

Cisco TrustSec: Enabling Switch Security Services

Abstract

As the separation between public and private networks become increasingly blurred, enterprise administrators have begun to recognize that they must find better ways to control access to corporate resources and information. Isolated best-in-class solutions no longer meet their operational requirements. Identity authentication needs to be applied across all access methods in a consistent manner. Access to critical applications and network resources must be provided to any user on any device or any platform across a variety of access points. With so many types of users and access methods, a converged policy engine is required to manage user roles and access control requirements. And the integrity and confidentiality of transactions frequently must be ensured, even within the campus.

Cisco® has developed a new architecture along with a set of products and technologies called Cisco TrustSec, which allows enterprise networks to transition from:

- Isolated identity mechanisms to secure campus access control
- Disjointed policies to converged policies
- Unplanned to pervasive integrity and confidentiality

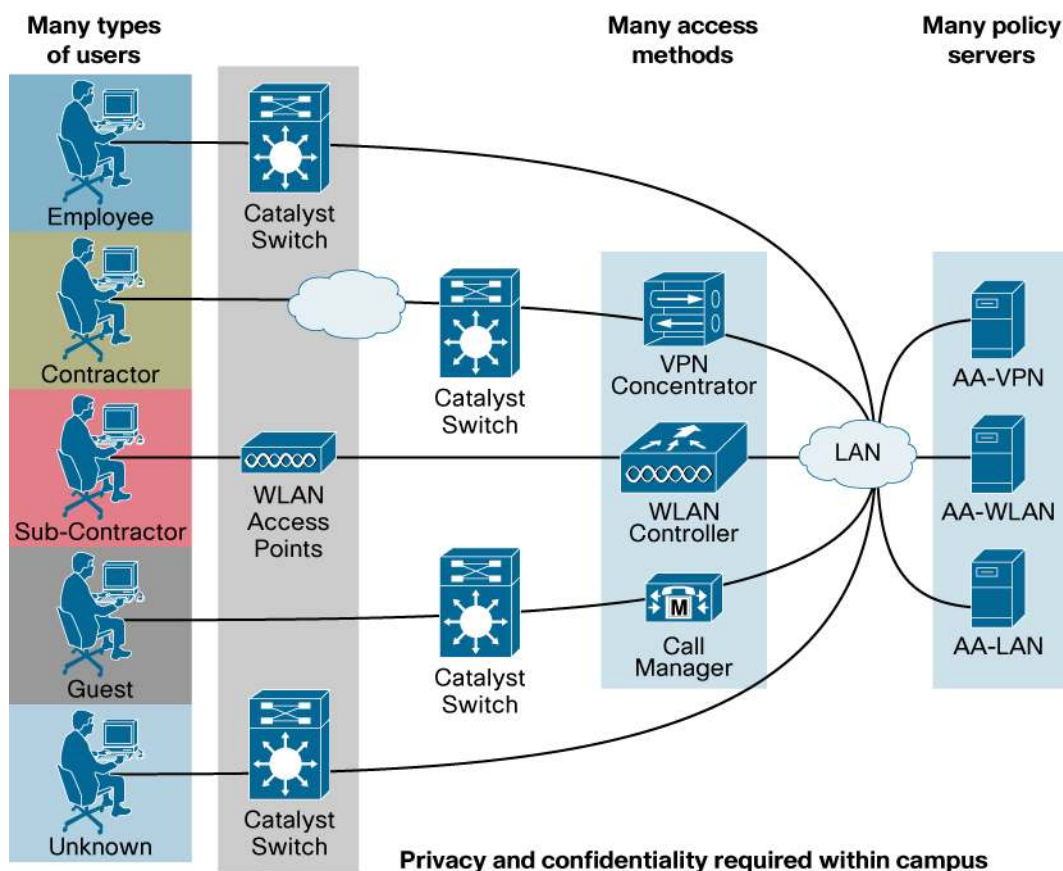
Ultimately, this transforms a topology-aware network into one that is role aware.

