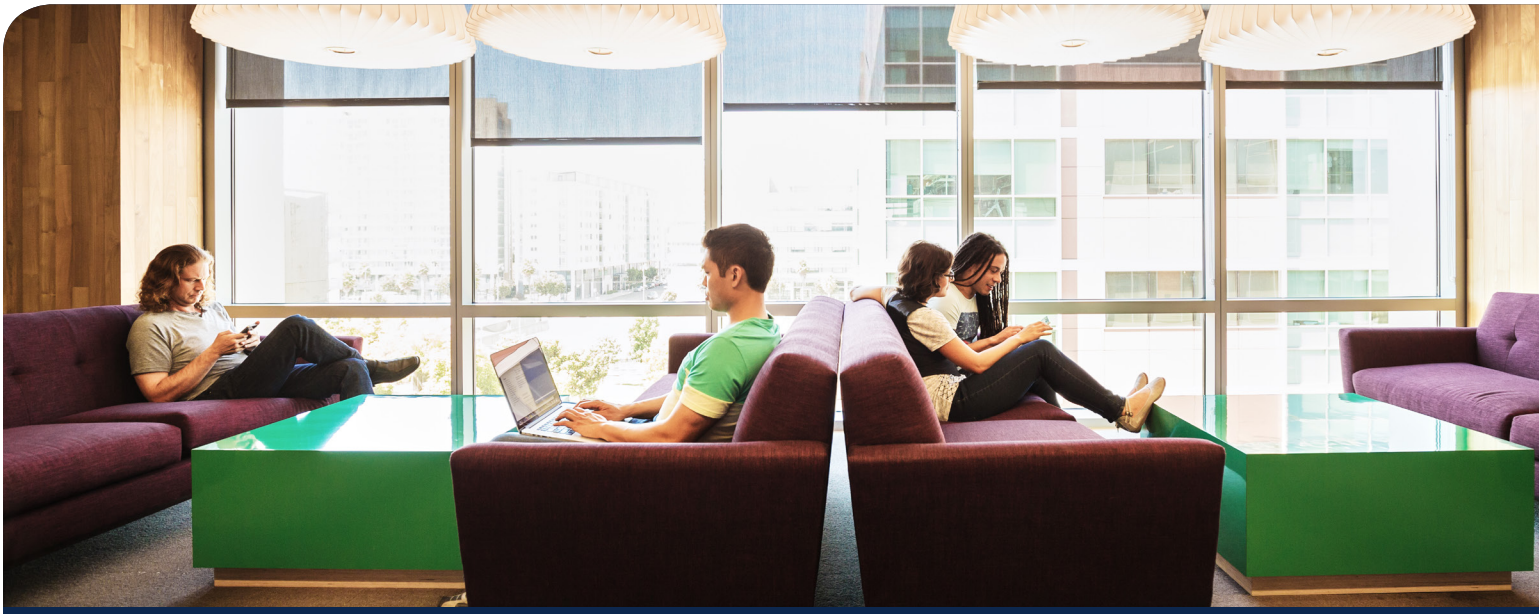
Cisco Secure Network Access Whitepaper

Uninterrupted and unplugged access experience



Introduction

Users, things and applications are everywhere, constantly moving, and becoming more "connected" to make our lives more convenient. But as our reliance on network connectivity grows, a need for a new architecture emerges. With expanding numbers of connected devices, increasing demand for data-intensive applications, and growing network threats, traditional networks simply cannot keep pace with the constant changes in their environment.

Network access and infrastructure are fundamental parts of any organization. From storing important design and financial documents to internal team collaboration and to communicating with customers, every business operation is contingent on reliable, scalable and secure network access.

The speed of change continues to accelerate. So, it's imperative for organizations to change not only the way they do their businesses but the way they apply connectivity to do it. As the customer expectation rises, the criticality of uninterrupted and unplugged network connection continues to increase and with it, the need for an intelligent network in a connected digital world.

