Cisco Identity Services Engine Integration with Cloud Access Security Brokers

Manage and secure consumer cloud apps alongside corporate apps

The enterprise network continues to evolve as organizations embrace cloud computing along with cloud-based and Software-as-a-Service (SaaS) applications. Employees are also demanding access to unauthorized consumer applications in the cloud, such as file-sharing apps, social media, and collaboration tools from the corporate network. The use of these applications reduces the ability of IT administrators to gain visibility into and control enterprise data, especially when it is accessed from unmanaged devices. Simply blocking access to unapproved cloud applications may lead an employee to find another, lesser-known, and potentially riskier service instead. These factors, combined with the rise in mobility and the increase in the number of connected devices on the network, mean that a different approach is required to manage and secure devices and their access to cloud-based applications, whether corporate sanctioned or not.

Benefits

- **Use cloud services while protecting corporate data:** Set precise access policies around cloud application access based on contextual data and custom attributes
- **Prevent unauthorized users from accessing cloud applications and data:** Create strict policy controls for sensitive data and applications that reside in the cloud
- **Improve the visibility and analysis of cloud access security broker platforms:** Associate anomalous traffic patterns in cloud usage with a specific user

Next steps

To learn more about the Cisco Identity Services Engine, visit http://cisco.com/go/ise.

For additional information regarding Cisco cloud access security broker partners, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html.

C45-734765-01 06/17

The Cisco® Identity Services Engine (ISE) integrates with leading Cloud Access Security Brokers (CASBs) to bring together a view of all cloud applications and services across the network as well as relevant user identity and device context to create precise access policies for highly secure usage. The Identity Services Engine uses Cisco Platform Exchange Grid (pxGrid) technology to share contextual data with leading CASB solutions to address security and compliance risks associated with cloud applications and services and to achieve greater visibility into, and control of, cloud application usage.

How Cisco ISE works with CASB integration

The Identity Services Engine, using pxGrid technology, provides its user identity and device contextual information to CASB partner platforms in the following ways:

- Cisco ISE contextual data is appended to CASB partner systems and enhances their detailed auditing controls over user, content and data movement for cloud services and platforms by enabling detailed user information for the cloud applications being accessed.
- This contextual user information enables CASB platforms to then create detailed policies around accessing cloud applications based on custom attributes such as not allowing access to certain cloud applications from specific devices or users.
- Cisco ISE can also be used to undertake a quarantine or access-block action on users and devices that violate these policies.

The Identity Services Engine collects and delivers contextual data that includes the following:

- User: Name, IP address, authentication status, location
- User class: Authorization group, guest, quarantine status
- Device: Manufacturer, model, OS, OS version, MAC address, IP address, network connection method (wired or wireless), location
- Posture: Posture compliance status, antivirus installed, antivirus version, OS patch level, mobile device posture compliance status through Mobile Device Management (MDM) ecosystem partners