Cisco IT Validates Rigorous Identity and Policy Enforcement in Its Own Wired and Wireless Networks

Identity Services Engine is an integral part of end-to-end policy control and security compliance.

Overview

The Cisco Identity Services Engine (ISE) is a policy engine that enables contextual network access control across wired and wireless networks, and extends to mobile connectivity as well (Bring Your Own Device, or BYOD). Contextual controls are based on multiple variables, including who (user identity), when (time of day), where (location), how (access method), and what (device). ISE works with existing Cisco infrastructure to enforce security policy on all devices that attempt to gain access to the network. To do this, ISE can use access switches, wireless controllers, and most Cisco network gear for edge authentication, as device profiling sensors, and as access enforcement points.

ISE is also capable of extending authentication services on other vendors' 802.1X-compliant hardware, and enabling web authentication as backup for non-802.1X-compliant devices.

ISE is deployed as an appliance or runs on a virtual machine (VM). Cisco IT deploys ISE on a VM, which is in step with Cisco's overall data center virtualization and footprint reduction goals. Cisco IT is taking a measured, controlled approach to rolling out new ISE capabilities. This approach helps IT ensure smooth adoption, collect user feedback, and build upon and leverage ISE capabilities in each phase.

"Turning on security capabilities such as ISE in a regulated fashion is not only good practice, but it's a better way to remediate issues and implement changes that will benefit the business," says Greg Rasner, program manager, Security, Global Infrastructure Services, Cisco.

Scalability and other improvements in ISE 1.2, as well as Cisco IT's early efforts with ISE 1.1.3, accelerated the deployment schedule. Guest networking on ISE 1.2 was implemented November 2013. The switch of wireless authorization from the Cisco Secure Access Control Server (ACS) to ISE and global deployment of 802.1X monitor mode are scheduled for January 2014.

Solution

When planning the phased rollout, Cisco IT began by aligning specific features provided by ISE with the use cases that most urgently needed those features. Based on business risk assessment, Cisco IT identified areas where it could realize immediate security benefits and started the pilot deployments in those areas.

One of the first pilots entailed deploying wireless policy enforcement (802.1X) and monitor mode with profiling for the wired network. In monitor mode, 802.1X and MAB authentications were used to validate credentials, pre-authentication authorization was completely open, and there was no policy enforcement so users who fail authentication could still get on the network. Users and endpoints continued to have the same connectivity before and after authentication, enabling IT to collect data on usage, devices connecting to the network, 802.1X non-compliance, and other issues.

Additional business requirements of the initial pilot included the following:

- Work and test machines could access Cisco production resources
- Multiple devices would be able to connect to a single switch port
- An authentication peak rate of 400 per second for Extensible Authentication Protocol (EAP) to help ensure that the system could handle the anticipated load
- Authenticate supplicants via EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP Transport Layer Security (EAP TLS), and Protected EAP (PEAP)
- Authenticate non-supplicants via MAC addresses

Innovation Center and ISE

In mid-2012, the Cisco IT Network Services team embarked on an accelerated program to upgrade the corporate network. Enter the Innovation Center, a production building at Cisco's headquarters campus in San Jose, California. This true production environment helps Cisco IT fast track new, innovative technologies, test and validate their use before companywide rollout, and provide timely feedback to the business units.

Cisco IT is leveraging the Innovation Center to accelerate deployment of ISE capabilities. In addition to authentication on wired and wireless networks, Cisco IT is delivering multiple capabilities, including:

- Guest networking that restricts unauthorized devices and users to Internet access only
- Profiling that identifies users and devices on the network
- BYOD onboarding (bringing a device onto the network for the first time) through context-aware networking and support for trusted devices standard

In the Innovation Center, Cisco IT has been able to validate BYOD onboarding with ISE 1.2.

"We've validated several different devices, with an initial focus on iOS and Android devices," says Rasner. "Onboarding is greatly improved with version 1.2 of ISE. The steps are very intuitive and easier to follow than in previous versions."

Guest Networking

In late 2012, Cisco's guest networking solution was nearing end of life, and Cisco IT wanted a simpler architectural design and a simpler end-user experience. Using the guest networking default capability built into ISE made sense. In addition to delivering guest networking, Cisco IT is required to provide a subset of connectivity for users and devices that might fail some policy controls. For example, a device that does not meet Cisco's standards might still be permitted Internet access, so the guest network was expanded to cater to these use cases.

Cisco IT has also upgraded its global guest networking solution to ISE 1.2 and is benefitting from improvements in this version. The tool now has several improvements for guest networking that are being leveraged:

- Suspension of guest removes the guest from the network
- Mobile templates (a mobile-optimized template to make login/AUP acceptance on mobile devices much easier)
- Localization of text for onboarding
- Login screens now sized for mobile devices
- Notification of the accounts sent to guests using email or SMS

- Supported API (today Cisco IT is using an unsupported API for OfficeExtend Access Point, or OEAP, on- and off-boarding)

As part of the simpler guest networking design, Cisco IT turned off the previous network SSID on the wireless LAN controller and advertised an Internet SSID instead.

