SD-WAN Best Practices for Security

by The Tolly Group

The goal of this paper is to provide a concise summary of important security considerations and options for SD-WAN deployments.

Presented courtesy of

CITRIX

Executive Summary

Perhaps more than in any other part of your network, your SD-WAN strategy needs to be equal measures networking and security. By definition, the SD-WAN interfaces with and runs across external, often public, networks - the source of many threats. Additionally, the site networks, whose traffic flows across your SD-WAN, are likely to be multifaceted.

Each site will likely handle critical business applications, provide access to cloud services, handle common web browsing and often handle Internet traffic generated by visitors and guests. Each of these traffic flows has different security needs. And, to these elements we add the need to secure the SD-WAN infrastructure itself. Growth in IaaS, PaaS and SaaS all impact your SD-WAN and attacks on branch office users can expose the corporate applications and data they use.

You will find no argument on this topic. Security is an essential aspect of SD-WAN. But start your research and prepare to be bewildered. Unsurprisingly, many vendors prefer to build security into their "bigger vision" for cloud architecture. Unsurprising because it is often easier just to get a customer to buy into the top-down "vision" than to try sell bottom-up features and capabilities. But a vision won't protect your corporate network, specific security features do.

An overarching question is where physically to implement security - at each branch office, in the cloud or at a central headquarters location? Security elements are likely required at all three.

So, where to begin? At the beginning. We can't provide a complete guide to SD-WAN security in a single document, but we can get the job started. In our view, the place to begin is with identifying the individual elements of the SD-WAN that require security.

Thus, this document will attempt to take structured approach to making the job of securing your SD-WAN more tangible by putting names and descriptions to the various elements of your SD-WAN.

The best practice is to implement security relevant to YOUR company requirements. Ultimately, that is what really matters. More than many things, security needs vary across companies. In these pages, Tolly will outline elements for consideration in building that strategy.

Contents

Concept-in-a-Nutshell

SD-WANs carry business-critical applications but, by necessity, are exposed to the outside world where risks abound. Security risks must be identified and solutions understood.

Scope

This document aims to provide practical, strategic guidance to enable users to identify areas of potential security risk and steps

About The Tolly Group

IT experts with over 30 years of experience

We provide product benchmarking and analyst services to the end-user and vendor community.

info@tolly.com   www.tolly.com

Citrix SD-WAN

Citrix is powering a better way to work with unified workspace, networking, and analytics solutions that help organizations unlock innovation, engage customers, and boost productivity, without sacrificing security. Citrix solutions are in use by more than 400,000 organizations including 99 percent of the Fortune 100 and 98 percent of the Fortune 500.

Citrix SD-WAN is a next-generation WAN Edge solution that accelerates digital transformation with flexible, automated, secure connectivity and performance to ensure an always-on workspace. With this, organizations can quickly add new sites, rollout new applications and monitor reliable connections to the cloud using automation, policy-based enforcement, zero-touch deployment and intelligent reporting.

Citrix SD-WAN benefits organizations of all sizes with:

- **Experience** – best performance for cloud and virtual applications
- **Security** – easiest options for protecting the network and cloud
- **Choice** – most flexibility to automate extending the network to the cloud

Citrix offers options for protecting users and data from multi-vector cyber threats across an expanding attack surface from branches, to data centers, and clouds with a multi-site, layered approach.

With an integrated ICSA-certified perimeter firewall, SD-WAN masks users and infrastructure from cyber surveillance. Global policy control provides zone-based policies for granular micro-segmentation of traffic and Internet breakout for enhanced application performance. Citrix SD-WAN also takes extra precautions by encrypting all branch-to-branch egress traffic, even when it is transported over a private MPLS line.

In addition, Citrix has partnered with industry leaders like Palo Alto Networks, Zscaler, and Symantec to deliver joint solutions that enable SD-WAN to be a transparent gateway for Secure Web Gateway (SWG) service.