Contents

Introduction

Network transformation

Network challenges

Reinventing Network Access

Cisco Secure Network Access

Conclusion

Network transformation

Gartner predicts that by 2023, over 60% of enterprises will consider networking as a core to their digital strategies, up from less than 20% today (1). As organizations embrace digital technologies like cloud, mobile and analytics to innovate faster and become more agile, one key metric sits clearly in their sights: user experience. Going beyond digitalization to digital transformation by setting up strategic goals – largely driven by the demands of the user experience – is where organizations are able to fundamentally transform their businesses to gain competitive advantages in their markets.

Since almost all of the digital technologies are inherently network-centric in nature, the network is deemed as the strategic enabler for these digital initiatives. The fast pace and unpredictability of a business environment requires networks to adapt quickly and support the speed of business without impeding successful digital transformations.

Businesses must transform their networks to handle a massive, ever-growing number of users, devices and applications and be able to tackle all sorts of connectivity and security challenges. They can drive their business priorities and enrich the customer experiences, only by harnessing the power and value of their networks. Hence, digital transformation is spurring the adoption of new network platforms or in other words, network transformation.

Network challenges

When navigating the journey to a digital-ready network, organizations need to look beyond core features such as fast connectivity and simplicity of management. Their best-effort connectivity and service delivery does not guarantee that changing customer expectations would be addressed. In today's world, the pressure is on for the network to securely connect all things digital; and while itis clear that the network is the source of transformational change, there are a myriad of challenges standing in the way.

Every day a new wireless product enters the market

Over 4 billion Wi-Fi devices hit the market every year. New computers and smartphones are not the only or even the major drivers for this chaotic growth of the IoTs—the everyday devices from thermostats and smoke detectors to smartwatches are. For example, a range of new specialized and diverse IoT devices such as Augmented Reality (AR) and Virtual Reality (VR) are quickly advancing into enterprises, schools, hospitals and businesses. So, how do we make sure these digital products seamlessly connect to the network and deliver the best possible user experience?

Everything is getting connected and always on

In today's digitally connected world, everything seems to become an internet conduit from light bulbs to medical equipment. And as more objects require access to the internet, it is predicted that by the year 2022 there will be 28.5 billion networked devices and connections worldwide. Since these things are enabling the way we do business and are less tolerant of downtime than humans, they must rely on an always-on connection. What would be the right strategy to have in place so that networks are not encumbered by latency and bandwidth deficiencies?

Everybody is looking for a unified experience

With exponential growth in the number and types of network connected mobile devices, IT organizations are tasked with delivering a unified experience for users. Users are looking for a consistent, untethered, and always-available experience from their connected devices from anywhere, anytime. Network administrators are constantly devising efficient ways to automatically identify, classify, and onboard mobile devices, to ensure consistent policy and management across wired and wireless environments, and to protect against sophisticated attacks. How do we help give back time to IT teams without compromising on security and productivity?

Everywhere you see an attacker trying new ways to disrupt

With opportunity comes risk. Mobility and IoT, by definition, expand the attack surface, and more and more of these products are left unmanaged and consequently vulnerable to threats. As attackers innovate, we need to be one step ahead with a smarter and more secure network that has deep visibility into traffic patterns and the latest intelligence to protect and defend the business. Is your security built-in or bolted-on?

Reinventing Network Access

The network challenges and trends dictate the need for a new network architecture - an architecture that not only supports optimizing connectivity of each user to multicloud but can seamlessly and securely onboard an increasingly diverse set of devices and applications.

It's time to re-invent the access network!

