

STORMSHIELD

Trusted SD-WAN: una combinazione di prestazioni e sicurezza

2022

Indice

04

Perché è necessario implementare la SD-WAN?

07

La minaccia informatica degli Stati Nazionali

11

SD-WAN : **miglioramento** dell'esperienza applicativa

14

SD-WAN : **adattabilità** per i diversi utilizzi

17

La necessità di proteggere le comunicazioni

20

Gestione efficace della SD-WAN

23

Trusted SD-WAN :

una scelta di fiducia

27

Trusted SD-WAN by Stormshield: **affidabilità e sicurezza in un unico prodotto**

Le aziende si sono lanciate in cambiamenti strutturali e digitali per offrire una migliore esperienza ai dipendenti e ai clienti, oltre a migliorare i processi informatici.

In questo contesto, la Software Defined Wide Area Network, in breve SD-WAN, occupa un posto di rilievo nella necessaria trasformazione digitale delle aziende, anche perché questa tecnologia semplifica la gestione delle reti su diversi fronti, ottimizzando i costi.

Si tratta di un approccio innovativo per migliorare le prestazioni e unificare la connettività su reti diverse, compreso il cloud ibrido. L'SD-WAN consente alle aziende di **adattare dinamicamente il traffico Internet** alle esigenze di priorità e di qualità della larghezza di banda di ciascuna postazione di lavoro.

Tuttavia, per proteggere al meglio la propria infrastruttura, **la tecnologia SD-WAN deve essere sicura e affidabile** in modo da poter affrontare le minacce informatiche e gli scenari geopolitici.

In un mercato ormai saturo, non è più sufficiente gestire interconnessioni affidabili, ma occorre anche disporre di elementi di protezione (filtraggio dei flussi, tunnel VPN, filtraggio degli URL, rilevamento delle intrusioni, ecc.) per le diverse reti, in modo tale da garantire la sicurezza degli accessi alla WAN e la protezione degli utenti in ogni circostanza. E per compiere una scelta oculata, è opportuno prendere in considerazione *almeno* i seguenti quattro aspetti: prestazioni, costi, sicurezza e fiducia.

Questo white paper descrive **i diversi aspetti che ogni azienda dovrebbe prendere in considerazione nell'implementare un approccio Trusted SD-WAN**, in altre parole un approccio tecnologico sicuro e affidabile. In particolare, si rivolge ai consulenti e ai responsabili della sicurezza IT per aiutarli a comprendere le sfide della Trusted SD-WAN di oggi.

Perché è necessario implementare la SD-WAN?

#1

PERCHÉ LA SD-WAN È INDISPENSABILE?

Gli ultimi sviluppi in materia di trasformazione digitale hanno modificato l'uso delle applicazioni, un tempo *on-premise* e utilizzate dai dipendenti collegati dagli uffici aziendali. A tal riguardo, è ancora possibile effettuare comunicazioni intersito utilizzando connessioni MPLS[1] per collegare i vari siti aziendali, ma il costo è spesso significativo.

Inoltre, l' uso di applicazioni basate sul cloud (Microsoft 365, Salesforce, ecc.) costituisce un secondo aspetto importante da considerare.

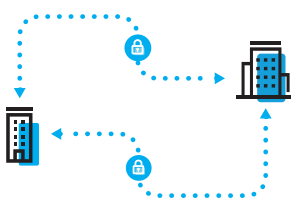
La trasformazione aziendale sta infatti contribuendo ad aumentare la richiesta di WAN per entrambi gli scenari.

Di conseguenza, anche il modo in cui i dati fluiscono si è evoluto e le aziende si stanno gradualmente rivolgendo alla SD-WAN per restare competitive e affrontare le varie sfide tecnologiche.

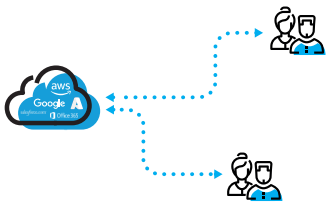
La SD-WAN è un paradigma architettonico che consente **la creazione di una WAN multi-sito e garantisce la qualità e la disponibilità dell'accesso alle applicazioni SaaS[2] / Web, il tutto gestito da un punto centrale**.

Questa tecnologia si sta rivelando un approccio interessante in termini di ottimizzazione dei costi. Come suggerisce il nome, è un sistema *Software-Defined* perché consente il controllo automatico dei dati attraverso il software per ottenere **migliori prestazioni e una maggiore resilienza delle applicazioni**.

È in grado di gestire il traffico di rete mediante politiche centralizzate basate su diversi criteri, quali applicazioni, utenti, orari, ecc. Il risultato è una WAN più veloce e affidabile.



Comunicazioni intersito sicure



Collegamenti di qualità alle applicazioni web
(AWS, Salesforce, Microsoft 365, ecc.)

1 Creato negli anni '90, il MultiProtocol Label Switching è una rete privata che non passa attraverso Internet. Si tratta di una tecnologia che viene utilizzata sempre meno.
2 SaaS : Software as a Service. Fonte

UN'AMPIA OFFERTA

> *Con l'espansione delle aziende IT a livello globale e il passaggio alle piattaforme cloud, è in aumento la richiesta* ***di un'architettura WAN robusta e sicura*** *che consenta di ottenere un'elevata connettività e di migliorare le prestazioni della rete.*
>
> **— Global Market Insights**

Lo sviluppo nel suo utilizzo ha contribuito al diffondersi della SD-WAN, in quanto consente una migliore gestione delle comunicazioni intersito e l'accesso ai servizi Web/SaaS. L'evolversi delle esigenze nell 'ambito della SD-WAN sta plasmando il mercato, che è strutturato su molteplici attori.

