Cisco TrustSec

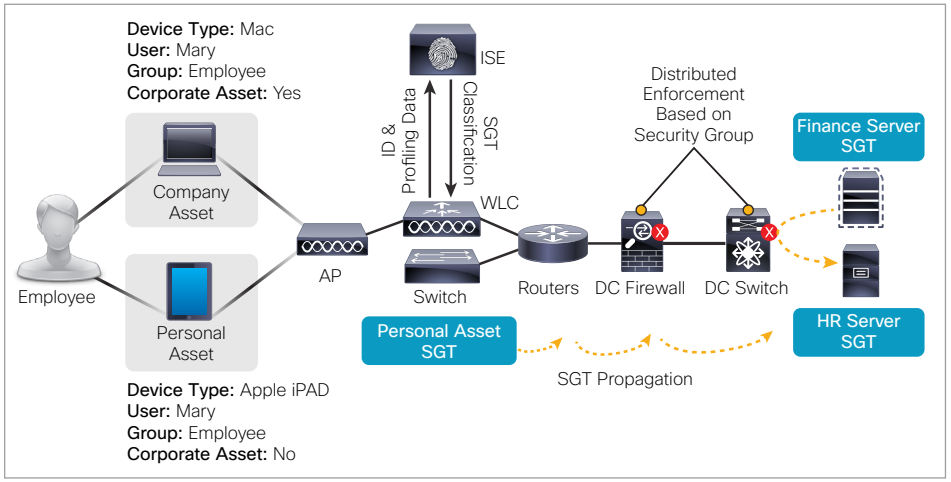
Cisco TrustSec® simplifies the provisioning and management of secure access to network services and applications. Unlike access control mechanisms that are based on network topology, Cisco TrustSec policies use logical groupings, so access is consistently maintained even as resources are moved in mobile and virtualized networks. Decoupling access entitlements from IP addresses and VLANs simplifies security policy maintenance tasks, lowers operational costs, and allows common access policies to be consistently applied to wired, wireless, and VPN access.

Introduction

Cisco TrustSec classification and policy enforcement functions are embedded in Cisco® switching, routing, wireless LAN, VPN and firewall products. By classifying traffic based on the identity of the endpoint instead of its IP address, Cisco TrustSec solutions provide more flexible access controls for dynamic networking environments and data centers.

At the point of network access, a logical tag called a Security Group Tag (SGT) is assigned to an endpoint, typically based on user, device and location attributes . The SGT denotes the endpoint's access entitlements and all traffic from the endpoint will carry the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions. Because SGT assignments can denote business roles and functions, Cisco TrustSec controls can be defined in terms of business needs and not the underlying networking detail (Figure 1).

Figure 1. How Security Group Tags Work



With Cisco TrustSec policies, a network administrator can implement extensive network segmentation and endpoint access controls without modifying the network topology (for example, by adding VLANs) rule administration. This capability greatly simplifies IT engineering and operations. Cisco TrustSec policies are centrally managed by the Cisco Identity Services Engine (ISE) with enforcement functions available in campus switches, data center switches, firewalls, and routers.

Business Benefits

Reduces Operational Expenses

Firewall and access control rules can be defined based on asset or application roles. The management of those rules is automated, saving significant operational effort and time.

Allows Secure, "Any Device" Access to Resources

Organizations gain visibility into, and effective control over, unmanaged mobile devices that access their networks. Flexible and scalable controls in network devices manage access to resources based on attributes such as user role, location, device type, and posture.

Provides Dynamic Campus Segmentation

Unlike traditional campus network segmentation techniques, Cisco TrustSec technology provides a scalable, agile and efficient means to enforce security policies in today's highly dynamic environments.

Caters for Changing Workforces and Business Relationships

Controlling access to resources for mobile users, contractors, partners, and guests has become operationally intensive and technically challenging for many enterprises. Instead of defining rules based on how someone connects to the network, Cisco TrustSec access controls are defined by business roles and may be used anywhere on the network.

Enforces Consistent Policies

Cisco TrustSec policies can be applied to wired, WLAN, and remote access VPN connectivity.

