Cisco TrustSec for Policy-Defined Segmentation

Taking Complexity Out of Network Security

Cisco TrustSec® simplifies the provisioning and management of secure network access, accelerates security operations and consistently enforces policy anywhere in the network. Unlike access control mechanisms which are based on network topology, Cisco TrustSec controls are defined using logical policy groupings, so resource segmentation and secure access are consistently maintained, even as resources move in mobile and virtualized networks.

Cisco TrustSec functions are embedded in Cisco® switching, routing, wireless LAN, and firewall products to protect assets and applications in enterprise and data center networks.

Policy-Defined Segmentation

Traditional access control methods segment and protect assets using VLANs and access control lists (ACLs). Cisco TrustSec instead uses security group policies which are written in a plain language matrix (Figure 1) and decoupled from IP addresses and VLANs. Users and assets with the same role classification are assigned to a security group.

Cisco TrustSec policies are centrally created and automatically distributed to wired, wireless and VPN networks so that users and assets receive consistent access and protection as they move in virtual and mobile networks. This helps reduce the time spent on network engineering tasks and compliance validation.

Figure 1. Cisco TrustSec Policy Management Matrix Example

Source \ Destination	Employee	E-Mail	Finance	Internet
Employee	Deny	Permit	Deny	Permit
Executive	Deny	Deny	Permit	Permit
BYOD	Deny	Permit	Deny	Permit
Guest	Permit	Deny	Deny	Permit

How Cisco TrustSec Helps

Cisco TrustSec simplifies repetitive and time-consuming network engineering tasks for both network and security operations, including VLAN, ACL and firewall rule engineering and administration. This helps IT optimize their time while improving the security posture of their organization.

Simplified Access Management

Creating and managing policies in a simple matrix using plain business language makes it easier to manage access control and segmentation across the enterprise. In addition, Cisco TrustSec makes it easy to control access to critical assets by their business role, which could denote user groups such as contractors, accountants or sales executives, or server roles such as HR databases or CRM systems.

Accelerated Security Operations

Cisco TrustSec simplifies management and engineering, saving IT organizations time and helping them keep up with the pace of business change. Newly provisioned servers can be onboarded in minutes; moves, adds and changes that require IT support can be done quickly; firewall rule and ACL management can also be automated.

Consistent Policy Anywhere

Cisco TrustSec consistently enforces policy anywhere in the network, ensuring that assets are protected and that users have unobstructed access to their resources. A central policy manager applies policies across wired, wireless, and VPN topologies. While traditional segmentation methods are difficult to extend across an enterprise, Cisco TrustSec is designed to scale for operations of any size, which may encompass mobile users, branches, campuses and data centers.

Using Cisco TrustSec

Campus Network Segmentation

Typical Situation

In enterprise campus networks it is common to segment different user groups into VLANs. Each VLAN requires address space and must be mapped to an upstream routed network interface, which may need to use static ACLs or virtual routing and forwarding (VRF) functions to maintain the isolation.

Controlled interactions between user groups tend to be defined in static switch and router configurations, which can become complicated. Moreover, controlling communication within a VLAN or segment is difficult.

Cisco TrustSec Solution

Cisco TrustSec uses security group tags (SGTs) to describe permissions on the network. The interaction of different systems are determined by security-group-based policies; this eliminates the need for additional VLAN provisioning, keepd the access network design simple and avoids VLAN proliferation. Interaction between user groups can be denied, or controlled interaction on specific ports and protocols can be allowed.

Cisco TrustSec security group ACLs (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 prevented.

Access Controls

Typical Situation

IP-address-based ACLs are simple to deploy, but require ongoing management. This may not be problematic for simple role structures, however, as the number of access roles increases it can become difficult to manage the required ACLs. Care may also be needed to 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 SG-ACLs for role-based access control. These lists contain source and destination roles and Layer 4 services (ports) that are easy to maintain because they don't contain IP addresses. SG-ACLs are dynamically downloaded from the Cisco Identity Services Engine (ISE) by the network device, which means that any changes to SG-ACLs do not need to be provisioned on those devices. SG-ACL enforcement functions run at line rate on many Cisco devices, so ACLs can operate at 10G, 40G, and even 100G.