Tra gli operatori storici del settore delle reti, in particolare quelli legati alla sicurezza informatica e i fornitori di servizi cloud, l'offerta è a dir poco generosa. La scelta in questo caso si basa su una proposta di valore in grado di soddisfare diversi criteri: ottimizzazione dei collegamenti WAN, semplicità di implementazione, facilità di gestione e monitoraggio, sicurezza delle comunicazioni, ecc.

Pertanto, **la scelta della soluzione SD-WAN si basa essenzialmente sui casi d'uso da implementare**, nonché sull'organizzazione dell'azienda e sulla sua sensibilità alle minacce informatiche.

Ad esempio, un'azienda che utilizza soluzioni SaaS per le proprie applicazioni aziendali critiche tenderà a scegliere un operatore Cloud. Un'organizzazione multi-sito preferirà una implementazione semplice, soprattutto nel caso di aziende di piccole dimensioni. Oppure, un'azienda particolarmente attenta alla cybersicurezza, in virtù del proprio settore di attività o delle proprie competenze, si rivolgerà a un fornitore di soluzioni di sicurezza informatica.

La minaccia informatica degli Stati Nazionali

#2

Oggi più che mai, la geopolitica internazionale ed europea considera la sicurezza informatica una questione strategica.

In effetti, la situazione geopolitica attuale è tesa e gli attacchi informatici stanno diventando sempre più organizzati, oltre ad essere caratterizzati dai seguenti elementi[1] : velocità, scalabilità, replicabilità e complessità, che conferiscono all'aggressore un vantaggio strutturale. Come sottolinea Philippe Piron, Presidente di GE Power Conversion & Grid Solutions[2], *" gli aggressori sono ovunque, difficili da individuare e autenticare, creativi e veloci nello sviluppare nuovi attacchi [...] "*.

In questo contesto, gli Stati coinvolti non sono da meno e si stanno armando di strumenti informatici direttamente o affidandosi a gruppi organizzati.

Come sottolinea il professor Mike McGuire[3], docente di criminologia presso l'Università del Surrey nel Regno Unito, gli Stati nazionali investono sempre più *"tempo e risorse per ottenere vantaggi informatici strategici al fine di promuovere i propri interessi nazionali, le capacità di raccolta di informazioni e il potere militare attraverso lo spionaggio e il furto"*.

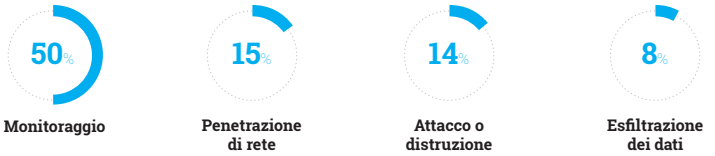
Mentre le aziende ad alto valore aggiunto (industriali, farmaceutiche, ecc.) sono le prime a essere colpite, più in generale l'82%[4] delle organizzazioni ritiene che la geopolitica e la sicurezza informatica siano strettamente collegate.

Pertanto, nella propria strategia di protezione **ogni azienda dovrebbe includere una frequente valutazione del rischio di attacchi** da parte di Stati nazionali. Come osserva, Kevin Bocek[5], vicepresidente della strategia di sicurezza e dell'intelligence sulle minacce di Venafi: *"Ogni azienda deve rafforzare le misure di gestione dei propri asset critici di sicurezza."*

I principali obiettivi degli attacchi informatici



Le principali armi informatiche utilizzate



1 Philippe Piron in *Difesa informatica, nuova arma geopolitica.* Fonte
2 *Ibid.*
3 Usine digitale. Fonte
4 Global Security Mag. Fonte
5 *Ibid.*

SD-WAN E SICUREZZA INFORMATICA

L'SD-WAN garantisce la disponibilità e la qualità delle connessioni intersito e verso le applicazioni cloud in modo efficiente e flessibile.

Tuttavia, il proliferare di nuovi utilizzi del Web / SaaS comporta un aumento dei rischi (dipendenza da Internet, applicazioni di terzi, ecc.),

con la conseguente necessità di applicare ulteriori livelli di sicurezza all'interno dell'architettura SD-WAN per ridurre il rischio significativo di intrusioni e di monitoraggio delle comunicazioni sensibili.

In sintesi, la connettività e la criticità delle comunicazioni WAN, al centro di tutti gli scambi aziendali, richiedono un **livello di sicurezza e fiducia tale da garantire la riservatezza dei dati una volta implementata la SD-WAN**.

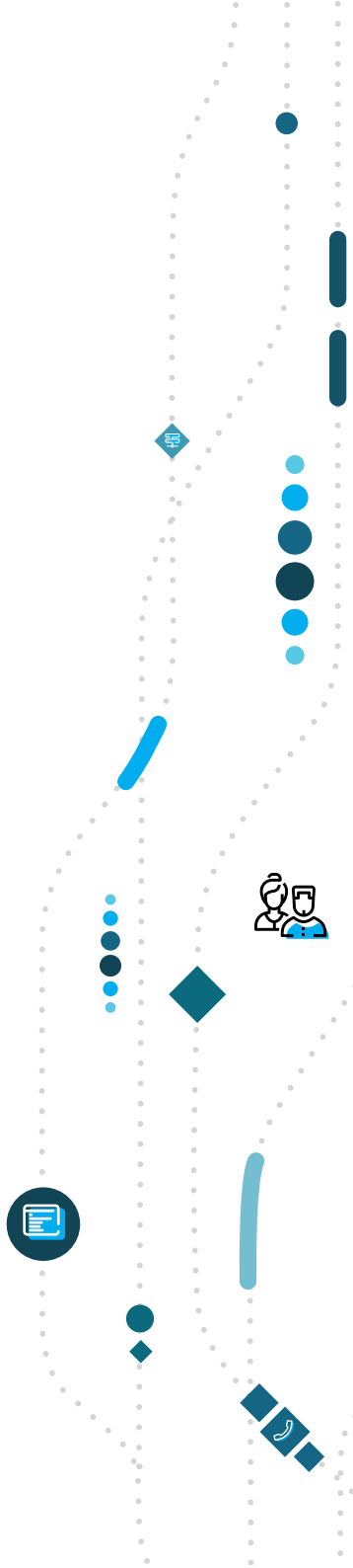
L'80%

delle implementazioni SD-WAN nei prossimi anni includerà requisiti di servizi di sicurezza afferma Gartner.

