شـــرکت ارتبـاطات زیرساخت وزارت ارتباطات و فناوری اطلاعات	مقاله عنوان: بررسی سرویس SD-WAN و پیاده سازی آن در شرکت ارتباطات زیرساخت تهیه کننده/گان رشته تحصیلی رشته شغلی اداره کل/دفتر مهدی مشیری کارشناس ارشد کامپیوتر/ معماری سیستم های کامپیوتری کارشناس زیرساختهای فناوری اطلاعات و ارتباطات طرح و توسعه شبکه
این قسمت توسط دبیرخانه کمیته علمی تکمیل می-گردد.	شماره مقاله: ۱۲۸ حوزه کاربردی: پیاده سازی انواع سرویس های SD-WAN با توجه به شرایط موجود شبکه زیرساخت

چکیده

در این مقاله سعی شده است یکی از سرویس‌ها وکارکردهایی که کاندیدای پیاده‌سازی در شبکه‌ی مبتنی بر SDN شرکت زیرساخت خواهد بود را بررسی کرده و توضیحاتی در مورد نحوه پیاده سازی آن ارائه نماییم. هدف از سرویس SD-WAN برقراری اتصال بین قسمت‌های مختلف یک شرکت و/یا دیتاسنترهای آن است که در مکان‌های مختلف قرار دارند. این اتصال بر اساس نیاز و درخواست مشتری برقرار می‌شود، و در نهایت به دلیل فراهم کردن امکان کنترل دقیق شبکه و applicationها و همچنین در نظر گرفتن QoS متناسب با نیازمندی‌ها برای جریان‌های مختلف، توانایی قسمت‌های مختلف سازمان با یکدیگر برابر خواهد بود و هیچ قسمتی به دلیل مشکلات شبکه‌ای با محدودیتی روبرو نخواهد شد (برای مثال دور بودن یک قسمت از سازمان از لحاظ جغرافیایی باعث ایجاد مشکل تأخیر در آن قسمت نخواهد شد). همچنین به دلیل داشتن دیدی شفاف از لایه‌ی کاربرد، applicationهایی که نیاز به اتصال دائم به سرورها و دیتاسنترها دارند، می‌توانند عملکرد مطلوب‌تری ارائه دهند.

در این مقاله سعی شده است کاربردها و استفاده های مختلف از SD-WAN در شرکت ارتباطات زیرساخت در موارد زیر بررسی گردد:

- استفاده از SD-WAN و ابر
- استفاده از SD-WAN و لینک های اینترنت
- استفاده از SD-WAN با WAN هایبرید

در این مقاله، گزینه‌های استقرار مختلفی را برای اتصال شعبات با SD-WAN را بررسی خواهیم کرد. برخلاف شبکه‌های سنتی WAN، که فقط از ارتباطات خصوصی مبتنی بر پروتکل MPLS استفاده می‌کنند، SD-WAN گزینه‌های ارتباطی منعطف مختلفی را برای دسترسی به برنامه‌های کاربردی ابر و برنامه‌های کاربردی با میزبانی مرکز داده[1] فراهم می‌کند.

اتصال سازمان ها به خدمات ابری با استفاده از SD-WAN

یکی از محرک‌های اصلی برای استفاده از لینک های ارتباطی اینترنت/پهن باند برای اتصال به سایت‌های شعب، تطبیق خدمات ابر از تامین‌کنندگان زیرساخت-به‌عنوان-خدمت (IaaS) است، نظیرخدماتی که وب آمازون (AWS) تا تامین‌کنندگان نرم‌افزار-به‌عنوان-خدمت (SaaS)، مانند Salesforce.com، Office 365 و WebEx ارایه می کنند. معماری سنتی WAN به‌خوبی نمی‌تواند شعبات شرکت را به خدمات ابر، متصل کند. چرا؟ به چندین دلیل که معمولا، کلیهٔ ترافیک اینترنت به سایت مرکزی از طریق لینک های WAN اختصاصی گران‌قیمت بک‌هال[2] شده‌اند:

---

[1] Data center-hosted

[2] backhaul

- شعب معمولا، اتصال قوی با اینترنت ندارند و لازم است تا از اتصال اینترنت در سایت مرکزی، استفاده کنند.
- ترافیک بک‌هال ، که معمولا به آن هایرپین[۳]یا ترومبون[۴]گفته می‌شود، ضمن ایجاد تاخیر غیرضروری که بر روی عملکرد برنامه و تجربهٔ کاربر نهایی اثر می‌گذارد، از پهنای باند خصوصی WAN نیز به‌صورت ناکارآمدی استفاده می‌کند.
- SD-WAN دارای انعطاف‌پذیری است که تلاش می‌کند تا از خطوط اینترنت/پهن باند جهت تقویت یا حتی جایگزینی با خطوط ارتباطی خصوصی گران‌قیمت WAN، استفاده کند. این فناوری همچنین ترافیک را به‌صورت مستقیم و با استفاده از اینترنت/پهن باند به خدمات ابر ارسال می‌کند. خط‌مشی کسب‌وکار SD-WAN نحوهٔ ارسال مستقیم برنامه‌های منتخب ابر را به اینترنت و به‌صورت غیرمستقیم به دیگر خدمات ابر برای دیگر خدمات شبکه یا بک‌هال به سایت مرکزی، مشخص می‌کند. برای مثال، ارسال برنامه‌های کاربردی امن SaaS نظیر Salesforce.com، مستقیم از طریق خطوط اینترنت/پهن باند به‌جای بک‌هال از طریق سایت مرکزی.
- نیاز برای ارسال ترافیک وب بر روی خطوط اینترنت/ پهن باندبه خدمات امنیت وب در ابر.
- نیاز به بک‌هال ترافیک ایمیل به سایت مرکزی که باید توسط ابزار جلوگیری از ازدست‌دادن داده[۵](DLP) پویش شود. همانطور که در شکل ۱-۱ می‌بینیم، بدون SD-WAN ترکیب اینترنت/ پهن باند و خطوط خصوصی WAN به تنظیمات پیچیده نیاز دارد، حتی برای این‌کار نیز صرفا به الگوهای سفت‌وسختی نیاز

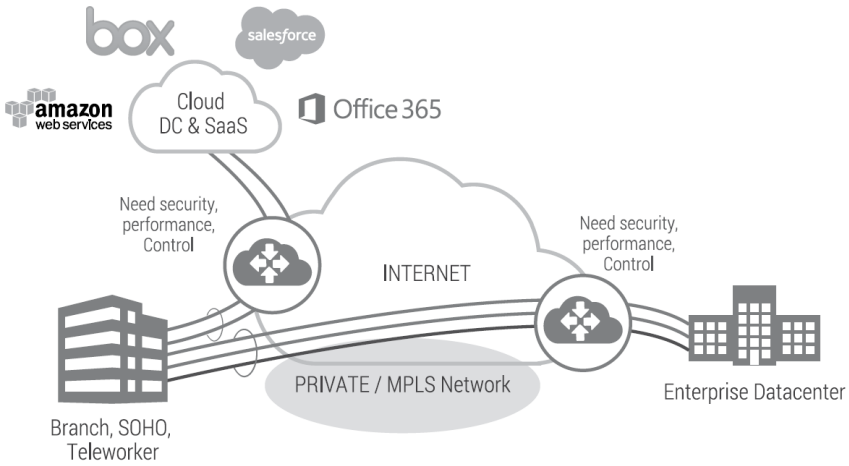
---

[۳] hairpinning

[۴] trombone

[۵] data-loss prevention

است. این قابلیت مهم مدیریتی به ردیابی تمام آدرس‌های IP از هر برنامه و تنظیم دستی مسیریابی آنها در طول هر لینک و بر اساس برنامه و موقعیت لینکهای ارتباطی می‌پردازد.



شکل ۱-۱ راه حل SD-WAN

SD-WAN باعث ساده‌سازی WAN با استفاده از خط‌مشی‌های کسب‌وکار و خودکارسازی می‌شود. چگونه؟ برای برنامه‌های SaaS، سازمان برنامه‌های کاربردی را انتخاب کرده و در مورد نحوهٔ ارسال مستقیم برنامه‌های کاربردی به ابر، درج خدمات ابر اضافی یا بک‌هال به سایت مرکزی با اولویت خاص کسب‌کار (بالا، متوسط یا پایین)، تصمیم‌گیری می‌کند. برای برنامه‌های کاربردی سازمان که در مرکز دادهٔ سازمان، میزبانی می‌شوند، سازمان می‌تواند اولویت کسب‌وکار را مشخص کند. راهکار SD-WAN مناسب‌ترین لینک ارتباطی را برای تحویل برنامه‌های کاربردی بر اساس اولویت کسب‌وکار و شرایط لینک ارتباطی بصورت بیدرنگ، انتخاب می‌کند.

