbedrohungen durch NATIONALSTAATEN

11

SD-WAN: **Verbesserung** der Benutzererfahrung

14

SD-WAN: **Anpassungsfähigkeit** für unterschiedliche Einsatzzwecke

17

Erforderliche Kommunikationssicherheit

20

Effektive Verwaltung von SD-WAN

23

Trusted SD-WAN: **eine Wahl des Vertrauens**

27

Trusted SD-WAN von Stormshield: **Vertrauenswürdigkeit und Sicherheit in Einem**

Unternehmen haben strukturelle und digitale Veränderungen vorgenommen, um eine bessere Erfahrung für ihre Mitarbeitenden und Kunden zu bieten und ihre IT-Prozesse zu optimieren.

Vor diesem Hintergrund kann ein Software Defined Wide Area Network – oder kurz SD-WAN – die erforderliche digitale Transformation in Unternehmen unterstützen, da diese Technologie die Verwaltung der Netzwerke an den verschiedenen Standorten vereinfacht und gleichzeitig die Kosten senkt.

Dieser Ansatz ist eine innovative Methode, um die Leistung zu verbessern und die Konnektivität verschiedener Netzwerke, einschließlich der Hybrid-Cloud, zu vereinheitlichen. Mit SD-WAN können Unternehmen **den Internet-Traffic** dynamisch an ihre Anforderungen im Hinblick auf die Priorität und Bandbreitenqualität an jedem Standort anpassen.

Um jedoch einen besseren Schutz Ihrer Infrastruktur zu erzielen, **muss die SD-WAN-Technologie sicher und vertrauenswürdig sein,** um Cyberbedrohungen abzuwehren und geopolitische Anforderungen zu erfüllen.

In einem überfüllten Markt reicht es nicht länger aus, Verbindungen zuverlässig zu verwalten, sondern es müssen auch Sicherheitsfunktionen (Traffic-Filter, VPN-Tunnel, URL-Filter, Intrusion Detection usw.) für die verschiedenen Netzwerke vorhanden sein. So können Unternehmen ihren WAN-Zugang sichern und Benutzer*innen in jeder Situation schützen. Um eine sinnvolle Auswahl zu treffen, sollten Sie *mindestens* die folgenden vier Aspekte berücksichtigen: Leistung, Kosten, Sicherheit und Vertrauenswürdigkeit.

In diesem Whitepaper werden **die verschiedenen Aspekte beschrieben, die Unternehmen bei der Einführung und Nutzung eines Trusted-SD-WAN-Ansatzes**, d. h. eines sicheren und vertrauenswürdigen Technologieansatzes, beachten sollten. Dieses Dokument richtet sich an Berater*innen sowie an Personen, die für die Sicherheit von Informationssystemen verantwortlich sind, um ihnen die Herausforderungen von Trusted SD-WAN in der heutigen Zeit bewusst zu machen.

Warum ist die Einführung von SD-WAN unverzichtbar?

WARUM IST SD-WAN UNVERZICHTBAR?

Durch die digitale Transformation hat sich die Nutzung von Unternehmensanwendungen, die früher *vor Ort* verfügbar und von Mitarbeitenden in den Büros des Unternehmens eingesetzt wurden, verändert. Zwar kann die standortübergreifende Kommunikation immer noch über MPLS[1]-Verbindungen erfolgen, um die verschiedenen Unternehmensstandorte miteinander zu verbinden, aber dabei entstehen oft erhebliche Kosten.

Ein zweiter wichtiger Aspekt ist die Nutzung von Anwendungen in der Cloud (Microsoft 365, Salesforce usw.).

Tatsächlich trägt die digitale Transformation in Unternehmen zu einem steigenden Bedarf an Wide Area Networks (WANs) für beide Fälle bei.

Infolgedessen hat sich die Art und Weise des Datenflusses verändert, und Unternehmen setzen immer häufiger SD-WANs ein, um wettbewerbsfähig zu bleiben und die verschiedenen technologischen Herausforderungen zu bewältigen.

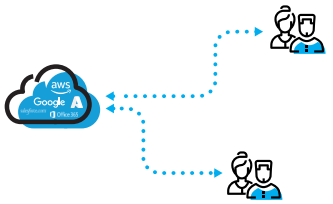
SD-WAN ist ein Architekturparadigma, das es ermöglicht, **ein Wide Area Network über mehrere Standorte aufzubauen und die Qualität sowie die Verfügbarkeit des Zugriffs[2] auf SaaS-Anwendungen/ das Internet zu gewährleisten, wobei das gesamte Netzwerk von einem zentralen Punkt aus verwaltet wird**.

Diese Technologie hat sich als attraktiver Ansatz zur Kostenoptimierung bewährt. Wie der Name andeutet, sind SD-WANs *Software-definiert* , weil sie eine automatische Kontrolle der Daten mittels Software ermöglichen, um **eine bestmögliche Leistung und Ausfallsicherheit der Anwendungen zu erzielen**.

Dabei kann der Netzwerk-Traffic gemäß zentralen Richtlinien nach verschiedenen Kriterien wie Anwendung, Benutzer*innen, Uhrzeit usw. verwaltet werden. Dies führt zu einem schnelleren und zuverlässigeren WAN-Netzwerk.



Geschützte Kommunikation zwischen Standorten



Qualitativ hochwertige Verbindungen zu Webanwendungen
(AWS, Salesforce, Microsoft 365, etc.)

1 MultiProtocol Label Switching wurde in den 1990er Jahren entwickelt und ist ein privates Netzwerk, das nicht über das Internet übertragen wird. Diese Technologie wird immer seltener eingesetzt.
2 SaaS: Software as a Service. Quelle

EIN UMFANGREICHES ANGEBOT

Da IT-Unternehmen ihre Geschäftsabläufe weltweit ausdehnen und zu Cloud-Plattformen wechseln, steigt die Marktnachfrage ***nach einer robusten und sicheren WAN-Architektur,*** *mit der Unternehmen eine hohe Konnektivität erreichen und die Netzwerkleistung verbessern können.“*

— Global Market Insights

Die veränderten Nutzungsgewohnheiten haben zu einer höheren Nachfrage nach SD-WANs beigetragen, da diese die Verwaltung der standortübergreifenden Kommunikation sowie des Zugriffs auf Web-/SaaS-Dienste vereinfachen. Dieser geänderte Bedarf an SD-WANs strukturiert einen Markt, der zahlreiche Akteure umfasst.