Alcuni attori sono riluttanti nel definire le regole del gioco per il confronto nel cyberspazio. ***Potremmo quindi trovarci di fronte a un'escalation rapida e incontrollata,*** *che porterebbe a crisi senza precedenti e a effetti a cascata imprevisti.*

— Florence Parly
Ministro delle Forze armate (Francia)

Dichiarazione sulla sicurezza e la difesa informatica, Lille, 8 settembre 2021.



SD-WAN: **miglioramento** dell'esperienza applicativa

#3

Come accennato in precedenza, le implementazioni SD-WAN si sono adattate ai nuovi utilizzi e alla trasformazione digitale in atto nelle aziende. Come riportato dall'istituto di ricerca IDC, il 70% delle applicazioni sarà cloud-native entro il 2024.

In vista di ciò, è necessario che sia presente una connessione di qualità che però potrebbe essere instabile (perdita di pacchetti e/o ritardi nella ricezione). A questo punto possono sorgere domande legittime: come si può garantire una qualità stabile per le applicazioni aziendali critiche? Qual è la qualità video e audio per gli utenti? Per quante postazioni?

La SD-WAN ottimizza la larghezza di banda migliorando le prestazioni per le diverse esigenze (VoIP, video, flussi di stampa, trasferimenti di file, applicazioni SaaS, ecc.) In questo modo si garantisce la continuità del servizio e un'esperienza ottimale per tutti i dipendenti.

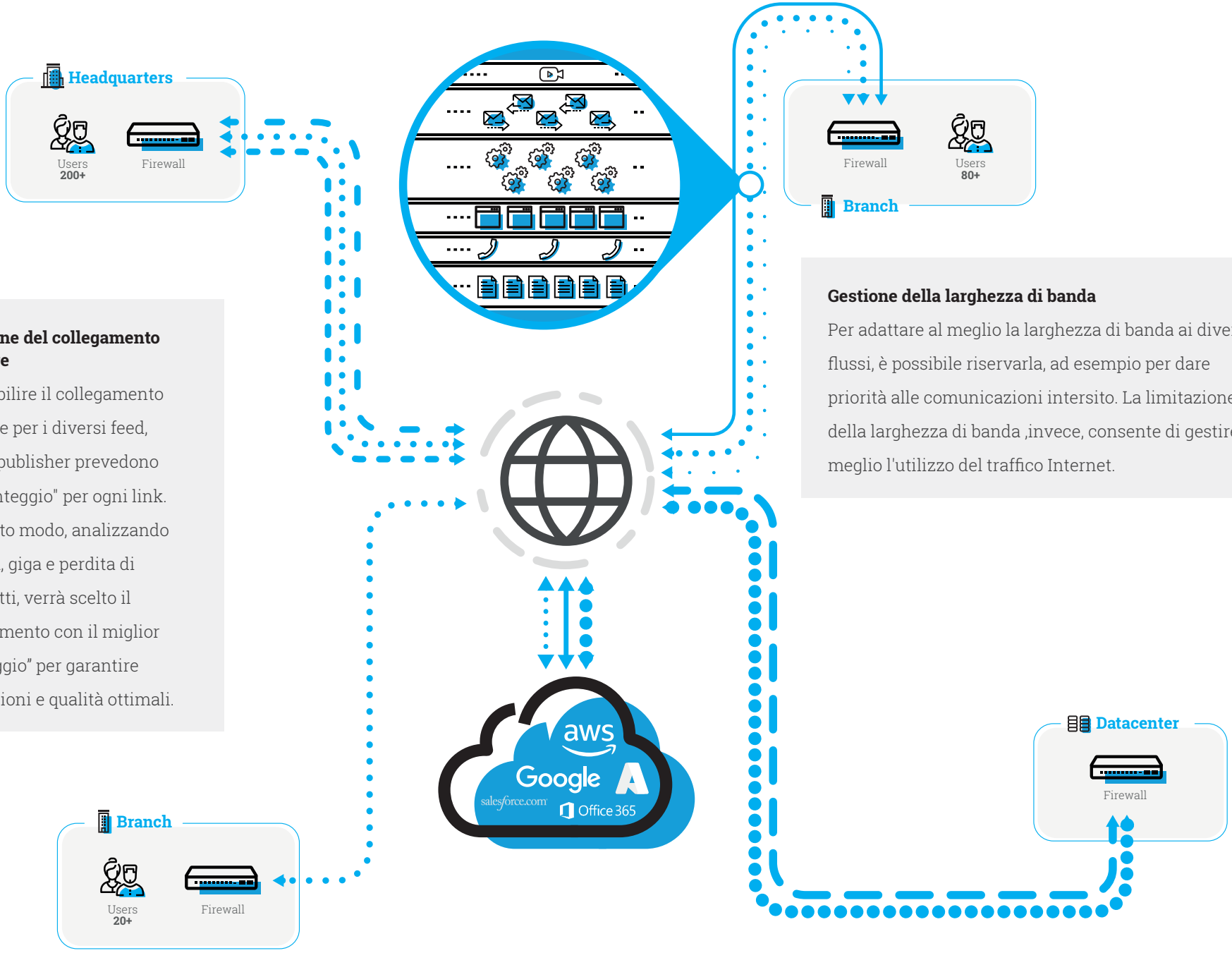
+ de 214 **miliardi di dollari** spesi in servizi di cloud pubblico nel 2019[1]

1 Stéphane Chmielewski in *Perché la SD-WAN è uno dei pilastri della trasformazione digitale?* Fonte

SCELTA DEL MIGLIOR COLLEGAMENTO E GESTIONE DELLA LARGHEZZA DI BANDA

Con gli accessi WAN multipli (Internet, filiali, ecc.) e l'emergere del cloud, **l'SD-WAN offre un vantaggio reale con velocità più elevate e un notevole risparmio economico**, evitando investimenti in collegamenti costosi. Tutto ciò a garanzia di connettività e prestazioni affidabili in ogni momento.

