Brought to you by

Secure Access Service Edge (SASE)

for dummies®
A Wiley Brand

Cisco Special Edition

Explore SASE networking

Extend cloud-native security everywhere

Reduce cost and complexity

Lawrence Miller, CISSP

About Cisco

Cisco designs and sells broad lines of products, provides services, and delivers integrated solutions to develop and connect networks around the world, building the Internet.

As a global market leader in our industry, we help our customers connect, digitise, and thrive. Together, we change the way the world works, lives, plays, and learns.

For more than 30 years, we have helped our customers build networks, automate, orchestrate, integrate, and digitize information technology (IT)-based products and services.

In an increasingly connected world, Cisco is helping to lead the way by transforming businesses, governments, and cities worldwide with differentiated innovation.

Getting started with Secure Access Service Edge (SASE)

umbrella.cisco.com/sase

With all the different security solutions (and acronyms) out there — DNS, SIG, SWG, CASB, FWaaS, SASE — it can be tough to sort out which approach is best, as well as which technologies you need to reduce complexity, improve speed and agility, and ultimately secure your network. Visit our website to learn more about SASE and the steps you can start taking to keep your organization safe and secure.

www.twitter.com/CiscoUmbrella

www.facebook.com/CiscoUmbrella

www.linkedin.com/company/OpenDNS

www.youtube.com/c/CiscoUmbrella

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Secure Access Service Edge (SASE)

Cisco Special Edition

by Lawrence Miller, CISSP

for dummies®
A Wiley Brand

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Secure Access Service Edge (SASE) For Dummies®, Cisco Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

Copyright © 2020 by John Wiley & Sons, Inc., Hoboken, New Jersey

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

Trademarks: Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco Systems, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

ISBN 978-1-119-68283-7 (pbk); ISBN 978-1-119-68287-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Jennifer Bingham

Acquisitions Editor: Ashley Coffey

Editorial Manager: Rev Mengle

Business Development Representative: Karen Hattan

Production Editor: Umar Saleem

Special Help: Rachel Ackerly, Lorraine Bellon, Robert Clarke, Josh DeButts, Tori Devereux, Meg Diaz, Barry Fisher, Kiran Ghodgaonkar, David Gormley, Rachel Haag, Kate MacLean, Jonny Noble, Iloyd Noronha, Natalie Pino, Nicole Smith, Christina Soriano, Cynthia Turner-De Vries

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Table of Contents

INTRODUCTION 1
About This Book 1
Foolish Assumptions 2
Icons Used in This Book 3
Beyond the Book 3

CHAPTER 1: **Networking and Security: Trends and Challenges** 5
The Way We Work Has Changed 5
Cloud adoption 6
Remote offices 7
Roaming users 7
More network traffic 8
Understanding Networking and Security Challenges 8
Rising costs of traditional networking architecture 8
Inefficiencies in the centralized network model 9
Performance issues with "run-the-business" SaaS apps 10
Too many siloed security tools and integration challenges 11
Security talent shortage and increasing personnel costs 11
New cyberthreats taking advantage of security gaps 12

CHAPTER 2: **The Evolution of Networking and Security Solutions** 13
Looking at Traditional WAN Technologies 14
Exploring SD-WAN Solutions 15
Tackling Internet Security Threats 17
Getting Sassy with SASE 18

CHAPTER 3: **SASE: Combining Security and Networking Functionality** 19
Recognizing Security Challenges 19
Key Characteristics and Benefits of SASE 20
Starting Your SASE Journey 23
Networking first step 23
Security first step 24

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CHAPTER 4: **SASE Components and the Cisco Approach** 25
Key SASE Solution Components 25
Software-defined wide area network 25
Domain name system layer security 26
Secure web gateway 26
Firewall as a service 26
Cloud access security broker 26
Zero Trust Network access 26
Cisco's Approach to SASE 27
Cisco SD-WAN: Flexible cloud-managed networking 27
Cisco Umbrella: Multi-function cloud-native security 28
DNS-layer security 29
Secure web gateway (SWG) 30
Cloud-delivered firewall 30
Cloud access security broker (CASB) functionality 31
Interactive threat intelligence 31
Umbrella and SD-WAN integration 32
Cisco SecureX 32
Zero Trust with Cisco Duo 33
Combined benefits unique to Cisco 33

CHAPTER 5: **Ten Key Takeaways** 35
More Remote Offices and Roaming Users 35
DIA Is the New Normal 36
SaaS Apps Are Taking Over 36
The Old Way of Networking Is Slow and Expensive 37
Network Architecture Is Meeting New Demands 37
Look for a Solution That Reduces Cost and Complexity 37
Don't Compromise on Network Performance 38
Always Keep Security Top-of-Mind 38
Make Life Easier for Your Operations Team 39
Every Journey Starts with a Single Step 39

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Introduction

Today's IT teams face a common challenge: how to securely enable the growing universe of roaming users, devices, and software as a service (SaaS) apps without adding complexity or reducing end-user performance — all while leveraging their existing security investments. Likewise, users in remote and branch offices need the same level of network performance and security as users in central locations. IT must develop strategies to protect users — wherever they work and on any device they use — from a variety of threats, including malware infections, command-and-control callbacks, phishing attacks, unauthorized access, and unacceptable use, among others.

This book examines the changing network and security landscape, gaps in the existing security stack, and the steps you can take to keep your organization safe and secure as your network evolves. These changes are paving the way to a new solution category that delivers multiple security functions from the cloud that are simple, scalable, and flexible to meet the unique needs of your business and its changing network architecture.

The goal of this book is to help you understand the newest trends in networking and security, the toughest challenges that these changes bring, and how networking and security technologies have evolved over time. Finally, the book introduces you to a new product category that has emerged to help solve these problems and how Cisco's approach can help your business today and in the future.

About This Book

This book consists of five chapters that explore:

- Key networking and security trends and their associated challenges (Chapter 1)
- Different networking and security options and key considerations (Chapter 2)

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- How an SD-WAN architecture addresses modern networking challenges (Chapter 3)
- How a multi-function cloud-native security service complements SD-WAN and addresses modern security challenges (Chapter 4)
- Key SD-WAN and cloud security takeaways (Chapter 5)

Each chapter is written to stand on its own, so if you see a topic that piques your interest feel free to jump ahead to that chapter. You can read this book in any order that suits you (though we don't recommend upside down or backwards).

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but here are a few assumptions nevertheless.

You have a technical background and work for an organization that, like many, is looking for a better way to manage your network and security challenges in a multi-cloud, hybrid enterprise. As such, this book is written for technical readers with a general understanding of cloud, networking, and security concepts.

Perhaps you're an IT executive or manager such as a chief information officer (CIO), chief technology officer (CTO), or chief information security officer (CISO), VP of IT, IT director, or network or security manager. Or perhaps you're a cloud, network, or security architect or engineer.

If any of these assumptions describe you, then this is the book for you! If none of these assumptions describe you, keep reading anyway! It's a great book and when you finish reading it, you'll know quite a bit about SD-WAN and cloud security!

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Icons Used in This Book

Throughout this book, you will find special icons to call attention to important information. Here's what to expect:

REMEMBER

This icon points out important information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

TECHNICAL STUFF

If you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon and is the stuff nerds are made of!

