Cisco TrustSec Solution: Intelligently Control Access to Corporate Data

What You Will Learn

The Cisco TrustSec® solution allows you to intelligently control access to corporate data allowing access control policies to be applied anywhere in the network using switches, routers or security appliances. Cisco TrustSec can greatly simplify the management of security policies and reduce risk by providing consistent enforcement anywhere on the network.

Challenge: Simplify Network Security

Organizations frequently have simple business goals that they want their security architecture to facilitate; for example, they may want only traders to access trading systems, or only doctors to access patient records. However, when these policies are implemented, they are frequently translated into complex network security rules that define users and servers by their IP addresses, subnet or site. The resulting network security rules are no longer simple to understand and may not clearly correlate with the original business goals.

In today's dynamic work environments, users are also frequently bringing their own devices to the workplace, which introduces yet more complexity in network security rules. The dramatic growth in virtualization and virtual private cloud technologies has also led to challenges in provisioning security requirements for new virtual servers and accommodating the movement of workloads while maintaining the desired security posture.

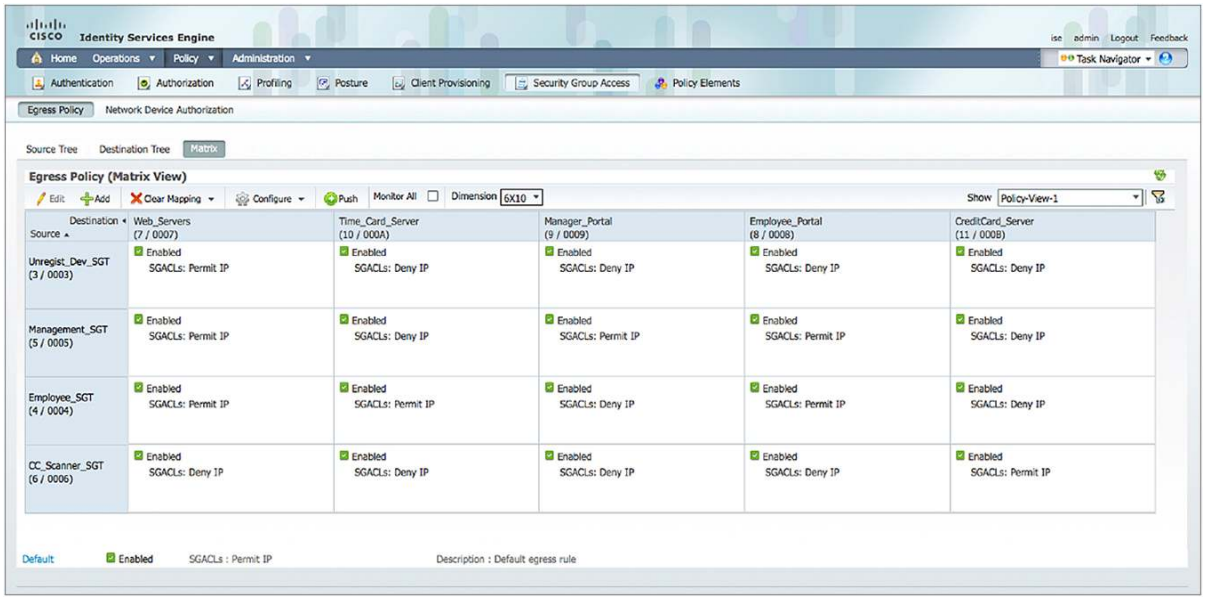
Cisco TrustSec Business Benefits

Cisco TrustSec allows you to group users and their devices so that rules and policies can be defined at a group level. For example, groups could be defined so that doctors using iPads will be classified differently from patients using iPads. After creation of a "Doctors Using iPads" group, all of the doctors connecting to a hospital network using an iPad can be automatically classified as members of that group, with common privileges. These security groups can also define the key assets that the organization would like to protect, so that the access control policy can be as simple as defining that the group of 'Doctors Using iPads' are allowed access to the 'Patient Records Databases', whereas the 'Patients Using iPads' group would be unable to access those resources. Those sample requirements could be met with three simple groups and a simple access control rule.

Without a Cisco TrustSec solution, the network address assignments for the different user groups may need to be referenced in multiple access control lists and firewall rules, using IP addresses and subnets to denote the users and protected resources.

With Cisco TrustSec, auditing of rules and policies is also much simplified. In the hospital example, any number of doctors working anywhere in the hospital will receive the same user experience and access to appropriate resources.

