At-a-Glance

Cisco TrustSec

Simplify Access Control without Network Redesign

Business demand for cloud services, mobility, and the Internet of Things (IoT) has created exponential network growth and complexity. It has introduced risk, too. Each new user, device, and data connection represents a potential attack entry point. So your attack surface is expanding.

But you can control the situation with Cisco TrustSec. Embedded in your existing Cisco network infrastructure, the TrustSec security solution simplifies the provisioning and management of network access control. It uses software-defined segmentation to classify network traffic and enforce policies for more flexible access controls. Traffic classification is based on endpoint identity, not IP address, enabling policy change without network redesign.

TrustSec is powered by the Cisco Identity Services Engine. The centralized policy management platform gathers advanced contextual data about who and what is accessing your network. It then uses security group tags to define roles and access rights and pushes the associated policy to your TrustSec-enabled network devices, such as switches, routers, and security equipment.

You get better visibility through richer contextual information, are better able to detect threats, and accelerate remediation. So you can reduce the impact and costs associated with a potential breach.

How It Works

Traditional network segmentation approaches use IP-address-based access control lists (ACLs), VLAN segmentation, and firewall policies that require extensive manual maintenance. Cisco TrustSec simplifies the effort by dynamically grouping machines into objects, called security groups, and provisioning security policies between those objects.

The interaction of systems is determined by the security-group-based policies, eliminating the need for VLAN or address-based policy provisioning. TrustSec is available in virtual and physical switches and treats virtual and physical workloads across the campus and data center consistently.

> "Effective network segmentation… reduces the extent to which an adversary can move across the network."
>
> **US Department of Homeland Security**
> United States Computer Emergency Readiness Team

Next Steps

For more information about the Cisco TrustSec solution, contact your local account representative or visit http://www.cisco.com/go/trustsec.

Benefits

- **Quickly isolate and contain threats** using technology already in your network.
- **Limit the impact of data breaches** by dynamically segmenting your network.
- **Centrally apply and enforce granular and consistent policies** across wired, wireless, and remote-access users and devices.
- **Reduce operational expenses** by defining firewall and access control rules based on asset or application context.
- **Easily provide dynamic campus segmentation** to enforce security policies in quickly changing environments without provisioning and maintaining access control lists.
- **Cater to changing workforces and business relationships** by defining security groups based on business roles, not IP addresses.

C45-577269-02 06/15