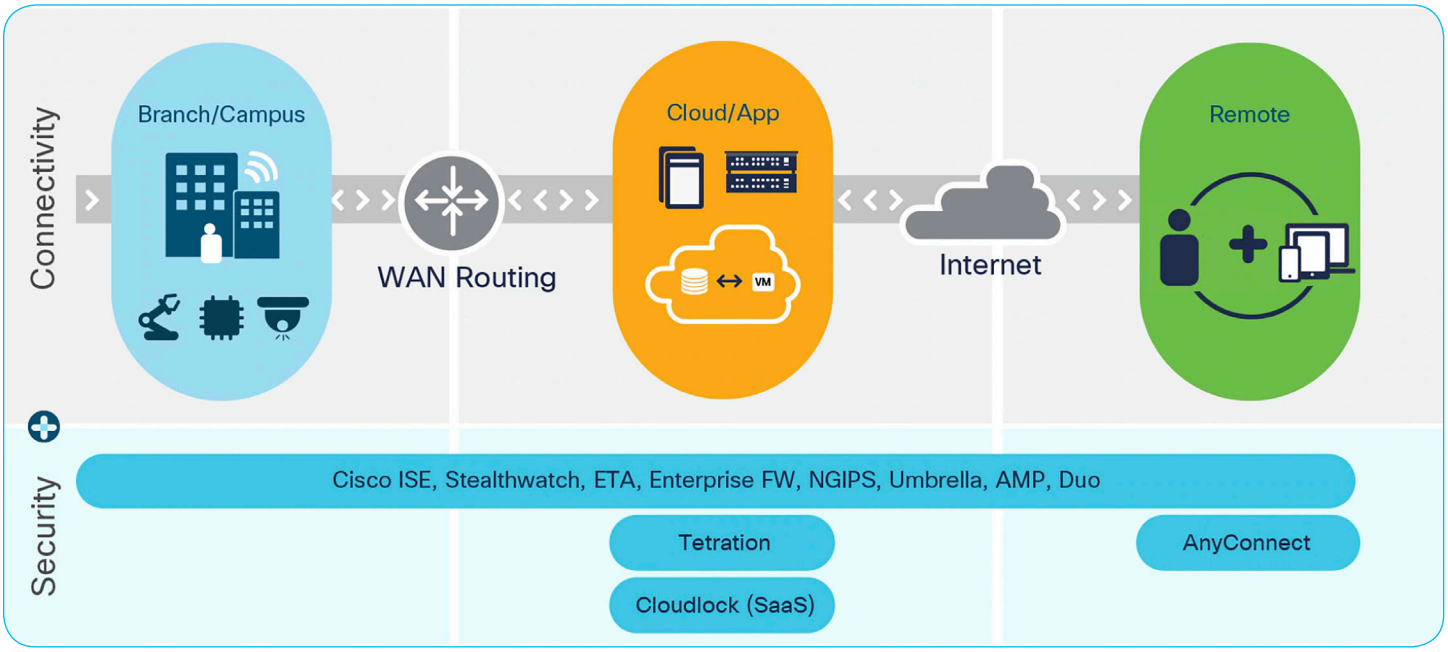
Cisco Secure Access is an evolved blueprint for a new network connectivity. As an intent-based networking architecture, it delivers a consistent connection experience for users and their devices to the right data and applications anywhere, anytime. It also ensures reliable and secure access between workloads wherever they reside (Figure 1).

By automating and unifying the access management policy for all switch and wireless products and by constantly analyzing the network data, it (Cisco Secure Access) makes sure the network is supporting the desired business objectives. It's designed to bring better reliability, agility and security and is capable of supporting and managing more users and devices, no matter where they might be.

The enabling networking products of this architecture extend to every Cisco switch and wireless solution such as Cisco Catalysts switches, access points and controllers. Cisco's security solutions are built-in into network products. The integration allows security applications and the network to work together to reduce time to prevent, detect, and mitigate threats.

Cisco Tetration and Cisco Cloudlock for cloud environments are security applications purpose-built to serve specific network domains, while others expand across multiple domains and can be triggered based on specific customer use case. For example, Stealthwatch can detect threats across the private network, public cloud, and hybrid environment, while Cisco Advanced Malware Protection (AMP) prevents breaches, detects and removes malware from endpoints as well as networks.

