Cisco TrustSec

Cisco SecureX Architecture

The Cisco SecureX Architecture™ brings the Cisco® security vision to customers across many market segments. It is a context-aware, network-centric, and integrated approach to security that enables consistent security enforcement throughout the organization and across security devices, greater alignment of security policies with business needs, integrated global intelligence, and simplified delivery. The result is intelligent security enforcement from endpoints to the data center and the cloud that is seamless to the end user and more efficient for the IT organization.

Context Awareness and Secure Access

The explosion in consumer IT devices, the need for global collaboration, and the move to cloud-based services and virtualization means that the traditional corporate network boundary is a thing of the past. Mobile workforce, collaboration, and productivity requirements have never been greater.

The Cisco TrustSec® architecture recognizes this fundamental change by telling you who and what is connecting to your wired or wireless network, and providing industry-leading control of what they can do and where they can go while they are there.

Cisco TrustSec technology helps to secure customer networks by building and enforcing identity and context-based access policies for users and devices while protecting critical data throughout the network.

Cisco TrustSec is a foundational security component of the Cisco SecureX Architecture and Cisco Borderless Networks. Cisco TrustSec can be combined with personalized, professional service offerings to simplify solution deployment and management.

Anyone can join the network. Cisco TrustSec makes it safe.

Identity and Context-Based Access Enforcement Is Critical to Securing Borderless Networks

- **Who?** Identify users and devices and provide differentiated access in a dynamic, borderless environment.
- **What?** Enforce policies for an expanding array of consumer and network-capable devices.
- **Where?** Traditional borders are blurred. Enforce access policy for users and devices located anywhere.
- **How?** Establish, monitor, and enforce consistent global access policies across all three access methods: wired, wireless, and VPN.

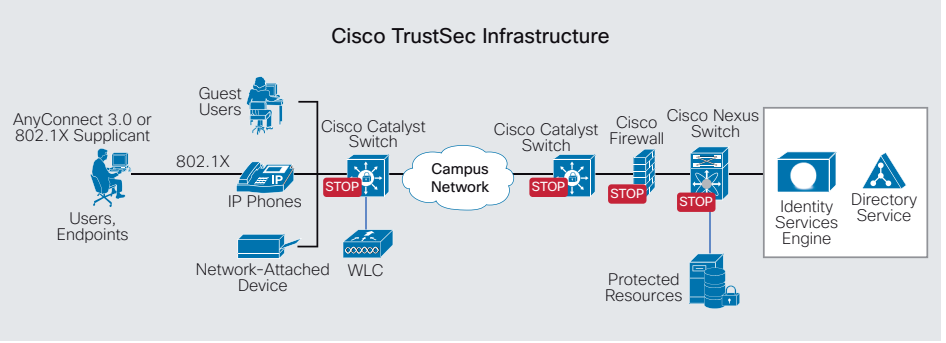
Cisco TrustSec Secures Borderless Networks

Cisco TrustSec provides a policy-based platform that offers integrated posture, profiling, and guest services to make context-aware access control decisions. Cisco TrustSec uniquely builds upon your existing identity-aware infrastructure by enforcing these policies in a scalable manner.

Benefits of the Cisco TrustSec Solution

- **Enables Business Productivity:** Gives increasingly mobile and complex workforces access to the right resources with assured security.
- **Delivers Security and Compliance Risk Mitigation:** Provides visibility into who and what is connecting to the network, and control over what they can access and where they can go.
- **Improves IT Operational Efficiency:** Reduces IT overhead through centralized security services, integrated policy management, and scalable enforcement mechanism.

Cisco TrustSec Overview



Comprehensive Visibility

- **Identity-Enabled Networking:** Cisco TrustSec delivers flexible authentication (FlexAuth) methods, including IEEE 802.1X, web authentication (WebAuth), and MAC Authentication Bypass (MAB), using the network to ascertain the identity of users and devices on your network.
- **Highest-Precision Device Profiling:** With Cisco TrustSec, the network 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.
- **Mobile Device Management (MDM) Integration:** Cisco is partnering with leading MDM vendors so that IT organizations can enable appropriate applications and services based on user and device, and to provide them with greater visibility and control over endpoint access based on company-defined policies. This technology will be available in the second half of CY12.
- **Guest User Access and Lifecycle Management:** Sponsored guests receive restricted access to specific resources (Internet, printers, etc.) through a customized web portal. Internal network access is blocked, and activity is tracked and reported.

