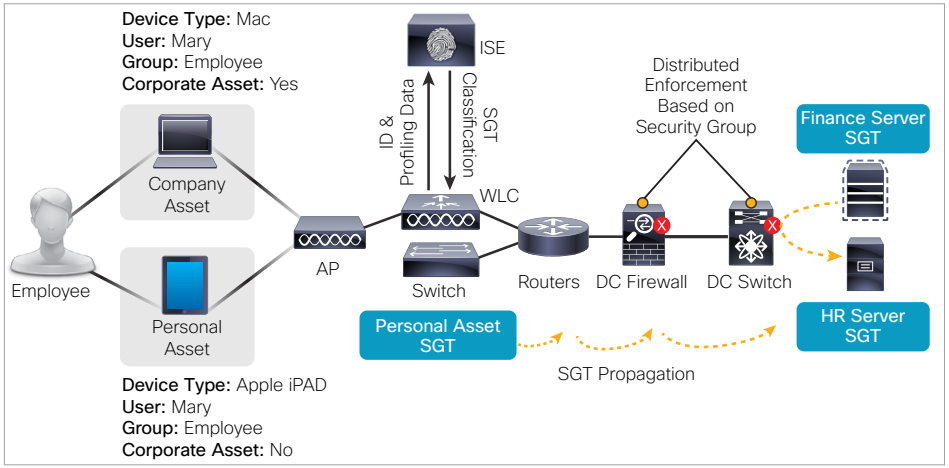
Cisco TrustSec

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

Introduction

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

At the point of network access, a Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint's 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 underlying networking detail (Figure 1).



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

Business Issues Addressed

Reduces Operational Expenses

Virtual footprints allow flexible and elastic operation. Cisco TrustSec allows firewall and access control rules to be defined by an asset or application's role, and automates management of those rules, saving significant operational effort and time.

Allows Secure, "Any Device" Access to Resources

To help organizations gain visibility into, and effective control over, unmanaged mobile devices accessing their networks, Cisco TrustSec provides flexible and high-performance controls in network devices to control access to resources based upon attributes such as user role, location, device type, and posture.

Dynamic Campus Segmentation

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

Caters for Changing Workforces and Business Relationships

Users are more mobile and businesses are more collaborative. Allowing controlled access to resources for mobile users, contractors, partners, and guests has become operationally intensive and technically challenging for many enterprises.

Using Cisco TrustSec

Campus Network Segmentation

Typical Situation

For user access in enterprise campus networks, it is common to map different user groups into appropriate VLANs to provide complete isolation between groups. Each VLAN requires address space and provisioning, and needs to be mapped to an upstream routed network interface, which may need to use static access control lists (ACLs) or virtual routing and forwarding (VRF) functions to maintain the isolation.

If some interaction between user segments is desirable or 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 communication within a VLAN or segment is difficult to enforce.

Cisco TrustSec Solution

Using a Cisco TrustSec role or SGT as the means to describe permissions on the network allows the interaction of different systems to be determined by comparing SGT values. This avoids the need for additional VLAN provisioning, keeping the access network design simple and avoiding VLAN proliferation and configuration tasks required as the number of roles grows. Interaction between user groups may be denied, or controlled interaction on specific ports and protocols can be allowed. This provides a much simpler and more flexible approach to managing security policies.

Cisco TrustSec SG-ACLs can also block unwanted traffic between users of the same role, so that malicious reconnaissance activities and even remote exploitation from malware can be effectively prevented.

Access Controls

Typical Situation

IP-address-based 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 not only manage these ACLs, but also ensure that downloaded ACLs will not exceed the memory and processing capabilities of any given network access device applying them.

Cisco TrustSec Solution

Cisco TrustSec uses secure group ACLs (SG-ACL) 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, even as the environment grows.

SG-ACLs are dynamically downloaded from Cisco ISE as required by the network device, so changes to SG-ACLs 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 10G, 40G, and even 100G.

Firewall Rule Automation

Typical Situation

Organizations are accustomed to defining access to protected assets based on the IP address of the asset. This often results in large firewall rule tables, which are difficult to understand and manage. In virtualized data centers, there may be growing numbers of logical servers to protect, and changes to them are more frequent for workload management and movement reasons.

Cisco TrustSec Solution

With Cisco TrustSec, firewall rules can be written using server roles and not the IP address of the individual asset. 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 virtual switching platform allow the role assignment of servers to be marked in a provisioning profile and automatically shared with Cisco firewalls. As more workloads are deployed for a given profile, or as the workloads move, the firewalls will be updated with group membership information immediately.

