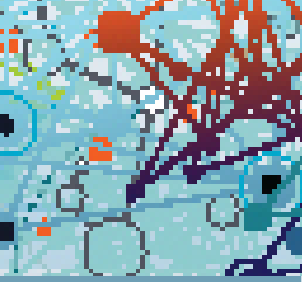
open systems

SPECIAL REPORT

The combination of security and agility: Managed Secure SD-WAN — the corporate network of the future

TechTarget Custom Media



1. INTRODUCTION

Digitalization and globalization are two factors that are determining the strategy and business activities of today's companies. Managed, software-defined wide area networks (SD-WANs), which are supplied by a service provider, make it easy for global companies to set up global communication infrastructures. They combine technologies such as Multi-Protocol Label Switching (MPLS) with broadband Internet links and mobile connections.

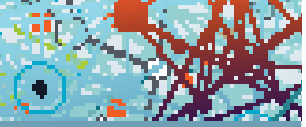
However, SD-WANs, like any other networks, need to be protected against cyberattacks, and security risks caused by operating errors need to be reduced. Multi-national companies can achieve this easily: by using a managed, software-defined WAN with integrated security services – a Managed Secure SD-WAN delivered by an experienced service provider.

2. THE KEY ROLE OF IT SECURITY WITH SD-WANS

With the help of a Managed Secure SD-WAN service, companies can easily manage a substantial challenge: they can provide staff in subsidiaries as well as customers and partner companies, with secure and flexible access to data and applications via a software-defined WAN. IT and data security are extremely important factors for multi-national companies because data loss through the carelessness of employees or hacker attacks can have both legal and financial consequences.

This can be seen from the following example: In the summer of 2017, a cyberattack was launched against the corporate network of the Danish shipping company A.P. Moller-Maersk using the ransomware NotPetya. The consequence: The company had to reinstall 4,000 server systems and 45,000 PCs in subsidiaries in four continents and reconfigure 2,500 applications. The costs caused by the downtime of applications and IT resources, as well as the removal of the damage, amounted to around 300 million USD.

This does not mean that software-defined WANs are not as secure as standard MPLS infrastructures. However, with SD-WAN you do need to remember that the benefits of increased flexibility and extended configuration options entail a certain amount of risk. This includes security gaps caused by errors during configuration and operation. In addition, you need to bear in mind that the increasing amount of data from «things» (i.e. the Internet of Things) will be transported via corporate networks in the future such as from sensors in vehicles, machines and storage systems. This



also makes it more complicated to protect SD-WANs against data loss or attacks.

3. ALTERNATIVE: MANAGED SD-WAN SERVICE WITH INTEGRATED IT SECURITY

SETTING UP and operating a secure SD-WAN is a real challenge even for multi-national companies with large IT departments. Special knowledge is required that only few companies possess. This means it is better to seek the assistance of a managed service provider when setting up a secure SD-WAN, instead of going it alone. This service provider should possess the following core competencies:

- Extensive experience with the operation of global, software-defined corporate WANs, including the «control» of providers as well as the management of IT and WAN resources.
- In-depth knowledge of all relevant IT security issues, from the setup of protected SD-WAN infrastructures to protection against malware and the authentication of users as well as the implementation of separate WAN zones.
- Experience with security operations (Security Operations Centers), in order to provide the processes required to protect, monitor, detect and restore overall systems.

One tried-and-tested approach here is to establish a software-defined WAN with IT security functions, which is provided to the users in the form of a Managed Secure SD-WAN. The benefit for a company is that this approach offers a sort of «all-round care-free package» — a global software-defined WAN with security services from a single source, including 24x7 operations and integrated security monitoring by the service provider. You could say the provider of a Managed Secure SD-WAN inserts an additional IT security level within the software-defined WAN.

IT SECURITY COMPONENTS OF A MANAGED SECURE SD-WAN

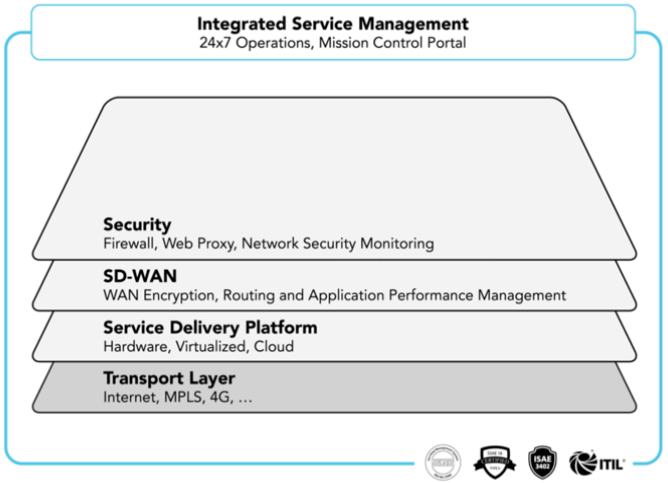
THE IMPORTANT point is that this «security layer» provides all functions that are required to protect data and applications in the managed SD-WAN. They include traditional IT security components like next generation firewalls, intrusion protection systems (IPSs) and VPN tunnels with strong encryption for data that is transported via the SD-WAN.