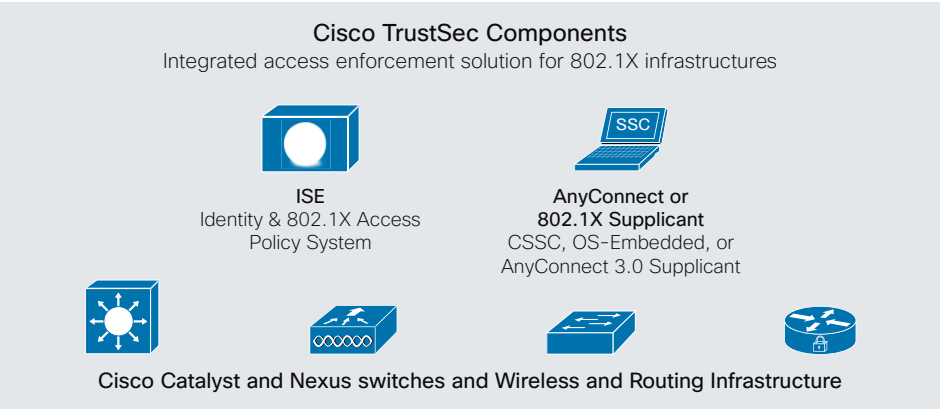
Exceptional Control

- **Centralized Policy and Enforcement:** A centralized policy platform enables coordinated policy creation and consistent context-based policy enforcement across the entire corporate infrastructure, including the head office, branch offices, and remote users. Noncompliant devices can be quarantined, remediated, or given restricted access.
- **Topology-Independent Access Control:** Security Group Access (SGA), a groundbreaking new technology, allows customers to translate their business objectives into network access control decisions. SGA combines role-based access control with scalable, consistent authorization and enforcement mechanisms that are network topology agnostic.
- **Data Integrity and Confidentiality:** Data paths can be encrypted via the IEEE MAC Security standard (802.1AE MACsec), from the endpoint client to the network core. MACsec delivers line-rate security while allowing inspection of data streams with technologies such as NetFlow.

Effective Management

- **Unified Platform:** Through the Cisco Identity Services Engine, the Cisco TrustSec framework combines authentication, authorization, and accounting (AAA), posture, profiler, and guest management functions in a single, unified appliance, resulting in simplified deployments, a single point of management, and lowering total cost of ownership.
- **Operational Efficiencies Advanced to the Next Level:** The Cisco TrustSec solution empowers the user to quickly on-board their devices through self-registration based on IT-defined policies. The framework provides automated endpoint security configuration (both certificate and supplicant) for the most common PC and mobile platforms (including iOS, Android, Windows, and OSX).
- **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 the Cisco Prime™ Network Control System (NCS):** The Cisco TrustSec framework provides a unified view of all network functions to streamline your network management efforts.

Cisco TrustSec Deployment Components



The Cisco Identity Services Engine

Cisco Identity Services Engine (ISE) provides a centralized, identity-based policy platform for context-aware access control decisions across the wired, wireless, and VPN infrastructure. The Identity Services Engine combines AAA, posture, profiler, and guest management features in a single, unified appliance, providing a single point for policy management, monitoring, and troubleshooting.

Infrastructure Powered by Cisco TrustSec

Use existing Cisco infrastructure with built-in Cisco TrustSec features:

- **FlexAuth (802.1X, WebAuth, MAB):** All Cisco Catalyst switch platforms.
- **Device Sensors:** Cisco Catalyst 3000 Series; Cisco Catalyst 4000 Series with Supervisor Engine 7-E; Cisco Wireless LAN Controllers.
- **Security Group Access:**
  - Cisco Catalyst 3000 and 4000 Series: SXP only
  - Cisco Catalyst 6000 Series: SXP, SGT, SGACL
  - Cisco Nexus® 7000 and 5000 Series: SXP, SGT, SGACL
  - Cisco Integrated Services Router: SXP, SG-FW
  - Cisco ASR 1000 Series Aggregation Services Router: SXP, SG-FW
  - Cisco Wireless LAN Controller: SXP only
  - Virtual desktop infrastructure (VDI) and Cisco AnyConnect™ Secure Mobility Client with Remote Desktop Protocol (RDP)
- **MACsec Encryption:** Windows clients with Cisco AnyConnect 3.0, Cisco Catalyst 3560-C/X and 3750-X Series, Cisco Catalyst 4000 Series with Supervisor Engine 7-E, Cisco Catalyst 6000 Series with Supervisor Engine 2T, or Cisco Nexus 7000 Series.

