



Cisco TrustSec Solution Overview

Contents

Introduction	3
Solution Overview	3
Architecture	5
Solution Components	7
Capabilities	9
Benefits	10
Summary	10

Introduction

The traditional desktop is no longer relevant. Customer networks must support all kinds of devices, such as personal mobile devices, or legacy devices with no users connected to them. With so many devices connecting to the enterprise network, customers need a solution that helps them to ensure that they're meeting their security policies when these devices use the network.

From a data center standpoint, applications are on the move. Customers used to think about securing their applications using access control lists (ACLs); in a virtualized data center, however, applications move between data centers via virtual machines (VMs). Customers need to think differently about how to secure their networks. As their applications are moving through the data center, they need an infrastructure that is as dynamic as the applications.

Solution Overview

Cisco TrustSec[®] is an intelligent access control solution. With minimal effort Cisco TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, as well as exceptional control over what and where they can go.

Whether you need to support employees bringing personal devices to work or you want to secure access to your data center resources, Cisco TrustSec provides a policy-based platform that offers integrated posture, profiling, and guest services to make context-aware access control decisions. Cisco TrustSec builds on an existing identity-aware infrastructure by enforcing these policies in a scalable manner; at the same time, it helps to ensure complete data confidentiality by providing ubiquitous encryption between network devices. A unique, single-policy platform that uses your existing infrastructure helps ensure highly effective management.

Although it is able to support any network, Cisco TrustSec offers a superior experience on a Cisco[®] infrastructure, using infrastructure-embedded features such as device sensors for visibility, security group access for access enforcement, and MAC Security (MACsec) encryption for data integrity.

Cisco TrustSec is a core component of the Cisco SecureX Architecture[™] for Cisco Borderless Networks. Its three key functional areas are visibility, control, and management.

Comprehensive Visibility

The differentiated identity features, next-generation network-based device sensors, and active endpoint scanning in Cisco TrustSec provide contextualized visibility of the “who, how, what, and when” for users and devices accessing the network, whether through wired, wireless, or remote connections. Because Cisco TrustSec provides comprehensive visibility into the broadest range of devices (whether smartphones, tablets, PCs, or even gaming devices), it lays a strong foundation for a Bring Your Own Device (BYOD) solution. This visibility is set to grow even further with planned integration with the leading mobile device management (MDM) solutions providing unprecedented visibility and control over mobile devices based on company-defined policies. **Available in the second half of CY12.**

Exceptional Control

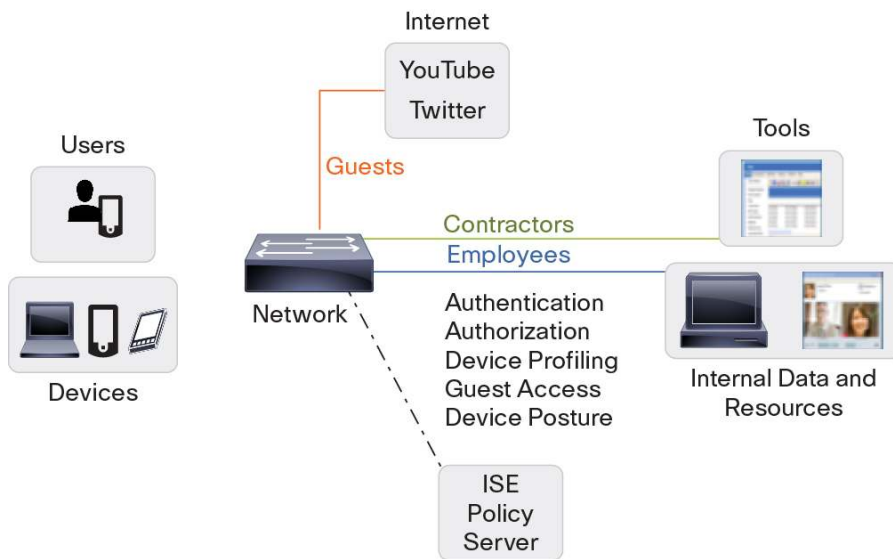
A centralized policy and enforcement platform enables coordinated policy creation and consistent context-based policy enforcement across the entire corporate infrastructure. Noncompliant devices can be quarantined, remediated, or given restricted access with scalable and flexible next-generation enforcement mechanisms using existing identity-aware infrastructure. Cisco TrustSec helps to ensure secure access for devices via automated endpoint security configuration for the most common PC and mobile platforms.