TIP

Tips are appreciated, never expected — hopefully, you'll appreciate these useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but they do offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much info that can fit in 48 short pages, so if you find yourself at the end of this book, thinking, "Gosh, this was an amazing book, where can I learn more?" check out `https://umbrella.cisco.com/sase`.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Considering how the network and security have changed
- Addressing modern network and security challenges

Chapter 1
Networking and Security: Trends and Challenges

The enterprise network has seen a huge transformation over the past decade. As a result, security products are evolving, too. The market is moving from single-purpose point products to multifunction security solutions tightly integrated in a cloud service offering. The goal is simple: to deploy security services how and where you choose, with the capability to control and secure direct-to-Internet access, cloud applications, and protection for central, remote, and roaming users alike, without the need for additional hardware.

This chapter discusses modern trends and challenges that drive the need for a new approach to networking and security.

The Way We Work Has Changed

Several key trends have evolved over the past decade to reshape the networking and security landscape.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud adoption

The use of public cloud apps and services has exploded over the past decade. Every year, enterprises produce more data, and increasingly this data is being stored in software as a service (SaaS) applications in the public cloud. The Enterprise Strategy Group's 2019 report, *The Rise of Direct Internet Access*, projects that 60 percent of organizations will use SaaS applications for greater than half of their business needs over the next two years, especially across highly distributed organizations.

TIP

The growth of enterprise cloud adoption is further evidenced in the 2019 *RightScale State of the Cloud Report* from Flexera, which found that public cloud adoption, including SaaS and infrastructure as a service (IaaS) has grown to 91 percent among organizations. Today, one-third of enterprise workloads run in public clouds and nearly half run in private clouds (see Figure 1-1).

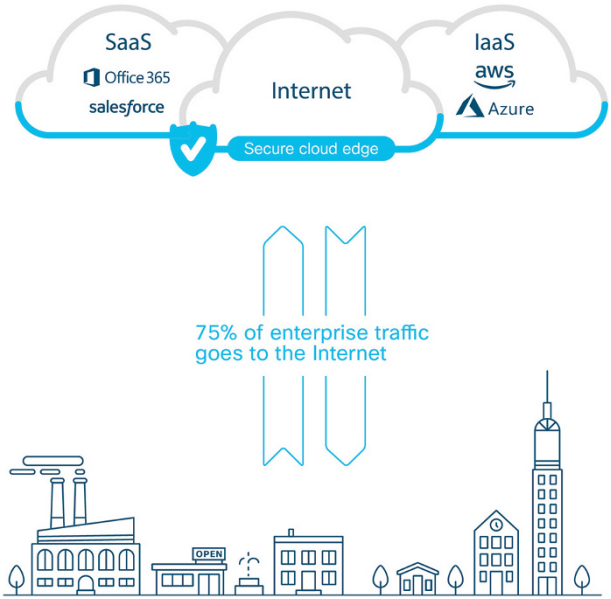


FIGURE 1-1: It's essential to have strong security protecting the increasing volume of Internet, SaaS apps, and IaaS traffic from all locations.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Remote offices

The days of employees working together in the same place — company headquarters — are long gone. As organizations expand into new markets, acquiring smaller companies and their office footprints, the number of remote and branch offices grows, too. For the average enterprise, remote or satellite offices generate most of the revenue — research from Enterprise Strategy Group suggests that 80 percent of users are located in remote or branch offices. These users need to be protected as well as their counterparts at main office locations, even if their network traffic is going directly to the Internet instead of backhauling to the corporate data center.

REMEMBER

A remote or branch office is a dedicated business (non-home) site that has more than one employee. This location may be connected to a central data center via a wide-area network (WAN) or may connect directly to the Internet. Remote and branch offices typically receive some level of technology support from headquarters locations and most (although not all) typically have one or more on-site servers to provide users with file, print, and other IT services.

Some remote office locations may be connected to a main office over a multiprotocol label switching (MPLS) WAN link. However, it is becoming more common for remote offices to connect to the main office over a virtual private network (VPN) via a direct Internet access (DIA) link, or to have a secondary DIA link to serve as a backup to the primary MPLS link.

TIP

As companies become more decentralized, the growing population of remote workers and branch offices need a new approach to networking and security.

Roaming users

Laptop computers have supplanted desktop computers to become the primary endpoint for many business users. Similarly, mobile computing has untethered workers as mobile devices have become more powerful than many desktop computers and their use has proliferated. Because of these technology trends, most work can now be performed from practically anywhere and modern organizations increasingly recognize that work is an activity, not a place. According to the Enterprise Strategy Group, 50 percent

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

of the workforce will be roaming by 2021, and a February 2019 Forbes article noted "Remote work is no longer a 'perk,' 'lifestyle' or 'policy'. Remote work, telecommuting and workplace flexibility have officially become a global industry."

REMEMBER

A *roaming user* is any employee that works from a home office or from another noncorporate location (such as at a customer's office or on the road) at least one day a week. Roaming users may use corporate-owned devices and/or personal devices and they may access the corporate network via a VPN or connect directly to the Internet to access cloud applications in order to perform their job functions.

More network traffic

New apps, including public cloud storage and video conferencing, are data-intensive and require large amounts of network traffic to support the increasing demand from employees. This increased traffic load is putting an ever greater strain on existing network infrastructure and centralized security processes, leading to reduced performance, lower productivity, and a poor overall user experience.

Understanding Networking and Security Challenges

Many new networking and security challenges have also been created over the past decade, requiring innovative new solutions to address them effectively.

Rising costs of traditional networking architecture

The traditional function of a WAN was to connect users at the branch or campus to applications hosted on servers in a centralized data center. Typically, dedicated MPLS circuits were used to help ensure security and reliable connectivity. However, these dedicated circuits are costly to provision and maintain, especially when compared to the widespread availability of other, less costly DIA options available to businesses today.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TECHNICAL STUFF

MPLS is a routing technique that uses virtual path labels instead of network endpoint addresses to direct traffic through the network, which reduces load on the routers and speeds up traffic delivery. MPLS provides more reliable quality-of-service (QoS) for bandwidth-heavy or latency-sensitive applications. MPLS technologies are applicable to any network layer protocol (hence the name, "multiprotocol") and are often used by enterprises, for example, to backhaul business-critical network traffic from branch offices to the data center.

Inefficiencies in the centralized network model

A centralized network model made sense when the enterprise data center was the primary destination for users to access applications and data across the network. Internet traffic was relatively insignificant and could easily be handled over the existing MPLS circuits. Network traffic could be routed and prioritized as necessary to ensure efficient, reliable performance — while limited and expensive IT staff resources, such as networking and security teams, could centrally manage the network for all locations.

Traditionally, an organization would backhaul (that is, reroute) network traffic from branch offices to headquarters to apply security policies, often using MPLS links. But in the modern digital era, this approach just isn't efficient. As businesses increasingly adopt SaaS applications, as well as platform as a service (PaaS) and IaaS resources and workloads delivered from multiple clouds, the user application experience has suffered. Backhauling Internet-bound traffic across MPLS networks that are designed to deliver fast and reliable access to the data center is expensive and can be slow. The bottom line is that MPLS networks aren't an efficient or effective way to handle the unprecedented explosion of Internet traffic that cloud adoption brings.