Problem Definition

Open networks and global access place new security demands on the network. Employees, contractors, vendors, and guests all need access to corporate networks. Devices such as laptops, phones, personal digital assistants (PDAs), wireless access points, and printers also need controlled access. When users join the network from the campus or remote branch, whether over a wireless or wired connection, their identity should be obtained through strong and flexible authentication mechanisms in a consistent manner. This identity information then must be available at all points in the network in order to grant consistent access control. Access control is not just for restricted business applications but also for applications such as voice and video. These access policies must also frequently adhere to compliance and regulatory requirements. Existing identity and access control mechanisms make these solutions difficult to manage and scale.

Enterprise networks ultimately must provide secure campus access control, which enables authentication of a user or device using any number of different credentials: user name and password, secure ID, device credential, device posture, and so on. Administrators must then have the ability to define and apply access rights, or privileges, based on a variety of different criteria.

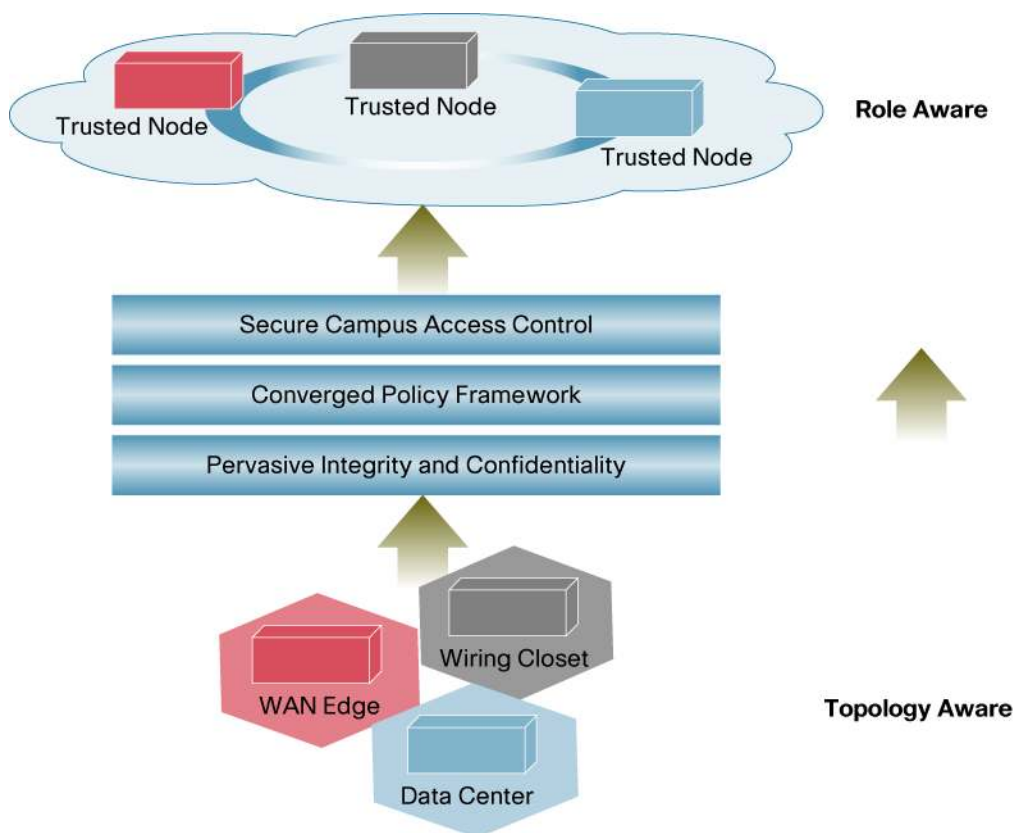
Access policies map users to roles, such as “guest” or “executive.” The authorities responsible for defining these policies tend to come from distinct parts of the company, and the rules that define these privileges frequently reside in separate locations. This complexity makes it difficult to provision and maintain consistent access policies. (See Figure 1.)