Es gibt eine Fülle von Anbietern, die Netzwerk- und Cybersicherheitslösungen oder Cloud-Dienste bereitstellen. Die Wahl beruht hier auf einer Abwägung von Vorteilen basierend auf mehreren Kriterien: optimierte Verbindungen, unkomplizierte Bereitstellung, vereinfachte Verwaltung und Überwachung, sichere Kommunikation usw.

Deshalb **hängt die Wahl der SD-WAN-Lösung hauptsächlich von den zu implementierenden Anwendungsfällen** sowie von der Struktur und der Anfälligkeit eines Unternehmens für Cyberangriffe ab.

Beispielsweise wird ein Unternehmen, das SaaS-Lösungen für seine geschäftskritischen Anwendungen nutzt, sich vermutlich eher für einen Cloud-Anbieter entscheiden, während ein Unternehmen mit mehreren Standorten sicherstellen wird, dass die Einführung vor allem für kleine Filialen einfach ist. Und ein Unternehmen, das aufgrund seines Geschäftsfelds oder seiner Kompetenz für Cybersicherheit sensibilisiert ist, wird sich an einen Anbieter von Cybersicherheitslösungen wenden.

Cyberbedrohungen durch NATIONALSTAATEN

2.

Die internationale und europäische Geopolitik befasst sich mehr denn je mit Cybersicherheit als strategische Herausforderung.

In der Tat ist die geopolitische Lage angespannt, und Cyberangriffe werden immer organisierter und zeichnen sich durch folgende Merkmale aus[1]: Schnelligkeit, Skalierbarkeit, Replizierbarkeit und Komplexität. Diese Faktoren verschaffen Angreifern einen strukturbedingten Vorteil. Wie Philippe Piron, Präsident von GE Power Conversion & Grid Solutions[2], erläutert: *„Angreifer sind überall, sie sind schwierig zu entdecken und zu identifizieren, und sie sind kreativ und schnell in der Lage, immer neue Angriffe zu entwickeln [...]“.*

Dabei stehen auch NATIONALSTAATEN nicht zurück und bewaffnen sich entweder direkt oder mithilfe organisierter Gruppen mit Cybertools.

Wie Professor Mike McGuire[3], Dozent für Kriminologie an der Universität von Surrey in Großbritannien, erklärt, investieren NATIONALSTAATEN zunehmend *„Zeit und Ressourcen in die Erlangung strategischer Cyber-Vorteile, um ihre nationalen Interessen, ihre Fähigkeiten zur Sammlung von Informationen und ihre militärische Macht durch Spionage und Diebstahl zu fördern“.*

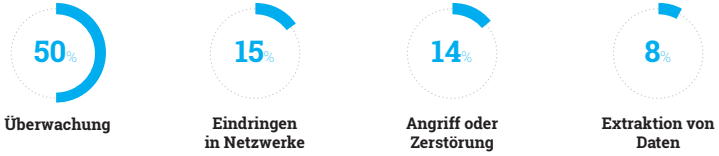
Zwar sind es Unternehmen mit hoher Wertschöpfung (Fertigungsindustrie, Pharmabranche etc.), welche die ersten Opfer darstellen, doch ganz allgemein sind 82 %[4] der Unternehmen der Ansicht, dass Geopolitik und Cybersicherheit eng miteinander verbunden sind.

Aus diesem Grund sollte eine häufige **Risikobewertung von Angriffen durch Nationalstaaten ein Punkt sein, der in der Sicherheitsstrategie** jedes Unternehmens berücksichtigt werden sollte. Kevin Bocek[5], Vizepräsident für Sicherheitsstrategie und Bedrohungsüberwachung bei Venafi: *„Alle Unternehmen müssen die Maßnahmen zur Verwaltung ihrer kritischen Sicherheitsressourcen verstärken.“*

Die wichtigsten Ziele von Cyberangriffen



Die wichtigsten Cyberwaffen im Einsatz



1 Philippe Piron in Cyberverteidigung, die neue geopolitische Waffe. Quelle
2 *Ibid.*
3 Digitale Anwendungen. Quelle
4 Global Security Mag. Quelle
5 *Ibid.*

SD-WAN UND CYBERSICHERHEIT

SD-WAN erhöht auf effiziente und flexible Weise die Verfügbarkeit und Qualität von Verbindungen zwischen Standorten sowie zu Cloud-Anwendungen.

Mit der Zunahme neuer Web-/SaaS-Anwendungen steigen auch die Risiken (Abhängigkeit vom Internet, von Drittanbieterdiensten usw.).

Deshalb sind zusätzliche Sicherheitsebenen innerhalb der SD-WAN-Architektur erforderlich, um die nicht unerhebliche Gefahr des Eindringens in Ihre Systeme und der Überwachung Ihrer vertraulichen Kommunikation zu verringern.

Kurz gesagt: Die Konnektivität und Kritikalität der WAN-Kommunikation, die im Mittelpunkt des gesamten Datenaustauschs innerhalb eines Unternehmens steht, erfordert eine **Sicherheits- und Vertrauensebene, um die Vertraulichkeit der Daten nach der Einführung von SD-WAN zu gewährleisten**.

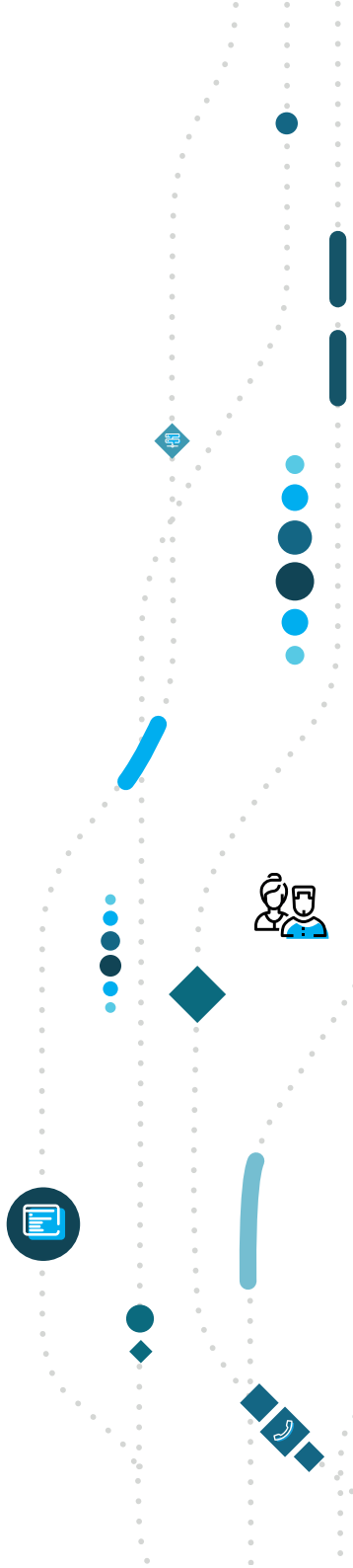
80 %

der SD-WAN-Implementierungen werden laut Gartner in den nächsten Jahren Sicherheitsservices erfordern .