Figure 1. Policy Matrix for Cisco TrustSec Security Group ACLs



Cisco TrustSec Solution Capabilities

Cisco TrustSec capabilities are embedded in Cisco® switches, wireless LAN (WLAN) controllers, routers, and firewalls. With TrustSec, when a user's traffic enters the network, it is classified according to characteristics such as user authentication, analysis of the device being used and it's network location. Based on these criteria, a user's endpoint is classified as a member of a particular security group; for example, it could be added to a group called Retail-Manager. Cisco switches and routers then propagate the security group information to policy-enforcement devices

Most Cisco switches and routers can transport this security group information with the user's traffic. This information is included by embedding a 16-bit Security Group Tag (SGT) value in each frame associated with the user device. The SGT can be transported over LAN, WAN and data center networks so that it is available for inspection and policy enforcement wherever appropriate.

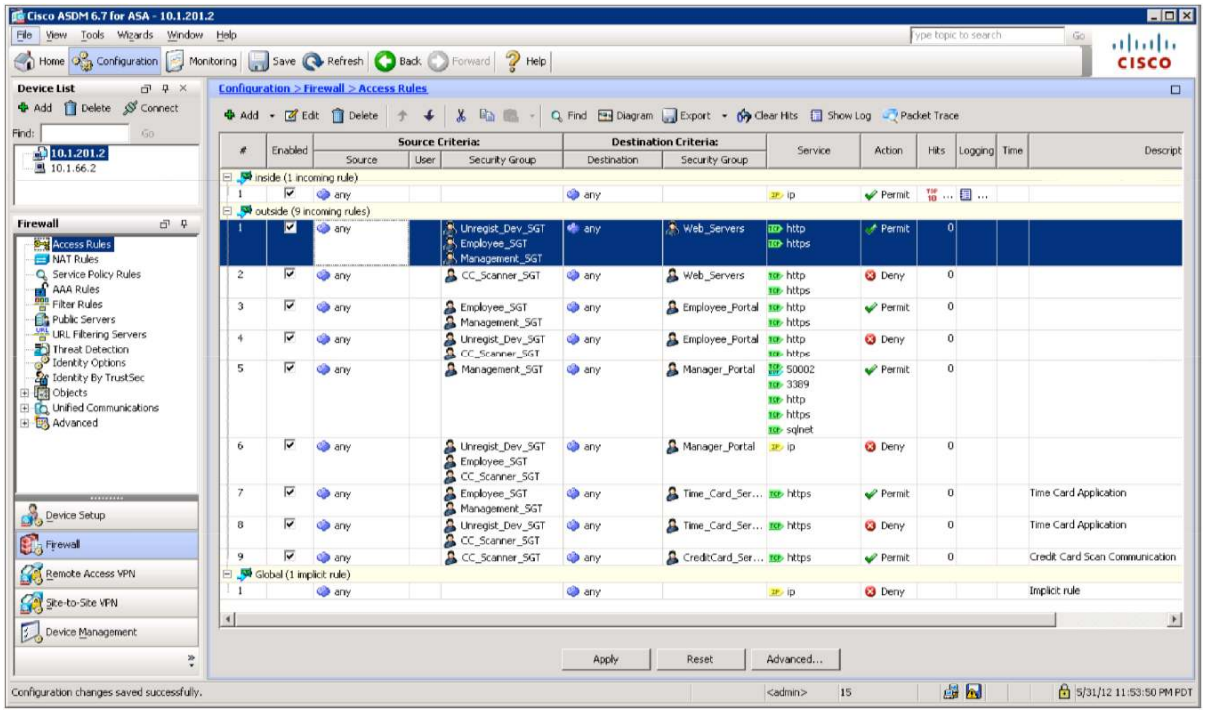
To traverse networks or network devices that do not understand or support SGT propagation, a control-plane protocol, the SGT Exchange Protocol (SXP), allows Cisco TrustSec SGT information to be transported over any IP network to enforcement points.

Policy enforcement can be performed by Cisco firewalls, routers, or switches. The enforcement device reads the source SGT (denoting the Retail-Manager role, for example). It then evaluates the Retail-Manager's privileges to access the destination resource, which would also have an assigned SGT, such as PCI-Compliant Server or HR Database. It then determines whether the traffic should be allowed or denied.

If the enforcement device is a switch, it will apply security group ACLs (SG-ACLs). These are policies automatically downloaded from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control Server (ACS). SG-ACLs have the benefit of being processed at wire rate on many switch platforms. Because they are downloaded from ISE, they do not need to be provisioned to switches, as traditional Access Control Lists need to be.

If the enforcement device is a Cisco firewall, it will perform stateful firewall processing using the source and destination SGTs, as illustrated in Figure 2. The Cisco Adaptive Security Appliance (ASA) Software can also make additional inspection decisions based on the source and destination SGT values. For example, it can selectively pass traffic through additional intrusion prevention analysis or direct traffic to Cisco Cloud Web Security services based upon SGT values.