TECHNICAL STUFF

Traffic destined for the Internet is effectively backhauled across the MPLS network to a headend (such as a corporate headquarters or data center) that directs it through a set of security checks and then provides Internet access — but unfortunately, it also acts as a bottleneck.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

TECHNICAL STUFF

Existing WAN links using MPLS are unable to handle increasing bandwidth demands from users who need fast, reliable access to the Internet, so they can be as productive as possible. To address the growing need for direct Internet access to cloud-based apps, more organizations (79 percent according to the Enterprise Strategy Group) are either investigating, or already using, broadband DIA at branch locations instead of backhauling traffic over MPLS. Although these DIA links address performance issues associated with backhauling traffic to an MPLS headend location, they're often provided by local Internet service providers (ISPs) as broadband links — it's important to check into resiliency, quality of service (QoS) prioritization, and service level agreement (SLA) guarantees.

Performance issues with "run-the-business" SaaS apps

Many SaaS apps today have become core "run-the-business" enterprise apps — some examples include Salesforce, Office 365, and Workday. Backhauling SaaS traffic across costly MPLS WAN links to a corporate headend creates network congestion and latency. This, in turn, causes performance issues that result in lost productivity and user frustration. Complexity in the WAN may cause additional performance issues due to less-than-optimal routing decisions, improper traffic classification and prioritization, and inefficient policy enforcement.

When users experience performance issues with corporate-approved apps, they often turn to unauthorized and potentially risky apps to get their jobs done. This shadow IT culture in which the IT department — and security controls — are circumvented is a big problem. More than 1,200 cloud services are used in the average large enterprise today and the Enterprise Strategy Group reports that as much as 98 percent of those services are unsanctioned and unvetted SaaS apps.

WARNING

Although many organizations implement security policies requiring remote or roaming users to backhaul their network traffic across VPN tunnels, 85 percent of organizations believe their users violate these corporate VPN policies, according to the Enterprise Strategy Group.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Too many siloed security tools and integration challenges

Security teams are frequently inundated by mountains of data from standalone, point security products that don't integrate with other products and require different knowledge levels and skill sets to operate and maintain. The Enterprise Strategy Group reports that 31 percent of organizations use over 50 disparate tools, and Cisco research indicates that the majority of them find it challenging to orchestrate alerts from these different tools. This lack of integration and interoperability makes it difficult, if not impossible, for security analysts to monitor and correlate security and threat information in real-time.

REMEMBER

These challenges have grown exponentially as connected branch and remote offices have proliferated. Each location typically requires a router and firewall at minimum. In remote and branch locations, these are often purchased as commodity components that provide limited functionality and remote management capabilities. When switching to DIA at remote locations, there is a need to deliver the right level of security to users — web security, firewalls, data loss prevention, and so on. However, it's impractical to buy a separate stack of security appliances for each location. Even if some of these components in branch locations do include security tools, there are usually no IT personnel in these locations to maintain them. Over time, the hardware can't cope with the ever-increasing traffic loads, so the security tools will need to be displaced from these appliances to the cloud where they can be applied and managed centrally.

TIP

There's light at the end of the tunnel. According to the Cisco CISO benchmark study, 93 percent of CISOs agree that moving security to the cloud has increased efficiency, allowing security teams to focus on other areas.

Security talent shortage and increasing personnel costs

The worldwide shortage of security professionals and the high ongoing investment necessary to train and retain qualified security staff is a very real problem for organizations everywhere. According to Cybersecurity Ventures, 3.5 million cybersecurity jobs worldwide will not be filled by 2021. The Enterprise Strategy

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Group and ISSA further report that 74 percent of respondents say that a shortage of skilled cybersecurity workers has had a significant impact on their organizations.

New cyberthreats taking advantage of security gaps

Advanced cyberthreats including ransomware, remote access trojans (RATs), and advanced persistent threats (APTs) have evolved to take advantage of the lack of visibility and control in the modern distributed network. Remote and branch users are particularly susceptible to many of these threats because organizations have moved away from a centralized security model and are often unable to enforce consistent security policies across the network. Limited security capabilities and IT staff in remote locations make these users even more susceptible to a successful breach or attack. Cybercriminals understand that remote workers are typically more vulnerable and thus target remote locations and roaming users.

WARNING

According to the Enterprise Strategy Group, 68 percent of organizations experienced attacks in the last 12 months in which a branch location or roaming user was the source of compromise.

TIP

Modern organizations need to consider innovative new networking and security options to successfully address the challenges in today's enterprise network. You can find more information on this in Chapter 2.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Recognizing the limitations of MPLS
- Getting innovative with SD-WAN
- Addressing security threats with SWGs and SIGs
- Introducing the secure access service edge (SASE)

Chapter 2
The Evolution of Networking and Security Solutions

The networking and security landscape is evolving from numerous, disparate point solutions to fully integrated, multifunction, cloud-delivered networking and security platforms. This shift is happening because businesses increasingly need the flexibility and power to deploy networking and security services how and where they choose. They need to control and secure Internet access, manage the use of cloud applications, and provide protection for roaming users while reducing strain on resources and eliminating the need for hardware.

In this chapter, you'll learn how networking and security evolved from traditional wide area networks (WAN) to software-defined WAN (SD-WAN) and from secure web gateways (SWGs) to secure Internet gateways (SIGs). There is also information about the new, combined concept of the secure access service edge (SASE).

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Looking at Traditional WAN Technologies

For nearly two decades, the go-to WAN technology for IT, voice, and data networking infrastructure has been multiprotocol label switching (MPLS) network architectures. MPLS networks provide a resilient network backbone for connecting enterprise headquarters and remote branch locations. MPLS provides the capability to prioritize voice, video, and data traffic on your network to meet unique business requirements, and packets can be sent over a private MPLS network.

However, enterprises today need more control, flexibility, and centralized management of their WAN environments than MPLS can offer, which is driving the need for change. The costs associated with provisioning and maintaining private MPLS WAN links alone can be enough of a catalyst for change. MPLS networks are typically provided by Internet service providers (ISPs) and other service providers — both the well-known telecoms and the not so well-known smaller companies.

Additionally, the inefficiencies of an MPLS network that backhauls Internet-bound traffic across branch office links to a corporate headend add cost, complexity, performance issues, and latency. Many organizations inevitably install a secondary direct Internet access (DIA) link at their branch locations to offload some of this Internet traffic. Such a solution increases recurring costs and introduces still more complexity. Network traffic may not necessarily be routed across the best link at a given time and bandwidth on one link or the other may be underutilized.

On the security side, Internet-bound traffic needs to be minimally secured by DNS-layer security or a firewall, but may also require web content filtering, data loss prevention, real-time malware detection, and other security services. The lack of visibility and a centralized policy enforcement point makes it difficult, if not impossible, for security teams to ensure a secure and compliant operating environment (see Figure 2-1).