Einige Akteure zögern nach wie vor, die Spielregeln für Konfrontationen im Cyberspace festzulegen. ***Wir könnten also mit schnell eskalierenden und unkontrollierten Situationen konfrontiert werden****, die zu neuartigen Krisen mit unvorhergesehenen Kaskadeneffekten führen.*

— Florence Parly
Heeresministerin

Erklärung zu Cybersicherheit und Cyberverteidigung am 8. September 2021 in Lille



SD-WAN : **Verbesserung** der Benutzererfahrung

3.

Wie bereits erwähnt, haben sich SD-WAN-Implementierungen an die neuen Einsatzzwecke sowie an die digitale Transformation in Unternehmen angepasst. Wie das IDC berichtet, werden bis zum Jahr 2024 70 % aller Anwendungen cloud-nativ sein.

Dies erfordert eine qualitativ hochwertige Verbindung – diese kann jedoch instabil sein (Verlust von Paketen und/ oder Verzögerungen beim Empfang). Dies kann berechtigte Fragen aufwerfen: Wie kann eine stabile Qualität für kritische Geschäftsanwendungen sichergestellt werden? Welche Video- und Audioqualität erhalten die Benutzer*innen? Für wie viele Standorte?

SD-WAN optimiert die Bandbreite je nach den verschiedenen Anforderungen (VoIP, Video, Print-Workflows, Dateiübertragung, SaaS-Anwendungen usw.), um eine bessere Leistung zu erzielen. Dadurch wird die Kontinuität des Dienstes und eine optimale Erfahrung für alle Mitarbeitenden sichergestellt.

+ von 214

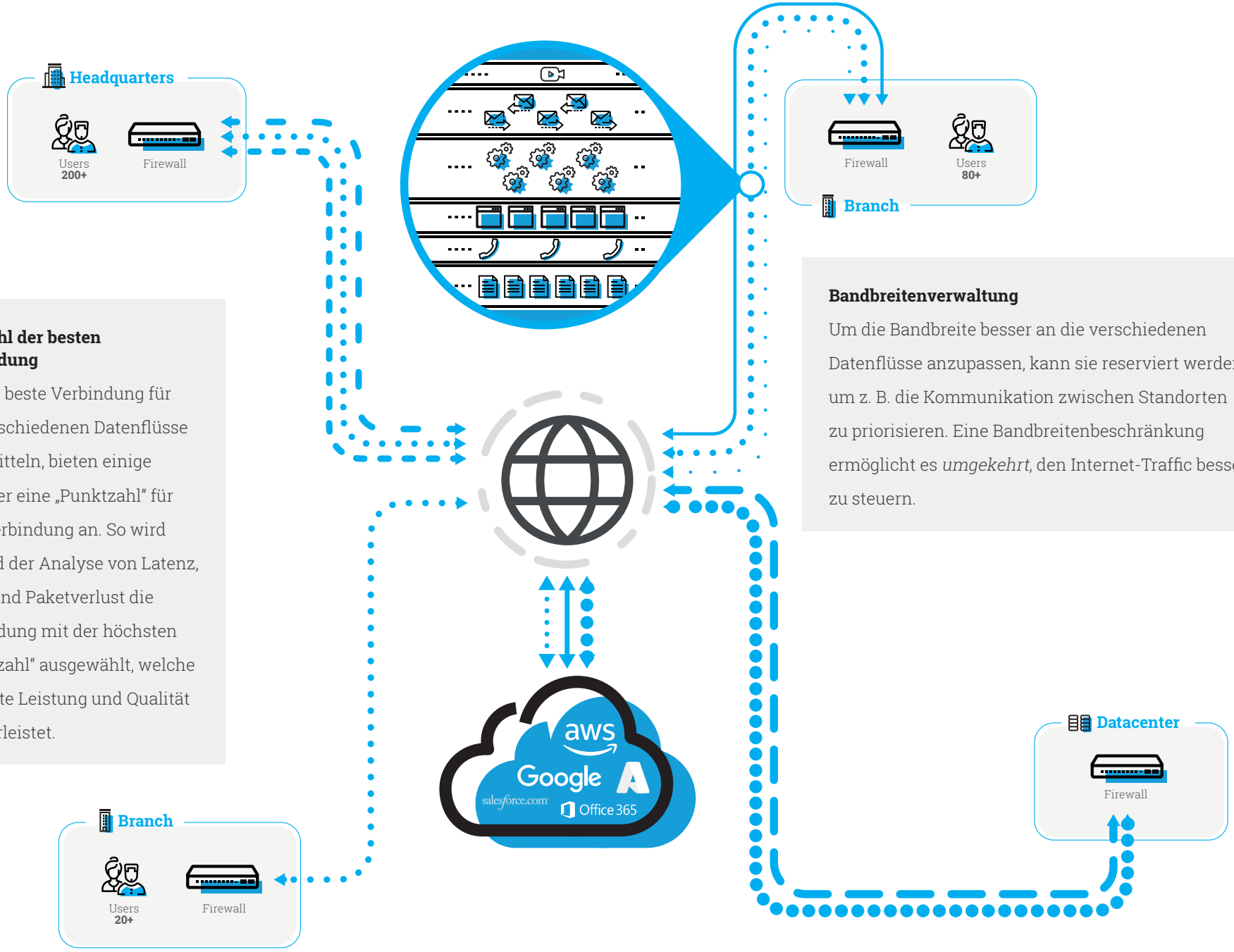
Milliarden Dollar wurden im Jahr 2019 für öffentliche Cloud-Dienste ausgegeben[1]

1 Stéphane Chmielewski in Warum ist SD-WAN eine der Säulen der digitalen Transformation? Quelle

AUSWAHL DER BESTEN VERBINDUNG UND BANDBREITENVERWALTUNG

Mit mehreren WAN-Zugängen (Internet, Filialen usw.) und dem Aufkommen der Cloud **bietet SD-WAN echte Vorteile, wie höhere Geschwindigkeiten und ein attraktives wirtschaftliches Verhältnis**, wodurch Sie Investitionen in teure Verbindungslösungen vermeiden können. So ist es möglich, jederzeit eine zuverlässige Konnektivität und Leistung zu erhalten.