To maintain strict compliance requirements or to maintain separation between Security Operations (SecOps) and Networking operations (NetOps) teams, Citrix offers an SDN/NFV-ready platform which host various virtualized network functions (VNFs) to provide advanced, next-generation firewall capabilities.

To learn more, visit: citrix.com/sdwan

Source: Citrix Systems

that can be taken to address those risks.

This document is not a step-by-step cookbook for implementing SD-WAN security. Tolly provides consulting services that can assist organizations in realizing specific design and implementation needs.

Business Goals

Before any discussion of benchmarking specifics the team should spend the required time to understand the business priority of each application. Only with that knowledge can one effectively design a relevant and meaningful security deployment plan.

Best Practices Goals

Identify areas where a security solution is needed to protect a system and underlying data from being compromised.

No Standard Approach

While it is standard for security to be an element of SD-WAN, there is no standard method or approach for deploying security.

Security vs. Performance

Always keep in mind that extra layers of security and longer, more secure keys can possibly have a negative impact on user experience. Every layer of security adds protection but adds small amounts of latency that, combined with other security layers, could be significant.

Similarly, while more complex keys can better protect your data in transit, they can also put a higher workload on security devices like secure web gateways that need to decrypt, inspect and re-encrypt traffic.

Security Services Deployment Location Choices

By definition, an SD-WAN connects branch offices with a central location via a wide area network. This connectivity enables network architects to choose where physically a given security service is to be implemented. See Figure 1.

More often that not, organizations deploy SD-WAN to enable their branch offices to directly connect to the Internet instead of always backhauling traffic through the headquarter servers. This makes it easy to establish local Internet breakouts and offers branch office users the ability to quickly and efficiently access cloud applications and services, like Office 365. SD-WAN greatly improves agility and simplifies branch IT.

In theory, any security service could be implemented locally at the branch office, remotely at a headquarters/data center location (in cases where the company still decides to backhaul traffic to a data center) or at a software-as-a-service SaaS provider's data center or a cloud-based security service.

"Local vs remote" is not an all-or-nothing choice. For example, it makes sense for basic firewall functions to be local to the branch for reasons of both basic protection and performance. Certainly, endpoint security needs to be in place for company company computers as the branch as part of a defense-in-depth approach.

A secure web gateway monitors and filters web user traffic to prevent interaction with restricted sites and to stop malware. For secure web gateways, it might make more sense for both administrative and economic reasons for that to be located at a centralized data center - either at your company's data center or at a service provider's data center.

Functions such as single-sign, federated ID and cloud access security broker (CASB) are good candidates for remote deployment.

As with many decisions there are tradeoffs when deciding to host branch security functions at the branch or "backhauled" to another location or use a cloud-based security service. Here are some to consider:

Partial Backhaul. SaaS providers will have multiple locations and typically be located on very high bandwidth links. Thus backhauling "partially" to a SaaS provider rather than to your corporate datacenter could provide better performance and use less

