

CHECK POINT and CISCO Context-Aware Security

Context-Aware Security

Benefits

- Enhance access control, threat prevention policies and overall security monitoring and reporting
- Enforce access and audit data based on identity through the mapping of users and machine identities to IP address
- 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

INSIGHTS

Today's cyber criminals are stealthy, technically competent and persistent. To combat this trend, security platforms can no longer exist in their own silos. The exchange of relevant, rich contextual information among security systems delivers better overall network security. That is why Cisco and Check Point have teamed up to deliver advanced, context-aware security tuned to the needs of today's enterprise networks.

SOLUTION

Cisco® Identity Services Engine (ISE) has been integrated with the Check Point® Identity Awareness and CloudGuard Controller to give you more detailed visibility into users, groups, and machines, combined with real-time, comprehensive identity and network privilege of the source user, device, or entity. 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 and the ISE External RESTful Services (ERS) API to share identity, device, and network information.

Check Point Identity Awareness and the CloudGuard Controller included in Check Point Next Generation security platforms collects data from multiple identity sources including Cisco TrustSec Security Group Tags from Cisco ISE. This information can then be used across the Check Point ecosystem, on premise and in the cloud, to provide better visibility and network security. Using Cisco ISE as an identity source for Check Point security policy augments what is known from other identity sources such as Windows Active Directory (AD), LDAP and SDN objects in private and public cloud environments.

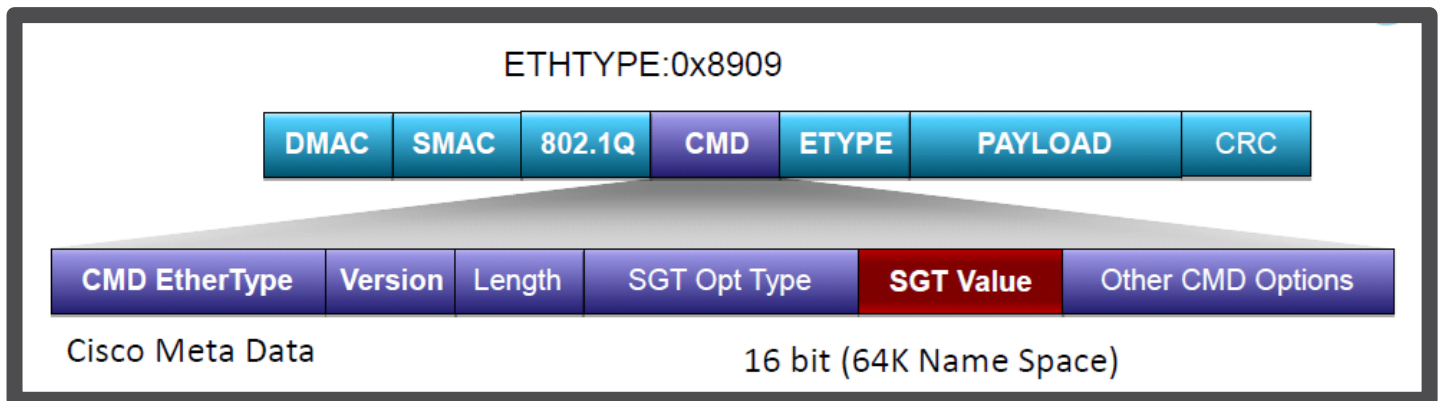
Check Point ISE Mappings

ISE Context	R80.20 Management	R80.10 Management	R80.10 CloudGuard Controller (HF1)
User	✓	✓	✓
IP Address	✓	✓	✓
Machine	✓	✗	✗
Security Group Tag	✓	✓	✓

CISCO TRUSTSEC SECURITY GROUP TAGS — CLASSIFY, TRANSPORT, ENFORCE

Classify

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. During endpoint authentication, a host (the endpoint IP address) accessing the Cisco TrustSec domain is associated with a Security Group Tag at the access device. A Security Group Tag is a unique 16 bit tag in a Layer 2 Cisco Metadata Header (CMD) that is assigned to a unique role. It represents the privilege of the source user, device, or entity and is tagged at the ingress of the Cisco TrustSec domain.