Um die Bandbreite optimal zu verwalten und ein entsprechendes Serviceniveau zu erreichen, sollten Sie sich an Lösungen orientieren, welche die Antwortzeiten bei Anwendungen und/ oder Streams, die an verschiedenen Standorten genutzt werden, verbessern, um eine höhere Dienstqualität zu gewährleisten.



Auswahl der besten Verbindung

Um die beste Verbindung für die verschiedenen Datenflüsse zu ermitteln, bieten einige Anbieter eine „Punktzahl" für jede Verbindung an. So wird anhand der Analyse von Latenz, Jitter und Paketverlust die Verbindung mit der höchsten „Punktzahl" ausgewählt, welche die beste Leistung und Qualität gewährleistet.

Bandbreitenverwaltung

Um die Bandbreite besser an die verschiedenen Datenflüsse anzupassen, kann sie reserviert werden, um z. B. die Kommunikation zwischen Standorten zu priorisieren. Eine Bandbreitenbeschränkung ermöglicht es *umgekehrt*, den Internet-Traffic besser zu steuern.

SD-WAN : **Anpassungsfähigkeit** für unterschiedliche Einsatzzwecke

4.

ANWENDUNGSERKENNUNG

Der SD-WAN-Ansatz konzentriert sich zunehmend auf die Optimierung der Infrastruktur, um Kosten zu senken und den Zugriff auf Cloud-Anwendungen zu verbessern.

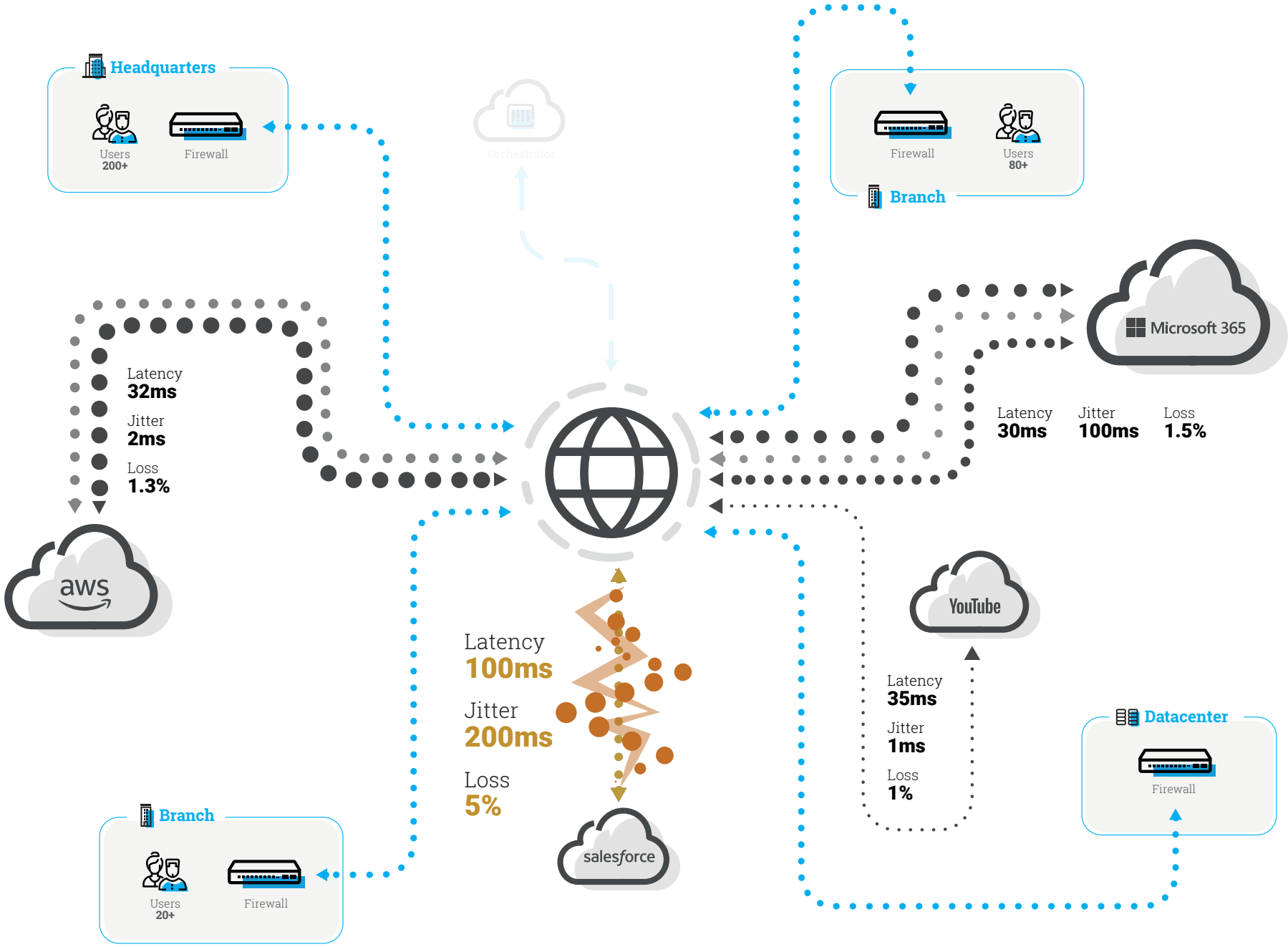
Diese Transformation von SD-WAN-Architekturen dreht sich um die Aufrechterhaltung der Qualität der Benutzererfahrung. Aus diesem Grund entscheiden sich die meisten Anbieter heute für eine gründliche Analyse des Daten-Traffics (z. B. HTTPS),

was die Möglichkeit bietet, die verschiedenen Cloud-Anwendungen (Standard oder benutzerdefiniert) genauer voneinander zu unterscheiden. **Diese Identifizierung verbessert die Transparenz und gewährleistet, dass spezifische Richtlinien für die Servicequalität (QoS) sowie die Spezifikationen des *Service Level Agreement* (SLA) in Übereinstimmung mit jeder Anwendung definiert werden können**.