Figure 1. Today's Network Identity Problems

Many corporate policies stipulate that confidentiality must be maintained for all information after access control has been granted. Confidentiality has historically been a top priority whenever information leaves the corporate network, but with many more exploits now coming from within the enterprise, it has become critical for administrators to seek campus confidentiality mechanisms that are simple yet maintain rich network services. Confidentiality within the campus starts with device integrity: if the network devices or endpoints are compromised, information at higher application layers might not be trustworthy. Second, higher layer encryption can also disrupt the ability to maintain network-based policy enforcement using services such as firewalls, intrusion prevention, load balancing, quality of service, and so on. A network encryption mechanism that preserves these network services provides more policy control..

Cisco TrustSec: Enabling Switch Security Services

Cisco TrustSec (Cisco Trusted Security) makes the network role aware through secure campus access control, a converged policy framework, and pervasive integrity and confidentiality. As a result Cisco TrustSec reduces the operational burden of managing identity and access policy. (See Figure 2.)

Figure 2. Cisco TrustSec Building Blocks

Role-Aware Networks

Networks typically forward traffic and administer access control policies based on IP addresses. Changes to policy are difficult to implement and touch many network entities. Since, in most cases, IP addresses are dynamically assigned and are independent of a user's role, it is impossible to leave the network statically configured for policy based on IP. User roles are more static, although role membership through secure campus access control is dynamic. Hence, if networks can provision and enforce policy based on roles, management of access control policies is tremendously simplified.

Role information is required at every point in the network where an access control policy enforcement decision needs to be made. Role-aware networks carry user role information to these points so that a single access authentication event provides identity information to all policy enforcement points. Role-aware networks go beyond just security policies and are able to provide role-based application quality of service to give preference for business-critical applications for only specific roles.

Roles are also not limited to end human users. More and more intelligent "headless" devices such as 802.1x-enabled printers or intelligent video cameras are being connected to corporate networks. Cisco TrustSec is able to identify such devices and enforce the appropriate policies.

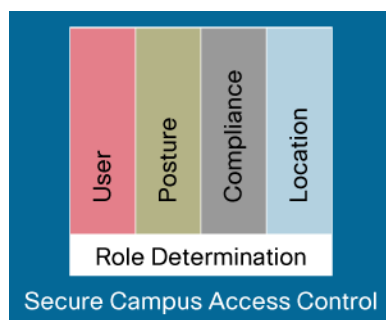
Secure Campus Access Control

In Cisco TrustSec, all IP-enabled entities are authenticated using a secure campus access control mechanism that is flexible enough to support different roles, access devices, operating systems, and access methods. Administrators can select from various authentication mechanisms, which

are client based or clientless. In the back end, identity can be mapped to roles (or groups) using standard directory services or authentication, authorization, and accounting (AAA) services. Device posture validation can supplement the authentication event to help ensure that the end device is compliant with appropriate software revision levels and loaded with authorized software only. The authentication mechanism is access method independent and therefore works transparently for wired, wireless, and VPNs.

After identity is authenticated, users and devices are mapped to specifically defined roles through a combination of identity, posture, compliance, location, and other administrator-specified information. (See Figure 3.)