Figure 1. Cisco Secure Access Architecture

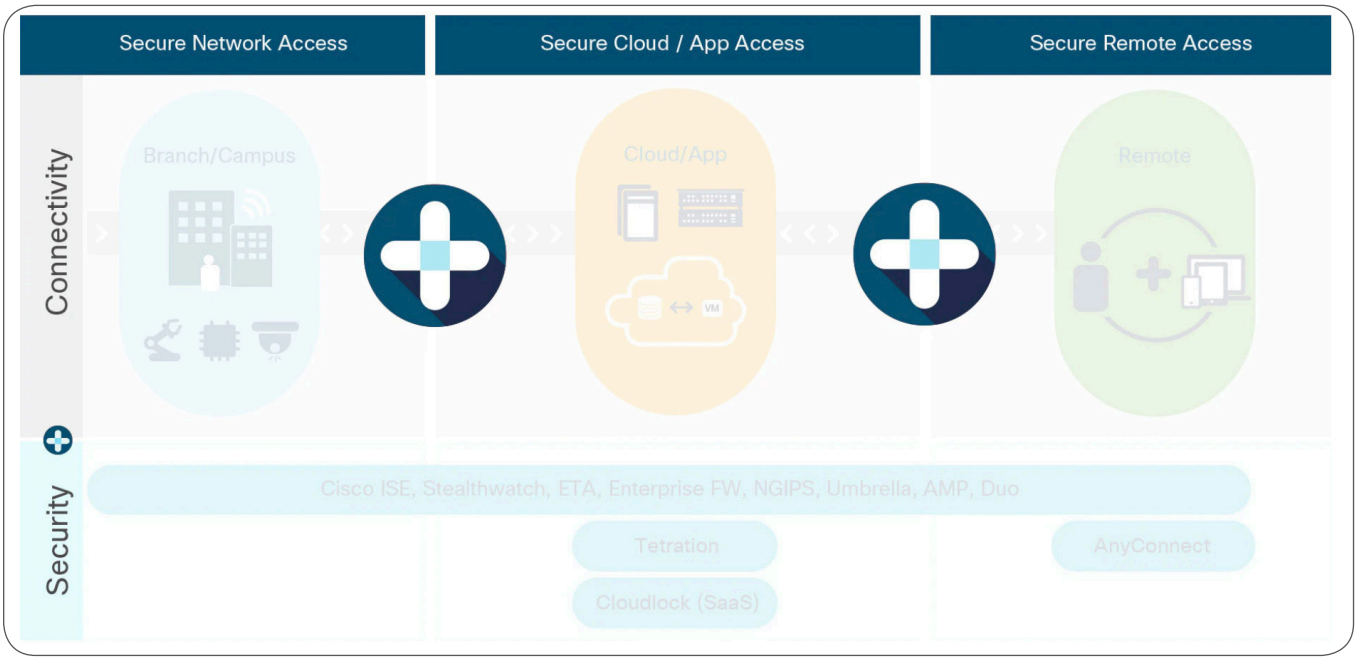


This seamless and secure connectivity (or access) experience must span across and between each network domain – branch, campus, remote, datacenter and multicloud. That means each network domain serves as a unique secure access solution (Figure 2):

- **Secure Network Access:** Ensures all users, devices, and application connections into and across branch or campus networks are secure
- **Secure Cloud/App Access:** Ensures only authorized users have access to data and applications wherever they reside.
- **Secure Remote Access:** Ensures remote users and devices have secure and consistent access to data and applications

What bonds these networking domains together is a shared access policy management that allows domains – while functioning independently – to join forces with each other to achieve the collective business intent. You can define a policy once, apply it everywhere, and monitor it systematically to ensure it is realizing its business intent (2). This access policy follows the users and workloads, no matter where they are and where they go.