Using Cisco TrustSec

Campus Network Segmentation

Typical Situation

In enterprise campus networks, user groups are commonly assigned to appropriate VLANs to isolate them. Each VLAN requires address space and provisioning. Mapping it to an upstream routed network interface may need static access control lists (ACLs) or Virtual Routing and Forwarding (VRF) functions to maintain its isolation.

If some interaction between user segments is desirable or if shared services are delivered to multiple user groups, controlled interactions tend to be defined in static switch and router configurations, which can become complicated. Moreover, controlling communications within a VLAN or segment is difficult to enforce.

Cisco TrustSec Solution

Using SGTs to describe permissions on the network allows the interaction of systems to be determined by SGT values. This process avoids the need for additional VLAN provisioning and configuration tasks, so that the access network design is kept simple even as the number of roles grows. Interaction between user groups may be denied entirely, or controlled interaction can be allowed on specific ports and protocols.

Cisco TrustSec Security Group ACLs (SGACLs) can also block unwanted traffic between users in the same role, so that malicious reconnaissance activities and malware propagation can be effectively prevented.

Access Controls for Wired, WLAN and Remote Access VPN Connectivity

Typical Situation

IP-address-based access control lists (ACLs) are simple to deploy, given an understanding of the network design and the specific assets that need to be protected. They require ongoing management, but for simple role structures this is not problematic. However, as the number of access roles increases, it can become difficult to manage these ACLs and make sure that they will not exceed the memory and processing capabilities of the network access device applying them.

Cisco TrustSec Solution

Cisco TrustSec solutions use SGACLs for role-based access control. These lists contain source and destination roles and Layer 4 services (ports). You don't need to maintain IP addresses in these ACLs, so they are simple to maintain as the environment grows.

SGACLs are dynamically downloaded from Cisco ISE as required by the network device, so changes to SGACLs do not need to be provisioned on the network.

On many Cisco platforms, the SG-ACL enforcement functions operate at line rate, allowing ACLs to be implemented at 10, 40, and even 100 Gbps.

Firewall Rule Automation

Typical Situation

Organizations are accustomed to defining access to protected assets based on the IP address of the asset. This process often results in large firewall rule tables, which are difficult to understand and manage. Virtualized data centers may comprise growing numbers of logical servers to protect, and changes to such servers for workload management are frequent.

Cisco TrustSec Solution

Cisco TrustSec firewall rules can be written using server roles and not the IP addresses of the individual servers. This simplifies the policies and makes them easier to understand, administer and audit.

For virtualized data centers, Cisco TrustSec functions embedded in the Cisco Nexus® 1000V switching platform allow server roles to be marked in a provisioning profile and role assignment to be automatically shared with Cisco firewalls. As more workloads are deployed for a given profile, or as the workloads move, the firewalls will be immediately updated with group membership information.

For new servers being mapped to existing roles, no changes to the firewall rule table should be needed (Figure 2).

Figure 2. Cisco TrustSec Firewall Rule Table

#	Enabled	Source Criteria: Source	Source Criteria: User	Source Criteria: Security Group	Destination Criteria: Destination	Destination Criteria: Security Group	Service	Action
inside (1 incoming rule)								
1	☑	any			any		ip	Permit
outside (9 incoming rules)								
1	☑	any		Unregist_Dev_SGT Employee_SGT Management_SGT	any	Web_Servers	http https	Permit
2	☑	any		CC_Scanner_SGT	any	Web_Servers	http https	Deny
3	☑	any		Employee_SGT Management_SGT	any	Employee_Portal	http https	Permit
4	☑	any		Unregist_Dev_SGT CC_Scanner_SGT	any	Employee_Portal	http https	Deny
5	☑	any		Management_SGT	any	Manager_Portal	50002 3389 http https sqlnet	Permit

Highly Secure "Any Device" Access

Cisco TrustSec technology can use the extensive profiling, posture validation, and mobile device management integration functions of Cisco ISE to classify user devices. Extensive controls can be implemented across the network, or specifically in firewalls if preferred, that take account of the contextual classification from Cisco ISE.