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

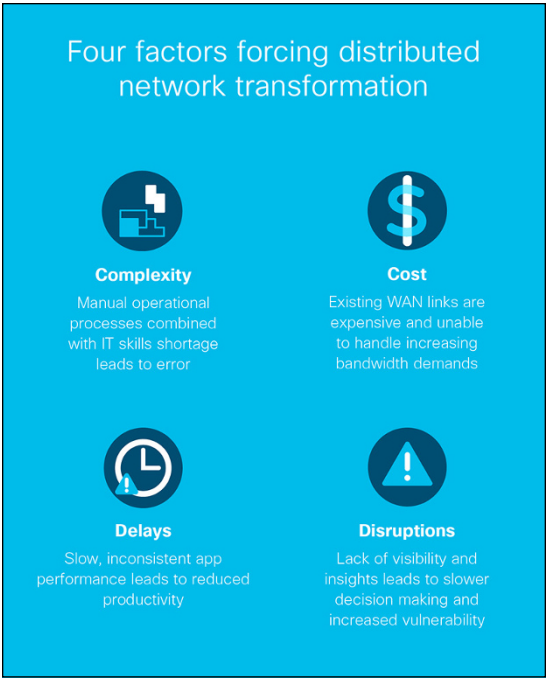


FIGURE 2-1: Challenges with current WAN architectures include complexity, cost, delays, and disruptions.

Exploring SD-WAN Solutions

Configuring multiple routers connected to different circuits (for example, an MPLS link and a broadband Internet link) to route network traffic efficiently and optimally can be challenging. In many cases, you may be limited to a simple round-robin load balancing option, particularly if you don't have networking staff available in your various remote locations.

Beyond simple load balancing, available bandwidth capacity may go unused during periods of congestion. For example, your broadband Internet connection may be running slowly during a given period of time, while your costly MPLS link is relatively uncongested and may actually be able to provide faster Internet connectivity. The inability to aggregate disparate links means wasted bandwidth capacity and lower employee satisfaction.

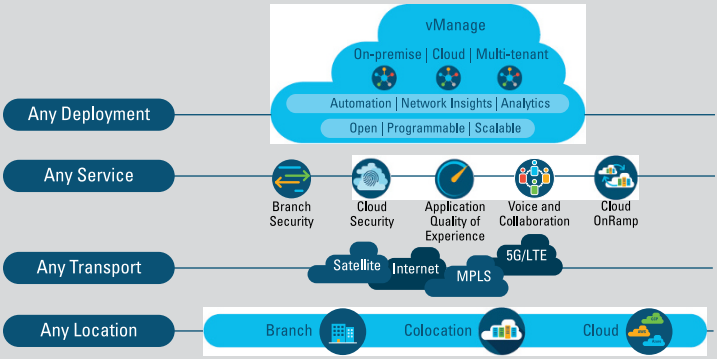
These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

CISCO SD-WAN EXAMPLE

Cisco SD-WAN is a secure, cloud-scale architecture that is open, programmable, and scalable. It quickly allows you to establish an SD-WAN overlay fabric to connect data centers, branches, campuses, and colocation facilities. This connection can improve network speed, security, and efficiency. Cisco SD-WAN supports (see the figure below):

- **Any deployment:** Flexible WAN management for on-premises, cloud, and multitenant environments.
- **Any service:** A full suite of services including branch security, cloud security, application quality of experience, voice and collaboration, and cloud on-ramp.
- **Any transport:** Deploy your WAN over any type of connection including satellite, Internet, MPLS, and 5G/Long-Term Evolution (LTE).
- **Any location:** Physical or virtual platforms are available for branch, colocation, and cloud.

Secure Cloud Scale SD-WAN Architecture



Source: Cisco.

TIP

An SD-WAN solution can address these scenarios and provide other advanced routing capabilities to optimize your network traffic as needed. Additional considerations and capabilities include:

- Routing traffic across different links based on destination
- Routing traffic across different links based on cost

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Aggregating multiple links to provide greater total bandwidth
- Rerouting traffic across an alternate link when a link is congested, unstable, or down
- Prioritizing certain application traffic, such as voice and video, to ensure quality of service

SD-WAN combines and optimizes traditional WAN technologies, such as MPLS and broadband Internet connections. This allows organizations to efficiently route network traffic to multiple remote branch locations while providing enhanced monitoring and management capabilities. SD-WAN monitors network traffic across all available links in real-time and dynamically selects the best route for each data packet traversing the network.

TIP

The International Data Corporation predicts that the global SD-WAN market will reach $8 billion by 2021, and research by Forrester reveals that 64 percent of U.S. organizations are planning to implement SD-WAN in the next year.

Tackling Internet Security Threats

For most of the past 25 years, network security has focused on detecting and preventing malware threats (such as viruses, ransomware, spam, and phishing), identifying and blocking unauthorized Internet use (such as browsing inappropriate content and downloading pirated content), and assuring network performance (with caching proxy and anti-distributed denial-of-service (DDoS) products).

REMEMBER

Back in 2017, several vendors and analysts in the industry defined a new concept — the secure Internet gateway (SIG). While the SWG is designed mainly for web traffic, this new type of cloud-native solution would offer multiple functions across more traffic types — such as domain name system (DNS) security, SWG, firewall as a service (FWaaS), and cloud access security broker (CASB) — to improve security and performance while reducing costs and maintenance tasks. A SIG provides a broad set of security from the cloud so organizations can protect users no matter where they are. It can easily scale to cover additional traffic and users more efficiently than the older on-premises SWG appliance approach.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Getting Sassy with SASE

In 2019, Gartner published a report called *The Future of Network Security Is in the Cloud*. In this report, Gartner introduced the secure access service edge (SASE) concept. The SASE concept includes an even wider set of security functionality than a SIG, and it includes the convergence of networking functionality as well. A SASE solution can secure the cloud, data center, and branch network edges and deliver a secure SD-WAN fabric across disparate connections (see Figure 2-2).

TIP

In *The Future of Network Security Is in the Cloud*, Gartner shared their prediction that "[b]y 2023, 20 percent of enterprises will have adopted SWG, CASB, [zero trust network access] and branch FWaaS capabilities from the same vendor up from less than 5 percent in 2019."

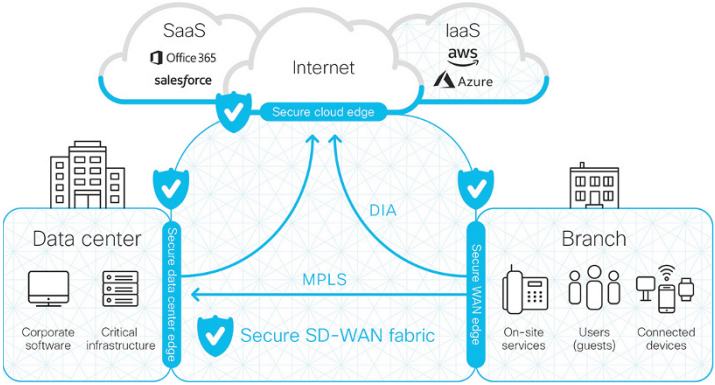


FIGURE 2-2: SD-WAN is a critical networking element in SASE solutions that can direct traffic for the protection of cloud, data center, and branch edge networks.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Looking at security challenges in the cloud era
- Recognizing key characteristics and benefits of SASE
- Getting started with SASE

Chapter 3
SASE: Combining Security and Networking Functionality

In this chapter, you learn about the security challenges created in the new network architecture model, what functionality you need in a security solution, what issues you need to consider when deploying your solution, and how a secure access service edge (SASE) solution can help.