Somit garantieren diese Lösungen eine hohe Leistung für die verschiedenen verwendeten SaaS-Anwendungen (Zoom, AWS, Salesforce, Google…) sowie für die Anwendungen, die direkt mit den Kunden verbunden sind.

Um die Analyse des Netzwerk-Traffics noch weiter zu optimieren, ist auch eine gute Sicherheitskomponente zum Schutz des Datenaustauschs erforderlich.

Dies geschieht durch eine umfassende Echtzeit-Webfilterung des Daten-Traffics, eine DPI-IPS-Analyse, um jede Gefahr der Nichtkonformität von Paketen, welche die Infrastruktur durchlaufen, auszuschließen, oder eine SSL-Inspektion der verschiedenen Webprotokolle, um eine Nutzung gemäß der festgelegten Sicherheitsrichtlinie zu gewährleisten.


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

Erforderliche Kommunikationssicherheit

5.

GESCHÜTZTE KOMMUNIKATION

Die Gewährleistung der Vertraulichkeit und Integrität von Daten, die mit der Kritikalität der WAN-Kommunikation innerhalb eines Unternehmens verbunden ist, beruht auf der Sicherung der Kommunikation zwischen Standorten. **Kritische Daten müssen verschlüsselt werden, um sicherzustellen, dass sie für Personen ohne Zugriffsberechtigung unbrauchbar sind**.

Das IPsec-VPN-Protokoll bietet eine Reihe von Standards und ermöglicht eine sichere Verbindung zwischen verschiedenen Standorten in einem WAN über das Internet – deshalb ist es bereits seit Jahren ein wesentlicher Bestandteil von erweiterten Netzwerken. Verbindungen dieser Art können für alle Zwecke und zu allen Zielen genutzt werden, und dies zu sehr geringen Kosten.

Ein SD-WAN-Netzwerk muss also über eine robuste End-to-End-Verschlüsselung verfügen. Aus diesem Grund muss die Sicherung der Daten, die zwischen den verschiedenen Standorten eines Unternehmens hin- und hergeschickt werden, über IPsec-VPN-Tunnel erfolgen.

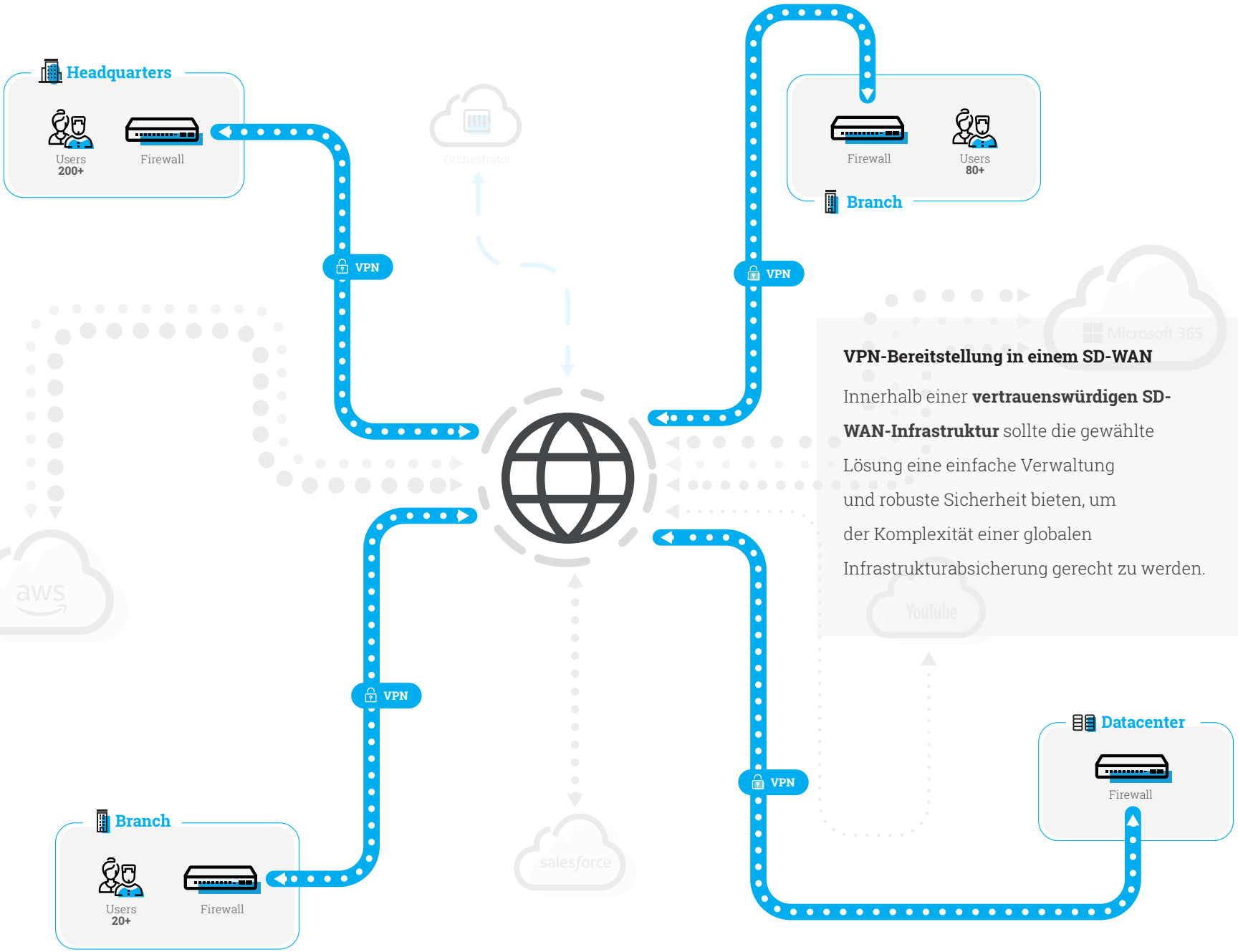


Wussten Sie schon?

