Cisco TrustSec and NAC Security Services Built on a Common Identity Framework

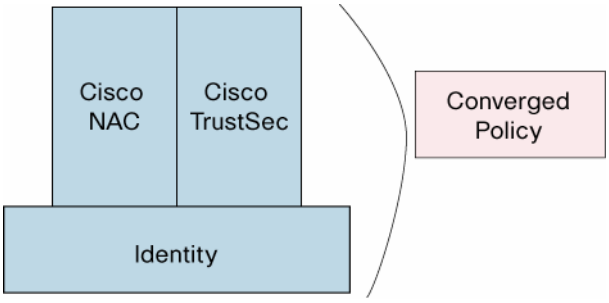
Abstract

Securing corporate networks is an ongoing challenge. Employees have become more mobile and connect to corporate networks via a variety of access mechanisms. Collaboration between employees, partners, and vendors, brings more users onto the network with a different mix of roles and privileges. Add in the growing regulatory compliance needs and you have a much more complex policy-management problem. Cisco® has helped customers deal with these issues since its inception starting with access control lists (ACLs) and subsequently through Cisco Identity Based Network Services (IBNS; the next phase of which is called Cisco Identity Based Privilege Networking [IBPN]). More recently, Cisco Network Admission Control (NAC) was developed to allow customers to authenticate on the basis of device “posture” as well as Identity. All of these products and feature sets are part of a larger Identity Framework that will include Cisco Trusted Security (or TrustSec). Each of these solutions focuses on different aspects of authenticating a user or a device onto a network as well as managing associated entitlements and access control. This document explains how these initiatives relate to one another and build upon a common Identity framework.

Introduction

A core design goal of Cisco IBPN is to provide customers with the flexibility to pick and choose which components to use individually or collectively to control access and protect information and infrastructure. While IBPN is currently focused on Layer 2 authentication, authorization, and accounting (AAA) mechanisms based on the 802.1X protocol, the architecture is designed to provide rich identity-based policy-control services across Layers 3 and 5 via a Flexible Authentication framework. As a result, customers will be able to define layered authentication policies to deal with the realities of their user communities.

Figure 1. Common Identity Framework



Cisco IBPN, thus forms a common identity framework that can be leveraged by other security services. Cisco NAC builds on this identity framework (see Figure 1) by providing the ability to authenticate based on credential types such as posture as well as alternate authentication methods such as web portals for guests and device profiling. Once these features are fully integrated, customers will be able to access the greater flexibility of the Cisco IBPN architecture.

The recently announced the Cisco TrustSec architecture also builds on Cisco IBPN by providing:

- Secure Campus Access Control
- Converged Policy Framework
- Pervasive Integrity and Confidentiality

By leveraging this common identity framework with Cisco TrustSec and Cisco NAC, customers will be able to more fully control the type of information collected as well as how users and devices are authenticated and authorized. This will be accomplished through a converged policy framework that works across Cisco's Catalyst® switching, wireless, routing, and security appliance product families.

Cisco Identity Based Privilege Networking

The fundamental goal of Cisco IBPN is to lower operational expenses by providing a framework of rich and flexible identity tools and services that can be built on by solutions such as Cisco NAC and Cisco TrustSec. More specifically Cisco IBPN will provide the following benefits:

- **Device Agnostic Access Control:** Enable traditional and unmanned devices (for example, printers) to access the network based on tailored policies.
- **Modularity:** Enable services like Cisco NAC and Cisco TrustSec to easily leverage a common authentication and policy framework.
- **Flexible Access Policy:** Support a wide range of policy control, such as quarantine, remediate, monitor, and constrain access.
- **Flexible Authentication:** Provide a range of interoperable authentication access mechanisms all the way from 802.1X to web-based authentication.
- **Service Centralization:** Enable services, such as guest management, device profiling, posture and remediation to be centralized

For background on Cisco IBNS refer to "Cisco IBNS: Secure Network Connectivity and Resources" at:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns75/networking_solutions_sub_sub_solution_home.html.

Cisco Network Admission Control

Cisco NAC enforces security policies on all devices requesting network access. Cisco NAC mitigates risks from emerging security threats by allowing only compliant and trusted endpoint devices, such as PCs, servers, and personal digital assistants (PDAs), onto the network.

Cisco NAC provides the following benefits:

- **Security-policy compliance:** Enable endpoints to conform to security policy, protect infrastructure and employee productivity, secure managed and unmanaged assets, support internal environments and guest access, tailor policies to your organization's risk level.
- **Investment protection:** Compatible with third-party management applications. Flexible deployment options minimize need for infrastructure upgrades.
- **Risk mitigation:** Reduce risks from viruses, worms, and unauthorized access. Reduce large-scale infrastructure disruptions and integrate with other Cisco Self-Defending Network components to deliver comprehensive security protection.

Recent additions to Cisco NAC include:

- **Secure guest management:** Providing efficient management and provisioning of visitors and guests.
- **Device profiling:** Offering device discovery, device type classification, and policy control for non-authenticating devices such as network printers and IP phones.
- **Temporal agent:** Enabling posture assessment of contractor, personal, and guest endpoints.

Cisco NAC can be deployed in all infrastructure scenarios, including corporate LAN, WAN, wireless, and remote access (VPN). It features rapid deployment, self-contained endpoint security posture assessment, policy management, and includes integration with identity remediation, and other services.