Firewall Rule Automation

Typical Situation

Controlling access based on an asset's IP address 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 can be frequent.

Cisco TrustSec Solution

With Cisco TrustSec, firewall rules can be written using server roles instead of server IP addresses. This simplifies the policies and makes them easier to manage and audit.

In virtualized data centers, Cisco TrustSec functions in Cisco Nexus® 1000V virtual switching platforms 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 are updated with group membership information immediately. For new servers being mapped into existing roles, no changes to the firewall rule table are needed (Figure 2).

Figure 2. Cisco TrustSec-Based Rules in Cisco Security Manager

Secure BYOD or “Any Device” Access

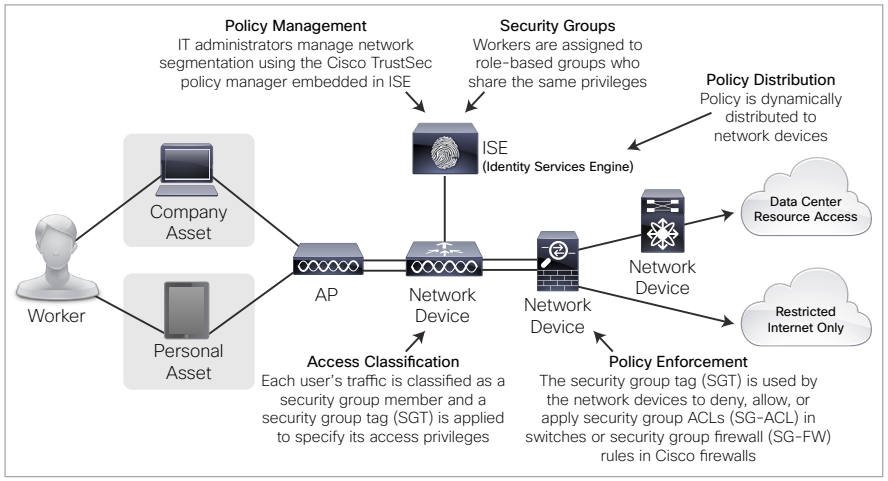
Typical Situation

BYOD access policies are typically applied using IP-based access control lists to control how authorized users access resources. IP-ACL management can become an administrative burden because of the frequent maintenance they tend to require.

Cisco TrustSec Solution

In a Cisco TrustSec design, the extensive ISE profiling, posture validation and mobile device management integration capabilities can be used as part of the BYOD classification process. Cisco TrustSec–capable switches and firewalls then take account of the BYOD classification and enforce policy based upon it. This approach provides not only very high-performance access control but also results in a very simple way to define access policies with significantly less management effort.

Figure 3. Cisco TrustSec in Operation



Cisco TrustSec Solution Components

Cisco TrustSec Supported Network Devices

- Cisco Catalyst 2960-S/SF/C, 3560-E/C, 3750-E Series: SXP only
- Cisco Catalyst 3560-X, 3750-X Series: SXP, SGT, SG-ACL
- Cisco Catalyst 4500 Series with Supervisor 6(L)-E, 7(L)-E: SXP only
- Cisco Catalyst 6500 Series with Supervisor Engine 2T: SXP, SGT, SG-ACL
- Cisco Nexus 7000 and 5000 Series: SXP, SGT, SG-ACL
- Cisco Nexus 1000v Series: SXP only
- Cisco Wireless LAN Controller 2500 and 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 and 5500-X Series Next-Generation Firewalls: SXP, SG-FW
- Virtual Desktop Infrastructure (VDI)
- Cisco AnyConnect® Secure Mobility Client with Remote Desktop Protocol (RDP)

Policy Management

- Cisco Identity Services Engine: Advanced License
- Cisco Secure ACS with Security Group Access System License
- Cisco Security Manager 4.4

C45-653057-04 09/13