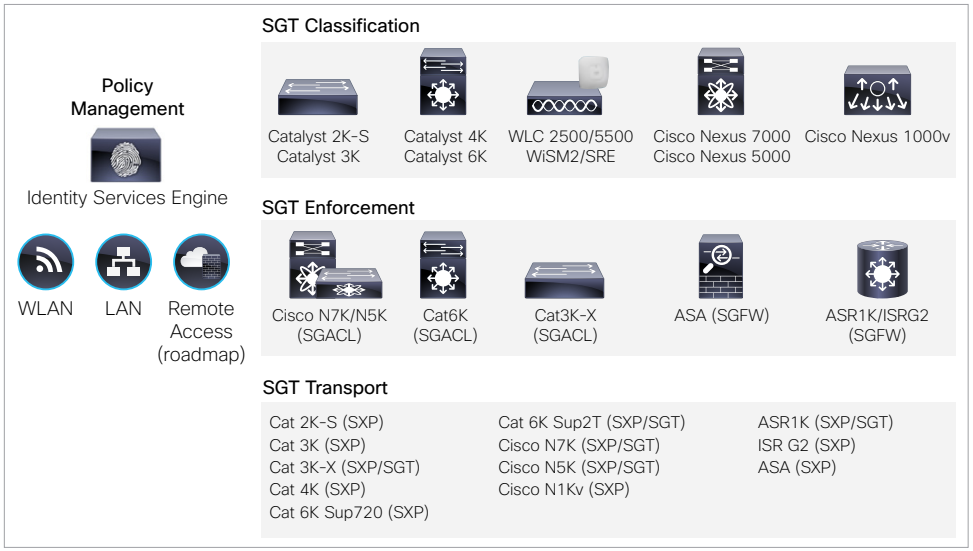
For new servers being mapped into existing roles, no changes to the firewall rule table should be needed (Figure 2).

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

Secure BYOD or "Any Device" Access

Cisco TrustSec can use the extensive ISE profiling, posture validation, and mobile device management integration functions as part of the classification process. Cisco TrustSec can provide extensive controls implemented across the network, or specifically in firewall functions if preferred, that take account of the contextual classification from ISE.



Summary of Benefits

- Simplified policy using business context
  - Based on meaningful business language, not networking detail
  - Based on groups that do not change when resources are moved
  - Returns policy administration to the security team
- Enhanced security and reduced complexity
  - Simplified design reduces traffic engineering and improves data center performance
  - Highly scalable line-rate marking and policy enforcement on capable devices
  - Less network complexity than other segmentation methods, such as VLANs
- Reduced operational expense
  - Automated firewall and access control administration
  - Reduction in ACL maintenance, complexity, and overhead
  - Increased agility from automating adds, moves, and changes

Cisco TrustSec and Secure Access Solution Components

- FlexAuth (802.1X, WebAuth, MAB): All Cisco Catalyst® switching platforms
- Device sensors: Cisco Catalyst 3000 Series; Cisco Catalyst 4500 Series with Supervisor 7(L)-E; Cisco Wireless LAN Controllers
- Cisco TrustSec:
  - Cisco Catalyst 2960-S/SF/C, 3560, 3560-E/C, 3750, 3750-E Series: SXP only
  - Cisco Catalyst 3560-X, 3750-X Series: SXP, SGT, SGACL
  - Cisco Catalyst 4500 Series with Supervisor 6(L)-E, 7(L)-E: SXP only
  - Cisco Catalyst 6500 with Supervisor Engine 2T: SXP, SGT, SGACL
  - Cisco Nexus 7000 and 5000 Series: SXP, SGT, SGACL
  - Cisco Nexus 1000v: SXP only
  - Cisco Wireless LAN Controller 2500, 5500, Cisco Wireless Service Module (WiSM) 2, Cisco Wireless Controller on Cisco Services-Ready Engine (SRE): SXP only
  - Cisco Integrated Services Router G2: SXP, Security Group Firewall (SG-FW)
  - Cisco ASR 1000 Series Aggregation Services Router: SXP, SG-FW
  - Cisco ASA 5500 Series Adaptive Security Appliances: SXP, SG-FW
  - Virtual Desktop Infrastructure (VDI) and Cisco AnyConnect® Secure Mobility Client with Remote Desktop Protocol (RDP)

For More Information

www.cisco.com/go/trustsec

C45-726831-00 02/13