Figure 3. Secure Campus Access Control



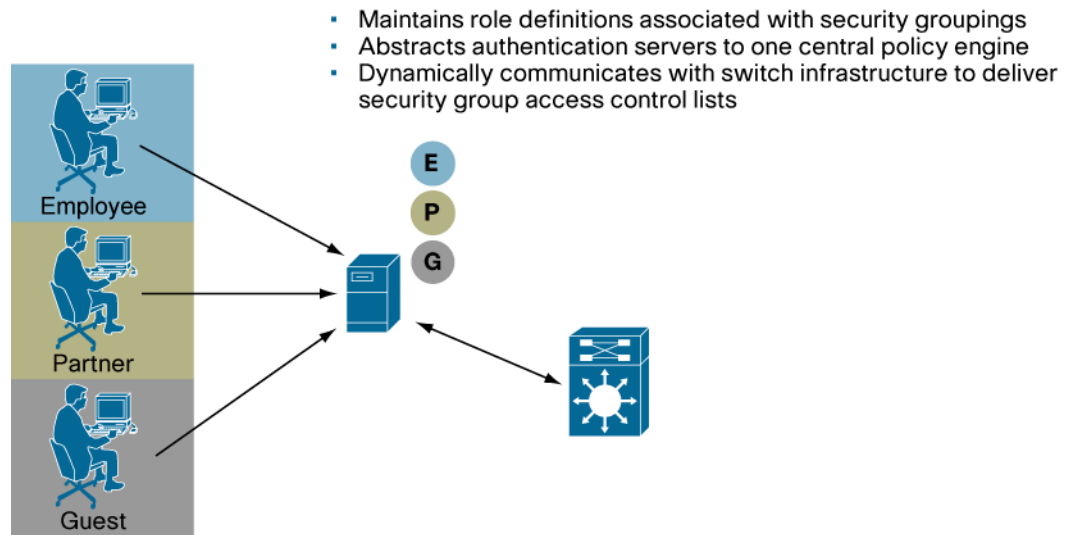
In a network enabled by Cisco TrustSec, devices cannot enforce access control until they themselves have been authenticated. Cisco TrustSec accomplishes this using a form of Network Device Access Control (NDAC). After the role in the network is established through Cisco TrustSec for every user and every device (including network devices such as switches), scalable security services can be applied for compliance, posture, and location-based services, and dynamic policies can be implemented. This simplifies the scaling of security services as they become defined by role, a much more natural definition in terms of compliance or security policies.

Through a new Cisco TrustSec mechanism of security group tags (SGTs) based on the IEEE 802.1AE standard, role information is available at every enforcement point in the network, which makes the entire network role aware. While the secure campus access control event involves many checks, the user credentials are obtained only once, and a global converged policy can then be administered anywhere in the network, since the role information is carried with the user traffic throughout the network.

Converged Policy Framework

While policy enforcement is completely decentralized, a converged policy framework allows merging of multiple policy requirements into a single configuration on a switch or any other policy enforcement point. This helps ensure that network and security administrators can map roles to policy from a central place, and this policy is intelligently mapped to a user port upon authentication. Policy is a very broad term and can include a simple permit or deny to a network address all the way to malware prevention. Whether the policy is to control access to applications, voice or video tools, or Web resources, the converged policy framework provides a simple mechanism to provision and monitor policy based on role ubiquitously throughout the network. Figure 4 shows how a central policy engine now converges policies for various roles.

Figure 4. Converged Policy Framework



A new concept called security group access control lists (SGACLs) based on role rather than IP subnets allows access control policy to be decoupled from physical topology. Since role membership is dynamically populated on campus switches through secure campus access control, and up-to-date role information is available everywhere through SGTs, SGACLs can also be deployed close to the protected resource to simplify configuration. Figure 5 shows the steps in Cisco TrustSec for secure campus access control and converged policy assignment through an SGACL.