Per gestire al meglio la larghezza di banda e ottenere il giusto livello di prestazioni, è importante orientarsi verso soluzioni che migliorino i tempi di risposta delle applicazioni e/o dei flussi utilizzati dalle diverse postazioni per una migliore qualità di servizio.



Selezione del collegamento migliore

Per stabilire il collegamento migliore per i diversi feed, alcuni publisher prevedono un "punteggio" per ogni link. In questo modo, analizzando latenza, giga e perdita di pacchetti, verrà scelto il collegamento con il miglior "punteggio" per garantire prestazioni e qualità ottimali.

Gestione della larghezza di banda

Per adattare al meglio la larghezza di banda ai diversi flussi, è possibile riservarla, ad esempio per dare priorità alle comunicazioni intersito. La limitazione della larghezza di banda ,invece, consente di gestire meglio l'utilizzo del traffico Internet.

SD-WAN: **adattabilità** per i diversi utilizzi

#4

RICONOSCIMENTO DELLE APPLICAZIONI

L'approccio SD-WAN è sempre più incentrato sull'ottimizzazione dell'infrastruttura per ridurre i costi e migliorare l'accesso alle applicazioni fornite nel cloud.

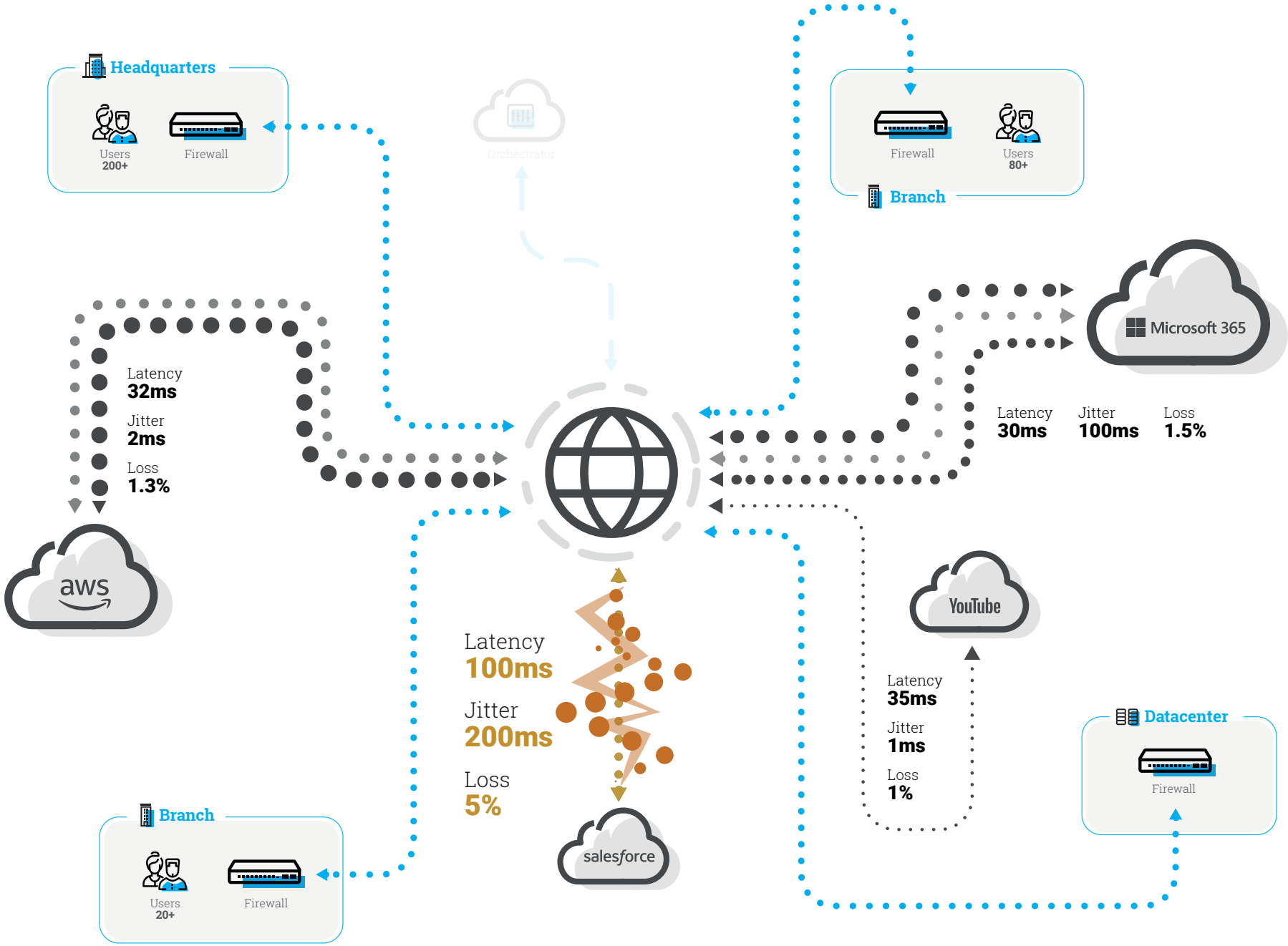
Questa trasformazione delle architetture SD-WAN ruota attorno al mantenimento della qualità dell'esperienza utente. Di conseguenza, la maggior parte dei publisher sta optando per un riconoscimento approfondito dei dati che passano attraverso i flussi (ad esempio, HTTPS),

in modo da distinguere più facilmente le diverse applicazioni cloud (standard o personalizzate). **Questa identificazione migliora la visibilità e garantisce la definizione di specifiche politiche di qualità del servizio (QoS) e di *Service Level Agreement* (SLA) per ogni applicazione**.