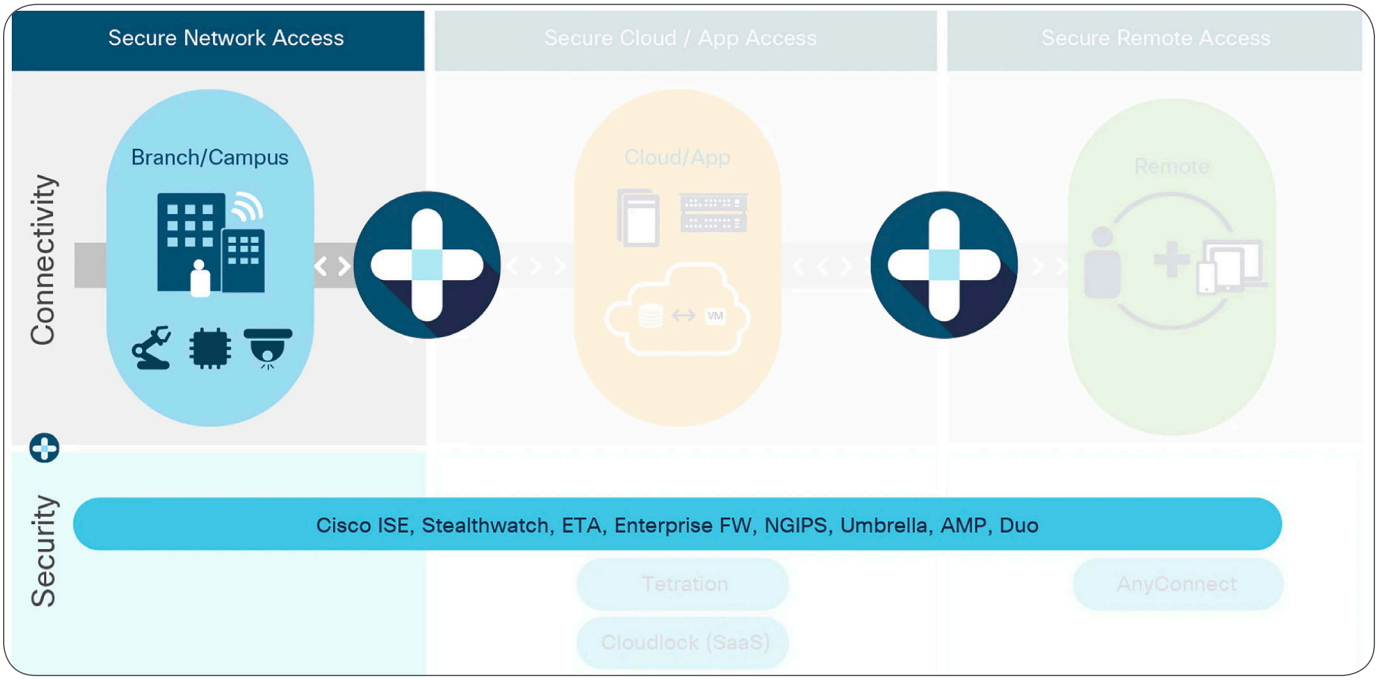
Figure 2. Cisco Secure Access Architecture Components



Cisco Secure Network Access

By coupling powerful policy automation and analytics network orchestration through Cisco software with a complete array of next-generation switches, access points and controllers for the campus, Cisco Secure Network Access helps IT securely onboards and segments everyone and everything that comes on the networks, leading to new levels of enterprise productivity and user experience.

Figure 3. Cisco Secure Network Access



The fundamentals of our secure network access solutions are anchored in four architectural principles and design points:

Wireless first

Today, business mobility and anywhere access has made wireless the preferred connection mode for applications and data. To deliver a great wireless experience, IT needs to look beyond Wi-Fi and create a pervasive wireless environment that is always-on and always-secure so users can seamlessly roam and things are always connected without interruption. Cisco Secure Network Access is powered by Cisco wired solutions to create optimal performance and reliability for any users or devices to any applications. Its software-defined fabric securely onboards and segments everyone and everything that comes on the networks, leading to new levels of enterprise productivity and user experience.

Cloud-driven

Cloud accelerates the pace of innovation to bring data-driven intelligence for IT and business operations. Cisco Secure Network Access leverages a cloud-based network software with unparalleled scale to deliver new innovations and adopt capabilities for faster time-to-value. It allows IT to shift from reactive to proactive, understand the state of the network and see trends before they impact users. The cloud-driven framework of the access network brings business agility, operational efficacies and consistent policy orchestration across the wired and wireless networks.

