Cisco TrustSec

A Foundational Component to Secure Borderless Networks

At-A-Glance

Address Customer Challenges

Physical boundaries are disappearing. Customers need to support a mobile workforce, manage outsourcing, and respond to IT consumerization. In addition, the threat environment demands more effective protection for business infrastructure and valuable information assets. Finally, regulatory and industry mandates impose strict requirements for many organizations. As a foundational component to secure Borderless Networks, the Cisco® TrustSec solution helps customers enable secure collaboration, strengthen security, and address compliance requirements.

Key Functions

Cisco TrustSec comprehensively secures networks and access to business-critical resources by establishing visibility and controls that apply to all users and discovering and monitoring IP-enabled devices. It does this through policy-based access control, identity-aware networking, and data confidentiality and integrity protection in the network.

Policy-based access control: Cisco TrustSec provides network access controls based on a consistent policy for users (such as employees, contractors, or guests), end point devices (laptops, IP phones, printers) and networking devices (switches, routers, and so on). Cisco TrustSec has the ability to control how a user or a device can be granted access, what security policies endpoint devices must meet, such as posture compliance, and what network resources a user is authorized to use in the network.

Identity-aware networking: Cisco TrustSec uses end user and device identity information as well as additional factors (such as time, location and user's role in the organization) to provide precise security policy controls. TrustSec also delivers further role-based networking services including support for Cisco Medianet and quality of service for business-critical applications associated with users in specific roles.

Data integrity and confidentiality: Cisco TrustSec secures data paths in the switching environment with IEEE 802.1AE standard encryption. Data confidentiality and integrity is instantiated between devices at the switch port level on a hop by hop basis. Cisco switching infrastructure maintains controls so that critical security applications such as firewalls, intrusion prevention, and content inspection can retain visibility into data streams.

Benefits

Enables secure collaboration: Cisco TrustSec dynamically assigns access and services for users and devices to support a dynamic workforce. The consistency, efficiency, and role-aware networking capabilities delivered by TrustSec enable a secure collaborative business environment and a seamless user experience.

Strengthen security: Cisco TrustSec secures access to the network and resources, whether wired, wireless, or VPN, ensuring that endpoint devices are authorized and healthy. TrustSec enforces security policies across the entire network. Furthermore, TrustSec protects network data confidentiality and integrity with switch port level encryption.

Address compliance: Cisco TrustSec helps address compliance requirements by knowing who's coming to the network, what they are doing on the network, and what type of resources they are allowed to access. Customers can use the information and capabilities for controls, auditing, and reporting as part of their effort to meet compliance requirements.

Product Portfolio

Cisco TrustSec includes three product component groups: infrastructure, policy, and endpoint.

Infrastructure components: Cisco Catalyst® Series 2900/3560/3700/4500/6500 switches and Cisco Nexus™ 7000 switches interact with network users for authentication and authorization. Access to the network is dictated by policy, user identity, and other attributes. Flexible authentication methods include 802.1X, web authentication, and MAC authentication bypass, all controlled in a single configuration for each switch port. Furthermore, Cisco switches can tag each data packet with user identity information so that further controls can be deployed anywhere in the network. In addition, Cisco Nexus switches support MACSec (IEEE 802.1AE standard encryption) today for data-in-motion confidentiality and integrity protection.

Policy components: Cisco Secure Access Control System (ACS) is a simple and yet powerful policy server for centralized network identity and access control. Cisco Secure ACS features a rule-based policy model and a new, intuitive management interface designed for optimum control and visibility. The latest Cisco Secure ACS also helps IT administrators quickly identify potential problems with comprehensive monitoring and troubleshooting capabilities.

Cisco TrustSec

A Foundational Component to Secure Borderless Networks

Cisco Network Admission Control (NAC) Manager is the policy and management center for an appliance-based NAC deployment environment to define role-based user access and endpoint security policies.

Cisco NAC Server assesses and enforces security policy compliance in an appliance-based NAC deployment environment.

Cisco NAC Profiler helps in deploying policy-based access control by providing discovery, profiling, policy-based placement, and post-connection monitoring of all endpoint devices.

Cisco NAC Guest Server manages guest network access, including provisioning, notification, management, and reporting of all guest user accounts and network activities.

Endpoint components: Cisco Secure Services Client (SSC) helps customers deploy a single authentication system to access both wired and wireless networks. It provides 802.1X user and device authentication and manages user and device identity and the network-access protocols for secure access. Cisco NAC Agent is an optional lightweight agent running on an endpoint device. It performs deep inspection of the device's security profile by analyzing registry settings, services, and files. In addition to the above two endpoint clients that support standard devices, Cisco IP Phones have advanced built-in client capabilities to integrate with the Cisco TrustSec solution.

Professional Services for TrustSec

Intelligent, personalized professional services from Cisco and our partners provide policy review, analysis, and design expertise to prepare the network to deploy a TrustSec solution. Cisco services use best practices to help organizations more quickly and cost-effectively deploy a full authentication and access solution while also providing knowledge transfer for ongoing operational efficiency.

Use Cases

Deployment option 1: 802.1X-based deployment

In this scenario, Cisco Secure ACS is the policy server to authenticate users who connect to the wired network. A Network Access Device (switch) provides access to the network and resources based on user credentials (collected by Cisco SSC) and their roles in the organization. Additional protection such as Security Group Tagging and Security Group ACLs can be applied for finer controls. Cisco NAC Profiler and Cisco NAC Guest Server can also be deployed with the 802.1X solution.

Deployment option 2: Appliance-based deployment

With an appliance-based approach, Cisco NAC Manager is the policy server that works with Cisco NAC Server to authenticate users and assess their devices over LAN, wireless, or VPN connections. Access to the network and resources is based on user credentials and their roles in the organization, as well as the policy compliance of endpoint devices.

TrustSec Innovations

TrustSec delivers many Cisco innovations. 802.1X monitoring and low-impact modes allow controlled and fully configurable network access prior to authentication for enhanced visibility, more flexible deployments, and improved operational support. Cisco NAC Profiler, Guest Server, and IP telephony integration with Cisco switching in a 802.1X environment dramatically improve IT and employee productivity. Security Group ACLs simplify security policy management by assigning security group membership to end users and appropriate resource permissions, instead of ACLs based on IP addresses. TrustSec delivers advanced security technologies such as 802.1X-REV and MACSec to customers.

Why Cisco?

Cisco TrustSec is a comprehensive solution that is flexible, user-friendly and efficient to deploy. It builds security into the infrastructure to support managed, unmanaged, and unknown assets as well as employees, guests, and contractors.

Cisco networks protected by TrustSec provide complete visibility and control. Trustsec improves network resiliency, consistency, and scalability.

Cisco and its partners deliver professional services to help customers meet their unique compliance and security needs.

For more information, please visit http://www.cisco.com/go/trustsec.

C45-577269-00 01/10