ارسال ترافیک به‌صورت مستقیم بر روی خطوط اینترنت/پهن باند بدون SD-WAN دارای دو پیامد است:

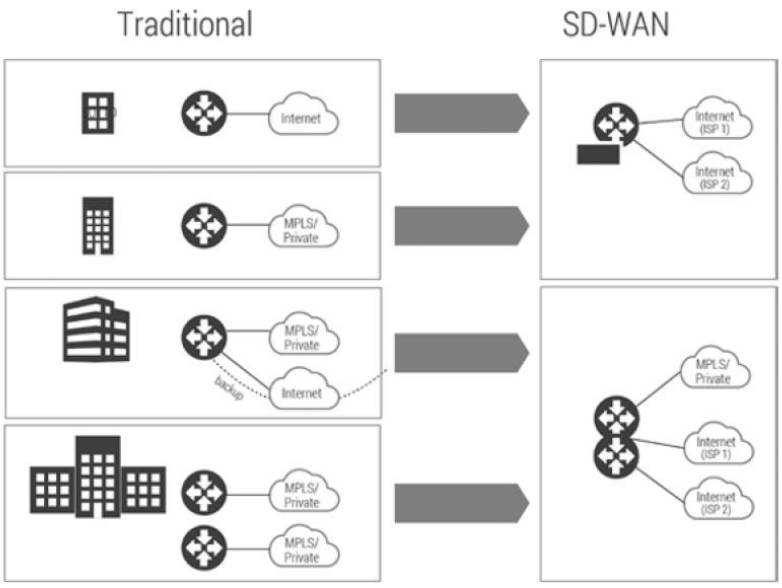
- سازمان نمی‌تواند به‌آسانی دسترسی‌پذیری یا عملکرد این برنامه‌های کاربردی را درسطح مدنظر به‌هنگام پیمایش شبکه‌های خصوصی شرکت، تضمین کند. خطوط اینترنت/پهن باند در تحویل عملکرد موردنیاز

توسط برنامه‌ها، شکست می‌خورد . برای مثال سازمان ، بر طبق گزارش کیفیت اینترنتVeloCloud (2H/2014)، در تحویل عملکرد خوب بصورت بیدرنگ به‌میزان ۲۵ درصد از مواقع، شکست می‌خورد.

- وقتی ترافیک به‌صورت مستقیم ارسال می‌شود، سازمان امکانی برای استقرار خدمات بیشتر امنیت و قابلیت service visibility، ندارد. SD-WAN سازمان را قادر به ارسال مستقیم برنامه‌های کاربردی SaaS و ترافیک وب اینترنت بر روی خطوط اینترنت/ پهن باند می‌کند، درحالیکه قابلیت‌دید، کنترل و عملکرد را نیز حفظ می‌کند. این امر میتواند تنها با داشتن طرح اضافی در ابر، انجام شود و ماهیت نرم‌افزاری SD-WAN این امر را ممکن می‌سازد. به‌علاوه، SD-WAN می‌تواند خدمات شبکه را صرفنظر از جایی که ترافیک ارسال می‌شود، درج کند.

نگاهی به گزینه‌های استقرار

سازمانی که از قبل دارای تنظیماتی با استفاده از اینترنت/پهن باند است، اغلب هنوز نیز از آن برای اهداف نسبتا مهم، ازجمله خطوط پشتیبان، استفاده می‌کند. اگرچه با افزایش در پذیرش ابر و برنامه‌های ویدئویی، تقاضا برای پهنای‌باند WAN نیز به شدت افزایش می‌یابد. قابلیت SD-WAN برای تقویت کامل خطوط اینترنت/پهن باند، معماری شعب دیگر را قادر می‌سازد تا به‌صورت کامل از خطوط اینترنت/ پهن باند به‌عنوان بخشی از WAN سازمان استفاده کنند، درحالیکه هنوز قابلیت اعتماد و عملکرد خطوط خصوصی را حفظ می‌کند. شکل ۱-۲ و جدول ۱-۱ نمونه‌هایی از گزینه‌های استقرار برای SD-WAN ذکر شده است.



