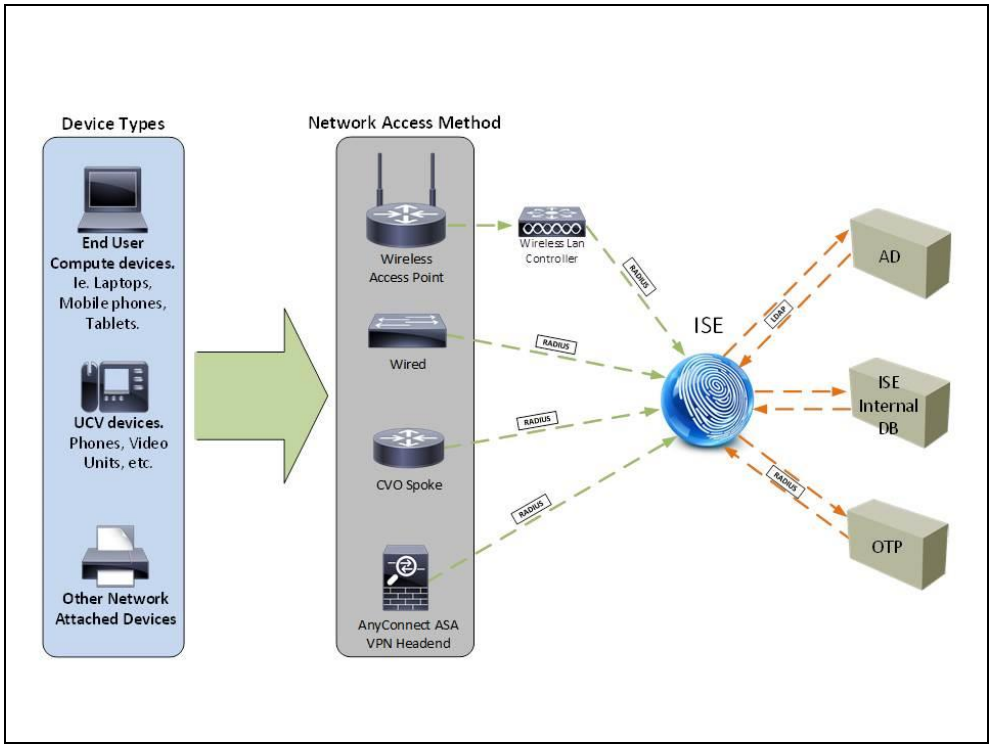
Improving Authentication of Network Users and Devices

New uses for Cisco Identity Services Engine makes access enforcement easier, consistent, and extensible

Cisco IT made its initial deployment of the Cisco® Identity Services Engine (Cisco ISE) in 2012. Since then we have expanded the implementation to cover more sites and add new capabilities. Cisco ISE gives us centralized visibility and policy-based control for access by users and devices to the Cisco network. By providing a single point for authentication and policy enforcement across wired, wireless, and VPN connections, Cisco ISE helps to simplify our IT operations, enhance security of the Cisco network, and support business activity faster and more efficiently.

Figure 1 shows how Cisco ISE provides a central point for authenticating all users and devices, regardless of their network access method. As part of this design, Cisco ISE can validate user and device credentials against multiple identity repositories including Microsoft Active Directory, the internal ISE database, and one-time password (OTP) systems.