HOME

THE COMBINATION OF SECURITY AND AGILITY: MANAGED SECURE SD-WAN — THE CORPORATE NETWORK OF THE FUTURE

In addition, you have security functions geared towards the respective users or specific user groups. For example, employees working out of the office or in home offices require special, secure access to applications in the company's SD-WAN (secure application access). In general, an SD-WAN infrastructure should protect the users in all situations, no matter whether they are using a PC in a subsidiary or a mobile system like a notebook or smartphone.

It is therefore helpful, especially for mobile users, if a mixture of cloud entry points and SD-WAN entry points are available. This would enable users to connect to the SD-WAN via the nearest access point, which would also increase the performance of the applications used by the employees. Furthermore, with the help of a managed services provider, a company can also integrate new subsidiaries and offices quickly and simply into the software-defined WAN.



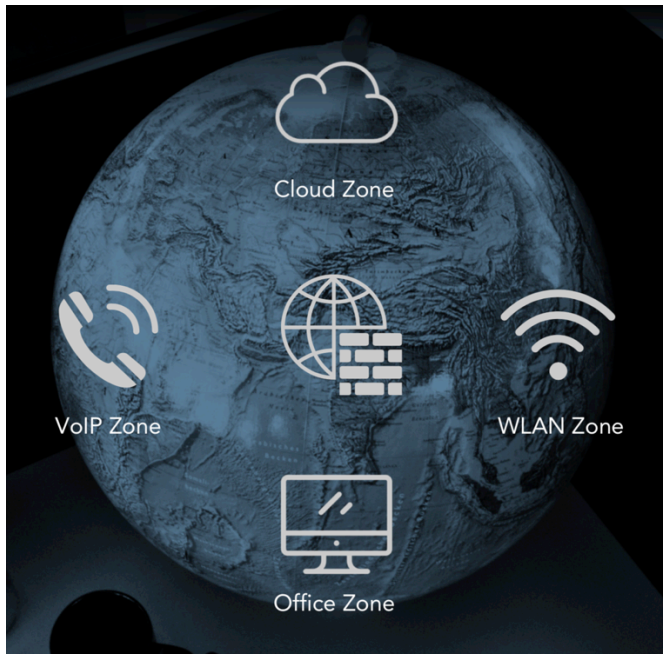
Elements of a Managed Secure SD-WAN

SEPARATE ZONES

ONE SECURITY component that very few service providers currently offer are separate zones within an SD-WAN. An example: A computer in a branch office has been infected with ransomware. In a standard SD-WAN, this could result in the entire company network becoming infected.

You can prevent this in a Managed Secure SD-WAN using secured zones for different areas, such as an IoT zone , a zone for server systems, one for Voice-over-IP

components or an additional zone for clients. These zones are separated from one another by using globally valid firewall rules. As a result of such a setup, an attack can only affect part of an SD-WAN, but not the entire infrastructure.



A global Managed Secure SD-WAN should include separate security zones for different areas.

HOME

THE COMBINATION OF SECURITY AND AGILITY: MANAGED SECURE SD-WAN — THE CORPORATE NETWORK OF THE FUTURE

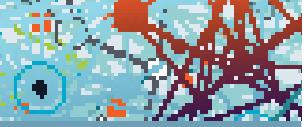
FOCUS ON THE APPLICATIONS

A CENTRAL aspect of a Managed Secure SD-WAN service is that the focus is not exclusively on the optimization and securing of the SD-WAN infrastructure. Rather, an approach is required that takes the performance and security of the applications into consideration as well as the network infrastructure.

A Managed Secure SD-WAN is thus geared more towards the needs of a company's specialist departments and business requirements. What's more, a corporate network, which is geared towards the «business», is essential in these times of digital transformation. Implementing new ideas and developing new business areas quickly necessitates a corporate network that can ideally be adapted within a matter of hours – without any security risks and without putting too much strain on the in-house IT department.