Recognizing Security Challenges

Network security is no longer confined to the data center — it's shifting to the cloud. As work moves outside the office and security moves to the cloud, the tried-and-true perimeter-based security model just can't keep up. To be successful, IT teams need to identify a new approach to control and secure users, apps, devices, and data — anywhere and everywhere.

Today, the wide-scale use of cloud applications has become fundamental to business operations at all locations. According to Enterprise Strategy Group research, 32 percent of organizations report that the majority of their apps are now software as

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

a service (SaaS) based and that number is expected to increase to 60 percent within two years. The centralized security approach has become impractical because of the high cost of backhauling traffic and the resulting performance issues for branch locations.

To overcome these cost and performance issues, many organizations are adopting a more decentralized networking approach to optimize performance at remote locations. This enables a more efficient direct Internet access (DIA) path for these offices, but also highlights a set of new security challenges, including:

- **Gaps in visibility and coverage:** Centralized security policies can't be effectively managed and enforced in a decentralized network. This is because most traffic from branch locations to the cloud and Internet doesn't cross a centralized policy enforcement point. This results in visibility and coverage gaps, which increase the risk of a successful breach or a compliance violation.
- **Volume and complexity of security tools:** Security teams already struggle to keep up with cybersecurity threats. Many of them have a large number of point solutions that are difficult to integrate and manage. These point products generate thousands of alerts — making it very difficult, if not impossible, for analysts to keep up. As a result, many alerts go untouched.
- **Limited budgets and security resources:** IT and security budgets are already constrained. Deploying multiple, costly point security solutions — such as firewalls, secure web gateways (SWGs), intrusion detection and prevention systems (IDS and IPS), and data loss prevention (DLP) — to multiple locations and remotely managing these solutions with limited security resources is both impractical and ineffective.

Key Characteristics and Benefits of SASE

In its August 2019 report, *The Future of Network Security Is in the Cloud*, Gartner defined the secure access service edge (SASE) concept as "an emerging offering combining comprehensive [wide area network] capabilities with comprehensive network security functions (such as SWG, [cloud access security broker], [firewall as a service] and [zero trust network access]) to support the dynamic secure access needs of digital enterprises."

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Here are four key characteristics of digitally transformed organizations that are laying the groundwork for this new concept:

- **Identity-centric:** Gartner suggests that "digital business transformation inverts network and security service design patterns, shifting the focal point to the identity of the user and/or device — not the data center." Moreover, the "identity of the user/device/service is one of the most significant pieces of context that can be factored into the policy that is applied."
- **Cloud-native:** Gartner describes modern digital enterprises as having "[m]ore sensitive data located outside of the enterprise data center in cloud services than inside" and "[m]ore user traffic destined for public cloud services than to the enterprise data center."
- **Edge computing:** To support the SASE concept, Gartner describes a "worldwide fabric/mesh of network and network security capabilities that can be applied when and where needed to connect entities to the networked capabilities they need access to."
- **Globally distributed:** Gartner describes the need for an "intelligent switchboard" where "identities are connected to networked capabilities via the SASE vendor's worldwide fabric of secure access capabilities."

REMEMBER

The SASE concept consolidates numerous networking and security capabilities and functions — traditionally delivered in multiple, siloed point solutions — in a single, fully-integrated cloud-native platform.

Potential business benefits of the SASE concept include the following:

- Reduce cost and complexity
- Enable secure remote and mobile access
- Provide latency-optimized, policy-based routing
- Improve secure seamless access for users
- Improve security with consistent policy
- Update threat protection and policies without hardware and software upgrades

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

- Restrict access based on user, device, and application identity
- Increase network and security staff effectiveness with centralized policy management

HOW AVRIL EXTENDS PROTECTION TO BRANCH OFFICES WITH CISCO UMBRELLA

Today, DIA allows branch offices to significantly improve network performance — eliminating latency by removing the need to backhaul traffic to the data center. But as a result, Internet traffic from these locations isn't seen or protected by the centralized security stack, which can leave users and sensitive data exposed.

To embrace the increasing use of DIA, IT teams need a simplified, cloud-delivered service that unifies the power of multiple point security solutions in a single console. That solution is Cisco Umbrella.

Avril, a French agro-industrial group, needed to provide their branch offices with a reliable security solution that could continue to expand as Avril acquired new businesses and divisions. To secure these locations while still providing them with fast DIA, they needed a cloud-delivered security service that could work at the outer edges of the network, providing a front line of protection.

Using Cisco Umbrella's integrated network and security architecture, Avril can protect branch users, connected devices, and app usage at tens of thousands of DIA breakouts. Leveraging Umbrella security to extend protection everywhere, Avril has been able to substantially reduce the risk of data exfiltration and malware across all ports and protocols. Simple to deploy and easy to manage from the cloud, Umbrella also allows Avril to keep expanding protection to keep up with new needs and new growth.

With Cisco Umbrella, the Avril Group was able to reduce ransomware by 100 percent, secure mobile users working off-network, and reduce security management time over previous solutions.

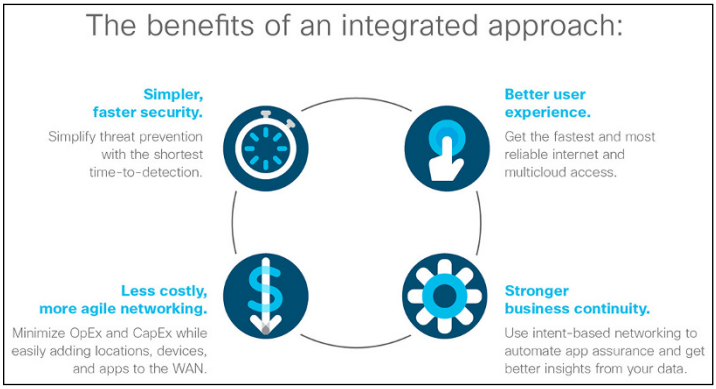
Marc Tournier, Information Security and Compliance Manager (CISO) at Avril, was impressed with the quick time-to-value. "Umbrella secured the whole company network in 10 minutes."

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

These benefits are critical for organizations that need to address the modern networking and security challenges of an increasingly cloud-first, distributed, mobile, and global workforce.

Starting Your SASE Journey

SASE is a broad concept. To keep things simple, you should look for a flexible way to get started and make demonstrable progress toward your organization's goals. That being said, two major SASE concepts are consolidation and simplification, so it makes sense to chart a course that includes both networking and security elements from a single vendor. There are many technical, cost, and end-user performance advantages to this type of combined approach (see Figure 3-1).



Source: Cisco

FIGURE 3-1: The benefits of an integrated networking and security approach.

With these combined benefits in mind it makes sense to look at the logical first step in both networking and security.

