Self-Defending Network

Overview of Self-Defending Network 2

Control Client Access 2

Secure Infrastructure 3

Network Services 4

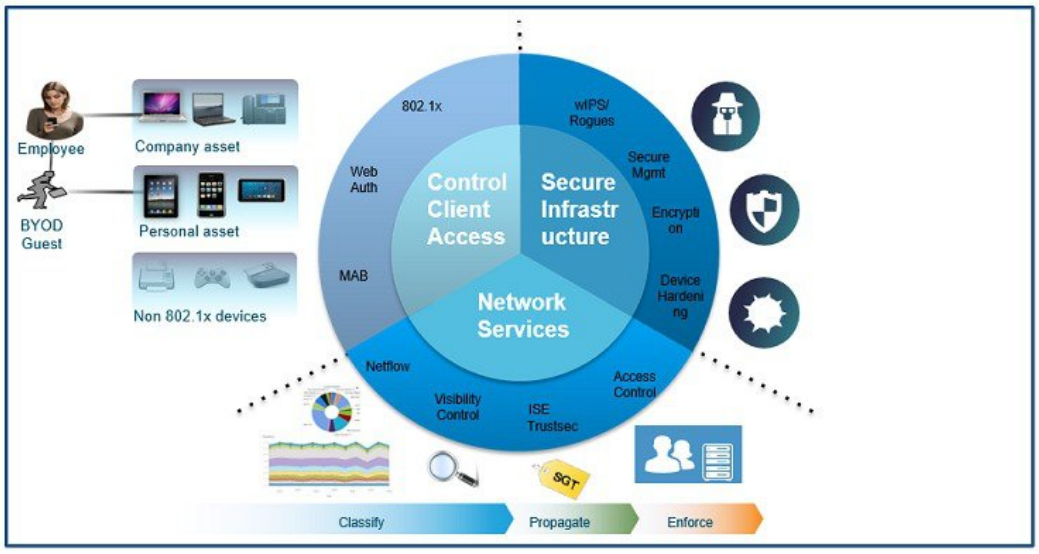
Revised: January 5, 2017,

Overview of Self-Defending Network

The dynamic nature of the threat landscape with changing business models adds to the complexity of how security policies have been implemented in the past. Cisco Unified Wireless Infrastructure opens up a completely new dimension to network security with a comprehensive defense strategy. Equipped with built in best practices, intelligent defaults and custom security profiles for threat mitigation, it uses policy based enforcement technologies to provide secure network access to any device anywhere anytime.

In order to secure every aspect of enterprise wireless architecture, security mechanisms must be enforced at all layers throughout the network to provide a highly secure wireless solution.

Figure 1: End to End Security



Control Client Access

With the trend of BYOD quickly becoming the new standard, rather than exception in workplace technology, it is important to note that such environments bring a number of security challenges with the risk of increased exposure to malware and opening up device access to sensitive corporate data. BYOD implementations comprise of a wide-range of devices including desktop PCs, laptops, netbooks, smartphones, tablets, e-readers etc. and endpoint security seeks to protect a network from the risks posed by the use of any such end device connecting to the network, be it a corporate asset, personal device or a guest user.

1 Authentication for the employee secure access network

- **a** Using a WPA2 encrypted passphrase, authentication is designed for client Wi Fi access usually for home or small office deployments.
- **b** Delivering enhanced security for business environments, 802.1X authentication with WPA2-Enterprise is still the gold standard for deploying wireless network security, offering individualized control and central management of network access. Cisco's Identity Services Engine enables creation and enforcement of security policies for endpoint devices connected to the company's routers and switches. With its advanced device classification capability, it simplifies identity management across diverse