Um die Sicherheitsstufe effektiv zu erhöhen, kann IPsec-VPN als zusätzliche Sicherheitsmaßnahme eingesetzt werden, um „Protokolle einzukapseln, die bereits durch andere Mechanismen gesichert werden[1]“.

Leitfaden zu ANSSI-NT_ IPsec Quelle





VPN-Bereitstellung in einem SD-WAN

Innerhalb einer **vertrauenswürdigen SD-WAN-Infrastruktur** sollte die gewählte Lösung eine einfache Verwaltung und robuste Sicherheit bieten, um der Komplexität einer globalen Infrastrukturabsicherung gerecht zu werden.

Effektive Verwaltung eines SD-WAN

6.

ORCHESTRIERUNG

Die Implementierung einer SD-WAN-Architektur mit zentraler Verwaltung erleichtert die Bereitstellung und Aktualisierung der Infrastruktur und bietet gleichzeitig einen umfassenden Überblick.

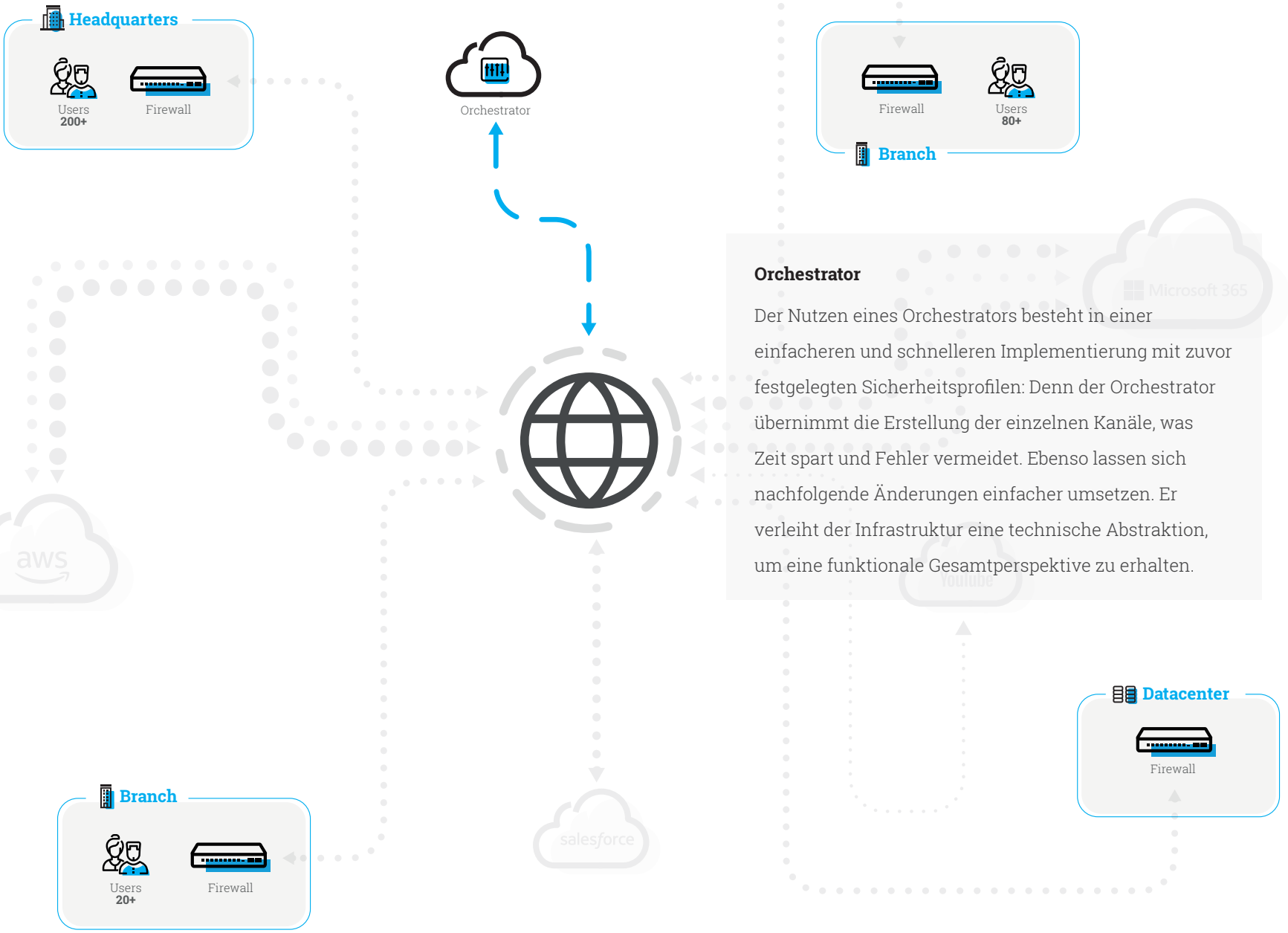
So können von einer einzigen Verwaltungskonsole aus Sicherheitsfunktionen und Routing-Richtlinien an mehreren Standorten implementiert oder verändert werden, anstatt einen Techniker zu schicken.

Mit wenigen Klicks lassen sich auch die verschiedenen Interaktionen zwischen den Standorten definieren, sodass der Orchestrator die Konfiguration der gesamten Verbindungs- und Sicherheitsausrüstung übernimmt.

Darüber hinaus ermöglicht die globale Sichtbarkeit von Orchestrierungslösungen **einen 360°-Blick auf den Status der Infrastruktur und die Leistung jeder einzelnen Anwendung**. Dieser umfassende Überblick bietet auch die Möglichkeit, SLA-Indikatoren (Latenz, Jitter, Paketverlust) hinsichtlich der Verbindungsqualität zurückzuverfolgen,

und ermöglicht somit eine effektive Bandbreitenverwaltung (QoS), um jederzeit eine zuverlässige Konnektivität zu gewährleisten. Und zuletzt birgt diese globale Sicht auch einen vorteilhaften Einblick in die Schatten-IT.

Zusammenfassend lässt sich sagen, dass die gewählte Orchestrierungslösung **das erforderliche Vertrauen in die Netzwerksicherheit bieten und gleichzeitig eine vereinfachte Konfiguration ermöglichen muss**. Mit den Überwachungsfunktionen können Benutzer die Indikatoren für die Verbindungsqualität überwachen und Ereignisse (Protokolle) sowie Sicherheitsvorfälle verwalten.