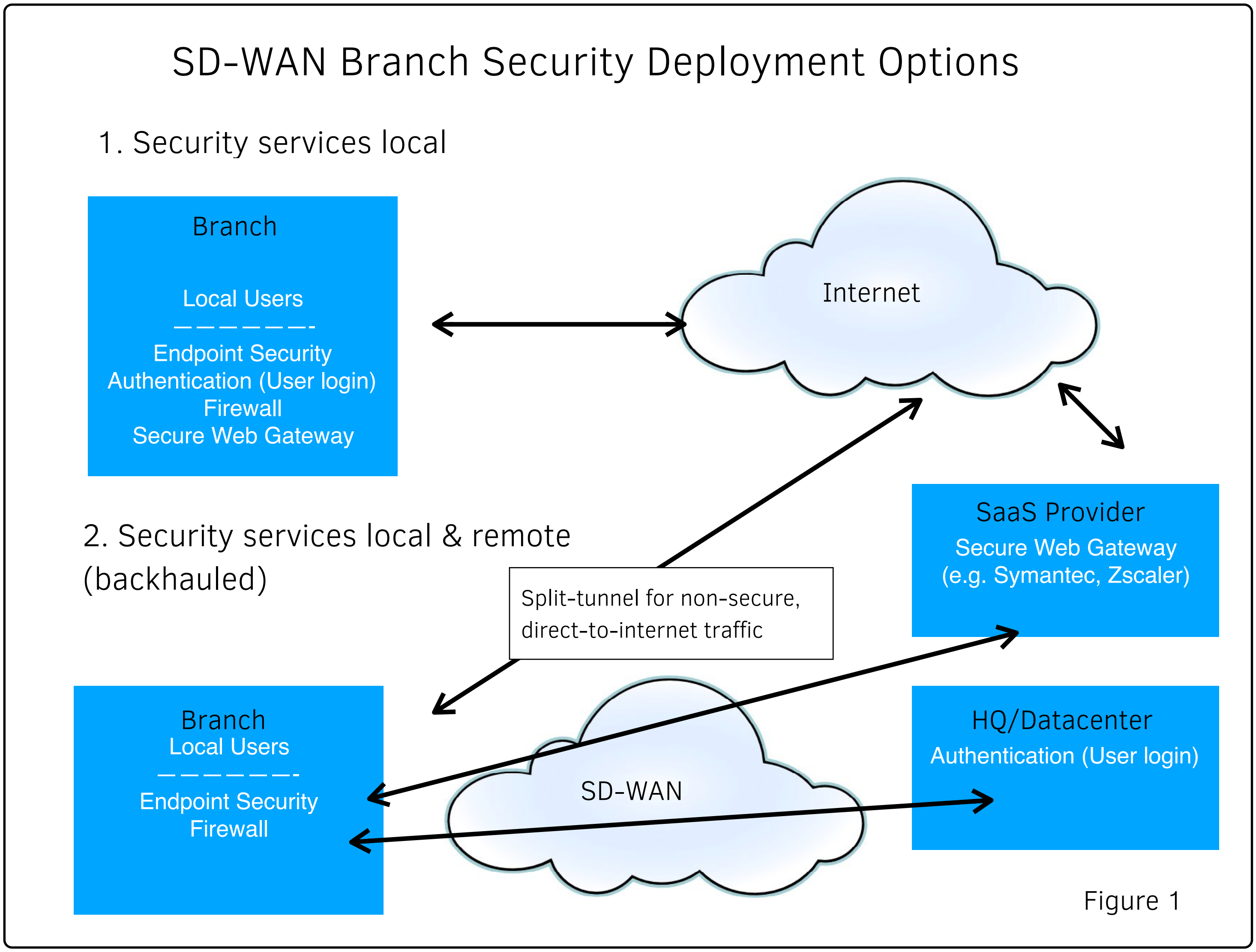
SD-WAN Branch Security Deployment Options
1. Security services local
Branch
Local Users
Endpoint Security
Authentication (User login)
Firewall
Secure Web Gateway
Internet
2. Security services local & remote (backhauled)
Split-tunnel for non-secure, direct-to-internet traffic
SaaS Provider
Secure Web Gateway
(e.g. Symantec, Zscaler)
Branch
Local Users
Endpoint Security
Firewall
SD-WAN
HQ/Datacenter
Authentication (User login)

Figure 1

bandwidth than the alternative approach.

Bandwidth. Backhauling a security service to another location necessarily consumes bandwidth not required when processing locally. The extra bandwidth used will depend upon the nature of the security service.

For example, authenticating credentials would take place relatively infrequently and would likely require little bandwidth. Backhauling firewall services or other constant traffic streams could generate considerable "back and forth" bandwidth usage.

Latency. Perhaps more of a concern that bandwidth is the extra latency (delay) incurred when backhauling security services. Every request/response sequence that gets backhauled over the SD-WAN is additional delay. While this additional delay can be on the order of milliseconds, it combines with other processing elements which, together, could quickly degrade the user experience.