HOLISTIC VIEW THANKS TO NETWORK SECURITY MONITORING

ONE CLEAR benefit of a Managed Secure SD-WAN is that any malicious or unauthorized behavior within the corporate network can be identified immediately, analyzed and stopped. This task is covered by Network Security Monitoring (NSM). In comparison with



service chaining, which is used with many SD-WAN services, NSM has a decisive advantage: it records all data – from the activities of systems that communicate via the SD-WAN, to web traffic and the results of local scanning activities.

After all, it is only possible to recognize and block complex attacks if both network specialists and IT security experts are able to analyze this information centrally. One essential requirement of a Managed Secure SD-WAN service is thus the provision of a centralized service platform, which grants access to the information to both groups of experts. This in turn is a prerequisite for ensuring that network and security specialists can respond efficiently to security-relevant incidents.

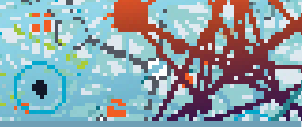
However, if the monitoring of SD-WAN traffic is limited to just web traffic, for example, recognized anomalies cannot be correlated with other activities in the network. This in turn makes it more difficult to detect attacks or non-authorized activities of users. Comprehensive Network Security Monitoring, which is handled by experienced IT security experts of an SD-WAN service provider, can provide assistance here. The timeframe within which cyber risks in the SD-WAN are identified and removed can be reduced to minutes and hours with such help, instead of days and weeks.

A comparison: According to details from IT security firms like FireEye, cybercriminals can be active within the networks of European companies for more than three weeks before being discovered by internal security experts. During this time, they can cause considerable damage by stealing sensitive data.

4. CONCLUSION: MANAGED SECURE SD-WANS REPRESENT THE FOUNDATION OF EVERY DIGITAL COMPANY

Multi-national companies with offices in many regions can benefit significantly from a service provider, which can take over operation of SD-WAN and also offer the required IT security functions. Use of a Managed Secure SD-WAN can thus save time, effort and money. This is because a «do-it-yourself» approach can quickly get out of hand when it comes to personnel and financial outlay.

Other benefits of a Managed Secure SD-WAN include a high level of transparency and security. This is also beneficial when it comes to audits, because in such cases, the providers of managed services are obliged to ensure conformity with security measures and compliance guidelines. What's more, the



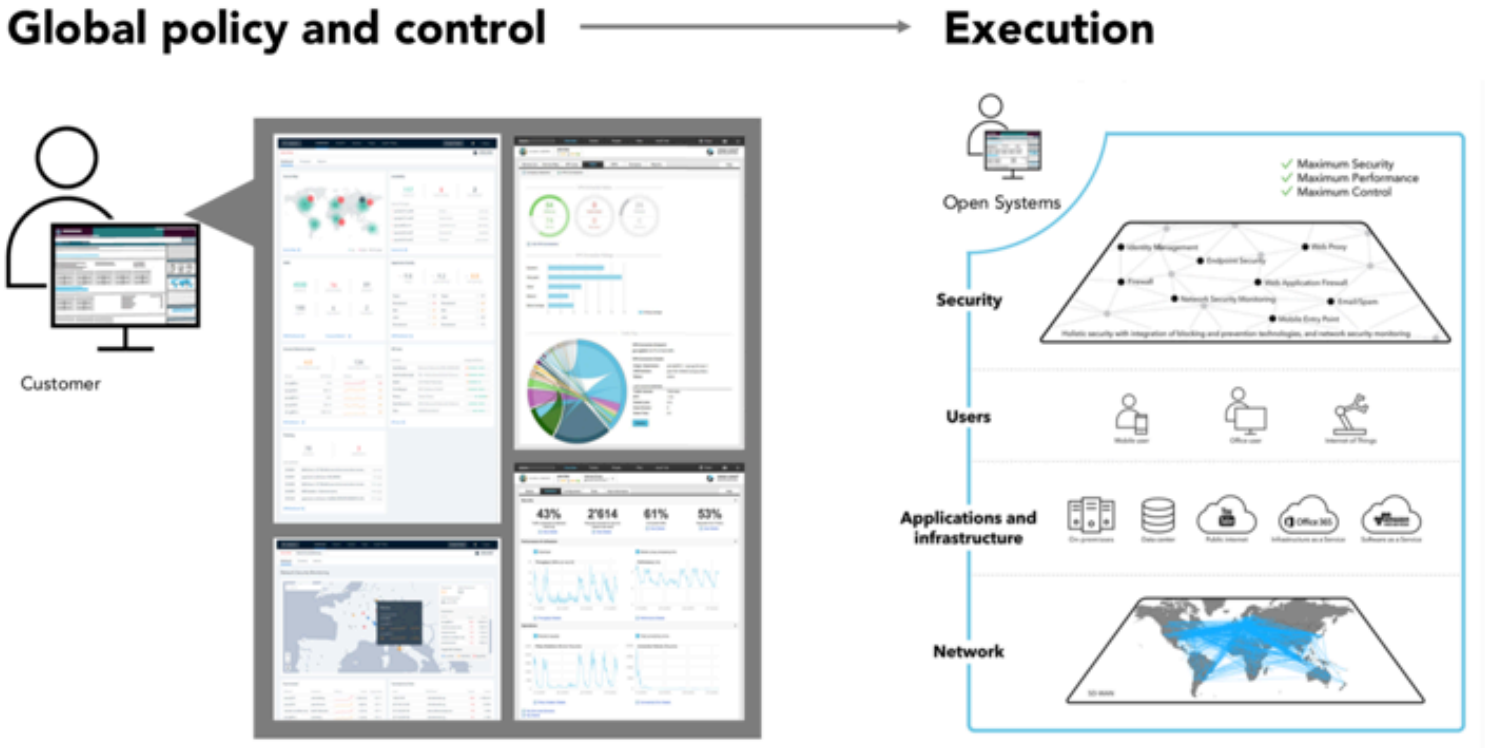
traditional benefits of a software-defined WAN include the possibility, for example, to provide users at the individual locations with data and applications in line with business requirements.