Cisco switches and wireless controllers embedded with Cisco TrustSec technology support the assignment of SGTs. An SGT can be assigned dynamically or statically. Dynamic classification occurs via an authentication sequence, via 802.1x, MAB (MAC Authentication Bypass), or web authentication. When authentication isn't available, static classification methods are necessary. In static classification the tag maps to some identification element (an IP address, a subnet, a VLAN, or an interface) rather than relying on an authorization from Cisco ISE. This process of assigning the SGT is defined as "classification." Static classifications are commonly used for static devices, such as data center servers, or topology based policies, such as a subnet based policy. These classifications are then transported deeper into the network for policy enforcement.

Transport

Packets tagged in line with a Layer 2 Cisco Metadata Header (CMD) is one possible transport mechanism. The Security Group Tag (SGT) Exchange Protocol (SXP) is another. This is a control protocol for propagating IP-to-SGT binding information across network devices that do not have the capability to tag packets. SXP uses TCP as its transport protocol to set up an SXP connection between two separate network devices. Each SXP connection has one peer designated as an SXP speaker and the other peer as an SXP listener. This process allows security services on switches, routers, or firewalls to learn identity information from access devices.

i In a TrustSec network Check Point gateways do not extract the SGT from the CMD in the tagged packets and do not forward the packet. We also do not integrate with pxGrid via SXP. Instead we use pxGrid APIs.

Enforce

The access device transmits that association or binding through SXP to Cisco TrustSec hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco TrustSec hardware-capable devices by applying security group access control lists (SGACLs). When packets pass the last TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

WELCOME TO THE FUTURE OF CYBER SECURITY

CHECK POINT ISE INTEGRATIONS

Identity Collector

Check Point Identity Collector is a Windows-based application that connects Cisco ISE and Microsoft Active Directory (AD) servers with Check Point Security Gateways acting as Policy Decision Points (PDP) and Policy Enforcement Points (PEP) in an organization.

i PDPs acquire and share identity elements. PEPs enforce identity-based policy

Cisco ISE provides session notifications over pxGrid when authorizing supplicants. ISE publishes active user session information as well as configuration information, such as TrustSec Security groups and configured device profiles. ISE provides active user session information which includes user identity and the associated context including IP address, user group, location, and device type using the Session Directory capability. This information can be retrieved on demand, for example by invoking query and bulk download APIs as well as through notifications.

A typical use case for the session information in a network is a Check Point upstream device that needs the user identity and context information for the network traffic to apply policy based on the user context, such as a user group, device type, or security group. Check Point registers with the ISE server as a consumer of Session Directory capability. Once the connection is established, it can invoke bulk download API to retrieve all active session context and also subscribe to notification for any further session updates. [[Cisco ISE Ports Reference](#)].

One Identity Collector can serve multiple Security Gateways even from different Check Point domains because trust is set using a shared key making it independent of the Check Point Secure Internal Communication (SIC) used between gateway and management server. Install Identity Collector directly on a Domain Controller following the installation requirements defined in the Identity Collector Technical Overview [[sk108235](#)].

i In addition to the Identity Collector ISE integration, Identity Collector also uses the Windows Event Log API to get Active Directory security events. Compared with the standard AD Query which uses Windows Management Instrumentation (WMI), this reduces the load on the Security Gateway and on Domain Controllers. Also instead of administrator permissions used in AD Query, the only permission required is read-only access to the domain security logs. Up to 35 Active Directory servers are supported and up to 1,900 Active Directory events per second can be processed.

i R80.20 adds Identity Collector support for syslog and NetIQ eDirectory LDAP servers as identity sources

CloudGuard Controller

The Check Point CloudGuard Controller connects to Software-Defined Data Centers (SDDC) and virtual cloud environments. The CloudGuard Controller automatically updates the security policy and security logs as virtual appliances, computers, devices and IP addresses change in these dynamic environments. With the CloudGuard Controller Check Point gateways integrate seamlessly with SDN solutions, such as VMware vCenter, VMware NSX, Cisco ACI and Cisco ISE.