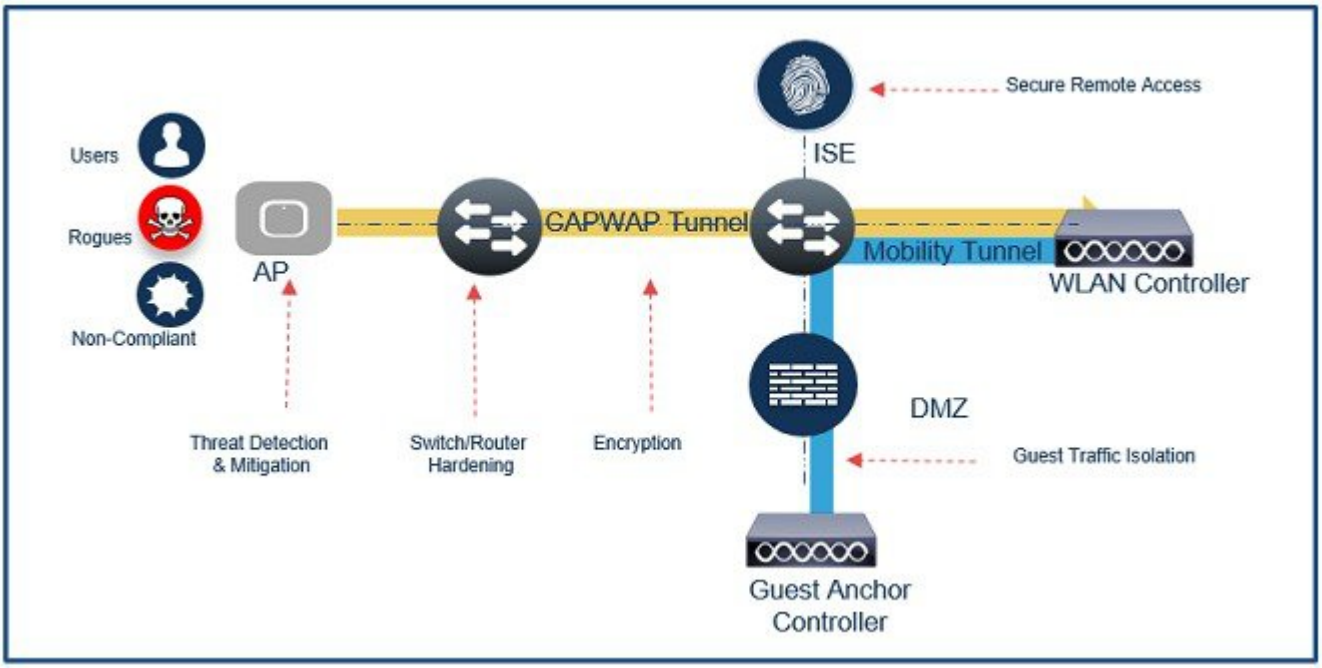
devices and applications. It also allows for integration with MDM platforms into posture of mobile devices to enforce appropriate network access policies.

2 Guest access solution for authorized visitors, contractors, customers, or other temporary users can be extended to support personal wireless devices for employees as well. It is available in flexible web based authentication deployment options: WLAN controller inbuilt portal customization, Hotspot guest portal and credentialed guest portal with ISE to provide simple on-boarding for guests to the internal network resources. BYOD smart solution using Identity Services Engine secures access to applications and systems across the organization using a single policy management plane including network access, client provisioning, guest services, posture assessment, and device profiling. Guests can create their own account using the self-registration portal or sponsors can create and manage guest users through the sponsored guest portal.

3 To accommodate non 802.1x endpoints such as gaming consoles, printers, Apple TV, cash registers and other legacy devices; Cisco's MAC Authentication Bypass offers visibility and identity based access control at the network perimeter to specific MAC addresses.

Secure Infrastructure

Figure 2: Secure Infrastructure



1 Cisco's Advanced wIPS delivers an intrusion prevention solution with advanced detection, including location and attack prevention capabilities from wireless threats and attacks. It performs automated wireless monitoring and assessment by scanning the wireless network for rogue access points, rogue clients, ad hoc connections and over the air attacks and interferences. Customers can set up classification rules to auto-classify incoming rogue events. It is equipped with default tuning profiles and a threat knowledge base with plain English attack descriptions for ease of operations. The solution is fully integrated into network management to provide long term security event archiving and reporting.

2 Switch/Router Hardening

a To prevent rogue access points from accessing the wired network, configure 802.1x security on the AP connected switchport. Cisco Identity Service Engine when deployed in the network will act as an authentication server ensuring that only trusted Cisco access points are allowed connection to the network.

b In addition, one can secure the AP connected switchport to limit and identify MAC addresses of the access points that are allowed access to the port. Wireless LAN Controller can also be configured to authorize lightweight Access Points based on their MAC address to ensure access only for trusted access points and no unauthorized users are allowed to associate to the network.

c Enabling layer2 security features on access switch interface mitigates IP, MAC Spoofing, Man in the Middle Attacks, etc are essential to defend against wired and wireless attacks.

3 User access to device management can be restricted to secure methods such as SSH and HTTPS. In addition, user can incorporate credential validation through TACACS+ protocol for management access with detailed accounting information and flexible administrative control over authentication and authorization processes.

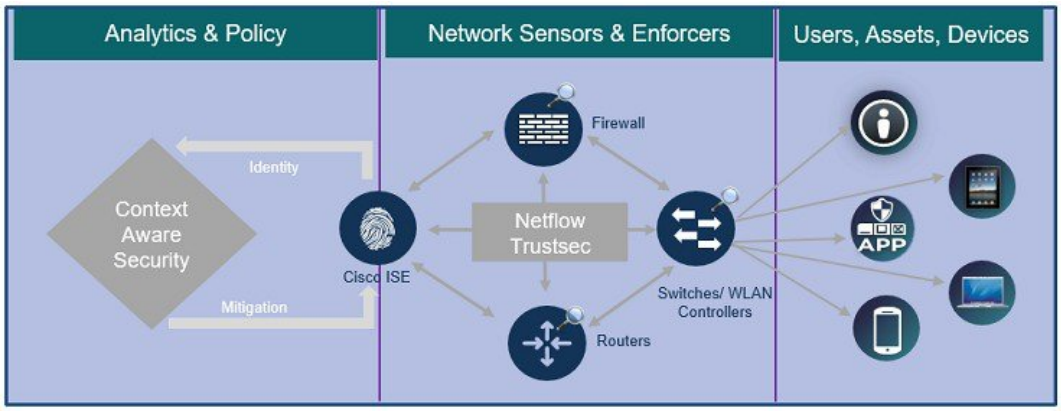
4 Cisco offers encryption for management, control and data packets in the wireless infrastructure. Access point establishes an encrypted control tunnel to the WLAN controller ensuring that management traffic cannot be hijacked by an intruder on the wired network. Data encryption can be enabled at any time to encrypt CAPWAP data packets. In addition, integrity checks on 802.11 management frames can be enabled to ensures frames exchanged in the wireless network are not tampered with. Cisco wired and wireless devices offer industry latest highly secure and reliable method of network management.