شکل ۱-۲- گزینه های استقرار SD-WAN

Branch Type	*Traditional WAN*	*SD-WAN*
SOHO, Small office	Single Internet branch	Dual-Internet WAN branch
Small office	Single private WAN	
Medium office	Private WAN with backup link	Hybrid WAN branch using one or more private WAN and Internet
Large office	Multiple private WAN	

جدول ۱-۱ –گزینه های استقرار بر اساس نوع شعبات

استفاده از SD-WAN برای شعبات اینترنتی WAN

این نوع از شعبه، یک یا چند لینک ارتباطی را ترمینه می کنند که می‌توانند هر ترکیبی از پهن باند، بی‌سیم (3G، 4G LTE) و فیبر را دارا باشند. این کار، اتصال قابل‌اعتماد و امن را برای مرکز دادهٔ سازمان و دسترسی متمایزی را برای خدمات ابر عمومی، فراهم می‌کند. برنامه‌های حیاتی کسب‌وکار و ترافیک کم‌اولویت در خطوط یکسان اینترنت، جابه جا می شوند، هرچند خدمات مختلفی را ارائه می‌کنند.

با وجود دو لینک ارتباطی اینترنت/پهن باند، قابلیت SD-WAN برای هدایت پویای برنامه‌های کاربردی به‌صورت بسته‌ای[۶] و در میان جلسات[۷] فعال، می‌تواند باعث بهبود بالای قابلیت‌اعتماد و عملکرد برنامه‌ها شود. علاوه بر هدایت، برای غلبه بر پیامدهای موقت عملکرد که در خطوط ارتباطی اینترنت/پهن باند، SD-WAN می‌تواند به‌صورت مبتنی بر تقاضا[۸] به اصلاح بپردازد، ازجمله اصلاح پیش‌روی خطا[۹] (FEC) برای کاهش پیامدهای عملکردی مهم. بر اساس گزارشات کیفیت اینترنت VeloCloud (2H/2014) نتیجهٔ نهایی، داشتن شعبهٔ WAN ی است که قادر به پشتیبانی بیدرنگ سازمان در ۹۹ درصد مواقع است.

شعبهٔ هایبرید WAN با استفاده از SD-WAN

WAN هایبرید ، ترکیبی از خطوط ارتباطی اینترنت و WAN را استفاده می‌کند. درحالیکه سازمان‌ها از خطوط ارتباطی خصوصی WAN دوگانه‌ای استفاده می‌کنند که پهنای باند WAN خصوصی را افزایش می‌دهند و می‌توانند جهت حفظ دسترسی‌پذیری مدار، هزینهٔ بالایی را تحمیل کنند یا سرعت پایینی داشته باشند. SD-WAN اگر به خوبی طراحی شود، می‌تواند چالش‌های مدیریت عملکرد برنامهٔ کاربردی را در بین چندین شبکهٔ ناهمگن، از بین ببرد. تجرید خط‌مشی کسب‌وکار SD-WAN می‌تواند باعث افزایش بهره‌وری از تمام خطوط ارتباطی موجود بدون نیاز به تنظیم دستی پروتکل مسیریابی توسط اپراتور برای هر برنامه در هر خط ارتباطی شود. برای مثال، برنامه‌های بیدرنگ با اولویت بالا می‌توانند با قابلیت اعتماد بالاتری خطوط ارتباطی WAN را بپیمایند درحالیکه هنوز قادر به استفاده از خطوط اینترنت/پهن باند برای حجم عظیمی از داده‌ها هستند. برنامه‌های

---

[۶] Packet

[۷] Session

[۸] On_demand

[۹] Forward Error Correction

انتقال فایل می‌توانند از پهنای باند تجمعی در طول تمامی خطوط، بهره ببرند. اگر سازمان به برنامه‌هایی نیاز داشته باشد که باید به دلایل سازگاری و امنیتی از خط ارتباطی خاصی، استفاده کند، دراینصورت SD-WAN گزینهٔ بسیاری آسانی را برای کنترل خط منتخب برای هر برنامهٔ کاربردی، فراهم می‌کند.

