Cisco DNA for Mobility: Lower the Risk to Your Network

Each year, the consequences of security breaches are increasing. In 2016, the average data breach cost organizations around the world an estimated $4 million, up 29 percent from 2013.[1] At the same time, the network is getting more complex to manage and there are more opportunities for attacks, increasing the risks to the network. With additional devices connecting to the network every day, driven in part by the Internet of Things (IoT), the risks to the network are likely to continue increasing without action.

What can you do to provide top-of-the-line wireless access while improving security? Start by identifying the benefits you want and then look for solutions that deliver. With Cisco's Digital Network Architecture (DNA™) for Mobility, one of the primary outcomes you can achieve is lower risk to your network and great wireless access.

[1] "2016 Cost of Data Breach Study: Global Analysis" by IBM and Ponemon Institute

Contents

What benefits should companies expect to realize?

To successfully confront the expanding attack landscape and manage an increasingly complex network, look for a solution that:

- **Prevents unauthorized access** to the most critical parts of the network using differentiated access.
- **Provides protection for and against all devices,** including new devices as well as legacy devices like printers and cash registers, which can pose significant risks.
- **Limits the direct and indirect financial impact** from any incident by providing greater visibility and enabling a quick response.
- **Demonstrates trustworthiness** through independent certifications and internal processes.

How can Cisco help?

Cisco understands the challenges that companies face, and Cisco continues to develop unique, innovative solutions. Our Digital Network Architecture (DNA™) for Mobility helps you reduce risks and reduce the impact if an incident does occur.

Specifically, Cisco's DNA™ for Mobility helps you lower the risk to your network in four ways. It all starts with being trustworthy. With that foundation, Cisco can help you protect the clients, protect the air, and protect the network with both integrated features as well as advanced capabilities.

Being trustworthy

Make sure that products are built and delivered in a trustworthy manner. Take advantage of the rigorous development, testing, certification, and compliance that Cisco offers and look for third-party verification to determine the trustworthiness of a vendor. With Cisco, you get the following:

- **Cisco® Trustworthy Systems** help ensure highly secure development across enterprise technologies, including wireless, routing, and switching.
- **Globally recognized certifications** that show compliance with the Wireless Common Criteria, Federal Information Processing Standard (FIPS), and Department of Defense Unified Capabilities (UC) Approved Products List (APL), among other standards.
- **Investment protection** with IPv6 certification.

Protecting the clients

Prevent unauthorized access and protect all devices. The network edge is the front line where most devices (smartphones, laptops, and others) connect to the most prized assets of organizations. With Cisco, you get the following:

- **Local profiling and policy** based on user role, device, and authentication mechanism with a single Secure Set Identifier (SSID).

Protecting the air

Provide consistent wireless connectivity and look out for rogues. Radio frequency is a shared medium with no physical boundaries and therefore presents unique challenges. With Cisco, you get the following:

- **Ability to identify rogues and wireless attacks** using rogue detection, basic wireless IPS (wIPS), and adaptive wIPS. These allow you to block nefarious agents before they cause service outages or other damage.
- **Ability to identify sources of interference** that cause air quality to drop, using CleanAir. CleanAir can locate and fix any drop in performance and quality.
- **Highly secure communication between access points and clients** using 802.11w and the Cisco Management Frame Protection, detecting and mitigating against wireless attacks.
- **First-hop security at the access point for IPv6 clients** using router advertisement (RA) guard and IPv6 source guard.
- Using an identity **preshared key (PSK)**:
  - **Simplified security without the overhead of 802.1X** for IoT and legacy devices (printers, cash registers, etc.) through per client overrides of authentication, authorization, and accounting (AAA).
  - **Ability to revoke access for specific clients** without the need to deploy a certificate infrastructure **Highly scalable** solution with the flexibility to support large networks with centralized policy.
- Using **Cisco TrustSec® security group tags (SGTs) and the Cisco SGT Exchange Platform (SXP)** (supported in AireOS 8.4 and later) in conjunction with Cisco ISE 2.2:
  - **Software-defined segmentation that differentiates access by user type**. Only authorized users have access to applications or data. Additionally, restrictions can be added to interactions between segments, so that, for example, employee and contractor interactions are prohibited.
- Using **Cisco ISE** (supported in version 2.2 and later):
  - **Simple, highly secure guest wireless access** for business-to-business environments.
  - **A single place to configure all settings**, including those for bring-your-own-device (BYOD) deployments, for a highly secure wireless network.
  - **Visibility and identify-based access control at the network perimeter**. This capability covers new devices as well as legacy devices like printers, gaming consoles, and cash registers.
  - **Integration with leading mobile device management (MDM)** software.

Protecting the network

Use integrated security features and run services on the network to prevent and limit the impact of any security incidents. Greater visibility and quick responses will help the network stay up and protect the assets on it. With Cisco, you get the following:

- **Security best practices** built into the products.
- **Highly secure communication between access points and the Cisco Wireless LAN Controller.** The Datagram Transport Layer Security (DTLS) protocol protects wireless traffic within the network and can also be used across the WAN as part of Cisco's OfficeExtend teleworker and small branch solution.
- Using **Cisco Umbrella Wireless LAN**:
  - **Greater control of web security through classification**. This is achieved using a single SSID across the organization with role-based web content control.
  - **Ability to stop threats before a connection is made**.

Conclusion

The result of your journey is a great wireless user experience that provides highly secure access to the network for any device from anywhere, anytime.

For more information, please visit:
www.cisco.com/go/wireless
www.cisco.com/go/DNA

- **Cloud-based security solutions** that are updated regularly to adapt to changing threats.
- **Easy deployment with low IT costs**.

- Using **Cisco Stealthwatch**:
  - **Network wide visibility and security intelligence**.
  - **Ability to identify users and devices**. See things like who was on your network, at what time, running which applications.
  - **Ability to identify and quarantine infected hosts** to prevent threats from spreading. Cisco TrustSec technology and ISE are required to quarantine.

How do you get started?

The journey to a more secure wireless network starts with Cisco access points and Wireless LAN Controllers, which have many security features built in. Next, you can enhance the network's wireless security with advanced policies, segmentation, and visibility (Figure 1).

Figure 1. Your journey to a secure wireless network

	Integrated security within APs and WLCs	Advanced policies, segmentation, and visibility
Being trustworthy	• Cisco Trustworthy Systems • Certifications (FIPS, Common Criteria, DoD UC APL)	
Protecting the clients	• Local profiling and policy based on user role, device, and authentication mechanism with a single SSID • RA Guard and IPv6 source guard provide first hop security at the AP for IPv6 clients	**Cisco TrustSec (with ISE)** • Software-defined segmentation that differentiates access by user type and restricts what segments can interact
	Identity PSK • Simplified security without the overhead of 802.1X for IoT and legacy devices • Ability to revoke access for specific clients • Highly scalable	**ISE** • Highly secure and simple guest access • Single place to configure all settings • Identify-based access control • Integration with leading MDM software
Protecting the air	• Basic wIPS to identify wireless attacks and contain rogues • Rogue detection over wired and wireless networks • CleanAir to identify and fix interference • 802.11w for highly secure communication between access points and clients	**Adaptive wIPS** • Ability to identify a wide range of wireless attacks and contain rogues
Protecting the network	• Security best practices turned on day zero • DTLS for highly secure communication between access points and clients	**Cisco Umbrella Wireless LAN** • Greater control of web security through classification • Regularly updated cloud-based security solutions • Easy deployment with low IT costs **Cisco Stealthwatch** • Networkwide visibility and security intelligence. • Identity of users and devices

C11-739040-01 08/17