Effective Management

Cisco TrustSec combines authentication, authorization, and accounting (AAA), posture, profiler, and guest management functions in a single, unified appliance, leading to simplified deployments and a single point of management. All of this results in lower total cost of ownership.

Figure 1 illustrates how Cisco TrustSec delivers these functions using a Cisco Identity Service Engine (ISE) server.

Figure 1. How Cisco TrustSec Works



Users and devices accessing wired, wireless, or remote networks are authenticated with a flexible access control mechanism that supports different user roles, device types, operating systems, and access methods.

(Authentication methods are discussed in the [Architecture section](#) of this paper.)

User identity can be mapped to roles using standard directory services or additional identity services. Depending on whether the users are employees, contractors, visiting guests, or members of other user groups, the security policy will dictate the appropriate network access to allow users to reach their network data, tools, and resources. Posture assessment of endpoint devices (such as printers and IP phones) is part of the policy-based access control process that helps ensure that the end device is compliant with the organization's security policies. The device assessment process also includes networking devices (such as switches, routers, and wireless access points). Cisco TrustSec authenticates these networking devices before they become part of the network. Cisco TrustSec supports many access methods transparently, including local LAN, branch offices, wireless, and remote access.

After users gain the initial network access, their identity information can be captured and associated with their subsequent network activities in a switching environment through Cisco Security Group Access technology (see the [Architecture section](#) for more details). Such identity information can be used in other parts of the network, where an access control policy enforcement decision can be implemented. Identity-aware networks carry user role information to these points so that a single access authentication event provides identity information to all policy enforcement points, including destinations where resources such as shared files, databases, and system

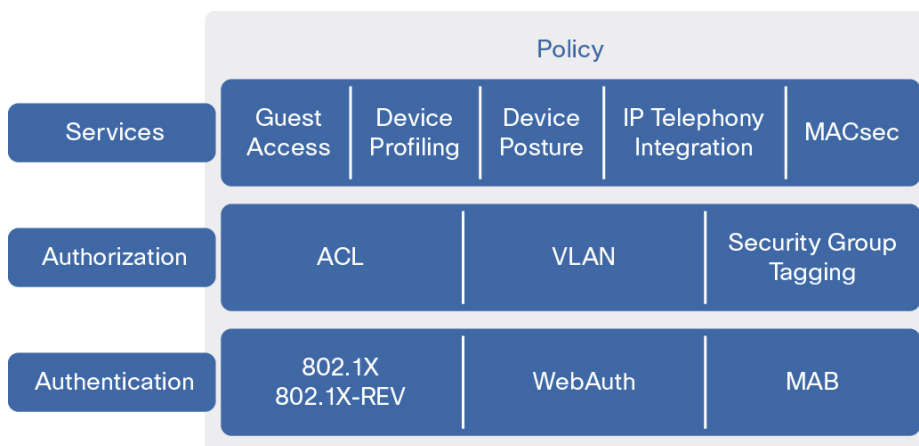
applications reside. Identity-aware networks go beyond just security policies and are able to provide identity-based quality of service to support business-critical applications for users with specific needs.

Cisco TrustSec provides the ability to secure a data path in a switching environment with switch port level encryption. The built-in Layer 2 encryption capability helps protect data confidentiality and integrity over the LAN. It relieves IT staff of the burden of retrofitting and encrypting at the application layer for all their applications in a high-security environment.

Architecture

As Figure 2 shows, the Cisco TrustSec solution architecture consists of authentication, authorization, and services modules. In addition, Cisco TrustSec provides a comprehensive policy framework.

