禪

افسانههایی که در مورد افزایش امنیت با SD-WAN گفته میشود

چهار معماری SD-WAN برای امنیت شبکه

SD-WAN یا WAN نرمافزار محور به عنوان یک فناوری جدید در شبکه معرفی شده است . یک WAN شبکهای از کاربران یا دفاتر مختلف است که از لحاظ جغرافیایی میتوانند در هر کجای دنیا قرار گرفته باشند . مدیریت WAN پیچیده و هزینهبر است و هدف SD-WAN این است که این پیکربندیها را به صورت نرمافزاری انجام داده و هزینهها و پیچیدگی را کم کند . اما در مورد امنیت باید گفت که وعدههای SD-WAN در رابطه با تغییرات امنیتی که قرار است اتفاق بیفتد، گمراه کننده است .

SD-WAN یا WAN نرمافزار محور به عنوان یک فناوری جدید در شبکه معرفی شده است . یک WAN(Wide) Area Network شبکهای از کاربران یا دفاتر مختلف است که از لحاظ جغرافیایی میتوانند در هر کجای دنیا قرار گرفته باشند . مدیریت WAN پیچیده و هزینهبر است و پیادهسازی و ایجاد تغییرات در سیستمها به راحتی انجام نمیشود . هدف SD-WAN این است که این پیکربندیها را به صورت نرمافزاری انجام داده و هزینهها و پیچیدگی را کم کند . SD-WAN اجازه ساخت شبکههای مجازی در سطح سازمانی را ممکن میسازد.

اما وعده SD-WAN در رابطه با تغییرات امنیتی که قرار است اتفاق بیفتد، گمراه کننده است . یکپارچگی ویژگیهای مختلف امنیتی در SD-WAN، گسترش دفاتر راه دور را سادهتر میکند . پس از اتمام این یکپارچگی، شرکتهای امنیتی قابلیتهای SD-WAN و تواناییهایی که خود به آن اضافه کردهاند را معرفی میکنند . در زیر چهار معماری با در نظر گرفتن موارد امنیتی برای SD-WAN ارائه شده و مشکلات آنها بیان شده است .

SD-WAN

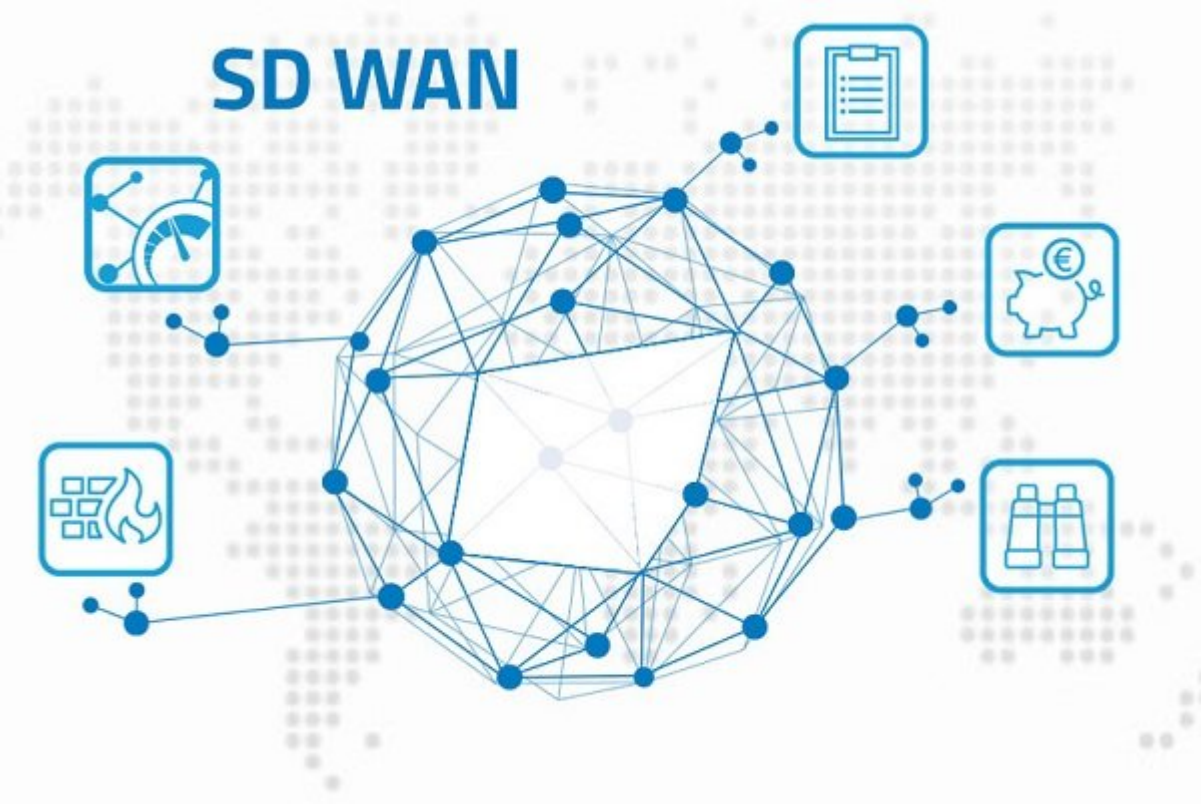
1.دستگاههای **SD-WAN** بر پایه دیوار آتش