Figure 2. Firewall Rules Using Cisco TrustSec Security Groups



Cisco TrustSec Capabilities for Policy-Defined Segmentation

A Cisco TrustSec system provides:

- Simplified access management
  - Manages policies using plain language
  - Controls access to critical assets by business role
  - Maintains policy compliance
- Accelerated security operations
  - Quickly provisions access to new servers
  - Speeds up adds moves and changes
  - Automates firewall and ACL administration

- Consistent policy anywhere
  - Segments networks using central policy management
  - Enforces policy on wired and wireless networks
  - Scales to support branch office, campus and data center locations

Components That Support Cisco TrustSec Capabilities

Table 1 lists components that support Cisco TrustSec capabilities and features. This list is frequently enhanced, please refer to the Cisco TrustSec platform support matrix available at Cisco.com/go/trustsec for the latest information.

Table 1. Components supporting Cisco TrustSec Features

Type	Platform	Function	Version
Policy Server	Cisco ISE	Policy server for Cisco TrustSec classification and SG-ACL policy creation	Cisco ISE Release 1.2
Campus Switches	Cisco Catalyst® 2960-S and 2960-SFSeries Switches	Classification and transport (SXP only)	Cisco IOS® Software Release 15.0(2)SE2
	Cisco Catalyst 3560-E, 3560-Cand 3750-ESeries Switches	Classification and transport (SXP only)	Cisco IOS Software Release 15.0(2)SE2
	Cisco Catalyst 3560-X and 3750-X Series Switches	Classification, transport (SXP and inline SGT), and enforcement (SG-ACL)	Cisco IOS Software Release 15.0(2)SE4
	Cisco Catalyst 4500 Supervisor Engine 7-Eand7L-E	Classification and transport (SXP only)	Cisco IOS-XE Software Release 3.3.0SG
	Cisco Catalyst 4500 Supervisor Engine 6-E and 6L-E	Classification and transport (SXP only)	Cisco IOS Software Release 15.1(1)SG
	Cisco Catalyst 6500 Supervisor Engine 2T	Classification, transport (SXP and inline SGT), and enforcement (SG-ACL)	Cisco IOS Software Release 15.1(1)SY1
	Cisco Catalyst 6500 Supervisor Engine 720	Classification and transport (SXP only)	Cisco IOS Software Release 12.2(33)SXJ2
Data Center Switches	Cisco Nexus® 5500 platform and Cisco Nexus 2000 Series Fabric Extenders	Classification (port, port profile), transport (inline SGT), enforcement (SG-ACL)	Cisco NX-OS Software Release 5.1(3)N2(1c)
	Cisco Nexus 7000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders	Classification, transport (SXP and inline SGT), and enforcement (SG-ACL)	Cisco NX-OS Software Release 6.2
	Cisco Nexus 1000V Switch for VMware	Classification (port profile) and transport (SXP only)	Cisco NX-OS Software Release 4.2(1)SC2(1.1)
Routers	Cisco 2951and 3945Integrated Services Routers Generation 2 (ISR G2)	Classification (static IP-SGT), transport (SXPv4 and SGT over GETVPN), and enforcement (zone-based security group firewall)	Cisco IOS Software Release 15.3(2)T
	Cisco 800, 1900, 2900 and 3900 Series ISR G2	Classification (static IP-SGT), transport (SXPv4), and enforcement (zone-based security group firewall)	Cisco IOS Software Release 15.3(2)T
	Cisco ASR 1000 Series	Classification (static IP-SGT), transport (SXPv4 and SGT over GETVPN)and enforcement (zone-based security group firewall)	Cisco IOSXE Release 3.9

Type	Platform	Function	Version
Wireless	Cisco 5500 and 2500 Series Wireless Controllers (WLCs), Cisco Wireless Services Module 2 (WiSM2), and Cisco Wireless LAN Controller Module for Integrated Services Routers G2 (WLCM2) **Note:** Cisco 7500 and 8500 WLC and virtual WLC platforms do not support Cisco TrustSec functions.	Classification and transport (SXP only)	Cisco AireOS Wireless LAN Controller Software Release 7.4.110
Firewall	Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580, 5585-X, 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X	Transport (SXP only) and enforcement (security group firewall)	Cisco ASA Software Release 9.1
Cisco Connected Grid Devices	Cisco 2010 Connected Grid Router(CGR)	Classification (static IP-SGT), transport (SXPv4), and enforcement (zone-based security firewall)	Cisco IOS Software Release 15.3(2)T
Management	Cisco Security Manager	Security group firewall for Cisco ASA support	Cisco Security Manager 4.4

For More Information

Read more about Cisco TrustSec solutions, or contact your local account representative.

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.**

Printed in USA C22-591771-02 10/13