Today, Cisco NAC leverages and extends Cisco IBPN for secure guest management and device profiling. Cisco NAC will be enhanced to deliver a full suite of services to the Cisco IBPN framework, allowing you to leverage existing or planned investments in existing Cisco NAC hardware components. This will enable you to leverage Cisco NAC posture and remediation services with the Cisco IBPN authentication and authorization framework and management utilities.

For more information about how Cisco NAC helps improve security, refer to “Cisco NAC: Help Customers Improve Security” at: http://www.cisco.com/en/US/netsol/ns466/networking_solutions_white_paper0900aecd8051f9e7.shtml.

Cisco TrustSec

Cisco TrustSec significantly reduces the operational costs of managing access control policies as well as protecting data across enterprise networks. Cisco TrustSec does this by building out trusted network segments based on trusted network devices as well as trusted users. It delivers three fundamental security services, which are discussed in the following sections:

Secure Campus Access Control

Cisco TrustSec leverages IBPN for authentication mechanisms and access to standard directory services. Cisco TrustSec works transparently for wired, wireless, and VPN. It authenticates users and devices regardless of role, device type, operating system, or access method. After successful authentication, Cisco TrustSec maps users and networking devices to specific roles based on criteria such as identity, job function, location, posture, device type, and so on. The role-based access control capability simplifies the scaling of security services and provides a more efficient approach to implementing compliance requirements and security policies.

Converged Policy Framework

Using the IBPN framework, Cisco TrustSec can coordinate and converge multiple compliance requirements and access policies when a user or device requests access to a network. With Cisco TrustSec, security policies can be collapsed into a centralized policy engine that acts as a broker between the campus network infrastructure and back-end policy directories, such as Active Directory. Cisco’s existing Access Control System (ACS) is being extended to provide policy aggregation and control of this converged policy framework. If deployed along with Cisco NAC, the

Cisco ACS also interacts with the NAC system to take advantage of endpoint posture, remediation, and other NAC services.

Pervasive Integrity and Confidentiality

Cisco TrustSec adds data protection by securing every data path in the campus switching environment based on digital device certificates and strong encryption based on the IEEE 802.1AE standard. Data confidentiality and integrity is instantiated between devices on a hop by hop basis. This allows mission-critical applications such as firewalls, intrusion prevention, and content inspection to maintain visibility into the packet streams at each switch boundary without disrupting the requirements for data integrity and confidentiality.

Most access control policies today are managed through Ingress Filter ACLs that require an understanding of network and application topology. As the network or services change, these ACLs must be modified and propagated throughout the network. It is very difficult to keep these ACLs synchronized with corporate requirements and as a result legacy access control implementations typically do not scale.

Cisco TrustSec dramatically reduces the cost of managing access control shifting from a classic Ingress Filter model to an Ingress Tag and Egress Filter model. Instead of having every entry point understand where every user can and cannot go, administrators can localize access rules to just those areas of the network that understand the policy for a given role. In other words, only those destinations that care about a given role need an ACL policy to deal with that role. This approach allows administrators to implement security policies independent of the location of the user or device. User roles need to be defined only once and are then pervasively and consistently applied across the entire infrastructure.

A new Cisco innovation, the Security Association Protocol based upon the IEEE 802.1af standard simplifies the key management between links and also facilitates interoperability with other 802.1AE-compatible devices. Cisco TrustSec also carries role information over secured links to make policies and confidentiality pervasive and scalable.

Cisco TrustSec will be available across the entire Cisco Catalyst switching portfolio over the next 18 months, beginning in the first quarter of calendar year 2008. To facilitate the deployment and adoption of this solution, Cisco will provide the Security Exchange Protocol (SXP) as a software solution to allow existing Cisco products to participate in the TrustSec architecture. Existing switches enabled with SXP can communicate user-to-roles mappings across third-party Cisco TrustSec-capable clouds. However, it does have scaling limitations as compared to Cisco TrustSec-enabled switches. Upgrading SXP-enabled switches to hardware-supported Cisco TrustSec capabilities as your organization goes through its natural refresh cycle will provide complete access-control services as well as line-rate integrity and confidentiality.

For more information about the Cisco TrustSec architecture and functions, refer to “Cisco TrustSec: Enable Switch Security Services” at: http://www.cisco.com/en/US/netsol/ns774/networking_solutions_white_paper0900aecd80716abd.shtml.

Deployment Considerations

Depending on your security and compliance needs, you can use Cisco TrustSec and NAC individually or collectively to enhance the protection of your information assets and infrastructure.

You can plan ahead to employ the security services as they become available by answering the following questions:

- Where do you intend to control access to the network (remote access, guest access, wireless, branch offices, main campus, etc.)?
- How will you consolidate your security polices into a centralized policy engine?
- What type of data and resources you need to protect the most?

If you intend to deploy both Cisco NAC and Cisco TrustSec, consider one of the following paths that help you get started right away while planning for upcoming Cisco IBPN and NAC advances and the release of Cisco TrustSec:

- **Non-802.1X start:** Deploy Cisco NAC first (with its posture and remediation services, plus device profiling and secure guest management), followed by 802.1X, and then Cisco TrustSec.
- **802.1X-start:** Deploy 802.1X combined with Cisco NAC profiling and secure guest services as appropriate first; then, in any order, deploy Cisco TrustSec and the Cisco NAC posture and remediation services.

In summary, Cisco TrustSec, NAC, and IBPN can work collaboratively to give you more scalable and agile deployment options for compliance and security.

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.**

Printed in USA C11-450527-00 01/08