Figure 1. Cisco ISE Authentication Design



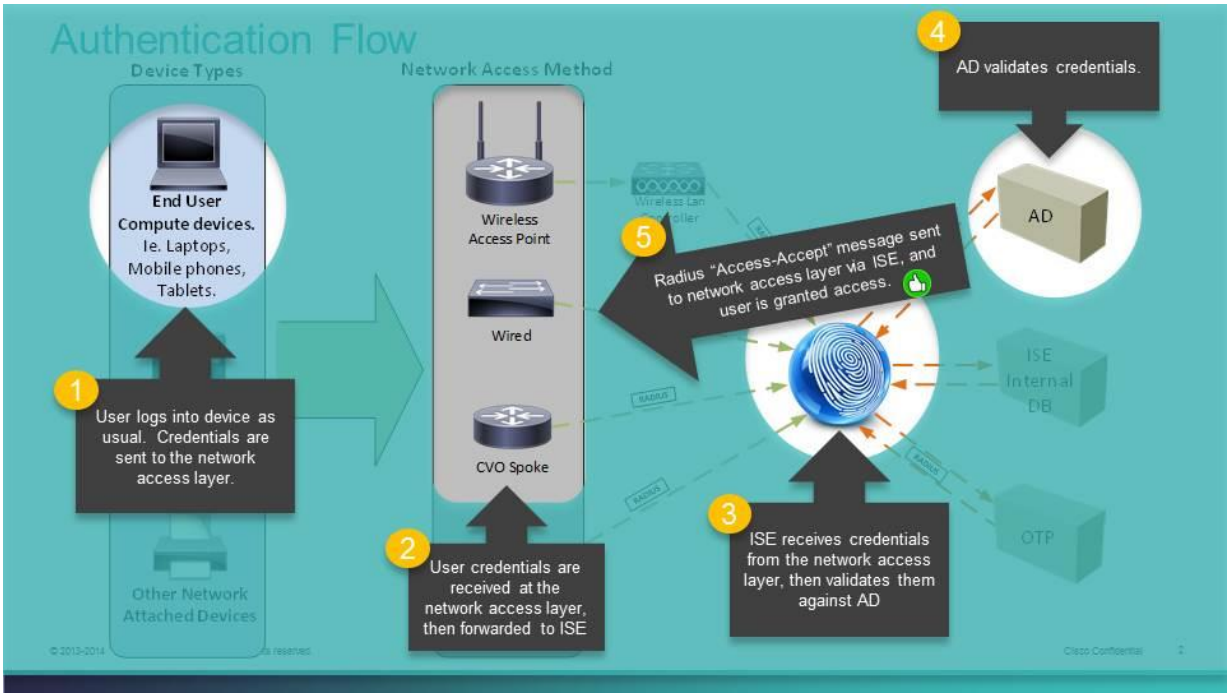
As of late 2016, we are using Cisco ISE to authenticate users and devices and protect network access from more than 400 Cisco sites worldwide, as well as to authenticate nearly one million devices that support 70,000 Cisco employees. This article describes recent enhancements to our ISE deployment, lessons learned from the deployment activity, and plans for future use of the solution.

Wireless and Remote User Authentication

We now use Cisco ISE to authenticate all users who access the Cisco network over the wireless LAN in a Cisco facility as well as remotely using the Cisco Virtual Office solution or the Cisco AnyConnect® Secure Mobility Client. The Cisco AnyConnect client has always required authentication, but Cisco ISE adds capabilities for device profiling and contextual policy control.

Figure 2 shows an example authentication with process steps for a user device that is authenticated through Cisco ISE using Active Directory credentials.

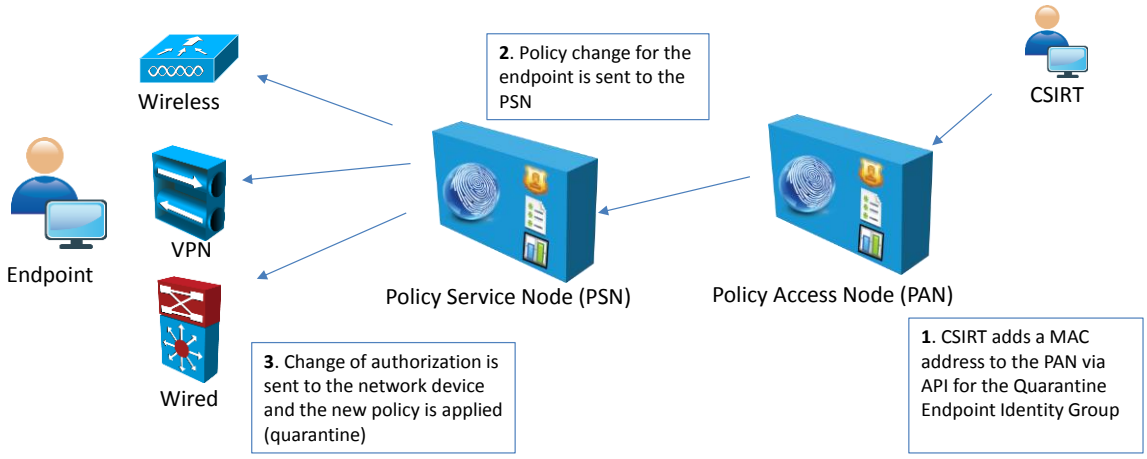
Figure 2. Authentication Flow for User Devices Connecting via Wireless, Wired, or Cisco Virtual Office Access



