



Cisco TrustSec

Identity-Based Secure Access for Borderless Networks

The Borderless Network

Cisco® Borderless Networks are changing the network landscape by delivering connectivity to anyone, anywhere, anytime, using any device. Cisco Borderless Network solutions provide expanded security, flexibility, and network services so organizations can expand geographically, embrace new business models, and become more innovative..

Securing the Borderless Network

As networks become borderless, organizations must respond to a wide array of new challenges, including:

- Greater end-user demand for mobility and device choice
- Consumerization and deployment of access devices
- An increasingly complex workforce — employees, guests, partners, etc.
- Purpose-built devices becoming network-enabled
- Increased use of virtualization
- A move to cloud-based access and services

This evolution brings important advantages, but also significantly increases the risks organizations face. One of the major security issues that organizations need to address is how to control user and device access to a borderless network.

Identity and Policy-Based Access Enforcement: Critical to Securing Borderless Networks



Who? Identify users and provide differentiated access in a dynamic, borderless environment.



What? Enforce compliance 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.

Cisco TrustSec Secures Borderless Networks

Cisco TrustSec™ provides policy-based management, identity-aware networking, and data integrity and confidentiality services to effectively control user and device access in the borderless network. The Cisco TrustSec solution:



Supports compliance — Enables corporate governance through a consistent access policy for all users and devices, addressing mandated monitoring, auditing, and reporting requirements.



Strengthens security — Extends security across the network by enforcing consistent security policy, ensuring endpoint health, expanding visibility into access events, and delivering a secure network fabric.



Increases efficiency — Reduces IT overhead through centralized identity management; integrated policy enforcement; dynamic registration and assignment of user, device, and guest access; simplified compliance checking on non-controlled assets; and a consistent user experience.

Cisco TrustSec Overview

Identity-Aware User and Device Access:

Dynamically provides role-based access. Noncompliant devices can be quarantined, remediated, or denied access.

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.

Non-User Device Discovery:

Non-user devices (printers, cameras, phones, etc.) are centrally discovered. Access is provided based on policy, and device behavior is monitored and audited to prevent spoofing.

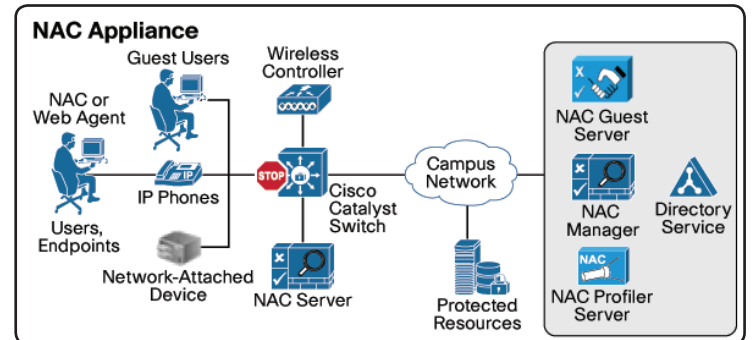
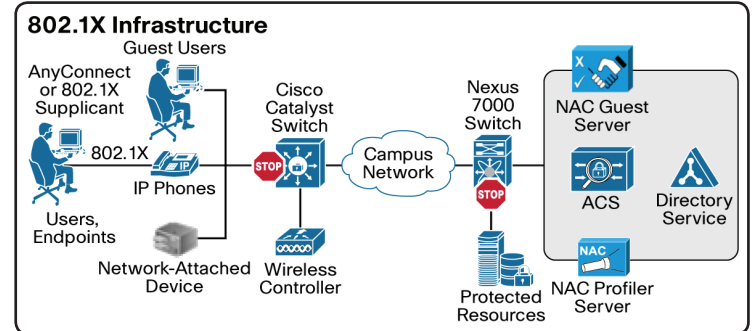
Data Integrity and Confidentiality:

Data paths can be encrypted via MACsec from the endpoint client to the network core, while allowing critical tools (firewalls, IPSs, content inspection, QoS, etc.) to retain visibility into data streams.