Licensing. Depending upon the type of security service, the vendor may charge you by how many instances you are running or, in the case of hardware, how many appliances you purchase. Thus, concentrating a particular service in, say, five regional data centers rather than implementing it separately in 200 branch offices could have a major impact on license costs.

Management & Support. It is safe to say that managing fewer security devices, either physical or virtual, is easier than managing more devices. Thus, backhauling certain branch security functions across the SD-WAN so as to allow many branches to use a single security device or service can simplify management and support and thus should be a consideration.

Summary. For performance reasons, it would be good to keep "noisy" (high volume) security functions local to the branch. For management and licensing reasons, lower volume security functions could be candidates to be backhauled to a central location. At a minimum, basic firewall functions should be implemented at the branch level. This can also assist in micro-segmentation of branch traffic.

Service Chain

SD-WAN is a single term that represents multiple services. These services can be related to the branch LAN, the WAN, traffic management, etc.

In addition to selecting which security services to implement (e.g. firewall), deciding where in the service chain to place a given service is an important consideration.

Feature Availability

Not all vendors will support all features. Some vendors might not believe that certain features are worthwhile implementing or a given feature may not yet be implemented but still in a vendor roadmap. Alternatively, the vendor may choose to offer certain features through partnerships with best-of-breed vendors.

Thus, with the security feature discussion below, one needs to add the obvious "if supported" to each entry. That limitation will be assumed and will not be noted explicitly.

Vendor Lock-In

While no vendor will require any contractual language to lock your company in to an SD-WAN solution for an extended period, one must consider that any SD-WAN commitment beyond a prototype phase is a serious, and likely long-term, commitment.

Historically, WANs are more complex than LANs and changes to WAN environments, e.g changing to a new SD-WAN vendor, would likely take much longer than, say, moving to a new LAN infrastructure vendor. Also, where one can easily "mix-and-match" gear from various vendors that will interoperate on the LAN, most SD-WAN solutions are proprietary and typically cannot be changed piecemeal as one could do with a LAN.

Foundational Security

SD-WAN branches can greatly benefit from using foundational network infrastructure - DNS, DHCP and IPAM for protection against malware threats. DNS can be used as an early warning signal for malicious activity by detecting "communications & control" traffic from compromised assets. DHCP and IPAM can help precisely identify where a compromised device is, who it is assigned to, what type of device it is and its historical activity. DNS security delivered from the cloud allows SD-WAN branches to be secured in a simple, cost-effective way, without deploying a full security stack, while offloading the burden from more expensive perimeter defenses.

Security Protection Focus Areas

We believe that the first step in forming an SD-WAN security strategy is identifying the specific areas and elements that require protection. The remainder of this document will be dedicated to identifying and profiling important areas where security protection should be implemented.

Default Security: SD-WAN & Security Infrastructure

Defined

Default security posture for your SD-WAN implementation.

Exposure

A default setting within your SD-WAN and/or related security service (e.g. firewall ports) can leave your system open to exploitation.

Protection Strategies

One might assume, incorrectly, that the default settings for security services are implicitly recommended by the vendor. That is likely an incorrect and unsafe assumption. In many cases, default settings (such as those for credentials) can be used to exploit a system.

You SD-WAN vendor likely assumes that each customer will examine settings during implementation and set them to the provide the appropriate security.

At the highest level, identify all security related services and identify the key security parameters and review the default settings to be sure that they are applicable. For example, having a firewall with open ports for unused protocols can assist hackers in breaching your systems.

Access Control & Management Plane Security

Defined

The user credentials for administering your SD-WAN and the data paths for management traffic including administration consoles and orchestration systems.

Exposure

If the the management credentials and/or traffic become compromised, the overall security and reliability of your SD-WAN is compromised.

Protection Strategies

Default Management Credentials

While obvious, this is always worth noting (and applies to on boarding devices as well). It is usually safe to assume that any security device or virtual appliance will come pre-configured either with no security or with a well-documented user id/ password combination to allow initial configuration by the customer. Be certain to change or delete these credentials so that they cannot be used by unauthorized individuals.