Quarantine

The Cisco Computer Security Incident Response Team (CSIRT) uses Cisco ISE as a robust method to quarantine users and devices that have an unacceptable level of security compliance. (Figure 3) By defining access policies in a policy access node, we are able to quarantine any device that attempts to connect to the network. Quarantine allows us to remove a malware-infected device or devices known to be non-compliant from the network in a scalable, supportable, and efficient manner. This method is also extensible to other business cases for changing endpoint policy in real time.

Figure 3. Cisco ISE Method for Quarantining a Network Device



Monitor Mode for the Wired Network

We have implemented Cisco ISE Monitor Mode across the wired network in preparation for enforcing device compliance with the IEEE 802.1x authentication standard. Monitor Mode helps us identify which devices are not currently compliant so we can contact the user to update the device and avoid the problem where a device cannot access the network once enforcement begins. We are also able to identify devices that are 802.1X-compliant but used inappropriately, such as wireless access points or network switches that are used for development projects but located outside of a secure lab.

In our initial use of Monitor Mode, we were able to identify and move several hundred devices from the desktop network into approved, secure labs. In one building, this meant overall network access compliance increased from 66 percent to 100 percent of devices.

“Although users understand that devices will be authenticated when they connect to the Cisco wireless LAN, they assume any device will be given network access if they plug it into a wired port,” says Chris Smead, Cisco IT program manager. “ISE gives us the capability to know about every device that wants to connect to our network, who owns it, and whether it is authorized so we don’t have any access by anonymous devices or unauthorized users.”

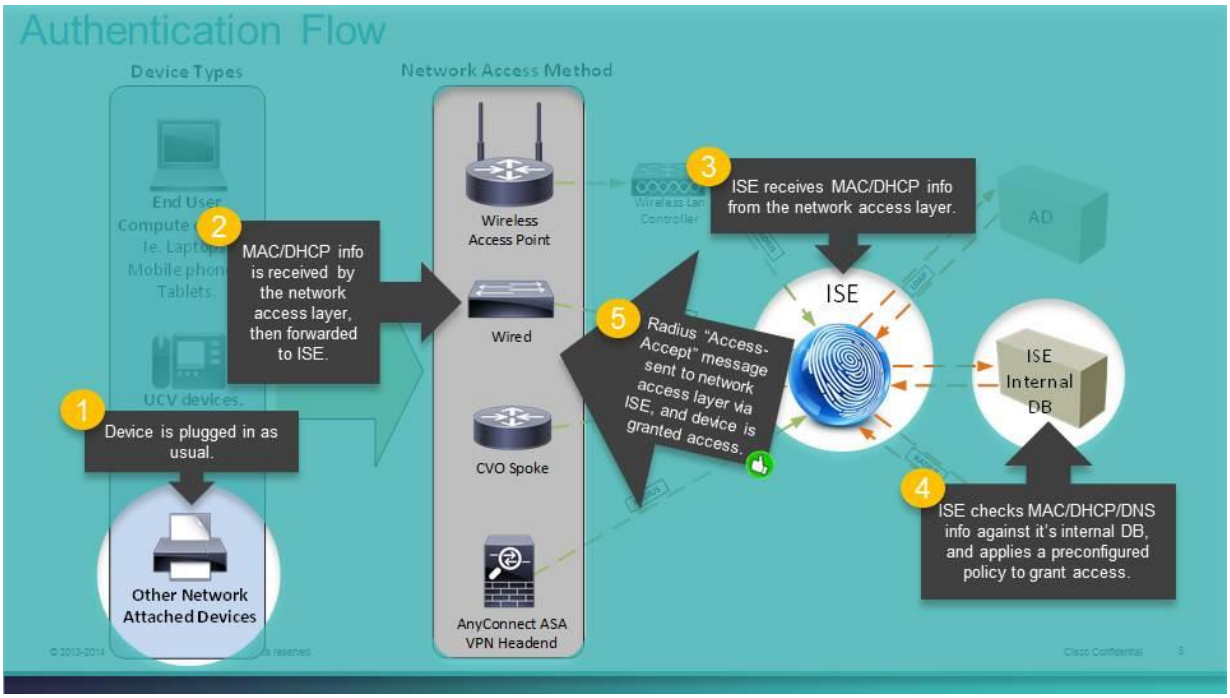
A key lesson learned from our use of Monitor Mode is that the network may not be actually configured as expected, so be prepared to find lots of exceptions. Additionally, upgrading devices to 802.1x or moving them into a lab involves effort and may make them less convenient for employees to use. Requests for exceptions and delayed enforcement may arise, especially in the early stages of identifying devices that do not meet the new access requirements.