Networking first step

Begin by looking at the many benefits of software-defined wide area networking (SD-WAN) and start a trial to show the impact it could have on your networking service costs, performance, and management tasks. As you develop a plan for SD-WAN, you should also decide the best way to secure the new traffic flows, especially from the increasing number of remote branches and

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

roaming users. Look for a vendor with a strong portfolio of network technology who will deliver a broad range of network as-a-service capabilities in the future.

Security first step

Look for a cloud-native solution that can flexibly replace and even improve on your current security stack capabilities. Look for a solution that can handle a broad set of security tasks and present data in a single console to help simplify deployment, investigations, and ongoing maintenance tasks.

WARNING

Don't re-create the challenges that resulted from on-premises security stacks with a large number of separate point solutions.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Knowing what to look for in a SASE solution
- How Cisco SD-WAN and Cisco Umbrella address core SASE requirements

Chapter 4
SASE Components and the Cisco Approach

In this chapter, you learn about the key components to look for in a secure access service edge (SASE) solution and read about an example of the approach that Cisco is taking to the convergence of cloud security and networking.

Key SASE Solution Components

Take a look at the key components that comprise a SASE solution. (You can learn more about SASE in Chapter 3.)

Software-defined wide area network

A software-defined wide area network (SD-WAN) is a virtual wide area network (WAN) that allows companies to use any combination of transport services — including multiprotocol label switching (MPLS), cellular Long-Term Evolution (LTE) and 5G, and broadband — to securely connect users to network locations. It can select the most efficient communication method while reducing costs and simplifying management.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Domain name system layer security

Domain name system (DNS) resolution is the first step when a user attempts to access a website or other service on the Internet. Thus, enforcing security at the DNS and IP layers is the first line of defense against threats and is a great way to stop attacks before users connect to bad destinations.

Secure web gateway

A cloud-based web proxy or secure web gateway (SWG) provides security functions such as malware detection, file sandboxing and dynamic threat intelligence, Secure Sockets Layer (SSL) decryption, app and content filtering, and data loss prevention (DLP).

Firewall as a service

Firewall as a service (FWaaS) is the cloud-based delivery of firewall functionality to protect non-web Internet traffic. This typically includes Layer 3 and Layer 4 (IP, port, and protocol) visibility and control, along with Layer 7 (application control) rules, and IP anonymization.

Cloud access security broker

Cloud access security brokers (CASBs) help control and secure the use of cloud-based, software as-a-service (SaaS). CASB solutions enable organizations to enforce their internal security policies and compliance regulations. The value of CASBs stems from their capability to give insight into cloud application use across cloud platforms and to identify unsanctioned use. CASBs use auto-discovery to detect the cloud applications in use and identify high-risk applications and users, plus other key risk factors. They typically include DLP functionality and the capability to detect and provide alerts when abnormal user activity occurs to help stop both internal and external threats.

Zero Trust Network access

The Forrester Zero Trust security framework takes a "never trust, always verify" approach to security. Zero Trust network access (ZTNA) verifies user identities and establishes device trust before granting access to authorized applications, helping organizations prevent unauthorized access, contain breaches, and limit an attacker's lateral movement on your network. ZTNA requires a strong, cloud-based, multi-factor authentication approach.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cisco's Approach to SASE

Cisco delivers core SASE capabilities, as well as additional functionality, through several key networking and security components.

Cisco SD-WAN: Flexible cloud-managed networking

Cisco's approach to SASE leverages a cloud-scale SD-WAN architecture (see Figure 4-1) designed to meet the complex needs of modern WANs through three key areas:

- Advanced application optimization that delivers a predictable application experience as the business application strategy evolves
- Multilayered security that provides the flexibility to deploy the right security in the right place, either on-premises or cloud-delivered
- Simplicity at enterprise scale, which enables end-to-end policy from the user to the application over thousands of sites

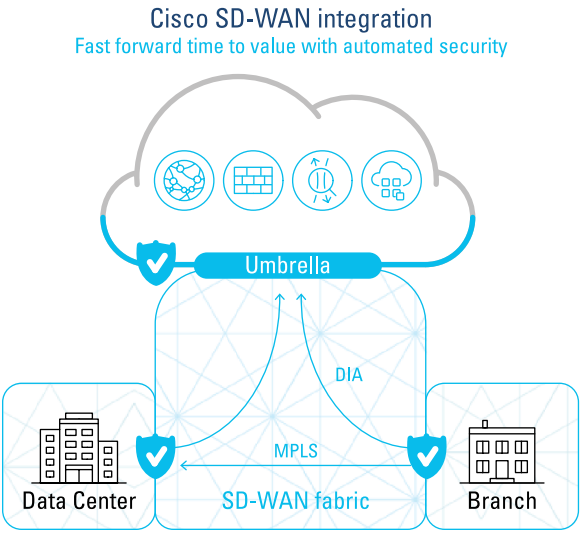


FIGURE 4-1: Cisco SD-WAN cloud-scale architecture.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The Cisco SD-WAN solution contains the following four key components that work together to form the Cisco SD-WAN fabric (see Figure 4-2):

- **Cisco vManage** (management plane)
- **Cisco vBond** (orchestration plane)
- **Cisco vSmart** (control plane)
- **Cisco WAN Edge routers** (network fabric)

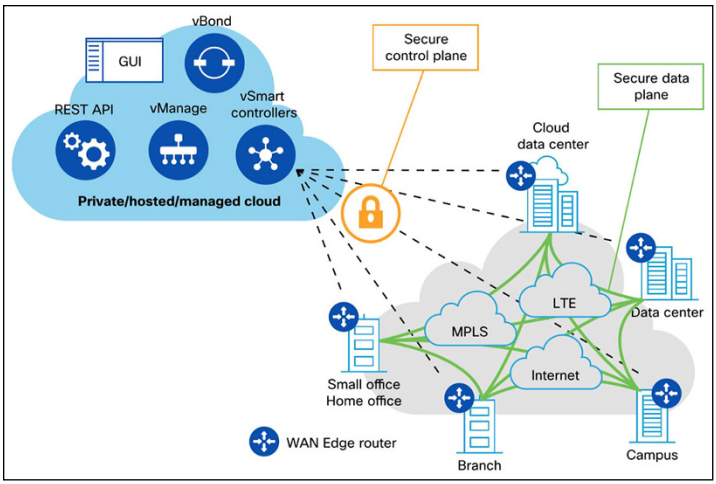


FIGURE 4-2: Cisco SD-WAN integration.

Cisco Umbrella: Multi-function cloud-native security

Cisco Umbrella is a cloud security service that delivers a secure, reliable, and fast Internet experience. By unifying multiple security functions into a single service, Umbrella helps businesses of all sizes embrace direct Internet access (DIA), secure cloud applications, and extend protection to roaming users and branch offices.