Physical Access

With some physical devices, there are switches or buttons that can be used to reset the device to factory default. Similarly, there can be special console ports that might be able to circumvent normal security protocols. Thus, it is important to consider the physical location of any SD-WAN hardware and restrict access so to authorized personnel.

Authorized IP Addresses

If there are a limited number of people at a limited number of locations that require admin login, you can restrict login to specific IP source addresses.

Network Isolation

You can isolate your management/ orchestration station so that its access port is not on a network accessible to the pubic internet.

Multi-Factor Authentication

As with many email systems and other services today, you can implement a two-factor authentication system so that, for example, a one-time code sent to the user's registered mobile phone number is required along with a password for admin login.

Encrypted Sessions

Management sessions between admin station/orchestrator and devices should be encrypted.

Configuration Data

Closely related to the admin function is the configuration data that is produced and used by the SD-WAN system. Verify that your SD-WAN provides a way to ensure the security of the configuration and management data "at rest" when stored on either management system or devices.

Single Sign-On

Single Sign ON (SSO) is another effective method to control access restriction to the management portal. It only restrict the access to the authorized users, it also allow to implement role based access to the management portal.

Logging

It is a best practice to log all of the access (logins) and changes in the management portal (this is requirement for regulatory compliance).

Onboarding

Defined

Adding a physical networking infrastructure device (e.g. router, switch, security appliance) to your SD-WAN environment.

Exposure

If a rogue device is allowed to become part of your network, that device could inspect and/or capture all traffic passing through it. This situation would expose the organization to data loss and possible network disruption

Protection Strategies

Default State = Not Allowed

Some of the earliest firewalls, were so secure that nothing got through. While that frustrated users, taking this approach to adding new devices to the SD-WAN infrastructure is probably a good idea. Make sure that your system requires positive identification before allowing a device to become part of the infrastructure.

Serial Number

A simple but effective method for authorization is entering a valid, known serial number into the admin system.

License or Token Authorization

Authorization/authentication via license or generated token can be an effective way of on boarding devices. This could also be tied into software feature licensing for the device as not all devices will require the same feature sets.

Certificate Authorization

Authorization/authentication via certificate prior to allowing tunnel establishment is another alternative.

Discovery

Leverage automatic discovery tools for layer 2 and layer 3 devices that can quickly and accurately discover new or rogue devices that join the network for a vulnerability scan or further authorization.

Service Chain

With every new device be certain to confirm where it sits in the chain of security services and verify with the appropriate security managers that the device is in its correct position so that it can be protected appropriately or provide protection appropriately based on its role in the infrastructure.

Data Plane Security

Defined

Securing the elements of the SD-WAN that carry the user data.

Exposure

If user data is not transported in a secure fashion it can easily be compromised. Sensitive data could be exposed to hackers or data could be manipulated.

Compliance. Certain government agencies have implemented guidelines that mandate certain aspects of data protection and storage of data at rest (e.g.GDPR and Eurozone requirements). That discussion is beyond the scope of this document but must be researched separately.

Protection Strategies

Encrypted Overlay

While the specific method might vary, the important point is that the data plane traffic be encrypted. There are various options to be found from different vendors.

There are three common approaches. 1) SSL/TLS, 2) IPSec, 3) Packet level

SSL/TLS

The most fundamental approach is to encrypt the user data using Secure Sockets Layer (SSL)/ Transport Layer Security (TLS). TLS is the successor protocol to SSL, but they are frequently still listed together. SSL/TLS encryption is dynamic and does not require pre-configuration.

Key exchange intervals are a consideration with SSL/TLS. The shorter the interval, the more secure the connection.

IPSEC Tunnels

IPSEC virtual private network (VPN) tunneling technology can be used to create static, encrypted "tunnels" across the network. Generally, these are preconfigured. Given that SD-WAN connections are long running (essentially permanent) a configuration requirement should not be an issue.