Data-optimized

The network offers millions of data points, providing context on users, their experience, and their vulnerabilities. By aggregating these data points collected from all sources – users, devices, applications, threats – and using powerful analytics and machine learning, you can make better business, IT and security decisions. Only Cisco provides you with the broadest access to network data through integration of the entire stack from ASIC to software and across switching and wireless. This data can deliver business insights for personalized experiences, IT insights to minimize downtime, and security insights to detect stop threats before they happen.

Always secure

Built-in security brings visibility into who and what is on the network, control over all connections, and software defined segmentation for a reduced attack surface based on business intent. Cisco is the only vendor that gives you an end-to-end converged wired and wireless solution that comes with security, segmentation and innovations such as Encrypted Traffic Analytics (ETA) which can detect malware activity disguised in encrypted network traffic without decryption.

Architectural components

As its name indicates, the building blocks of Cisco Secure Network Access consists of two functional layers: network and security (Figure 4).

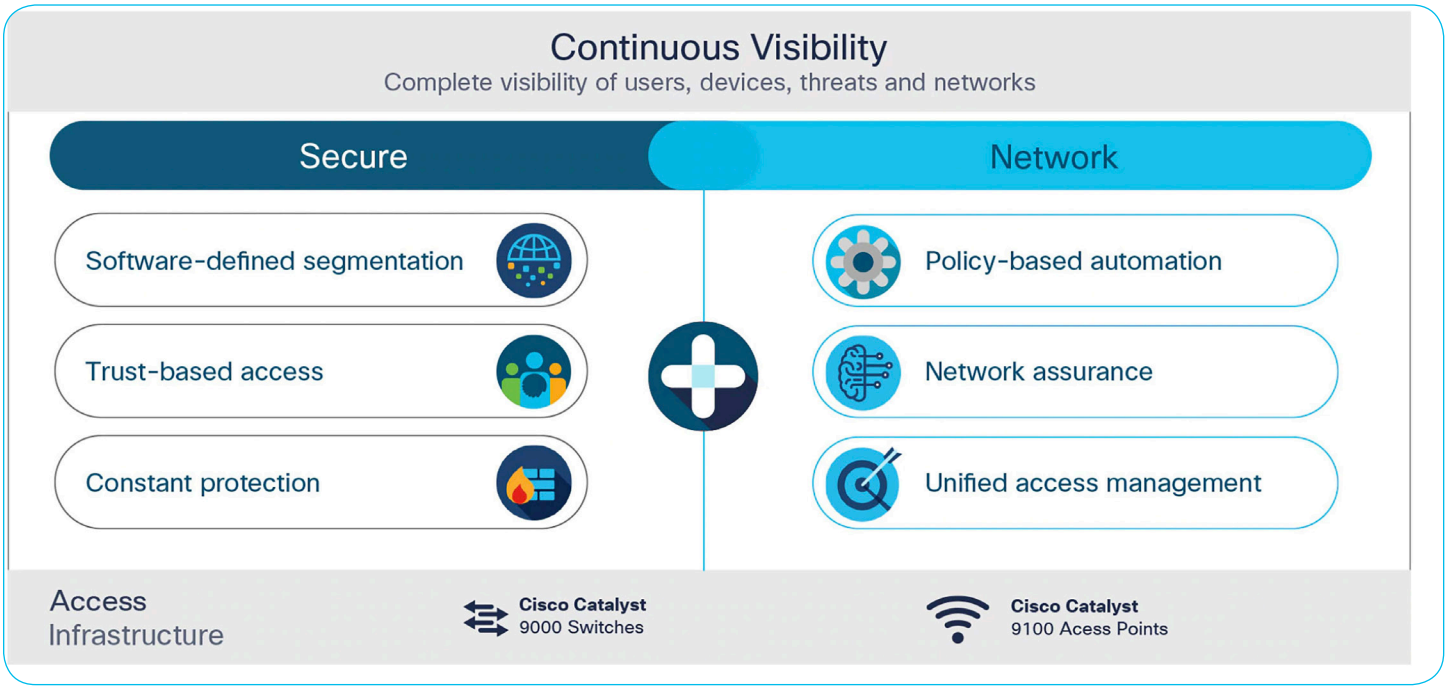
A complete set of Cisco Catalyst portfolios Cisco Catalyst 9000 switches and Cisco Catalyst 9100 access points is the primary infrastructure for this solution. Cisco Catalyst 9000 switches are the next generation of enterprise-class switches built for security, IoT, mobility and multicloud. These switches are optimized to handle traffic for Wi-Fi 6 and support full programmability and serviceability as well as convergence between wired and wireless over a single platform.