Orchestrator

Der Nutzen eines Orchestrators besteht in einer einfacheren und schnelleren Implementierung mit zuvor festgelegten Sicherheitsprofilen: Denn der Orchestrator übernimmt die Erstellung der einzelnen Kanäle, was Zeit spart und Fehler vermeidet. Ebenso lassen sich nachfolgende Änderungen einfacher umsetzen. Er verleiht der Infrastruktur eine technische Abstraktion, um eine funktionale Gesamtperspektive zu erhalten.

Trusted SD-WAN : **eine Wahl des Vertrauens**

7.

TRUSTED SD-WAN

Wie bereits erwähnt, optimiert SD-WAN die Remote-Kommunikation und den Cloud-Zugriff – aber auch die Sicherheit muss Teil der Gleichung sein. DABEI stellt sich eine berechtigte Frage: Gibt es sichere SD-WAN-Architekturen, die von einer unabhängigen Stelle zertifiziert und/oder zugelassen wurden?

Die Antwort auf diese Frage lautet aktuell, dass es keine anbieterunabhängigen SD-WAN-Zertifizierungen oder Qualifikationen gibt, die diesen technologischen Ansatz befürworten.

Deshalb ist es wichtig, die ausgewählte SD-WAN-Lösung anhand von konkreten Anhaltspunkten objektiv zu beurteilen. BEI der Auswahl eines Anbieters unter mehreren Hardware- und Softwarelösungen müssen unter anderem die Robustheit des Produkts und die Vertrauenswürdigkeit in Bezug auf geopolitische und wirtschaftliche Herausforderungen hinterfragt werden.

ANSSI[1] zufolge besteht die **Robustheit zum Einen darin,** *„die Fähigkeit zu testen Computerangriffe in einem bestimmten Nutzungskontext und Bedrohungsniveau abzuwehren.“*.

Folglich sollten Lösungen bevorzugt werden, die diesen Faktor bei der allgemeinen Absicherung einer SD-WAN-Infrastruktur berücksichtigen.

Zum Anderen ist es wichtig, den Begriff der **Vertrauenswürdigkeit** auf klare Weise in der Produktstrategie wiederzufinden, um die Verpflichtungen, die gegenüber einer offiziellen Zertifizierungs-/Qualifizierungsstelle eingegangen wurden, einzuhalten.

Zusammenfassend lässt sich sagen, dass Unternehmen angesichts der fehlenden offiziellen Zulassung von SD-WAN auf die verschiedenen Produktzertifizierungen/ -qualifikationen sowie die verschiedenen von Regierungsbehörden bereitgestellten Sicherheitsstandards zurückgreifen müssen, um eine Trusted-SD-WAN-Architektur aufzubauen.

Wussten Sie schon?

Das „Hardening“ oder Härten ist der Prozess der Absicherung eines Systems.

Dabei werden **die auf dem System installierten Softwarekomponenten, Tools, Benutzer und Rechte, die nicht unbedingt erforderlich sind, auf das Wesentliche reduziert** und gleichzeitig die für den reibungslosen Betrieb erforderlichen Funktionen bereitgestellt.

1 ANSSI, Quelle

GEWÄHRLEISTUNG DER SOFTWARE-QUALITÄT

Verbindungen zu Remote-Standorten und Cloud-Zugänge über SD-WAN verbessern die Konnektivität, können aber auch ein Sicherheitsrisiko darstellen, wenn diese Komponente nicht berücksichtigt wird:

Denn die Lösungen, die ein SD-WAN bilden, stellen ein Angriffsziel für Cyberkriminelle dar. Wie das ANSSI[1] betont, müssen die Softwarekomponenten einer Infrastruktur vor der Inbetriebnahme überprüft und ihre Konfiguration gehärtet werden.

Außerdem sollten Sie **vertrauenswürdige Anbieter bevorzugen, deren Produkte durch legitime externe Stellen qualifiziert oder zertifiziert sind**, wie das ANSSI in Frankreich, das CCN in Spanien, das BSI in Deutschland oder die ENISA auf europäischer Ebene. Diese stellen sicher, dass die gesetzlichen, technischen und sicherheitsrelevanten Anforderungen erfüllt werden und

gewährleisten einen robusten Schutz durch das Produkt und, wie ANSSI [...] feststellt, „das *Streben des Lösungsanbieters hinsichtlich der Einhaltung von Vertrauenskriterien*“[2]. Um ein hohes Maß an Robustheit zu erreichen, müssen sich die Produkte außerdem in einem bestimmten Rahmen als widerstandsfähig gegen Cyberangriffe erweisen. Dies wird unter anderem durch eine Prüfung des Quellcodes des betreffenden Produkts ermittelt.

Wie wir dargelegt haben, gibt es derzeit keine zertifizierten und/ oder qualifizierten SD-WAN-Lösungen auf dem Markt. Um diesen Mangel zu beheben, müssen die Elemente im Vorfeld unabhängig voneinander analysiert werden, um einen oder mehrere Anbieter auszuwählen, die robuste und vertrauenswürdige (vorzugsweise qualifizierte) Produkte mit SD-WAN-Funktionen (Orchestrierung, QoS-Optimierung ...) sowie Sicherheitsoptionen (Firewalls, Flow-Filter, VPNs ...) anbieten, um ein effektives Gesamtpaket zu schnüren, das Ihre Infrastruktur jederzeit schützt.

DR IPsec-VPN

Verbindungsschutz

„DR-IS-Verbindungen sollten mithilfe von VPN-Tunneln gesichert werden, die den Schutz des gesamten Datenaustauschs (Vertraulichkeit, Integrität, Anti-Replay, gegenseitige Endauthentifizierung) gewährleisten“. Zu diesem Zweck hat die Organisation ein DR-IPsec-VPN-Protokoll definiert.

ANSSI, Leitfaden ANSSI-PG-075 Quelle

1 ANSSI in *„Leitfaden mit Empfehlungen für Architekturen und Systeme für sensible Informationen“.* Quelle
2 ANSSI. Quelle

Die vier wichtigsten Aspekte **bei der Auswahl Ihres Trusted SD-WAN**

1.

Entscheiden Sie sich für einen von einer offiziellen und unabhängigen Stelle (ANSSI, CCN etc.) anerkannten Anbieter.

2.

