At-a-Glance

Benefits

- **Centralize and unify highly secure access control** based on business role to provide a consistent network access policy for end users whether they connect through a wired or wireless network or VPN.
- **Gain greater visibility and more accurate device identification** with Cisco Identity Services Engine device profiling and device-profile feed service, which together reduce the number of unknown endpoints.
- **Simplify guest experiences** for easier onboarding and administration through fully customizable branded mobile and desktop guest portals, created in minutes with dynamic visual workflows that let you easily manage the guest experience.

Cisco Identity Services Engine

A New Way to Secure and Manage Your Changing Network

The enterprise network no longer sits within four secure walls. It extends to wherever employees and data travel. Employees today demand access to work resources from more devices and through more nonenterprise networks than ever before. Mobility, digitization, and the Internet of Things (IoT) are changing the way we live and work. Enterprises are challenged with supporting a proliferation of new network-enabled devices as myriad security threats and highly publicized data breaches clearly demonstrate the importance of securing access to the evolving enterprise network.

As the modern network expands, the complexity of marshaling resources, managing disparate security solutions, and controlling risk grows as well. Factor in the ubiquitous connectivity of noncorporate devices with already constrained IT resources, and the potential impact of failing to identify and remediate security threats becomes very large indeed.

A different approach is required for both the management and security of the evolving enterprise network. It's called the Cisco® Identity Services Engine (ISE).

Narrow Your Exposure and Reduce Your Risk

Get ahead of threats by using visibility and control. That includes deep visibility into the users and devices accessing your network and the dynamic control to ensure that only the right people with the right devices get the right access to enterprise services.

The redesigned ISE 2.1 further simplifies the delivery of consistent, highly secure access control across wired and wireless multivendor networks and remote VPN connections. With far-reaching, intelligent sensor and profiling capabilities, Cisco ISE can reach deep into the network to deliver superior visibility into who and what is accessing resources. Through the sharing of vital contextual data with technology partner integrations and the implementation of Cisco TrustSec® policy for software-defined segmentation, Cisco ISE transforms the network from simply a conduit for data into a security enforcer that accelerates the time to detection and time to resolution of network threats.

- **Accelerate bring-your-own-device (BYOD) and enterprise mobility** with easy out-of-the-box setup, self-service device onboarding and management, internal device certificate management, and integrated enterprise mobility management (EMM) partner software for device onboarding both on and off premises.
- **Construct software-defined segmentation policy to contain network threats** by using Cisco TrustSec technology to enforce role-based access control at the routing and switching layer. Dynamically segment access without the complexity of multiple VLANs or the need to redesign the network.
- **Share user and device data with partner network and security solutions** to improve their overall efficacy and accelerate time to containment of network threats.
- **Automatically contain threats** through integration with the Cisco Firepower Management Center and other technology partners as ISE contains infected endpoints for remediation, observation, or removal.

Important ISE 2.1 updates and enhancements include:

- **Threat-centric Network Admission Control (NAC):** ISE now incorporates vulnerability assessment and threat-incident intelligence to influence network policy. This also allows ISE to change network privileges dynamically in the event that an endpoint's threat score changes.
- **Cisco TrustSec and Application Centric Infrastructure (ACI) policy plane integration:** You can now apply a cohesive security policy across the enterprise, incorporating user roles and device types together with application context.
- **EasyConnect:** This quick, easy, and flexible method authenticates users when an endpoint doesn't support 802.1X.
- **Streamlined visibility:** Gain enhanced out-of-box visibility into users and devices on the network through a simple, flexible, and easily consumable interface.
- **Cisco Rapid Threat Containment:** Cisco Rapid Threat Containment now supports the integration of Cisco ISE 2.1 with Cisco Firepower™ Management Center 6.1 to automatically and dynamically contain threats before they spread further in the network.

Additionally, ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share rich contextual data with integrated technology partner solutions. This technology accelerates their capabilities to identify, mitigate, and remediate security threats across your extended network. Overall, access control is centralized and simplified to deliver vital business services more securely, enhance infrastructure security, enforce compliance, and streamline service operations.

Through its integrations with leading security information and event management (SIEM) and threat defense solutions, its deep network visibility, and its secure access control capabilities, ISE plays an integral role in the Cisco Cyber Threat Defense, network-as-a-sensor, and network-as-an-enforcer solutions. Ultimately, ISE allows organizations to control all access to the network from one location, see and share user and device details, and stop and contain threats to effectively implement security that targets the entire attack continuum. This includes managing network access before an attack, providing visibility into threats during an attack, and improving time to containment after an attack.

Next Steps

To learn more about the Cisco ISE, visit http://www.cisco.com/go/ise or contact your local account representative.

C45-654884-14 06/16