The Check Point CloudGuard Controller [[from R80.10 Hotfix 1](#)] uses the ISE External RESTful Services (ERS) API to connect to ISE and automatically retrieve Security Groups. In Check Point SmartConsole ISE servers are represented as Data Center server objects. We pull TrustSec security groups and use these in the security policy according to the static IP-to-SGT mappings in ISE. For redundancy, it is possible to provide both primary and secondary ISE administration nodes. Prerequisites include Cisco ISE version 2.1, an ISE administrator with the ERS-Operator or ERS-Admin group assignment and ERS enabled on ISE.

i CloudGuard Controller also integrates with Amazon Web Services (AWS), Microsoft Azure, Cisco ACI, Cisco ISE, Google Cloud Platform (GCP), Nuage Networks VSP, OpenStack, VMware vCenter and VMware NSX.

WELCOME TO THE FUTURE OF CYBER SECURITY

RADIUS Accounting vs Identity Collector

Radius Accounting is also a supported identity source. Customers can configure network access points to work with ISE via RADIUS and send RADIUS Accounting messages to a Check Point gateway so that we can map the user's identity to the assigned IP address. However, the SGT is not included in the accounting message.

CHECK POINT IDENTITY AWARENESS — COLLECT, SHARE, ENFORCE

Collect

For security gateways to enforce a user-based policy, first enable Identity Awareness on the gateway. In the Check Point ecosystem Identity Awareness uses a database that contains session information where the session relates the IP address to user, device, AD group or Cisco SGT for example. The full list of identity sources include;

- Active Directory (AD) Query
- Browser-based Authentication
- Identity Agents (installed on the Endpoint)
- Terminal Servers Agents
- Radius Accounting
- Remote Access Clients
- Identity Collector
- Web API

Identity Collector subscribes to pxGrid notifications and distributes them throughout the Check Point ecosystem. For a Security Gateway to connect to Identity Collector, in SmartConsole enable Identity Collector in the gateway object and enter a shared key that it will use to connect securely to Identity Collector and install the policy.

Share

Returning to the Identity Collector management interface, Query Pools describe a list of identity servers, ISE or AD. Gateways in the Identity Collector management interface are assigned to one Query Pool. Only the identity sources collected from that Query Pool are fed to the Policy Decision Point (PDP) process on the gateway. Each gateway must be assigned with a Query Pool. As mentioned earlier, gateways may be from different Check Point SIC domains. The secure gateway connection to Identity Collector is via TCP port 443 using a shared key set in the gateway object.

Within the same SIC domain a gateway learning identities from a Query Pool can use Identity Sharing to share what it has learned with other gateways managed by the same Check Point Management Server or Multi-Domain Management domain. PDPs can share identities with the PEPs inside their management domain by “pushing” the session information to the PEP.

i In large distributed environments with lots of identity sessions memory consumption on the PEP and network traffic is reduced using a “pull” model. Instead of sending every session, the PDP notifies the PEP that it knows about a network. When the PEP receives a connection it queries the PDP for the identities for that network and then proceeds to match the connection against its security policy using the sessions sent from the PDP. This isn't enabled by default, but is available using GuiDBedit to do the configuration changes.

WELCOME TO THE FUTURE OF CYBER SECURITY

Enforce

Check Point Security Gateways are Policy Enforcement Points (PEP) which enforce user-based policy defined using Access Role objects in the security policy. In an Access Role object security administrators may define groups retrieved from identity stores such as AD and Cisco ISE and further define the network and device. Once Access Roles have been defined they are ready to be used in the source and/or destination column of access control and threat prevention policies.

Name	Source	Destination	Services & Applications	Action	Track
File sharing	EngineeringGroup	adserver	microsoft-ds	Accept	Log

Access Role objects have multiple dimensions: network, user/group, machine and remote access client type. These dimensions have AND as logical relation. The SGTs content consumed from the Cisco ISE is referenced in the user's dimension of the Access Role object.

The image shows four configuration panels for an Access Role object, all set to 'EngineeringGroup'. The panels are:

- Networks:** 'Any Network' is selected.
- Users:** 'Specific users/groups' is selected, with 'EngGroup' listed.
- Machines:** 'Any machine' is selected.
- Remote Access Clients:** 'Any Client' is selected.