Tali soluzioni garantiscono prestazioni elevate per le varie applicazioni SaaS utilizzate (Zoom, AWS, Salesforce, Google, ecc.) e per quelle a diretto contatto con i clienti.

Volendo approfondire l'analisi del traffico di rete, non bisogna dimenticare che per garantire una buona protezione degli scambi deve essere presente la giusta componente di sicurezza.

Questa include il filtraggio completo del traffico web in tempo reale, l'analisi DPI IPS per eliminare eventuali rischi di non conformità dei pacchetti che passano attraverso l'infrastruttura e l'ispezione SSL dei vari protocolli web per garantire un utilizzo in conformità con la politica di sicurezza stabilita.


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

La **necessità di proteggere** le comunicazioni

#5

COMUNICAZIONI SICURE

La garanzia di riservatezza e integrità dei dati, legata alla criticità delle comunicazioni WAN all'interno di un'azienda, si basa sulla protezione delle comunicazioni intersito. **Occorre criptare i dati critici per garantire che non possano essere utilizzati da chi non ha il diritto di accedervi**.

LA VPN IPsec è un elemento essenziale delle WAN da molti anni: si tratta di un protocollo con una serie di standard che consente di collegare in modo sicuro diverse postazioni su una WAN tramite Internet. Questo metodo di interconnessione può essere utilizzato per qualsiasi scopo, verso tutte le destinazioni e a un costo irrisorio.

Pertanto, **la SD-WAN deve garantire una robusta crittografia end-to-end.** La sicurezza dei dati che transitano tra le varie postazioni aziendali deve quindi essere tutelata attraverso l'implementazione di tunnel VPN IPsec.



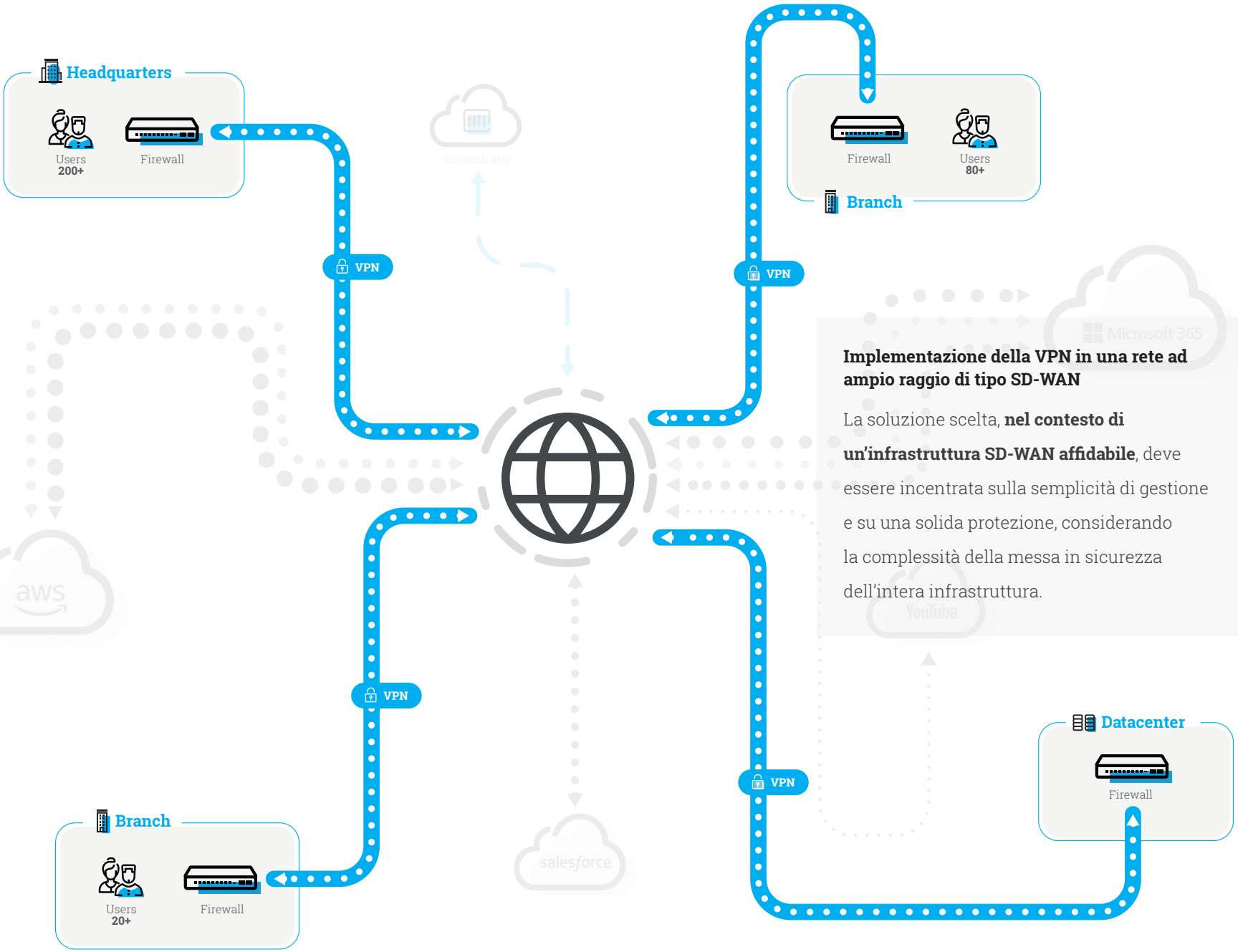
Lo sapevate?