Summary of Benefits

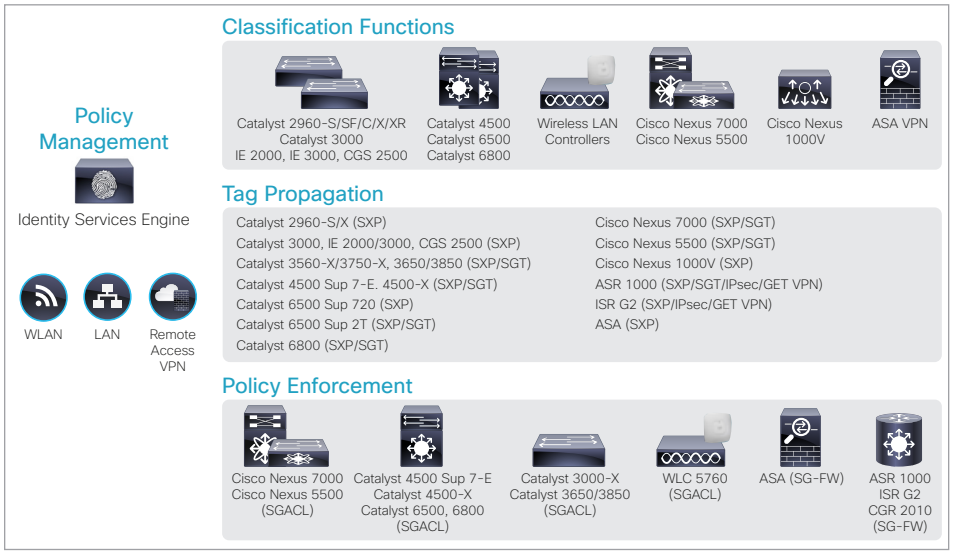
- Simplified policy determined by business context
  - Uses meaningful business language, not networking detail
  - Is based on groups that do not change when resources are moved
  - Returns policy administration to the security team
- Enhanced security and reduced complexity
  - Reduces traffic engineering and improves data center performance
  - Provides highly scalable line-rate marking and policy enforcement on capable devices
  - Avoids the complexity of other segmentation methods, such as VLANs
- Lower operational costs
  - Automates firewall and access control administration
  - Reduces ACL maintenance, complexity, and overhead
  - Automates adds, moves and changes

Cisco TrustSec Solution Components

Figure 3 shows the various solution components involved in a Cisco TrustSec system. They comprise the following:

- Cisco Catalyst® 2960-S/SF/C/X/XR, 3560, 3560-E/C, 3750, 3750-E Series: SGT Exchange Protocol (SXP) only
- Cisco Catalyst 3650, 3850, 3560-X, and 3750-X Series: SXP, SGT, SGACL
- Cisco Catalyst 4500 Series with Supervisor 7(L)-E: SXP, SGT and SGACL
- Cisco Catalyst 4500-X: SXP, SGT and SGACL
- Cisco Catalyst 6500 Series with Supervisor Engine 2T: SXP, SGT, SGACL
- Cisco Catalyst 6800 Series: SXP, SGT, SGACL
- Cisco Nexus 7000 and 5500: SXP, SGT, SGACL
- Cisco Nexus 1000V: SXP only
- Cisco Industrial Ethernet 2000 and 3000 Series Switches: SXP only
- Cisco 2500 Series Connected Grid Switches: SXP only
- Cisco Wireless LAN Controller 2500, 5500, Cisco Wireless Service Module (WiSM2), Cisco Wireless Controller on Cisco Services-Ready Engine (SRE): SXP only
- Cisco Wireless LAN Controller 5760
- Cisco Integrated Services Router G2: SXP, SGT, and Security Group Firewall (SG-FW)
- Cisco ASR 1000 Series Aggregation Services Routers: SXP, SGT, and SG-FW
- Cisco 2010 Connected Grid Router: SXP, SGT, and SG-FW
- Cisco ASA 5500 and 5500-X Series Firewalls: SXP, SG-FW
- Cisco ASA Services Module: SXP, SG-FW
- Cisco Identity Services Engine

Figure 3. Cisco TrustSec Solution Components



For More Information

www.cisco.com/go/trustsec

C45-577269-01 04/14