بیشینه کردن مزیت‌های عملکردی استفاده از شبکه‌های ناهمگن

استقرار SD-WAN از شبکه‌های ناهمگن، پشتیبانی می‌کند، ازجمله خطوط ارتباطی دوگانهٔ اینترنت/پهن باند، خطوط ارتباطی سیمی و بی‌سیم و خطوط ارتباطی خصوصی و عمومی. این خطوط ارتباطی مختلف، بر اساس نوع خطوط و حتی زمان استفاده، دارای تنوع ویژگی‌های عملکردی زیادی هستند. اغلب این خطوط در ماهیت خود حتی، غیرهمزمان هستند. برای مثال، DSL، کابل و خطوط بی‌سیم معمولا دارای سرعت بارگذاری و دانلود مختلفی هستند، خطوط بی‌سیم دارای تاخیر در جهات جریان بالارونده[۱] و پایین‌رونده[۱] هستند. کاهش کیفیت عملکرد از جمله جیتر[۲]، گم‌شدن بسته و افزایش در تاخیر، معمولا در اثر ازدحام در شبکه، ایجاد می‌شود که در ماهیت خود یکطرفه است. به عبارت دیگر، ازدحام در شبکه، در جهت بالارونده، از جهت پایین‌رونده، مستقل است. SD-WAN برای بیشینه‌سازی مزیت‌های داشتن چندین خط ارتباطی در شبکه‌های ناهمگن، عملکرد جهات بالارونده و پایین‌رونده را به‌صورت مجزا، اندازه‌گیری می‌کند. چرا؟ اگر ازدحامی در جهت بالارونده رخ دهد که باعث افزایش قابل‌توجه تاخیر یا گم‌شدن بسته در جهت بالارونده شود، اندازه‌گیری زمان تاخیر چرخشی[۳] (RTT) یا تعداد کلی بسته‌های گم‌شده می‌تواند مشخص کند که کدام خطوط، قابل استفاده نیستند، درحالیکه در این مورد، هنوز امکان

---

[۱] upstream

[۱] downstream

[۱] jitter

[۱] Round Trip Time

استفاده از جهت پایین‌رونده، وجود دارد. برای SD-WAN مطلوب است تا در صورت وجود خطوط جداگانه، ترافیک بالارونده از جریان یکسانی را در یکی از خطوط ارتباطی ارسال کند و ترافیک بالارونده را در خط دیگری ارسال کند و عملکرد موردنیاز برنامه را تامین کند. SD-WAN می‌تواند از خطوط ارتباطی و جهات انتقالی متفاوتی برای کاربر نهایی و برنامه‌ها، استفاده کند.

برای اینکه راهکار بتواند قابلیت خدمات مدیریت‌شده (MSP) را تامین کند، باید تمامی لایه‌ها دارای قابلیت چندتننت[۴۱] با ذخیرهٔ بخش‌بندی شدهٔ داده و طراحی قابل‌اعتمادی باشند که هیچ‌گونه نقطه شکستی نداشته باشد. این قابلیت باید در چندین سطوح، مقیاس‌پذیر باشد تا صدها و هزاران شعبه را دربر بگیرد.

مهاجرت به SD-WAN

سازمان‌ها باید قادر به مهاجرت به SD-WAN بدون ایجاد مشکل یا جایگزینی دستگاه‌های قدیمی WAN خود باشند.از نظر تجربی، بهتر است تا استقرار SD-WAN به‌صورت افزایشی و با تعامل با دستگاه‌های موجود سازمان، انجام شود. در اینجا برخی مثال‌ها در این حوزه را مطرح می‌کنیم:

- **مثال ۱: اتصال شعب SD-WAN جدید به مرکز داده:** افزودن سایت‌های SD-WAN نباید به معنی، جایگزینی نقاط انتهایی WAN باشد یا نیاز به دستگاه مرکز دادهٔ جدیدی داشته باشد. راهکار SD-WAN نباید نقاط انتهایی SD-WAN را جایگزین کند بلکه باید از استاندارد IPSec پشتیبانی کند که در حال حاضر به‌صورت گسترده توسط سازمان، استفاده می‌شود. و این به این معنی نیست که تمام دستگاه‌های SD-WAN باید اتصال IPSec را با نقطه انتهایی VPN سازمان برقرار کنند، زیرا این‌کار سادگی SD-WAN را ازبین می‌برد. درعوض SD-WAN می‌تواند طرح اولیه‌ای را در ابر ارائه کند که اتصال از

---

[۱۴] multitenancy

دستگاه‌های SD-WAN را قطع می‌کند. سپس تنها به یک IPSec VPN از ابر SD-WAN به نقطه انتهایی VPN سازمان، نیاز خواهد بود.

- **مثال ۲: دستگاه و شعبهٔ دیوارهٔ آتش SD-WAN**: در مکان شعبی که سازمان، از قبل دارای دیوارهٔ آتش است، تجهیز SD-WAN در قسمت جلویی اینترفیس public دیوارهٔ آتش، قرار دارند. این کار اتصال WAN را قطع کرده و پهنای باند تجمعی را برای دیوارهٔ آتش شعبه فراهم می‌کند. سازمان‌ها می‌توانند خط مشی‌های امنیتی خود را که قبلا بر روی دیوارهٔ آتش خود داشتند را حفظ کند اما حالا به پهنای باند بیشتری نیاز دارند، همچنین مدیریت این سیستم آسان است و اتصال امن و قابل‌اطمینانی توسط SD-WAN فراهم می‌شود. به دلیل مواجهٔ مستقیم دستگاه SD-WAN با اینترنت، این سیستم باید دارای قابلیت دیوارهٔ آتش اساسی برای قبول ترافیک مناسب باشد.
- **مثال ۳: مسیریاب MPLS WAN موجود با انتقال و بارگیری SD-WAN**: سازمان‌هایی که قصد انتقال ترافیک معینی به دستگاه SD-WAN بدون انجام تغییرات پیکربندی مهمی در زیرساخت موجود خود هستند که این زیرساخت شامل: مسیریاب و سوئیچ لایه ۳ شبکه LAN می‌شود. در این مورد، دستگاه SD-WAN باید قادر به جذب قسمتی از ترافیک مورد ارسال از طریق SD-WAN باشند. دستگاه SD-WAN از طریق پروتکل مسیریابی ازجمله OSPF، زیرشبکه‌هایی[۱۵]را که قصد ارسال ترافیک از آنها را دارد، انتشار می دهد. وقتی ترافیک مشخصی به دستگاه SD-WAN رسید، خط‌مشی SD-WAN تصمیم می‌گیرد تا ترافیک را از طریق پوشش SD-WAN ارسال کند یا اینکه با استفاده از دستگاه قدیمی WAN آن را مدیریت کند.

---

[۱۵] subnet

- **مثال ۴: ارتباط امن یا بهینه مابین شعب SD-WAN:** سازمان باید اطمینان حاصل کند که دارای خطوط ارتباطی بهینه و امن مابین شعب SD-WAN است. معماری قدیمی hub & spoke[۴۱] استاتیک است و می‌تواند به عملکرد کاربردی غیربهینه‌ای منجر شود. به‌عنوان مثالی، گفتگوی ویدئویی مابین کارکنان در دو اداره از شعب در استان A با مرکز دادهٔ آنها در استان B، معمولا به هایرپین از طریق استان B، نیاز دارد. برای رفع این مشکل، WAN قدیمی، تونل استاتیک دیگری را مابین ادارات شعب در استان A، برقرار می‌کند. هرچند با افزایش تعداد ادارات شعب که به‌صورت راه‌دور از VPN اینترنت به هم متصل هستند، علاوه بر مواجه مشتریان آنها با چالش‌های مقیاس‌پذیری و مدیریت، WAN که به‌صورت استاتیکی تعریف‌شده است نیز قادر به عملکرد قابل‌اطمینان نیست.

دستگاه SD-WAN باید مقیاس‌پذیری، قابلیت مدیریت، قابیت اطمینان و امنیت را برای ارتباطات مابین شعب، رفع کند.

---

[۱] hub-and-spoke