Per potenziare efficacemente il livello di sicurezza, la VPN IPsec può essere utilizzata come misura di sicurezza complementare per "incapsulare protocolli già protetti da altri meccanismi [1] ".

Guida ANSSI-NT_ IPsec Fonte







Implementazione della VPN in una rete ad ampio raggio di tipo SD-WAN

La soluzione scelta, **nel contesto di un'infrastruttura SD-WAN affidabile**, deve essere incentrata sulla semplicità di gestione e su una solida protezione, considerando la complessità della messa in sicurezza dell'intera infrastruttura.

Gestione efficace della SD-WAN

#6

L'implementazione di un'architettura SD-WAN che si basa su una gestione centralizzata facilita lo sviluppo e l'aggiornamento dell'infrastruttura, fornendo al contempo una visibilità globale.

Ad esempio, da un'unica console di gestione è possibile implementare o modificare le funzioni di sicurezza e i criteri di routing in più postazioni, invece di inviare un tecnico sul posto.

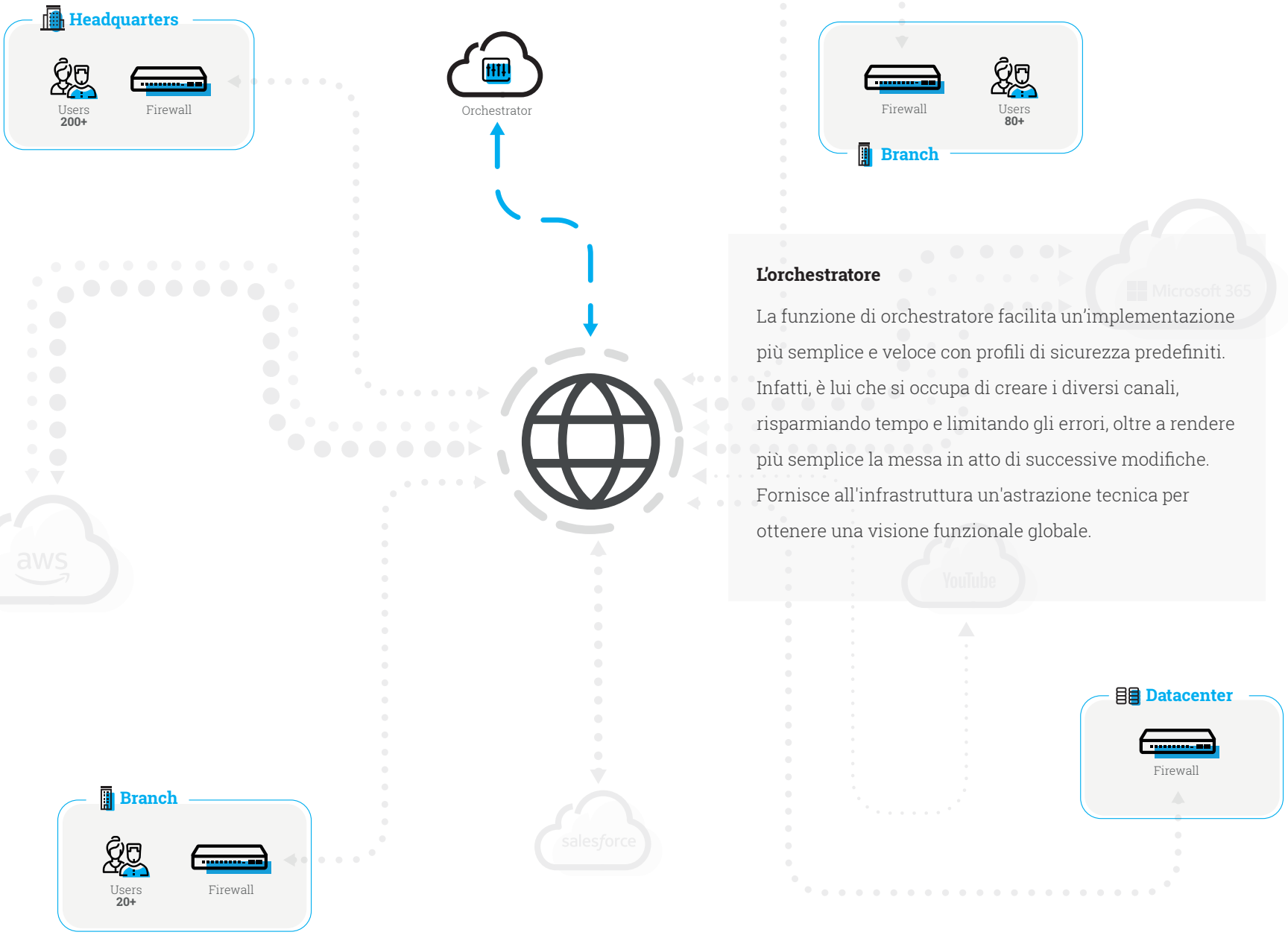
Con pochi clic è inoltre possibile definire le varie interazioni tra le postazioni aziendali, mentre l'orchestratore si occuperà di configurare tutti i dispositivi di connessione e sicurezza.

ORCHESTRAZIONE

D'altra parte, la visibilità globale fornita dalle soluzioni di orchestrazione garantisce **una visione a 360° dello stato dell'infrastruttura e delle prestazioni di ogni applicazione**.
Un sistema di monitoraggio in grado anche di segnalare gli indicatori SLA (latenza, giga, perdita di pacchetti) sulla qualità del collegamento.