5 Guest traffic is segregated from the internal wireless controllers to a dedicated guest controller in the demilitarized zone of the network behind a firewall. Since security posture of the guest devices cannot be determined, this provides a higher level of security isolation of the guest wireless traffic from rest of the corporate network.

6 Secure Roaming is paramount to maintain voice and video communications across a highly mobile environment. The Cisco implementation of Fast Secure Roaming, including 802.11r, can ensure that highly mobile devices maintain WPA2 enterprise-secured communications while delivering seamless roaming and mobility throughout the enterprise.

Network Services

Figure 3: Intelligent segmentation for Differentiated Access



1 Incident Detection and Response–Using network-based capabilities and security controls, Cisco infrastructure provides a powerful and scalable solution to gain deep visibility, control, and analytics in the network. Network as a sensor and enforcer provides

visibility into what's on the network and provides policy enforcement capabilities to limit device access and activities. These actions will not altogether eliminate but can be used to greatly decrease the attack surface.

With the proliferation of API based tools, cybercriminals have become adept at exploiting new attacks. Cisco's Network as a Sensor and Enforcer solutions are designed to embed security throughout the extended network (including the branch) to implement a comprehensive, network-enabled approach to cybersecurity.

a Network as a Sensor solution provides broad and deep visibility into network traffic flow patterns to obtain greater insight into who and what is on the network, and gathers threat intelligence for rapid identification of security threats. Enhanced visibility into network traffic through NetFlow is at the core of the network as a sensor solution. It leverages the existing network capabilities to identify anomalous traffic and security breaches on the network. The network is capable of generating NetFlow data, providing comprehensive visibility into all corners of the network. The Cisco Stealthwatch leverages the network as a sensor and integrates with ISE and NetFlow data as input to help organizations collect and analyze network telemetry and user data for identifying and investigating attackers on the network interior. This allows for conducting faster root cause analysis and effective forensic investigations. Through the collection of telemetry and sophisticated analysis, Stealthwatch detects and mitigates threat in real time without extensive management or the need to route traffic through a centralized location.

b Once suspicious behavior is detected, the goal is to contain the threat exposure and fix the problem as soon as possible. Network as an Enforcer solution leverages the network to take action against these threats, enforce security policies, quarantine threats and segment network traffic. Cisco Netflow, ISE with Trustsec primarily form the network as an enforcer solution. Cisco application visibility also facilitates control of application performance, allowing for application classification, quality of service marking, and prioritizing business-critical applications in the network.

In a Cisco TrustSec design, the extensive ISE profiling, posture validation and mobile device management integration capabilities can be used as part of the BYOD classification process. Cisco TrustSec–capable devices take account of the BYOD classification and enforce policy based upon the classification, delivering device differentiated access. TrustSec includes tagging packets so that networks can be segmented without the need for creating separate vlans. Cisco digital ready networks enable tagging on Access Points and switches. Based on intelligent network segmentation, it is aimed at simplifying the provisioning and management of network access, accelerating security operations and enforcing consistent policies across the network.

Together, Network as a Sensor and Network as an Enforcer enable visibility, threat detection and policy enforcement of security policy once a threat is detected.

2 Policy management–Device profiling and policy enforcement is available natively on the WLAN controller as well as on ISE. For designing a network where wireless clients should be separated in sub networks for security reasons, such that each one inherits different security policies, ISE provides a single policy pane across the entire organization that combines multiple services, including authentication, authorization, and accounting (AAA), posture, profiling, device on-boarding, and guest management, on a common platform. This reduces complexity and provides consistency across the enterprise.

3 Wireless LAN Controller can be configured to block communication and data exchange between clients on the same WLAN to prevent potential attacks between clients on the same subnet by forcing communication through the router. Traffic filtering capabilities with access control can be configured for protocols to limit the network traffic, restrict the access of users to a network, and prevent the traffic from leaving a network.

4 IPv6 Security–The IPv6 feature set within the Cisco Unified Wireless Network software allows the wireless network to support IPv4 and IPv6 only clients, offering feature support including mobility, security, guest access, quality of service, and endpoint visibility.

A security-conscious company culture with carefully managed and enforced policies is pivotal in protecting data and systems with ongoing vigilance. Cisco's network security architecture plays a starring role in the overall effort for increased cyber security and ensuring smooth network operations.

© 2016 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.