Device Profiling

Cisco ISE includes profiles for many common devices such as IP phones, printers, cameras, smartphones, and tablets. However, many devices cannot support 802.1X or are not capable of authenticating on a wired network. When these devices or any new types of endpoint attempt to connect, ISE can obtain information from the network in order to associate a correct device profile and policy for network access. (Figure 4)

Profiles also help us detect and block unauthorized devices that attempt network access by using techniques (e.g., changing the MAC address) that make it appear to be a device that simply does not authenticate. For example, if a device pretends to be a printer, Cisco ISE can use contextual network information to determine it is not and automatically block network access.

Figure 4. Cisco ISE Authentication Flow Using Device Profiles



Based on our experience, it is important to define the device profiles and access policies carefully. "We've learned that it's best to take a hierarchical approach to defining device policies," says David Iacobacci, member of the technical staff, Cisco IT. "Defining policies as much as possible at a higher family or system level reduces the number of unique policies you'll need to create for individual devices."

Additionally, "Defining policies before rolling out Cisco ISE helps to avoid the problem of adding definitions on top of each other and creating a big management and update challenge for the future," says Raj Kumar, member of the technical staff, Cisco IT. And given the growing numbers of network-connected devices, we use Cisco TrustSec capabilities for scalability of access policies.

Dynamic User Access Policies

Some of our sites have a mix of Cisco employees and users from our partners who need appropriate access to the Cisco network. Additionally, some sites are considered more sensitive for potential risk of intellectual property loss. To manage network access at these sites, we developed a new solution called dynamic user policy. The policy combines access control capabilities in Cisco ISE and the security group tagging feature in Cisco TrustSec® technology.

We configure policies in Cisco ISE to define which users are authorized (according to their security group tag) and which applications (e.g., email) and resources (e.g. Cisco WebEx®) they can access on the Cisco network. This solution provides granular security that follows the user, enforcing the same policies regardless of where the user

connects to the Cisco network. This design is simpler for Cisco IT to administer because it does not require users to connect to specific switches or to maintain overlapping policies across the network.

Extranet Wireless Authentication

We have begun work to extend the ISE capabilities to connections in our extranet, which connects more than 400 partner sites. Initially we are deploying Monitor Mode for wired networks we control as well as for wireless controls and VPN authentication. We will use dynamic user policies to segment extranet users logically instead of through firewalls and other dedicated network infrastructure. Cisco and our partners will benefit from the ability for these users to access the Cisco extranet with the same security policy applied regardless of where they are working and which network access method they use.

For More Information

Product information: Cisco Identity Services Engine

Initial deployment article: Cisco IT and the Identity Services Engine

Cisco ISE and access policy articles: Dynamic Policies to Control User Access and A Quick, Temporary Solution to Secure Wireless Extranet Access

To read additional Cisco IT articles and case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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.