Questa visione globale consente di attuare una politica efficiente di gestione della larghezza di banda (QoS) per garantire una connettività affidabile in qualsiasi momento, oltre a fornire visibilità sullo shadow IT.

In sintesi, la soluzione di orchestrazione scelta deve **assicurare un adeguato livello di fiducia nella sicurezza della rete, offrendo al contempo una configurazione semplificata**.
Le funzioni di supervisione prevedono il monitoraggio degli indicatori di qualità dei collegamenti, consentendo al contempo la gestione degli eventi (log) e degli incidenti di sicurezza.



L'orchestratore

La funzione di orchestratore facilita un'implementazione più semplice e veloce con profili di sicurezza predefiniti. Infatti, è lui che si occupa di creare i diversi canali, risparmiando tempo e limitando gli errori, oltre a rendere più semplice la messa in atto di successive modifiche. Fornisce all'infrastruttura un'astrazione tecnica per ottenere una visione funzionale globale.

Trusted SD-WAN: **una scelta di fiducia**

#7

TRUSTED SD-WAN

Come già detto, la SD-WAN ottimizza le comunicazioni remote e l'accesso al cloud, ma questa equazione deve comprendere anche la sicurezza. A tal proposito, sorge una domanda legittima: esistono architetture SD-WAN sicure certificate e/o approvate da un organismo di certificazione indipendente?

Allo stato attuale, non esistono certificazioni o qualifiche SD-WAN indipendenti da fornitori che promuovano questo approccio tecnologico.

Pertanto, è importante disporre di elementi concreti per giudicare oggettivamente la soluzione SD-WAN scelta. Quando si sceglie un fornitore tra diverse soluzioni hardware e software, si deve considerare, tra le altre cose, la solidità del prodotto e la fiducia nei confronti degli interessi geopolitici ed economici.

Da un lato, come sottolinea l'ANSSI[1], la **solidità** «*consiste nel testarne la capacità di resistere agli attacchi informatici in base a un contesto d'uso e a un livello di minaccia definiti*».

1 ANSSI, Fonte



Lo sapevate?

Il potenziamento o hardening è il processo che rende un sistema più sicuro.

Questo approccio consiste nel **ridurre all'essenziale i componenti software installati sul sistema, gli strumenti, gli utenti e i diritti non essenziali,** pur mantenendo le funzionalità necessarie per un corretto funzionamento.

Pertanto, è preferibile preferire soluzioni che tengano conto di questo aspetto per la sicurezza generale dell'infrastruttura SD-WAN.

Dall'altro lato, è importante che la nozione di fiducia sia chiaramente inclusa nella strategia di prodotto, al fine di rispettare gli impegni assunti nei confronti di un organismo ufficiale di certificazione/qualifica.

In sintesi, data l'assenza di una certificazione ufficiale SD-WAN, è necessario affidarsi alle varie certificazioni/qualifiche di prodotto e ai vari standard di sicurezza forniti dalle autorità governative per ottenere un'architettura di tipo Trusted SD-WAN.

GARANTIRE LA QUALITÀ DELSOFTWARE

Il collegamento a postazioni remote e l'accesso al cloud tramite SD-WAN aumentano la connettività, ma possono anche accrescere i rischi per la sicurezza se non si tiene conto di questa componente.

Infatti, le soluzioni che compongono la SD-WAN sono un bersaglio appetibile per gli attacchi dei criminali informatici. Inoltre, come sottolinea l'ANSSI[1], è necessario verificare gli elementi del software di un'infrastruttura e temprarne la configurazione prima dell'utilizzo.

Peraltro, come già accennato, si dovrebbe **dare la preferenza a fornitori affidabili in grado di offrire prodotti qualificati o certificati** da organismi terzi riconosciuti, come l'ANSSI in Francia, il CCN in Spagna, il BSI in Germania o l'ENISA a livello europeo. Solo in questo modo sarà possibile garantire la conformità ai requisiti normativi, tecnici e di sicurezza per ottenere la massima protezione del prodotto e, come indicato dall'ANSSI, [...] " *un impegno da parte del fornitore di soluzioni a rispettare i criteri di fiducia* "[2]. Inoltre, per ottenere un elevato livello di solidità, i prodotti devono dimostrarsi resistenti agli attacchi informatici in base a un criterio specifico che include una verifica del codice sorgente del prodotto in questione.

Come abbiamo appena visto, attualmente non esistono soluzioni SD-WAN certificate e/o qualificate sul mercato. Per colmare questa lacuna, è necessario analizzare preventivamente gli elementi in modo indipendente per scegliere uno o più fornitori che offrano prodotti solidi e affidabili (preferibilmente qualificati), con funzionalità SD-WAN (orchestrazione, ottimizzazione QoS, ecc.) e opzioni di sicurezza (firewall, filtraggio dei flussi, VPN, ecc.) per ottenere un pacchetto efficace che protegga la propria infrastruttura in qualsiasi momento.

VPN IPsec

DR

Protezione delle interconnessioni

"Le interconnessioni SI DR (diffusione limitata del sistema informatico) devono essere protette da tunnel VPN che garantiscano la protezione di tutti i flussi scambiati (riservatezza, integrità, anti-rigetto, autenticazione reciproca degli endpoint)". A tal fine, l'organizzazione ha definito un protocollo VPN IPsec DR.

ANSSI, Guida ANSSI-PG-075

1 ANSSI in *Guida alle raccomandazioni per le architetture e i sistemi informatici sensibili.* Fonte
2 ANSSI. Fonte

I 4 punti essenziali
per scegliere la propria Trusted SD-WAN

#1

Scegliere un fornitore riconosciuto da un organismo ufficiale e indipendente (ANSSI, CCN ecc.)