Figure 5. Converged Policy Framework

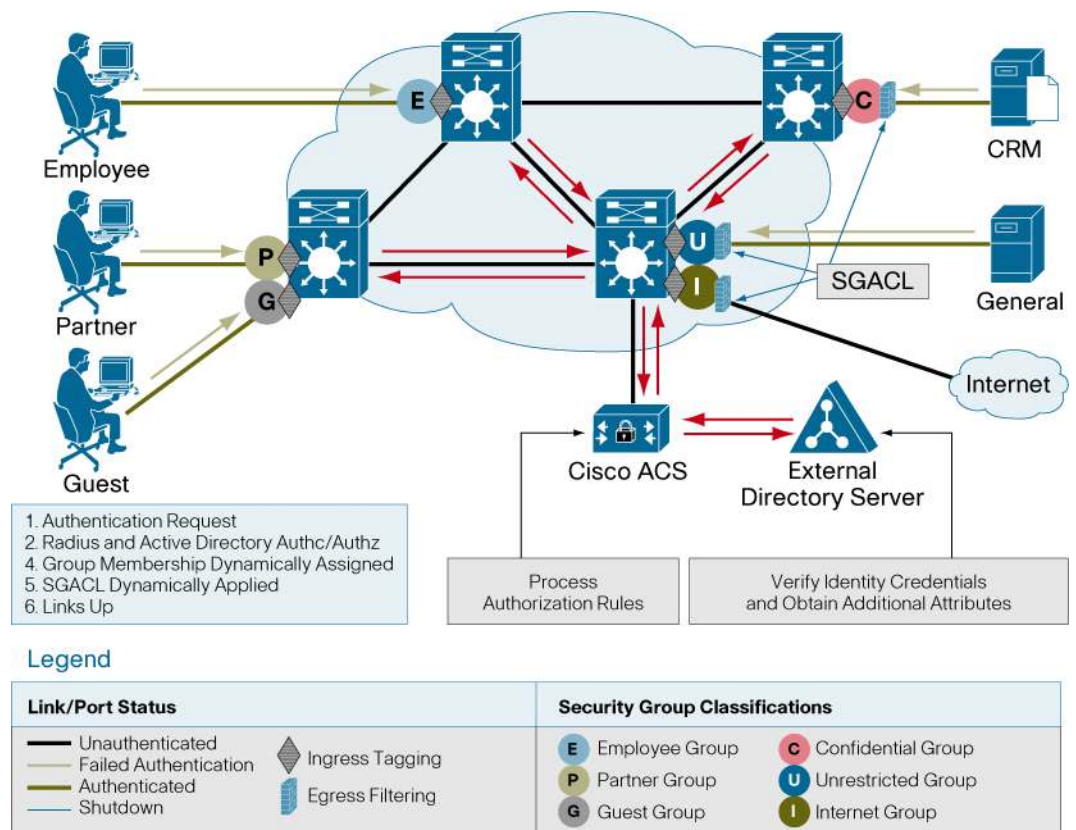


Figure 6 shows how SGACLs can now be administered by simply specifying which roles or groups are permitted or denied from communicating with each other. Because role membership is dynamic and pervasively available, administrators no longer have to rely on IP address and network topology information to administer policies.

Figure 6. Security Group ACL Definition

SGACL Matrix		Destination Groups		
		C	U	I
Source Groups	E	✓	✓	✓
	P	✗	✓	✓
	G	✗	✗	✓

Pervasive Integrity and Confidentiality

Authenticated users with authorized access also need the peace of mind that their information and transactions are completely confidential. Rather than attempting to encrypt individual applications, Cisco TrustSec provides the ability to secure every link in the campus with strong encryption. A new Cisco innovation, the Security Association Protocol (SAP), simplifies the management of each link's encryption keys. This not only helps secure the LAN but also provides security for every application without having to retrofit and encrypt at the application layer.

Switch integrated security mechanisms block man-in-the-middle attacks to disallow traffic redirection and snooping. Switch protection features and controlled access to the switch itself help ensure that network device integrity is maintained, since compromised devices can be used to intercept information. Cisco TrustSec also carries role information over secured links to make roles, policies, and confidentiality pervasive and scalable, while preserving traffic visibility within the switches to deliver the entire breadth of Cisco network services and security.

Roadmap

Cisco TrustSec will be delivered in the following phases.

- Phase 1: High-end switching (Cisco Catalyst® 6500 Series) with Cisco ACS support in 2008
- Phase 2: Additional Cisco Catalyst switches

Conclusion

Cisco TrustSec makes networks role aware with trusted devices, trusted users, and a trusted network. With secure campus access control, a converged policy framework, and pervasive integrity and confidentiality, Cisco TrustSec creates the role-aware network with powerful switch services to meet networked identity requirements of the future.

For More Information

For more information about switch security services and its use cases, visit <http://www.cisco.com/go/switchsecurity>.

**Americas Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)