Figure 2. Cisco TrustSec Solution Architecture



Authentication

Cisco TrustSec provides a group of flexible authentication (FlexAuth) methods, including IEEE 802.1X, web authentication (WebAuth), and MAC authentication bypass (MAB). Cisco TrustSec delivers the latest 802.1X technologies to reduce the operational overhead associated with deploying IEEE 802.1X in primarily wired environments. Some of the latest Cisco technology advances include a single switch port configuration that can accommodate all potential types of hosts, as well as managed, unmanaged, known, and unknown users. FlexAuth allows IT administrators to configure a single switch port with a consistent configuration that enables 802.1X, MAB, and WebAuth in any sequence to accommodate desired authentication requirements. Cisco Open Mode technology provides IT administrators with the flexibility to selectively open, or pinhole, certain traffic types through the restricted 802.1X-enabled port. The most common use for this technology is to enable host management operations to function normally in an identity-based access control port implementation. Protocols such as Preboot Execution Environment (PXE), Short Message Service (SMS), Microsoft Software Update Services (SUS), and others that assume network connectivity can be allowed to flow through the access-controlled port in a controlled manner. This technology also brings auditing and monitoring of 802.1X deployment readiness before 802.1X enforcement begins.

Cisco Network Edge Access Topology (NEAT)-powered compact switches extend 802.1X capabilities to the network edge (conference rooms, for example), providing the same level of security as the main switch in the wiring closet. Such simple and secure configuration delivers the Borderless Networks experience without sacrificing security.

Cisco TrustSec also supports the IEEE 802.1X-REV MACsec Key Agreement (MKA) standards-based key exchange protocol. 802.1X-REV builds on 802.1X to support additional capabilities such as authentication of multiple devices on a single switch port and keying material exchange for 802.1AE devices. 802.1X-REV enhances crypto key management capabilities to assist 802.1AE standard-based data encryption.

Authorization

After network users and devices are authenticated and confirmed to comply with an organization's security policy, they are allowed network access. Their subsequent resource and service entitlement is accomplished by the authorization process. Cisco TrustSec supports multiple authorization methods, including ACLs, VLANs, and Security Group Access (SGA).

These choices help organizations design their security architecture and services offerings with maximum flexibility and effectiveness. Downloadable, per-session ACLs and dynamic VLAN assignments can be implemented at the ingress point where users and devices gain their initial entry to the network. In addition, SGA allows user identity information to be captured and tagged with each data packet. Security Group Access Control List (SGACL) can be implemented at an egress point where a network resource (such as a file server) is located. SGA-based access control allows organizations to keep the existing logical design at the access layer, and with flexible policies and services, to meet different business requirements without having to redeploy the security controls. Cisco TrustSec also delivers Change of Authorization (CoA) based on RFC3576 RADIUS Disconnect Messages, which allows session-based, on-demand authorization to support advanced services such as IP telephony integration.

Services

Cisco TrustSec provides secure guest access while delivering a high-quality user experience. The guest access service supports guest access provisioning, notification, management, and reporting. Supported guest access methods include both local LAN and wireless.

Cisco TrustSec delivers high-precision endpoint profiling by automatically identifying and classifying devices by collecting endpoint data through the built-in ISE probes or network-based device sensors on the Cisco Catalyst[®] switching and wireless infrastructure, and further refining the classification with directed, policy-based active endpoint scanning technology. This service provides visibility, intelligence, and automation to Cisco TrustSec deployments in the most efficient and scalable manner, reducing the ongoing maintenance cost.

Many organizations have strict endpoint device posture requirements such as the appropriate operating system, configurations and required system patches, as well as security software such as antivirus applications. The Cisco TrustSec solution includes endpoint agents that provide posture assessment and remediation to bring endpoint devices into compliance with security requirements. These services integrate with a wide range of endpoint security applications, and support built-in policies for more than 350 applications from leading antivirus and management software solution providers. Advanced features such as single-sign-on with Active Directory and silent remediation greatly reduce the impact on end users. Planned integration with the leading MDM solutions will further enhance organizations' ability to ensure mobile device compliance with their security policies.

Cisco TrustSec supports Multi-Domain Authentication (MDA) that allows for the secure deployment of IP telephony, whether a Cisco or a third-party IP phone is used. Cisco Catalyst switches can be configured to secure data and voice VLANs on a single switch port. With MDA, a phone, with or without a supplicant, is authenticated and subsequently placed in the voice VLAN (or domain). Any device connecting through the phone Ethernet port will be authenticated first before access is allowed via a data VLAN.

Cisco TrustSec provides switch-port-level encryption based on IEEE 802.1AE (MACsec). Data encryption supports the Advanced Encryption Standard (AES) cipher using a 128-bit key. Network traffic is encrypted to block man-in-the-middle attacks, snooping, and other forms of network attacks. Such Layer 2 encryption is implemented between an endpoint device and an access switch (for Cisco Catalyst 3560-X and 3750-X Series Switches) or between switch ports (for Cisco Nexus® 7000 Series Switches). Cisco switches preserve traffic visibility within each switch to deliver the entire breadth of Cisco networking and security services.