A central banner displays the resulting configuration string: **AnyNetwork@EngGroup@AnyMachine@AnyRemoteAccessClient**


As an example it is possible to configure an Access Role object describing a User/Group object that is AND related with the IP address range of a network. An Access Role object like this will only match if both dimensions match: a user is part of a group AND the connection is initiated from the IP network range configured.

i In R80.20 Identity Tags let you include external identifiers (such as Cisco Security Group Tags, or any other groups provided by any Identity Source) in Access Role matching. These external identifiers act like a tag that can be assigned to a certain user, machine or group. First create a User -> Identity Tag object using the Cisco SGT as defined on the ISE server or acquired through Identity Collector. For example BYOD is one of the default ISE SGTs. Then include the Identity Tag in the machine dimension of your Access Role object.

The image shows the 'New Identity Tag' configuration window. The 'External Identifier' is set to 'BYOD'. The 'Machines' dimension is selected, with 'ISE_BYOD' listed. A central banner displays the resulting configuration string: **AnyNetwork@AnyUser@BYOD@AnyRemoteAccessClient**

WELCOME TO THE FUTURE OF CYBER SECURITY

In addition to access control, Access Role objects can also be used in threat prevention policies. The following example shows an Access Role object referring to a server that is an Active Directory element used in a threat prevention policy.

Name	Protected Scope	Action	Track
Protect WinServer	 WindowsServer	 Strict 	 Log  Packet Capture

USE CASES

On Premise

Check Point Identity Collector provides SGT bindings from ISE for users and other transient entities on the network. SmartEvent automatic reactions can be used to signal ISE to quarantine compromised hosts.

Private Cloud

Check Point enforces Security Group Access Control List (ACL) policy matrices in NSX using CloudGuard for NSX, which provides hypervisor-level enforcement. Check Point CloudGuard controller for NSX provides all Check Point physical and virtual enforcement points near real-time SGT bindings for Virtual Machines (VMs) within NSX based on mappings between NSX security gateways and ISE SGTs. NSX security groups and VM objects are dynamically fetched from NSX and vCenter via the CloudGuard Controller.

Public Cloud

Security Groups and VM objects are dynamically fetched from Azure and AWS. Cisco ISE device mappings and SGTs can be combined with NSX security groups and VM info via CloudGuard Controller and leveraged within the security policy at any gateway within the organization.

SUMMARY

Cisco TrustSec allows customers to logically segment their flat networks using label-based access control. Inter-segment communications are best controlled using Check Point Security Gateways leveraging Security Group Tags (SGTs) as part of the granular security context used on behalf of next generation access control and threat prevention. Together the Cisco/Check Point solution provides customers with a seamlessly integrated whole that is greater than the sum of its parts.


WELCOME TO THE FUTURE OF CYBER SECURITY

References

Cisco

- [1] Cisco TrustSec Switch Configuration Guide;
https://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/sxp_config.html
- [2] Cisco ISE Administrator Guide, Release 2.1
https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_00.html
- [3] pxGrid Developer Guide for Cisco ISE
<https://developer.cisco.com/docs/pxgrid-api/#!overview/pxgrid-developer-guide-for-cisco-ise>
- [4] Cisco ISE API Reference Guide, Release 1.4
https://www.cisco.com/c/en/us/td/docs/security/ise/1-4/api_ref_guide/api_ref_book/ise_api_ref_ers2.html

Check Point

- [5] Identity Collector Technical Overview
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108235
 - [6] CloudGuard Controller Hotfix 1 R80.10 Administration Guide
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_vSEC_Controller_Hotfix_v1_AdminGuide/html_frameset.htm
 - [7] R80.10 Identity Awareness Administration Guide
https://sc1.checkpoint.com/documents/R80.10/WebAdminGuides/EN/CP_R80.10_IdentityAwareness_AdminGuide/html_frameset.htm
 - [8] Identity Collector Support in R77.30
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk120979
 - [9] Identity Collector Support on Scalable Platforms
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk122157
 - [10] Identity Collector Support on SMB Appliances
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk123858
 - [11] Ports Used by Check Point Modules
<https://community.checkpoint.com/docs/DOC-2740-basic-ports-and-modul-communication>
-  R80.20 online help
https://sc1.checkpoint.com/documents/R80.20/SmartConsole_OLH/EN/html_frameset.htm?topic=documents/R80.20/SmartConsole_OLH/EN/4x3HIUbSkxYhtcFgIKIq0w2

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.comU.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-628-2117 | www.checkpoint.com