Cisco IT separates employee and non-employee traffic using a single VLAN and two inbound ACLs (IPv4 and IPv6) and applies a blacklist approach to deny all access to internal networks. All traffic past the ACL goes to the Internet. For redundancy the VLAN is configured on both default gateways and is Hot Standby Router Protocol (HSRP) enabled for solid fault tolerance.

Cisco's guest networking solution has been dramatically simplified on both the backend and frontend using the Identity Services Engine. Cisco's prior guest networking support infrastructure had limited redundancy, and consisted of 36 servers globally and hundreds of ACLs for managing access. By using ISE, the number of servers dropped from 36 to 2 globally, and only 1 ACL is required. The ISE solution is also highly redundant with built-in fault tolerance. If one of the servers fails, the other takes over all global guest networking functions until the failed server is restored.

Profiling

Profiling is used to classify and manage devices that are trying to access the network. This ISE capability profiles devices at the network edge using the sensing features embedded in Cisco switches, wireless LAN controllers, and wireless access points. The ISE Profiler classifies devices using the most appropriate endpoint profile, which is configured within ISE and specifies the endpoint identity group. The identity group can be used when defining conditions for authentication and authorization policies.

"As a step toward 802.1X enforcement, you need a clear picture of what's on your network. You need to know what devices are capable of doing 802.1X, what devices aren't, and where they're located. Then you can assess the user experience changes you might have to make as a result," says Rasner. "Profiling, in conjunction with monitor mode, allows IT to understand what devices are failing authentication and take appropriate action."

For profiling, Cisco IT uses RADIUS, Simple Network Management Protocol (SNMP), Dynamic Host Configuration Protocol (DHCP) Helper, Domain Name System (DNS), and HTTP. With the ISE Profiler, Cisco IT can:

- Perform automatic endpoint profiling
- Provide endpoint behavior monitoring
- Build an endpoint repository without Cisco Network Admission Control

At the end of September 2013, ISE was being used for global monitoring of all devices accessing Cisco's network, differentiated policy-based networking for 120,000-plus Cisco employees and visitor accounts, and access layer control enforcement in heightened risk locations. The Cisco IT team is gathering profiling data on more than 80,000 devices and plans to complete global profiling on ISE in December 2013.

BYOD Onboarding

In the Innovation Center, Cisco IT is testing and validating ISE BYOD capabilities such as onboarding. Through ISE policy and posture enforcement, personal devices are secured and granted access via a customized self-service registration portal. ISE BYOD automation requires minimal IT intervention, and provides easy onboarding of all employee-owned devices while ensuring that the right level of security is in place and policy enforcement is maintained continually.

To test and validate the ISE BYOD capability, Cisco IT created a second SSID called ".E2N." Cisco IT learned that placing a dot in front of E2N causes it to rise to the top of most device SSIDs on the list of wireless networks. If a device cannot be onboarded, the user can default the device back to the existing corporate SSID.

Known operating systems with supplicants used in Cisco's production network include Android, Windows 7, Mac OS, and iDevices such as iPads and iPhones. Authentication on the onboarding network was set to EAP TLS with certificates enabled.

ISE and Cisco TrustSec work together to give users seamless anywhere access to network resources. TrustSec classification and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. By classifying traffic based on the contextual identity of the endpoint versus its IP address, Cisco TrustSec enables more flexible access controls for dynamic networking environments and data centers.

In only the first day of Cisco IT's BYOD onboarding pilot, more than 150 users and 200 devices participated. User feedback is essential to improving the BYOD onboarding process further as well as future versions of ISE.

"The Cisco IT team continues to push BYOD onboarding beyond the Innovation Center," says Rasner. "While the onboarding feature in ISE 1.2 is well developed, the push into a global network for a company the size and breadth of Cisco requires continuing cooperation and input from the user experience teams."

Onboarding in ISE 1.2 has been greatly improved and validated in production at Cisco's San Jose, California, campus. Included among the onboarding improvements Cisco IT has validated and pushed out:

- Reduction of steps to fewer than six on most devices
- Simplified interface for users (improving customer satisfaction in the process)
- Optimization for mobile devices that allows smaller screens to navigate without using finger commands

Sizing Up the ISE Deployment

Cisco IT's initial global ISE deployment encompasses 120,000 employees, 109 ISE servers, 9 data centers, and 4 regional ISE clusters (Figure 1): Americas West; Americas East; Europe, Middle East, Africa, and Russia (EMEAR); and Asia Pacific, Japan, and China (APJC). An additional ISE cluster is used for Cisco's global guest networking. Internally, Cisco IT refers to these regions as "ISE cubes" and is deploying ISE feature bundles region by region.

After reviewing data and analyzing usage trends, Cisco IT decided on a plan of 3+1 devices per user, or three endpoints plus one other. The three devices are phone, laptop, and tablet. The additional device can be a printer, wired IP phone, server, etc.