Stellen Sie sicher, dass der Anbieter die erforderlichen SD-WAN- und Sicherheitselemente bereitstellt, um eine bessere Funktionsabdeckung zu erreichen. Sichere All-in-One-Architektur: Einsatz einer Appliance, um u. a. SD-WAN, Firewall und sichere End-to-End-Verbindungen zu vereinheitlichen.

3.

Bevorzugen Sie Technologien, die über eine einheitliche Sichtbarkeit verfügen. Optimierte Verwaltung und verbesserte Zentralisierung der verschiedenen Funktionen.

4.

Implementieren Sie eine effiziente Verwaltung für Cloud-Anwendungen (Microsoft 365, Salesforce etc.).

Trusted SD-WAN von Stormshield: **Vertrauenswüdigkeit und Sicherheit in Einem**

8.

Stormshield unterstützt Sie **bei der sicheren und effizienten Integration des Trusted SD-WAN** in Ihre Infrastruktur.



Vereinfachen Sie die Verwaltung Ihres erweiterten Netzwerks

Mit den SD-WAN-Funktionen von Stormshield **können Sie Ihre standortübergreifenden Verbindungen sowie den Zugriff auf die Cloud** innerhalb ihrer erweiterten Infrastruktur zentralisieren und steuern.



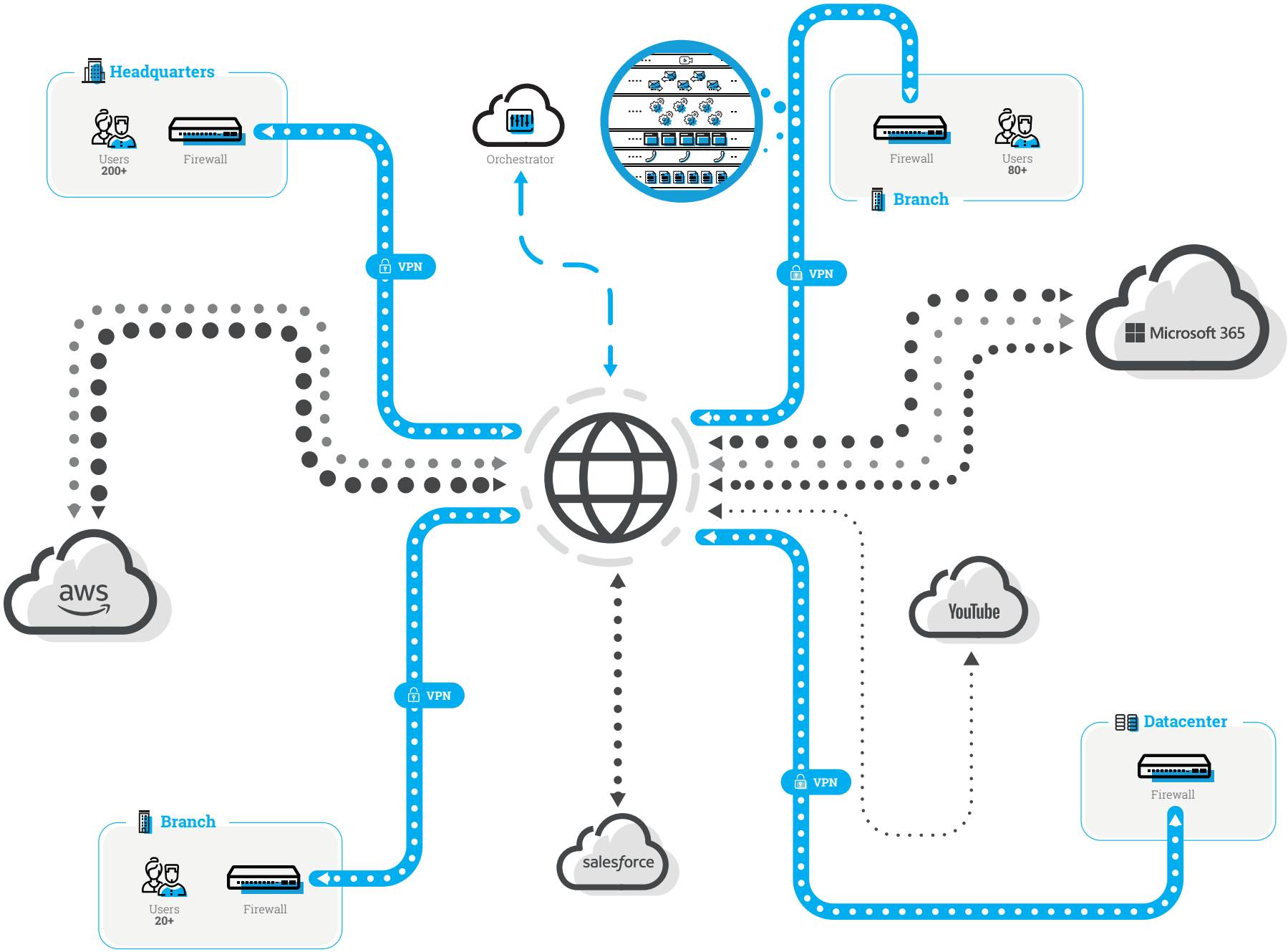
Schützen Sie Ihr SD-WAN jederzeit

Seien Sie unbesorgt, denn Stormshield bietet Ihnen eine sichere SD-WAN-Technologie **für einen unübertroffenen Schutz all Ihrer Verbindungen**. Ihre Mitarbeitenden erhalten sicheren Zugriff auf Unternehmensressourcen – an jedem Ort und über jedes Endgerät.



Wählen Sie ein vertrauenswürdiges SD-WAN

Stormshield SD-WAN basiert auf einer Technologie, die auf höchstem europäischen Niveau zertifiziert ist, und bietet Ihnen das nötige Vertrauen, um Ihre Infrastruktur zu schützen.


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

DER **EUROPÄISCHE ANBIETER DER WAHL** FÜR **CYBERSICHERHEIT**

www.stormshield.com

Jegliche Verbreitung, Vervielfältigung oder Präsentation dieses Whitepapers, auch auszugsweise, auf einem beliebigen Datenträger zu anderen Zwecken als zur privaten Nutzung ist untersagt und kann zivil- und strafrechtliche Folgen für Personen nach sich ziehen, welche dieses Verbot missachten.

Copyright © 2022 Stormshield