Packet Level Security

Some vendors offer packet-level encryption as an alternative to SSL/TLS or IPSec tunneling techniques.Because the packet data is encrypted user data is protected. Vendors will establish their own methods of key exchange and key rotation.

Strong Encryption Overlay

Encryption effectiveness depends largely on the length of the encryption key and the frequency of key rotation. Longer keys are harder to break and frequent key rotation would reduce the usefulness of a key in the event it was compromised.

Many experts recommend AES-128 or AE-256 encryption. Have your SD-WAN vendor confirm its key rotation implementation and analyze optimal key rotation frequency for your needs.

For maximum security you might want to consult with your SD-WAN vendor that they support unique keys per tunnel, per appliance pair. This gives higher security. Common keys across appliances/ tunnels may increase exposure.

May experts recommend the public key structure for key exchanges.

Traffic Steering by Security Level

The ability to automatically detect the application running and steer that application to the links that have the required security posture is also important, i.e. PCI traffic must take a private MPLS or IPSec link, if not available then drop those packets even if the unencrypted internet link is available.

"Back Door" Security

Make sure the back doors to your data are secured and not exploited for data exfiltration. One such back door is the DNS protocol. Use DNS security technology that can take advantage of behavioral analytics on the queries to detect misuse of DNS in stealing data.

Application Programming Interface (API) Framework Security

Defined

Securing the programming interface of the management orchestration framework.

Exposure

APIs are used to provide powerful, programmatic access that can automate various aspects of your SD-WAN. Should this interface become compromised, the entire SD-WAN infrastructure could be at risk for misconfiguration or even be exposed to outages caused by unauthorized use of the API

Protection Strategies

API Token/Key

Typically, an API "key" or token is used as the identifier that authorizes a program to interact with the SD-WAN orchestration environment. Identify the mechanism that your vendor uses for this function.

API Authorization Levels

Many API functions will be concerned with analyzing existing elements or performance. Such access can be done with just "read only" access to the environment.

Verify whether your vendor provides for different levels of access for API programs.

Perimeter Security: Basic

Defined

Generally, core functions dedicated to protecting the SD-WAN location from external attacks (e.g. firewalls).

Exposure

Without perimeter security, user, server and networking devices within the SD-WAN location perimeter can be attacked and compromised.

Protection Strategies

Here you must decide whether specific perimeter security services are internal to your SD-WAN architecture or external to your SD-WAN architecture.

This report discusses both “basic” and “advanced” perimeter security. This categorization is subjective and what one user considers advanced or optional might be a basic requirement for another business.

In many cases, IT security groups (rather than SD-WAN groups) will be charged with implementing some or all of a company’s perimeter security protection.

In either case, you will still need to understand where each service is placed in the service chain as, for example, a firewall sitting BEHIND a router, cannot protect a router.

“Basic vs. advanced” will always be influence by business and the list will vary. Below are some core perimeter security services that should be considered:

- Basic firewall
- Web application firewall (WAF)
- Secure Web Gateway (content filtering)
- Intrusion Detection Service (IDS)
- Intrusion Prevention Service (IPS)
- Specialized Advanced Anti-Malware or Web Isolation services
- Integration with Identity and Access Management (IAM)

Perimeter Security: Advanced

Defined

Generally, advanced functions dedicated to protecting the SD-WAN based applications and users from various threats.

While advanced functions could be implemented locally at each branch, such a strategy is typically cost prohibitive. Additionally, such a deployment approach can vastly complicate management and administration of your security perimeter.

Exposure

Without advanced perimeter security, users and applications could be compromised.

Protection Strategies

Many advanced security services involved SD-WAN vendors/users integrating with specialized security companies.

Be sure to identify any 3rd-party security vendors that your SD-WAN integrates with and determine the depth of integration between your prospective SD-WAN vendor and relevant security services.

