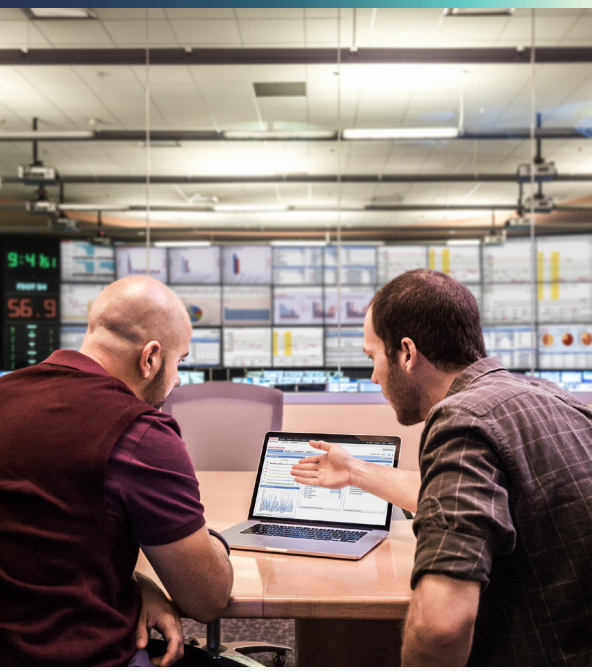
At-a-Glance



Cisco Identity Services Engine and Check Point Integration

Apply a Consistent Network-wide Security Policy

Now the best-selling Cisco® Identity Services Engine (ISE) has been integrated with the Check Point® Identity Awareness Software Blade to give you more detailed visibility into users, groups, and machines, combined with real-time, comprehensive identity and network privilege context. The result? Better protection of your infrastructure and resources moment to moment.

Cisco ISE provides a wealth of user identity, endpoint device, and network context information that is useful to many IT platforms for customers around the globe. To bring greater insight to risky user activities on the network, Cisco ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share identity, device, and network information. The IT infrastructure can serve more use cases and operate more effectively by becoming identity, device, and network aware. Cisco pxGrid is a unified framework that supports multivendor, cross-platform network system collaboration among IT infrastructures such as security monitoring and detection systems, network policy platforms, identity and access management platforms, and virtually any other IT operations platform.

Cisco ISE and Check Point: Identity and Network-Aware Security and Access Control

The Check Point Identity Awareness Software Blade provides detailed visibility into users, groups, and machines. It provides application and access control through the creation of identity-based firewall policies in a Check Point deployment along with event monitoring and reporting. Cisco ISE integrates with Check Point's software blade to provide real-time and comprehensive identity and network privilege context. That includes user IP address, name, group, and Cisco TrustSec® security group tag information.

Benefits

- Enhance firewall and access control policies and overall security monitoring and reporting through detailed Check Point Identity Awareness
- Enforce access and audit data based on identity through the firewall mapping of users and machine identities
- Use Cisco ISE as the source of data for security policies to deliver real-time identity data on a network-wide basis – not just for users and devices known to Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) – for greater accuracy and the ability to capture any user or device authenticated to the network
- Bring policy consistency across the Cisco network infrastructure by using Cisco TrustSec tags with Check Point

This integration provides Check Point gateways with better visibility of user activities while improving control of corporate resources. ISE helps the Check Point console to display contextual information associated with an event, such as the user's identity and level of access. This capability allows your security team to make access policy decisions using identity information that provides far greater policy details than traditional firewalls, which are limited to information like IP addresses or port numbers. This finer level of detail from ISE can reduce threats and data loss by restricting access to resources by users and devices.

The solution is composed of Cisco ISE running pxGrid context-exchange capabilities, an ISE Plus or Advanced Feature license, and the Check Point Identity Awareness Software Blade.

How the Cisco ISE and Check Point Integration Works

- Cisco ISE provides its user identity and device information to Check Point Identity Awareness
- Identity Awareness uses the accurate, real-time user identity context provided by ISE in its firewall rule base
- ISE contextual data is also appended to associated events in Check Point to provide the additional context of the user, device, and access level, helping analysts to better understand the significance of a security event
- All of these functions can be logged and reported on within the Check Point console, which provides unified user behavior for security threat reporting

Some of the main ISE attributes available for use by Check Point for user-related context include:

- User: user name, IP address, authentication status, location
- User class: authorization group
- Cisco TrustSec: security group tag (SGT)

Next Steps

To learn more about the Cisco Identity Services Engine, visit http://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html

To learn more about Cisco pxGrid, visit http://www.cisco.com/go/pxgrid

For additional information regarding the Identity Services Engine and other ecosystem partner integrations, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html

C45-736265-00 11/15