The Cisco Catalyst 9100 access points powered by Wi-Fi 6 technology and supporting Cisco's intent-based networking architecture are ready for the growing user expectations, IoT devices and next gen cloud-driven applications. With the ability to handle the increased mobile traffic as well as support IoT at scale, Cisco's Wi-Fi 6 access points have superior RF innovations and will expand wireless access with intelligence to provide a secure, reliable high-quality wireless experience for all networks. Besides Wi-Fi 6 capabilities, Cisco Catalyst 9100 extends the power of intent-based networking with hardware and software innovations, with advanced analytics and multi-RF (Wi-Fi, BLE and Zigbee) support. Along with a better industrial design, they offer improved RF performance, and deliver reliability, security, and intelligence at scale.

The Cisco Catalyst 9100 access points consist of the Cisco Catalyst 9115, 9117, 9120 and 9130 APs and are the next generation products to the Cisco Aironet Access Points. The Catalyst 9120 and 9130 access points are powered by Cisco RF ASIC that perform advanced RF spectrum analysis and delivers unique features that go above and beyond the standard for a superior RF experience including:

- Cisco CleanAir® technology to mitigate the impact of wireless interference and protect performance.
- Cisco Wireless Intrusion Prevention System (wIPS) to detect, locate, mitigate, and contain wired and wireless rogues and threats at Layers 1 through 3.
- Dynamic Frequency Selection (DFS) detection to avoid interference for optimal performance.

Figure 4. Building blocks of Cisco Secure Network Access



Networking tier

The network function of Cisco Secure Network Access solution is built on intent-based networking principles – capturing the business intent and aligning the network continuously with that intent. This layer is driven by advanced automation and unified orchestration and is able to scale from hundreds to thousands and even to millions of connected users and devices. The manual process of managing individual devices – be it wired or wireless – as part of a unified fabric, is replaced by a globally managed intent-based policy, controlled from a single location. Moreover, use of machine learning and the contextual analysis of data before, during, and after deployment to bridge the gap between what your business needs and what your network delivers in terms of scalability, operational effectiveness and security.

The key features of network layer can be defined in three main categories:

Unified access management

A unified management tool - Cisco DNA Center – is about deploying and managing a network infrastructure where wired and wireless are recognized as equally mission -critical, complementing each other. This console handles not only common network functionalities such as provisioning, configuring, connection monitoring, and reporting but is capable of wireless specific management such as spectrum monitoring and location-based tracking functionality. With its common Cisco IOS software, Cisco DNA Center is intended to streamline the operation, add efficiency and simplify management tasks through using one interface from discovering and onboarding new users and devices to creating and enforcing access policies across wired and wireless networks.

Policy-based automation

To further streamline the operation, in addition to unified management, Cisco wired & wireless networks extend and integrate across multiple domains via policy-driven automation for users, devices, and things. This is a unique and instrumental capability for zero-touch deployment, easy software updates/upgrades and simplified segmentation of applications, users and devices. Automation removes many manual and menial operations and gains faster response time to business by ensuring the right policies are established for any user or device with any application across the network.

Network assurance

This critical function deals with continuous verification, insights and corrective actions. Cisco has vast access to network data across wired and wireless infrastructures. With the help of advanced analytics and AI/ML, the Cisco DNA Assurance is able to bring key business insights and provide greater network visibility and to accelerate remediation for troubleshooting network issues.