Listed below are some advanced security services that could be considered. Some of these could be too advanced for most branch needs today but might be good to note for future needs and plans:

- Next-Generation Firewall (NGFW)
- Unified Threat Management (UTM)
- Cloud access security broker (CASB)
- Network Detection and Response (NDR)

Further Considerations

Cloud-Based Gateways - Physical Security

"If your gateway is hosted in the cloud, you should be aware of the physical security that is provided for the gateway device and/or virtual appliance to make sure that it meets with your overall security requirements.

Cloud-Based Credential Storage

If your service provider needs to store your network credentials, in whole or in part, in a cloud-based facility, be sure to be aware of the protections put in place to secure these credentials.

Security Information & Event Management (SIEM) Integration

Many companies use SIEM solutions to help track and correlate the security posture of their organizations. If your company currently uses or plans to use an SIEM system, you might want to consider any SIEM integration options your SD-WAN vendor might offer for current or future consideration.

Security Patch/Update Process

Security vulnerabilities are discovered constantly and vendors typically provide patches and updates almost immediately to address those. Frequently, though, companies are compromised because they fail to install available updates in a timely fashion.

Experts recommend putting a formal process in place to review findings of vulnerabilities and schedule maintenance to update/ patch relevant software and/or firmware in a timely fashion to protect from possible exploits.

Compliance

Depending upon geographic region and vertical market there may be specific security considerations for your SD-WAN.

This section will reference several specific areas to provide examples but is not meant to be exhaustive by any means.

Eurozone Privacy Regulations

There are specific regulations involving privacy with respect to data/users from Eurozone countries. You should investigate any that might be relevant to your business.

If you are using security services based at a service-provider and these services store information (such as login credentials or web browsing history), that information might also be subject to various Eurozone-Specific regulations.

CIPA - Content Filtering

CIPA is an acronym for the US Child Information Protection Act. This legislation requires certain levels of filtering for web traffic that would be used by students in a school setting.

Cryptographic Compliance

There are specific regulations that cover SD-WANs that carry controlled information such as criminal justice and US government information. In such cases you might need to implement encryption that meets FIPS 140-2 or similar specifications.

Security Expertise

Certified Security Consultant

Very few areas in IT are as challenging and fast moving as security. To assist in your implementation you might consider hiring someone certified in specific security skills. That way, you have greater assurance that your initial deployment will be as secure as possible.

Advanced Topics

Service Chain

While discussed previously, this is likely to be an evergreen advanced topic.

There are different viewpoints as th where security should be “inserted” into the SD-WAN. As there are multiple components, there are multiple options for the placement of the various security elements.

Over time, industry views on the placement of security in the service chain may evolve so it is good to revisit this element of security periodically.

IoT Security & Microsegmentation

IoT devices (e.g., sensors, video cameras) are increasingly commonplace at all business locations. If your branch locations have or are planning for IoT, you will want to take that into consideration in your security planning.

Many IoT devices have relative primitive security. These can often easily be hacked and misused and/ or have malware installed.

Keeping IoT traffic separate from your line-of-business using microsegmentation is a recommended method for enhancing the security of your SD-WAN against any possible IoT-borne threats.

Next Steps/Follow-On Work

Incident Response Plan

No matter how good your plan and implementation, a security breach can always occur.

Thus, you should prepare an incident response plan that can be ready to implemented in the event of security breach.

Not only should the plan include the process that you will use to remediate the breach, it should also include specifics for what documentation you want to preserve for investigation and a process for notifying stakeholders and, if required, government agencies about the breach.

Conclusion

This document should assist in identifying core SD-WAN security exposure areas and remediation options.

Security is one area that requires constant vigilance, however. Hackers can be assumed always to be trying to find new ways to circumvent existing security features.

New product features bring with them the potential for new surfaces for hackers to attack.

Monitor security logs and reevaluate existing SD-WAN security on a regular basis.

About Tolly…

The Tolly Group companies have been delivering world-class IT services for over 30 years.
Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.
Tolly also assists medium-sized businesses and large enterprises evaluate, benchmark and select IT products for deployment.

You can reach the company by email at sales@tolly.com, or by telephone at
+1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.