One aspect that is particularly important for globally active companies, however, is the high level of security provided by a Managed Secure SD-WAN. The professional IT security teams of a managed services provider can identify all kinds of cyberthreats quickly and eliminate them within a very short period of time – 24 hours a day. This means expensive data leaks, which can damage a company's image, are a thing of the past. Furthermore, the users of a Managed Secure SD-WAN can concentrate on the really important things: their core business and the adaptation of their offers and business processes to the digital age.

CHECKLIST: FIND THE RIGHT MANAGED SECURE SD-WAN

MULTI-NATIONAL COMPANIES that wish to use a Managed Secure SD-WAN service need to consider a number of points when choosing an appropriate service provider. The ten most important criteria are:

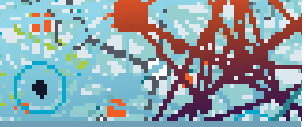
- Global availability of the Managed Secure SD-WAN: To ensure this, the provider should work with leading, global «Tier-1» providers and local partners. These would be ISPs in regions where the customer has offices, for example.
- Central WAN and security management for both existing and new connections.
- Application control: Extensive control of applications across all layers.
- Around-the-clock availability: The Managed Secure SD-WAN service should be available 24x7. This applies in particular to functions like security and performance management.
- Support via a team of experts of the service provider: External specialists can take over the management of the SD-WAN environment as well as security aspects; furthermore, such specialists can provide assistance when choosing a suitable SD-WAN and IT security components.
- Central management via a web portal: Users should be able to manage the Secure Managed SD-WAN via an intuitive web front-end. It must provide an overview of configurations, statistics and all change management activities, in order to deliver a central audit trail.



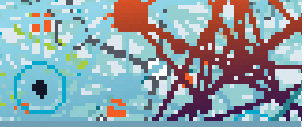
THE ADMINISTRATORS A MANAGED SECURE SD-WAN HAVE ACCESS TO ALL RELEVANT INFORMATION AND CONTROL FUNCTIONS VIA A WEB PORTAL.

HOME

THE COMBINATION OF SECURITY AND AGILITY: MANAGED SECURE SD-WAN — THE CORPORATE NETWORK OF THE FUTURE



- Support of different architectures: Ideally, the SD-WAN will support different network topologies at the same time, such as mesh topologies or a setup similar to a hub and spoke topology.
- Provision of all relevant IT security functions: This includes next generation firewalls (NGFW), intrusion detection and prevention systems (IDS/IPS), distributed web proxies, data encryption (WAN encryption) as well as strong authentication of users.
- Monitoring of data traffic: All data flows, which run via the managed secure SD-WAN to the subsidiaries of a customer, are recorded in order to be capable of analyzing performance and security incidents quickly. When recording the data traffic, the de-facto standard Netflow should be used.
- Parallel support of different implementation and usage types: On-premises (in-house data center), hybrid cloud infrastructure and public cloud.



TechTarget Custom Media

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more — drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers — all to create compelling and actionable information for enterprise IT professionals across all industries and markets.

HOME

THE COMBINATION OF SECURITY AND AGILITY: MANAGED SECURE SD-WAN — THE CORPORATE NETWORK OF THE FUTURE