#2

Accertarsi che il fornitore disponga degli elementi SD-WAN e di sicurezza per una migliore copertura funzionale. Architettura sicura in un unico prodotto: utilizzo di un'appliance per unificare, tra le altre cose, SD-WAN, firewall e connessioni end-to-end sicure.

#3

Preferire le tecnologie con visibilità unificata. Ottimizzazione della gestione e migliore centralizzazione delle diverse funzioni.

#4

Disporre di una gestione efficiente delle applicazioni cloud (Microsoft 365, Salesforce ecc.)

Trusted SD-WAN by Stormshield: **affidabilità e sicurezza in un unico prodotto**

#8

Stormshield contribuisce a **integrare la Trusted SD-WAN** nella propria infrastruttura **in modo sicuro ed efficace**



Gestione semplificata della rete ad ampio raggio

Grazie alle funzionalità SD-WAN di Stormshield, **sarà possibile centralizzare e controllare le connessioni intersito e l'accesso al Cloud** per la propria infrastruttura ad ampio raggio.



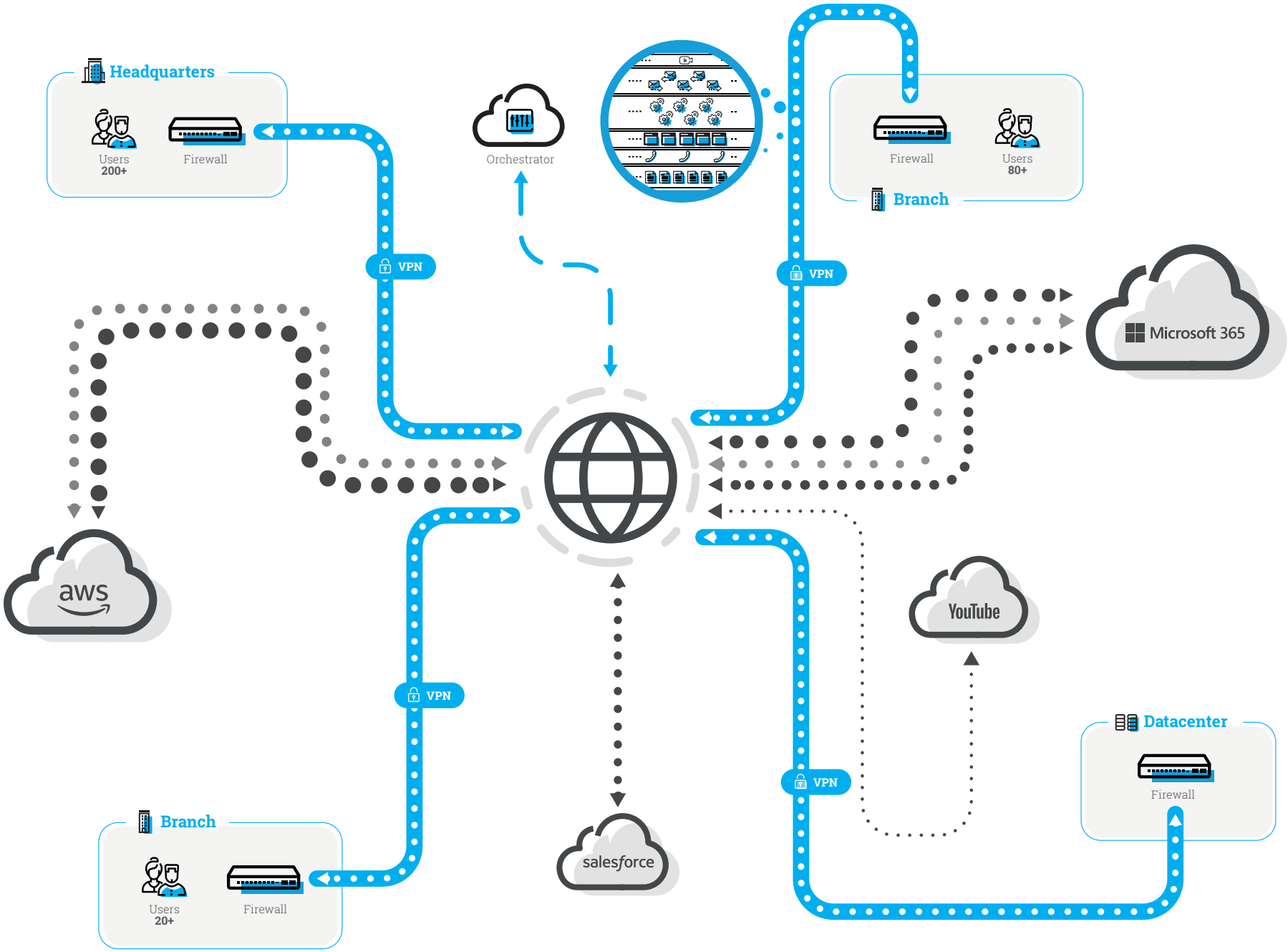
Protezione costante della SD-WAN

State tranquilli: la tecnologia SD-WAN offerta da Stormshield garantisce una **protezione impareggiabile di tutte le vostre connessioni**. I dipendenti potranno usufruire di accesso sicuro alle risorse aziendali ovunque si trovino e da qualsiasi dispositivo.



Scegliete la vostra SD-WAN di fiducia

Basata su una tecnologia certificata secondo i più elevati standard europei, la SD-WAN di Stormshield offre la possibilità di ottimizzare la sicurezza all'interno della propria infrastruttura.


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

LA **SCELTA EUROPEA** DELLA **SICUREZZA INFORMATICA**

www.stormshield.com

Qualsiasi diffusione, riproduzione o rappresentazione, anche parziale, del presente white paper per scopi diversi dall'uso privato su qualsiasi supporto è vietata e può comportare la responsabilità civile e penale per chiunque non si attenga a tale divieto.

Copyright © 2022 Stormshield