REMEMBER

By enabling these functions together instead of through point solutions, Umbrella significantly reduces the time, money, and resources typically required for deployment, configuration, integration, and management of a stack of standalone security products.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cisco Umbrella provides a core set of security functions in one cloud-based console (see Figure 4-3):

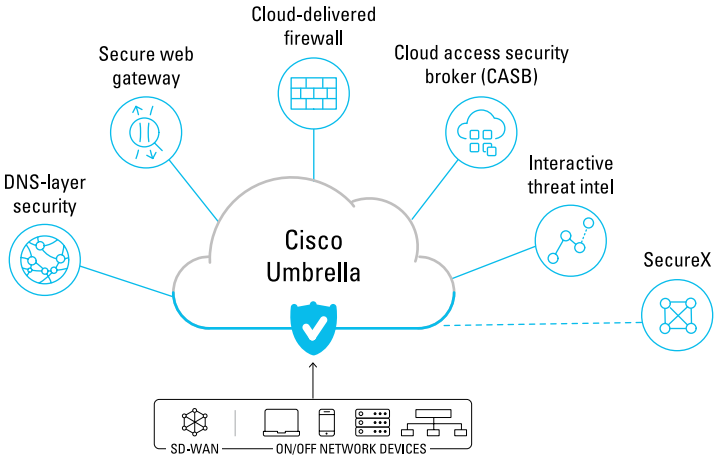


FIGURE 4-3: Cisco Umbrella delivers SASE security capabilities and more.

DNS-layer security

Cisco Umbrella blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints. As a cloud-delivered service, Umbrella:

- Provides the visibility needed to protect Internet access across all network devices, office locations, and roaming users
- Logs and categorizes DNS activity by type of security threat or web content and the action taken, whether it was blocked or allowed
- Can be implemented quickly to cover thousands of locations and users in minutes to provide immediate return on investment

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Secure web gateway (SWG)

Cisco Umbrella includes a cloud-based proxy that can log and inspect all your web traffic for greater transparency, control, and protection. This includes:

- Real-time inspection of inbound files for malware and other threats using the Cisco Advanced Malware Protection (AMP) engine and third-party resources
- Advanced file sandboxing provided by Cisco Threat Grid
- Full or selective SSL decryption to further protect against hidden attacks
- Blocking of specific user activities in select apps (for example, file uploads, attachments, and posts/shares)
- Content filtering by category or specific uniform resource locators (URLs) to block destinations that violate policies or compliance rules

TECHNICAL STUFF

Internet Protocol Security (IPsec) tunnels, AnyConnect agents, proxy auto-config (PAC) files, and proxy chaining can be used to forward web traffic to Cisco Umbrella.

Cloud-delivered firewall

With Cisco Umbrella's firewall, all activity is logged, and unwanted traffic is blocked using IP, port, and protocol rules. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Umbrella dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment.

Cisco Umbrella's cloud-delivered firewall provides:

- Visibility and control for Internet traffic across all ports and protocols
- Customizable IP, port, and protocol policies in the Umbrella dashboard
- Layer 7 application visibility and control

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cloud access security broker (CASB) functionality

Cisco Umbrella exposes shadow IT by providing the capability to detect and report on the cloud applications that are in use across your environment. Umbrella App Discovery provides:

- Extended visibility into cloud apps in use and traffic volume
- App details and risk information
- Capability to block/allow specific apps

TIP

CASB insight enables better management of cloud adoption, risk reduction, and the capability to block the use of offensive or inappropriate cloud applications in the work environment.

Interactive threat intelligence

Cisco Umbrella analyzes over 200 billion DNS requests daily, taken from Cisco's global network into a massive graph database. It also continuously runs against statistical and machine learning models. This information is constantly analyzed by Umbrella security researchers and supplemented with intelligence from Cisco Talos to efficiently discover and block an extensive range of threats. Umbrella is powered by this threat intelligence, and Cisco provides you access to that data to enable you to accelerate threat response and detection.

Analysts can leverage Umbrella Investigate for rich intelligence about domains, IPs, and malware across the Internet. Investigate provides:

- Deep visibility into current and future threats
- Better prioritization of incident investigations
- Faster incident investigations and response

TIP

Cisco's unique view of the Internet enables Umbrella to uncover malicious domains, IPs, and URLs before they're used in attacks, and helps analysts to accelerate investigations.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Umbrella and SD-WAN integration

With the Cisco Umbrella and Cisco SD-WAN integration, you can deploy Umbrella across your network and gain powerful cloud-delivered security to protect against threats on the Internet. Umbrella offers the flexibility to create security policies based on the level of visibility and protection that you need — all from one dashboard.

TIP

For DNS-layer security, Umbrella can be deployed across hundreds of devices with a single configuration in the Cisco SD-WAN vManage dashboard. For additional security and more granular controls, Umbrella's SWG and cloud-delivered firewall capabilities can be deployed through a single IPsec tunnel. Cisco has broken new ground in the automation, connection, and deployment of the tunnels, which connect SD-WAN traffic to cloud-based security services. This integrated approach efficiently protects your branch users, connected devices, and application usage from all DIA breakouts.

Cisco SecureX

The Cisco SecureX platform connects the breadth of Cisco's integrated security portfolio and additional third-party tools for a consistent, simplified experience to unify visibility, enable automation, and strengthen your security. It aggregates data from AMP for Endpoints, Umbrella, SWE, SWC, ESA/WSA through SMA, NGFW Eventing through SSE, Orbital, Threat Grid, Duo, CDO, and Tetration for improved intelligence and faster response time.

You can immediately visualize the threat and its organizational impact and get an at-a-glance verdict for the observables you are investigating through a visually intuitive relations graph. It enables you to triage, prioritize, track, and respond to high-fidelity alerts through the built-in Incident Manager. Then you can take rapid response actions across multiple security products: isolate hosts, block files and domains, and block IPs — all from one convenient interface (see Figure 4-4).

SecureX empowers your security operations center (SOC) teams with a single console for direct remediation, access to threat intelligence, and tools like casebook and incident manager. It overcomes many challenges by making threat investigations faster, simpler, and more effective.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

FIGURE 4-4: Cisco SecureX simplifies security with better visibility and automation.

Zero Trust with Cisco Duo

For organizations of all sizes that need to protect sensitive data at scale, Cisco Duo's trusted access solution is a user-centric Zero Trust security platform for all users, all devices, and all applications. Duo's multifactor authentication (MFA) lets you verify the identity of all users — before granting access to corporate applications. You can also ensure devices meet security standards, develop and manage access policies, and streamline remote access and single-sign-on (SSO) for enterprise applications.

Combined benefits unique to Cisco

Leveraging insights from Cisco Talos, one of the world's largest commercial threat intelligence teams with more than 300 researchers, Cisco Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. Cisco Umbrella also feeds huge volumes of global Internet activity (more than 200 billion requests per day) into a combination of statistical and machine learning models to identify new attacks being staged on the Internet.

Umbrella has a highly resilient cloud infrastructure that boasts close to 100 percent uptime since 2006. Using Anycast routing,

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

any of Cisco's 30-plus data centers across the globe are available using the same single IP address. As a result, your requests are transparently sent to the nearest, fastest data center and failover is automatic. Umbrella peers with more than 900 of the world's top Internet service providers (ISPs), content delivery networks (CDNs), and SaaS platforms to deliver the fastest route for any request — resulting in superior speed, effective security, and excellent user experience.

TIP

For more information on the Cisco Umbrella SASE solution visit `https://umbrella.cisco.com/sase`.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

IN THIS CHAPTER

- Recognizing the changing nature of work and networking
- Dealing with cloud-delivered apps and services
- Addressing modern threats and attracting and retaining top security talent
- Getting started with SASE

Chapter 5
Ten Key Takeaways

Here are ten key takeaways about software-defined wide area networking (SD-WAN) and cloud security to keep in mind.