بسیاری از سازندگان SD-WAN از قابلیتهای دیوار آتش (فایروال) استفاده میکنند . این فایروالها مشابه فایروالهای stateful هستند و ممکن است در روترهای دفاتر داده دیده شوند . توانایی آنها شامل فیلترینگ بر اساس سیاست و بلوکه کردن بر اساس آدرس IP و پورت است. مثالهایی از آنها □□□□□) ،Viptela، Silver Peak و Velocloud) است.

ایجاد امکانات پایه فایروال ممکن است برای اتصال مکانهای راه دور به اینترنت در SaaS کافی باشد اما برای فراهم کردن در یک فضای بزرگتر خیر . راهحل آن ایجاد تواناییهای کنترلی در لایه 4 تا لایه 7 مانند فایروالهای نسل □□□□(NGFW)، سیستمهای جلوگیری از نفوذ و فیلترینگ URL است.

2.دستگاههای **SD-WAN** با فایروال پیشرفته

برخی سازندگان SD-WAN از قابلیتهای امنیتی پیشرفتهای استفاده کردهاند . اما نکته منفی این است که آنها معمولاً مدیریت بخشهای شبکهای و سایر جنبههای امنیتی را رها کردهاند . این دقیقاً همان بهم ریختگی است که جلوی کنترل و بینایی مدیران IT را میگیرد . دستگاهها در طول حیات خود هزینههای جاری قابل توجهی مانند تست، گسترش، نگهداری و مدیریت دارند . محدودیت منابع در وسیلهها معمولاً نیاز به ارتقا سختافزاری را میطلبد . محدودیتهای دیگر باعث میشود آنها کاری برای امنیت کاربران موبایل انجام ندهند که معمولاً مشکل کارایی بوجود میآورد .



SD WAN

3.ابزارهای فایروال با SD-WAN

همزمان چندید تأمین کننده امنیت، قابلیتهای SD-WAN را در فایروالهای NGFW معرفی کردند . بر اساس گزارش گارتنر برخی از آنها عبارتاند از : Fortinet ، Barracuda و Cisco Meraki.

SD-WAN باید بتواند در چند ثانیه به یک اتصال دیگر هم سوئیچ تا بتواند وضعیت نشست را نگهداری کند . این تفاوت اصلی بین SD-WAN و مسیریابی IP است که میتواند تا 40 ثانیه برای اتصال به یک ارتباطات دیگر، طول بکشد . با این حال برای برخی از شرکتهای امنیتی مانند Cisco Meraki این زمان تا 300 ثانیه طول میکشد .

4.امن کردن SD-WAN به عنوان یک سرویس

برخی از سازندگان در حال حذف دستگاهها با تغییر در SD-WAN و قابلیتهای امنیتی هستند . Cato Networks بهترین مثال از این نوع نگرش است که خدمات امنیتی و SD-WAN یکپارچهای را فراهم میکند . Cato Cloud همچنین با استفاده از backbone خودش در حال رفع مشکلات backbone اینترنت است.

دیگر سرویسهای SD-WAN در حال فراهم کردن قسمتهایی از امنیت SD-WAN هستند. مانند Aryaka که تواناییهای فایروال پایه را دارد اما کنترلهای لایه 4 تا لایه 7 ، IPS ، NGFW و آنتی ویروس را فراهم نکرده است .

نویسنده :
فرشاد رضایی
منبع :
نتورک ورلد
دسته بندی:
ترفند امنیت
فناوری شبکه
تاریخ انتشار :
11:20 - 27/10/1396

:□□□□□
SD-WAN □□□□□□□ - □□□□□□□□ - □□□□ □□□□□□ □□□ SD-WAN - WAN

□□□□□
:□□□□https://www.shabakeh-mag.com/tricks/security-tricks/11472/%DA%86%D9%87%D8%A7%D8%B1-%D9%85%D8%B9%D9%85%D8%A7%D8%B1%DB%8C-sd-wan-%D8%A8%D8%B1%D8%A7%DB%8C-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87