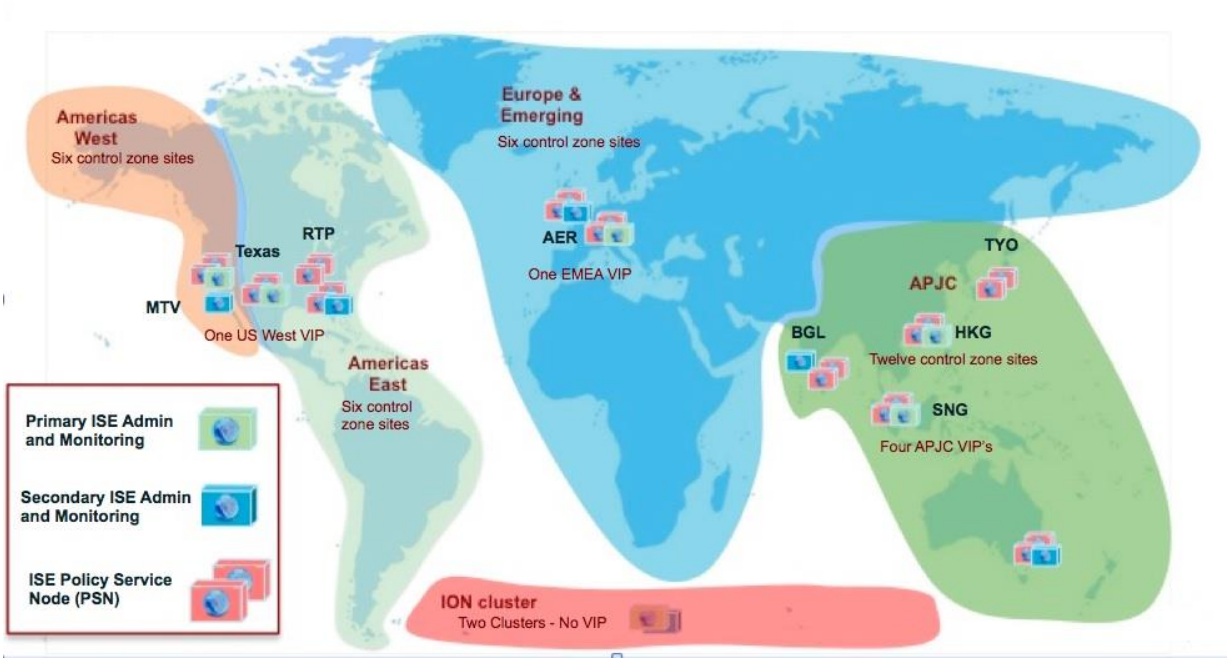
Cisco's ISE 1.2 deployment can scale to 250,000 devices per cluster, with planned increases of 500,000 devices in 2014, rising to more than 1 million by 2017. At the time of this writing (December 2013), Cisco IT upgraded its infrastructure to ISE 1.2 Patch 2 and is deploying 802.1X monitor mode with profiling.

At the end of August 2013, Cisco IT was using ISE to profile more than 60,000 devices and had 802.1X wired monitor mode in 20 percent of its intellectual property control zone sites. By the end of 2013, Cisco IT plans to switch wireless and wired authentication from the Cisco Secure ACS to ISE 1.2.

"The Cisco IT team has already established its presence in the ISE 1.3 Beta program," Rasner notes. "We want ISE 1.3 Beta to be integrated into the Innovation Center. This will help us ensure that IT is not only validating the features and capabilities, but also helping develop and support customer-focused use cases and providing valuable feedback to the business unit."

With ISE 1.3 Cisco IT will also seek a larger deployment of the Endpoint Protection Services (EPS) feature in intellectual property control zone sites. EPS is used for monitoring and controlling network access of endpoints.

Figure 1. Cisco's Global Guest Networking Deployment by Region



Lessons Learned

Cisco IT applies best practices and lessons learned from controlled ISE rollouts to its global deployments. Topping the list of lessons learned from the wireless policy enforcement and Innovation Center pilots:

- Engage all stakeholders (Architecture, Design, Implementation, Support, Hosting, Storage, etc.) from the beginning of the project.
- Provide hands-on training for Implementation and Support teams to help ensure smooth deployment and support transitions.
- Set expectations about what devices will be 100 percent supported and what devices will be supported but not fully tested.
- Assess the existing Access Control System-based wireless authenticaition status.
- Assess Active Directory server performance in different regions.
- Assess the existing wireless RADIUS authentication log.
- Develop an internal Wiki page for the most common end-user supplicants configuration.
- To avoid inconsistent authorization policies, use either PEAP "machine authentication" only or "user authentication" only, not the "machine or user authentication" from Windows supplicant.

- For failover use two Cisco Application Control Engine Virtual IP Addresses (ACE VIPs) instead of one VIP in the Wireless LAN Controller, even though there are multiple Identity Service Engines behind a VIP already.
- Use logging discriminator to filter unnecessary syslog. Access layer switches are flooded with 802.1X SNMP authentication / authorization syslog.
- Allow UDP port 1645/1656 or 1812/1813 for authentication / accounting traffic from ISE.
- Authentication status is “unknown” after enabling dot1X on access layer switches. This situation requires manual shut/noshut switch port or manual plug/unplug endpoints.
- Ensure MAB authenticaiton is not permitted for wireless access mechanisms.

For More Information

- Cisco Identity Services Engine product documentation
- To read additional Cisco IT 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.**