For a matrix of Cisco TrustSec features available on the different Cisco platforms, visit www.cisco.com/go/trustsec.

Cisco AnyConnect Secure Mobility Client and 802.1X Supplicant

- Cisco AnyConnect Secure Mobility Client provides 802.1X-enabled Cisco network devices, including Cisco switches, routers, and wireless access devices, with authentication credentials for registered users.
- Cisco AnyConnect 3.0 includes an 802.1X supplicant for Windows, and 802.1AE MACsec first-hop encryption to MACsec-enabled Cisco switches (Cisco Catalyst 3560-C/X and 3750-X Series, Cisco Catalyst 4500 Series with Supervisor Engine 7-E).

Professional Services

Expert, cost-effective services for planning, deploying, and managing any Cisco TrustSec solution:

- Security policy review
- Security architecture analysis
- Customized design strategy development
- Controlled and full solution deployments
- Staff training and knowledge transfer

New in Cisco TrustSec 2.1

- Cisco TrustSec 2.1 includes device sensor support across Cisco Catalyst 3000 Series and 4000 Series and Cisco Wireless LAN Controllers to provide the most comprehensive and scalable visibility into what's on the network.
- SGA support extends to Cisco ASR 1000 Series Aggregation Services Routers, Cisco Integrated Services Routers, Cisco Nexus 5000 Series Switches, and Cisco Wireless LAN Controllers, offering consistent policy and topology-independent access-control enforcement from remote office to data center.
- Cisco TrustSec 2.1 includes Security Group Firewall enforcement for Cisco Integrated Services Routers and Aggregation Services Routers, allowing more access control points.
- Industry-leading end-to-end, line rate (Gigabit Ethernet and 10 Gigabit Ethernet) 802.1AE MACsec encryption support on new MACsec-enabled Cisco Catalyst 4500 Series switches with Supervisor Engine 7-E.
- Cisco Identity Services Engine enhanced policy engine offers:
  - Active endpoint scanning, which uses targeted, real-time, policy-based scans to collect information from the endpoint to gain more relevant insight
  - Device sensor integration
  - Internationalization in 10 languages

- FIPS 140-2: Identity Services Engine 1.1 offers Federal Information Processing Standards (FIPS) 140-2 certification for enterprises or federal agencies needing proof of compliance
- Improved user experience with ability to easily self-provision enables IT to offer mobile business freedom with policy for when, where and how users may access the network (Q2-CY'12).
- Partnerships with multiple Mobile Device Management vendors AirWatch, Good Technology MobileIron and Zenprise in Q4-CY'12 will offer:
  - Greater visibility into the endpoint for IT
  - Enablement of appropriate applications services based on the user and device
  - Control over endpoint access based on company-defined compliance policies: for instance, requiring pin lock or disallowing jail-broken devices or implementing remote data wipe on lost or stolen mobile devices

Cisco TrustSec handles the proliferation of mobile devices with comprehensive visibility, enhanced identity and profiling, and Bring Your Own Device (BYOD) self-registration features, and provides full support for the Cisco Network Access Control (NAC) product portfolio and Cisco Secure Access Control System (ACS).

Why Cisco?

Cisco is the market leader:

- Cisco TrustSec is the only network access control solution that can provide consistent policy and enforcement across wired, wireless, and VPN environments.
- Cisco is the leader in the NAC, LAN switching, routing, and AAA markets.
- Cisco has been rated #1 by leading industry analysts in the NAC market.
- Cisco pioneered the original NAC technology and developed numerous industry standards.

For More Information

www.cisco.com/go/trustsec.

C45-653057-03 03/12