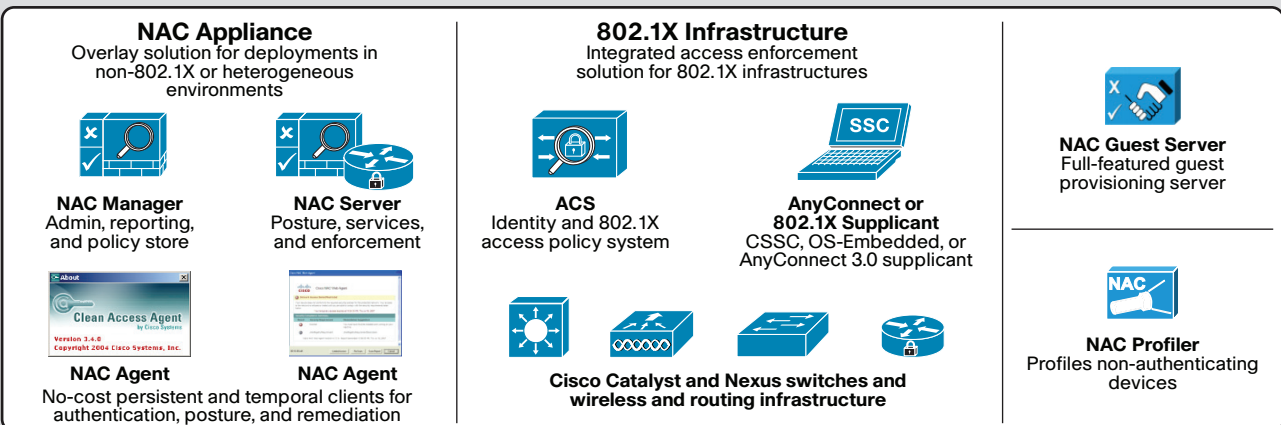
Monitoring, Management, and Troubleshooting:

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.

TrustSec Deployment Options: Cisco TrustSec can be deployed as Cisco NAC, an appliance-based access and device posture assessment overlay solution, or with an integrated 802.1X infrastructure-based approach which uses Cisco switches and Cisco Secure ACS to extend access enforcement through the network.



Cisco TrustSec Components



Cisco NAC Manager Appliance

Provides granular, centralized creation, administration, and management of role-based user access and endpoint security policies across multiple Cisco NAC Server appliances. Monitoring and reporting tools allow administrators to review access transactions and refine access policies.

Cisco NAC Server Appliance

Assesses and enforces policy compliance and endpoint and device posture. Delivers remediation services to devices that do not meet policy and security standards.

NAC and Web Agents

Endpoint clients, available free of charge, provide the Cisco NAC Server appliance with endpoint device security credentials. These credentials include device authentication and security posture information, and are used to ensure policy compliance and to help facilitate device remediation.

NAC Profiler for NAC and 802.1X deployments

Provides discovery, profiling, policy-based placement, and post-connection monitoring of all endpoint devices. Identifies non-authenticating or agentless devices and scans them for policy compliance or potential security threats.

NAC Guest Server for NAC and 802.1X deployments

Manages guest network access, including browser-based guest access portals, guest access provisioning, guest notification, and management and reporting of guest accounts and network activities.

Cisco Catalyst and Nexus Switches

802.1X-based access control provides uniform access policy enforcement across Cisco switch platforms using dynamic VLANs, dACLs, and Secure Group Access (SGA). This approach simplifies rollout, enables consistent functionality, and provides integrated monitoring, logging, and reporting.

SGA assigns network access rights to traffic with Security Group Tags (SGTs) based on user or device role. 802.1X-enabled Cisco switches can then read those tags and enforce access policy with Security Group ACLs (SGACLs.)

AnyConnect/802.1X Supplicant

Provides 802.1X-enabled Cisco network devices, including Cisco switches, routers, and wireless access devices, with authentication credentials for registered users.

AnyConnect 3.0 includes an 802.1X supplicant for Windows, and MACsec for encryption to MACsec-enabled Cisco switches in the network (Nexus, Catalyst 3750-X, etc.)


Cisco Secure Access Control Server (ACS)

Provides centralized identity, access control, and policy management and distribution. Cisco Secure ACS also quickly identifies potential problems with comprehensive monitoring and troubleshooting.

New in Cisco TrustSec:

- AnyConnect Secure Mobility Client 3.0:** Modular client now includes an 802.1X supplicant for Windows-based (XP, Vista, 7) machines, and MACsec (802.1AE) support to provide data encryption from the endpoint.
- LAN Management Solution 4.0:** Identity Work Center provisions and monitors Cisco TrustSec™ deployments in Cisco switches. Workflows simplify deployment and configuration of identity services in the network.

Why Cisco?

Technology and solution leadership: 

- Identity enforcement throughout the network using dynamic VLANs, dACLs, and SGA
- Role-based differentiated access control for users, endpoints, and non-user devices
- 802.1X-2010 provides standards-based encryption to secure data traffic combined with appropriate data inspection
- World-class professional, maintenance, and support services

Market leadership:

- Leader in NAC, LAN switching, routing, and AAA markets
- Pioneered the original NAC technology and developed numerous industry standards
- The only comprehensive, single-vendor solution available today

Professional services:

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

- Security policy review
- Design strategy development
- Controlled and full-solution deployments
- Staff training and knowledge transfer

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