Security tier

Security applications from Cisco ensure complete protection over all networking domains. With security built-in to the Cisco Catalyst solutions, you are able to get visibility into who and what is on the network, contribute to a complete zero-trust access security model, and build threat prevention, detection and response policies for constant protection. Within the campus and branches, for example, Cisco Advanced Malware Protection (AMP) provides maximum protection against advanced malware and Cisco Umbrella™ uses DNS to stop threats over all ports and protocols. Also, Cisco ISE prevents threats with its adaptive and dynamic network partitioning, and Cisco Encrypted Traffic Analytics (ETA) detects malware activity disguised in encrypted network traffic without decryption.

The key features of security layer of Cisco Secure Network Access can be defined in three main categories:

Software-defined segmentation

With the ability to segment networks, organizations are able to control the access level to certain sections of an enterprise's network from unauthorized users, devices and applications. The traffic isolation that comes with segmentation prevents attacks from easily propagating across the entire network and turning into destructive breaches. Cisco Identity Services Engine (ISE) makes it easy to control segmentation policy consistently across wireless and wired connections. With ISE you can configure role-based groups for users and devices and map those groups to the appropriate levels of access they need, automatically enforcing those access policies using the contextual identities of each endpoint.

Cisco wired and wireless solutions ensure complete isolation and security of traffic among segments as well as protection of data within each segment by a set of natively integrated security capabilities such as enterprise firewall, URL filtering, intrusion prevention and DNS monitoring.

Trust-based access

Cisco Zero Trust is a comprehensive approach to securing all access across users, devices, APIs, IoT and many more within your networks. It helps protect your workforce, workloads, and workplace.

Cisco Software-Defined Access (SD-Access) – a Cisco Zero Trust solution for campus network – enables and enforces consistent security policy groups for enterprise wide role-based access control. It improves the user experience by automating access policy and applying the right level of access to users and devices with network authentication and authorization. Through integration with an ecosystem of other security applications and products such as Umbrella or AMP, you can provide a complete zero-trust security for your enterprise campus environment.

Constant protection

Integrated security applications and solutions from Cisco give you the scope, scale, and capabilities to keep up with the complexity and volume of threats. They provide advanced security features that protect the integrity of the hardware as well as the software and all data that flows through the switch and the network. They ensure a constant protection that can be achieved only by building threat prevention, detection, and response into every network device.

With access to the best solutions such as Cisco Stealthwatch you can find out who is on your network and what they are doing using network infrastructure telemetry.

Continuous visibility

Complete visibility of fast-changing, mobile-first and cloud-driven IT environments is critical to fill the gaps in traditional perimeter network solutions. In a campus environment, visibility begins with classifying who and what is on the campus network, where personally owned mobile devices or rogue wireless access points are connected, and how users or IoT devices converse with services or applications. Gaining a baseline understanding of all network communications – even in the cloud – provides a full inventory that a group-based policy can be built around. It enables the monitoring of unusual behavior, which could represent a threat or policy violation. Also machine learning is critical to better classify all types of devices or workloads and more quickly identify anomalies from the baseline.

Conclusion

Organizations of all sizes can accelerate their digital transformation journey with a strong intent-based network foundation provided by Cisco Secure Network Access. It delivers the new age of wired and wireless connectivity – powering a new era of immersive network experiences – with the ability to deploy network software in the cloud to deliver new innovations at scale. It is wireless-first, cloud-driven and data-optimized with security at the core. Unlike other solutions, Cisco Secure Network Access offers a simplified operational model with one management, one common OS, pervasive security, and common policy across wired and wireless networks. With it, IT teams can automate and scale network connectivity to thousands of users and devices, anticipate change and pivot quickly and securely as they adopt best practices with a network that's built for the future.

Cisco DNA Software Demo Series

50% off Catalyst 9800 Series

Resources

Cisco Secure Network Access

An intelligent network with built-in security infographic

Cisco Catalyst 9100 access points

Cisco Catalyst 9000 wireless and switching family

Cisco Wi-Fi 6 (802.11ax) solution

Sources

(1) Cisco Networking Trends Report

(2) Cisco multidomain integrations for intent-based networking

C11-743492-00 02/20