More Remote Offices and Roaming Users

The number of remote office, mobile, and roaming users is growing — and these users are often some of your most susceptible targets for an attacker. The opportunity for mistakes — such as clicking on a malicious email link or visiting a malicious website — is growing, too. Because these remote and roaming users may not have access to a local IT resource, they may be less inclined to contact the help desk or security team when an issue arises.

Similarly, mobile and roaming users often don't think twice about connecting to a public Wi-Fi hotspot. Cybercriminals take every opportunity to exploit Wi-Fi vulnerabilities and the inherent trust that a coffee shop patron or hotel guest places in a "secure" Wi-Fi connection.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

DIA Is the New Normal

With the advent of the cloud era, network architectures designed to provide robust connectivity to a corporate data center are now obsolete and must evolve. The majority of network traffic today occurs either within the data center itself (East-West traffic) or from an organization's various locations to the cloud via the Internet (North-South traffic). As a result, backhauling network traffic from remote or branch locations over multiprotocol label switching (MPLS) wide-area network (WAN) links, or roaming user traffic over virtual private network (VPN) connections, is no longer an efficient or viable option. Organizations are increasingly providing direct Internet access (DIA) broadband links for their remote, branch, and roaming users to access their software as a service (SaaS) applications without the slow performance and latency associated with backhauling traffic to a corporate office with a single security stack.

SaaS Apps Are Taking Over

Once limited to personal apps that employees downloaded to their smartphones, SaaS apps have now become core business apps supporting critical business functions in the modern digital workplace. Salesforce enables customer relationship management (CRM), Workday delivers payroll services, and Concur provides expense management. Other apps such as Office 365 provide email and collaboration, and still other apps such as Box, Dropbox, Google Drive, and OneDrive provide file storage and management.

Of course, part of the allure of SaaS apps is ease of use. To deliver this convenient user experience, many SaaS apps provide only weak access control and security mechanisms — or none at all. Others have robust access control and security, but at the cost of convenience.

A multi-function, cloud-native security solution can provide cloud access security broker (CASB) services to ensure robust and consistent security and access control policies are applied to all apps — for example by enabling single sign-on (SSO) and integrated threat intelligence.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

The Old Way of Networking Is Slow and Expensive

Costly MPLS WAN links connecting remote branch locations and backhauling all of their traffic to a corporate headend are inefficient and introduce complexity, performance, and user satisfaction issues.

Network Architecture Is Meeting New Demands

SD-WAN as a standalone networking solution is great for solving enterprise networking challenges, particularly in remote and branch locations. SD-WAN enables organizations to set up new sites quickly, without having to wait weeks or months to provision new MPLS WAN links. Instead, a local Internet service provider (ISP) can provide a DIA link, often within just a couple of days.

But agility and simplicity introduce new challenges for enterprise security teams. In the rush to get connected, security may be an afterthought to the business. Once the Internet connection is live, the business is ready to go — with or without security. And if the SD-WAN solution doesn't have built-in security capabilities, the security team may need to ship a separate firewall and/or other security appliances to the remote office. Plugging in one appliance is fine, but two or three – well, that's just asking for too much!

Look for a Solution That Reduces Cost and Complexity

In the not too distant past, enterprise security teams routinely deployed "best-of-breed" point security solutions from different vendors to address single purpose needs — firewalls, secure web gateways (SWGs), intrusion detection and intrusion prevention systems (IDS and IPS), web content filtering, domain name system (DNS) security, data loss prevention (DLP), distributed

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

denial-of-service (DDoS) prevention, and malware protection, to name just a few. These standalone products all have different operating systems and management consoles and typically provide only limited, if any, integration with other security products.

Unfortunately, in the pursuit of a "defense in depth" strategy, many organizations end up with "defense ad nauseam" as these various siloed security tools add complexity and often create performance issues in the network.

Don't Compromise on Network Performance

Ultimately, the user experience is what drives successful adoption of digital transformation initiatives in an organization. Poor network performance guarantees a poor user experience and drives frustrated employees to turn to potentially risky shadow IT apps and solutions.

Ensure your network and security platform can deliver the performance (and security) your users require to stay productive — whether they are in the headquarters location, a remote or branch office, or roaming on a mobile device.

Always Keep Security Top-of-Mind

Cyberthreats are becoming more advanced and attackers are employing new techniques to exploit vulnerabilities and breach targeted networks. Phishing emails that were once easily identifiable by their spelling and grammatical errors have become much more difficult to spot. Ransomware has become far more prevalent as well, with ransomware as a service (RaaS) making it easy for practically anyone to launch an attack. And these are among some of the less sophisticated threats today. Organized crime and nation-states launch far more advanced attacks with vast resources that can take years to detect and eradicate.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Make Life Easier for Your Operations Team

The worldwide shortage of qualified security professionals is a trend that will continue for the foreseeable future. The good news for security professionals is that there will be well-paying security jobs for years to come. The bad news is that the already difficult job of securing an enterprise network is only getting harder as threats are getting more advanced, and the proliferation of siloed security tools requires specialized knowledge and experience that must constantly be updated and refreshed.

Attract and retain top talent by implementing innovative networking and security solutions that integrate functionality in a single, cloud-delivered platform and make life easier for your entire operations team.

Every Journey Starts with a Single Step

With Cisco Umbrella, you can start small with DNS-layer security and build up with additional capabilities from there as your organization is ready.

A fully integrated SD-WAN and cloud-native security solution can help organizations address the networking and security challenges of the cloud and mobile computing era. These secure access service edge (SASE) products provide advanced networking and security functionality in a single pane of glass, enabling enterprise networking and security teams to confidently build out their networks with the agility that modern businesses require.

TIP

Learn more about Cisco's approach to SASE at `https://umbrella.cisco.com/sase`.

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Notes

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Notes

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Notes

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Notes

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Cisco Umbrella

An evolving network architecture requires a new security approach.

76% of organizations are looking for multi-function cloud security services.*

Get protected – visit:
umbrella.cisco.com/sase

*Enterprise Strategy Group, 2019

These materials are © 2020 John Wiley & Sons, Inc. Any dissemination, distribution, or unauthorized use is strictly prohibited.

Discover multi-function, cloud-native security

Enterprise networks are undergoing a significant transformation. Internet traffic from branch offices has traditionally been routed back to a central location where security functions are performed. Today, business-critical cloud applications make it impractical to backhaul traffic from branch offices due to cost and performance issues. Enterprises need a fully integrated networking and security solution built for the cloud. In this book, you'll learn how SASE addresses modern networking and security challenges.

Inside...

- Leverage SD-WAN capabilities
- Optimize edge network performance
- Secure remote and mobile access
- Simplify network and security management
- Consume security functions as a service
- Access interactive threat intelligence
- Implement Zero Trust network access

CISCO

Lawrence Miller served as a Chief Petty Officer in the U.S. Navy and has worked in information technology in various industries for more than 25 years. He is the co-author of CISSP For Dummies and has written more than 150 For Dummies books on numerous technology and security topics.

Go to Dummies.com™
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-68283-7
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.