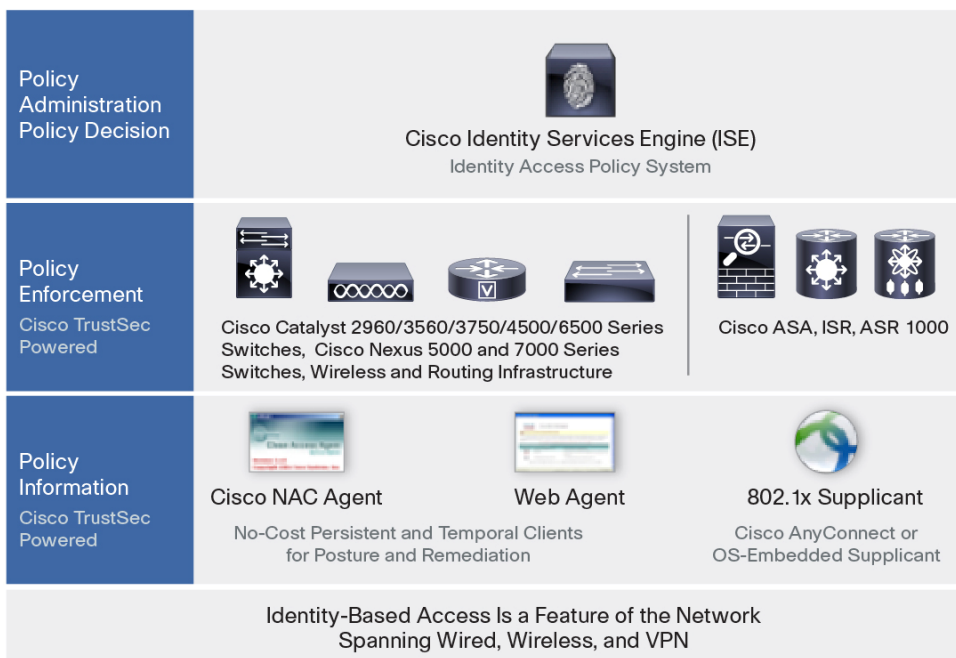
Policy

A converged policy framework is an essential factor to ensure policy consistency and efficiency to a distributed workforce. With the Cisco Identity Services Engine, Cisco TrustSec helps network and security administrators map user identity information to user groups based on their role in the organization. The policy intelligently directs network enforcement devices upon successful user authentication. The Cisco TrustSec policy framework provides a simple mechanism to provision and monitor policy based on user identity information throughout the network. This enables distributed enforcement with a central management system.

Solution Components

As Figure 3 shows, the Cisco TrustSec solution includes three product component groups (infrastructure, policy, and endpoint), as well as Cisco and partner professional services.

Figure 3. Cisco TrustSec Solution Portfolio



Infrastructure Components

Cisco Catalyst 2960,3560,3750,4500, and 6500 Series Switches, Cisco Nexus 7000,5000, and 2000 Series Switches, Cisco Wireless LAN Controllers, Cisco Integrated Services Router Generation 2 (ISR-G2) platforms, and Cisco ASR 1000 Series Aggregation Services Routers interact with network users for authentication and authorization. Access to the wired or wireless 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. Device sensors in the wired and wireless infrastructure automatically detect and help to classify devices attached to the network with minimal effort. Furthermore, Cisco switches that use SGA technology 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.

For the latest matrix of the TrustSec features available on different Cisco platforms, please refer to <http://www.cisco.com/go/trustsec>.

Policy Components

The Cisco Identity Services Engine is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline service operations. Its unique architecture allows enterprises to gather real-time contextual information from networks, users, and devices to make proactive governance decisions by enforcing policy across the network infrastructure. The Cisco Identity Services Engine is an integral component of the Cisco TrustSec solution that helps secure and govern Borderless Networks.

The Cisco Identity Services Engine provides a highly powerful and flexible attribute-based access control solution that combines authentication, authorization, and accounting (AAA); posture; profiling; and guest management services on a single platform. Administrators can centrally create and manage access control policies for users and endpoints in a consistent fashion, and gain end-to-end visibility into everything that is connected to the network. The Cisco Identity Services Engine automatically discovers and classifies endpoints, provides the right level of access based on identity, and provides the ability to enforce endpoint compliance by checking a device's posture. The Cisco Identity Services Engine also provides advanced enforcement capabilities, including SGA through the use of Security Group Tags (SGTs), Security Group Access Control Lists (SGACLs), and Security Group Firewalls (SG-FW).

Endpoint Components

Cisco AnyConnect™ provides reliable and easy-to-deploy encrypted network connectivity from any Apple iOS 4 device by delivering persistent corporate access for users on the go. Cisco AnyConnect enables business-critical application connectivity. In addition, the Cisco NAC Agent provides endpoint information regarding device posture and assists with endpoint remediation. It can be deployed as a persistent agent or as a temporal web-based agent.

Professional Services

Cisco and our partners deliver intelligent, personalized, professional services to help organizations with the planning, design, and implementation of the Cisco TrustSec solution to meet their unique requirements. These services include security policy review, design strategy development, controlled deployment, full deployment, training, and knowledge transfer. Services from Cisco and our certified partners can help organizations more quickly and cost-effectively deploy a fully integrated Cisco TrustSec solution.

Capabilities

Cisco TrustSec uses your networking infrastructure to scalably deliver the following technical capabilities:

- **Identity-enabled networking:** Cisco TrustSec delivers flexible authentication (FlexAuth) methods, including IEEE 802.1X, WebAuth, and MAB, using the network to ascertain the identity of users and devices on your network.
- **Context awareness:** The next-generation, distributed, granular scanning and endpoint inspection elements in Cisco TrustSec provide contextualized visibility into the “who, how, what, and when” for the identities of users and devices accessing the network.
- **Highest precision device profiling for any endpoint:** Automatically identifies and classifies devices by collecting endpoint data through the built-in ISE probes or network-based device sensors on the Cisco Catalyst switching and wireless infrastructure, and further refines the classification with directed policy-based active endpoint scanning technology.
- **Guest user access and lifecycle management:** Sponsored guests receive restricted access to specific resources (Internet, printers, and so on) through a customized web portal. Internal network access is blocked, and activity is tracked and reported.
- **Centralized policy and enforcement:** A centralized policy platform enables coordinated policy creation and consistent, context-based policy enforcement across the entire corporate infrastructure, spanning the head office, branch office, and remote users (wired, wireless, and VPN). Noncompliant devices can be quarantined, remediated, or given restricted access.
- **Topology-independent access control:** Broader SGA technology provides a scalable and flexible way to assign roles via network “tags” to authorize users and devices, and to enable any network to enforce policies based on these tags. This offers a unique, scalable architecture for network enforcement without network redesign using VLANs or having to manage a multitude of ACLs.
- **Data integrity and confidentiality:** Hop-by-hop standards-based MACsec encryption provides data confidentiality with visibility in the flows for security-based access policy enforcement.
- **Monitoring, management, and troubleshooting:** Centralized, policy-based corporate governance and compliance includes centralized monitoring and tracking of users and devices to maintain policy compliance. Provides sophisticated troubleshooting, detailed auditing, and historical and real-time reporting.
- **Integration with Cisco Prime™ Network Control System:** Provides a unified view of all network functions to streamline your network management efforts.

Benefits

The benefits of the Cisco TrustSec solution include the following:

- **Enables business productivity:** Cisco TrustSec gives an increasingly mobile and complex workforce access to the right resources, with assured security.
- **Delivers security and compliance risk mitigation:** Cisco TrustSec mitigates security risks by providing visibility into who and what is connecting to the network, as well as control over what they can do and where they can go.
- **Improves IT operational efficiency:** Cisco TrustSec reduces IT overhead through centralized security services, integrated policy management, self-registration device portals, and scalable enforcement mechanisms.

Summary

Cisco TrustSec provides consistent policy, distributed access control and data confidentiality and integrity protection by taking full advantage of your identity-aware infrastructure. Integrated, pervasive, and efficient, Cisco TrustSec is a foundational component of the Cisco SecureX Architecture that scales to meet growing customer security requirements - today and in the future.




Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C22-591771-01 03/12