



Corporate
Alliance



MANAGE BOTH THE USERS AND THE DEVICES THAT
CONNECT TO THE ENTERPRISE TO MAXIMIZE SECURITY.

WHITE PAPER

Your **security** demands the integrated **resources**
of **trusted** providers.

Rev 1
October 2004

Table of Contents

- 2 Overview
- 3 Insufficient User Identity Information Can Pose a Security Threat
- 4 Security Compliance for Devices Represents Another Challenge
- 4 Implement a Policy-Based Approach to Manage Both User Identities and Devices
- 5 Verify Identities That Seek Network Access
- 6 Manage the User Population
- 7 Leverage Automation to Manage Rapid Changes That Affect Access Rights
- 7 Delegate Management, Self-Care and Regulatory Compliance
- 8 Establish Security Compliance Policies for Device Connectivity
- 10 Manage Device Compliance Policies Effectively
- 11 Isolate and Remedy Devices That Do Not Comply with Security Policies
- 13 Achieve a Highly Secure Enterprise Computing Infrastructure with IBM and Cisco Products
- 15 For More Information

Overview

To address today's competitive On Demand Business challenges, organizations leverage their IT investments in networks, systems and applications to efficiently connect with customers, suppliers and partners. While enabling more users and organizations to connect to many parts of the IT infrastructure drives immense benefits, it also can yield corresponding risks. The recent spate of viruses, worms and Internet attacks caused significant IT infrastructure damage and a massive loss of productivity within enterprises. Businesses have been forced to spend more to combat these evolving threats, yet their security capabilities often have not risen to meet these challenges.

In addition to tackling electronic threats, enterprises now must comply with a variety of industry and governmental regulations, including the Sarbanes-Oxley Act (SOX) of 2002, the Health Insurance Portability and Accountability Act (HIPAA) and the Basel II Accord. Additionally, some organizations use compliance initiatives to streamline and optimize the quality of existing IT operations by automating key processes.

For enterprises addressing security and regulatory exposures, this paper describes two key areas where IBM and Cisco Systems can help:

- Managing the identities of users that connect to the enterprise. When an enterprise implements identity management, it can prevent users without valid IDs from connecting to the corporate network. Furthermore, the enterprise enables the organization to better control the varying levels of access that different individuals should have, based on their roles within—and outside—the enterprise.

Insufficient User Identity Information Can Pose a Security Threat

- Monitoring the security vulnerabilities and policy violations of devices that connect to the network. By establishing specific security compliance requirements for devices that connect to the network, the enterprise helps limit exposure to corrupted or infected devices. An enterprise can isolate devices that lack—for example—an operating system patch level, antivirus protection or Cisco Security Agent. Additionally, the enterprise can establish remediation procedures that help devices meet the requirements for accessing the secure network.

In both identity management and security compliance, the establishment of policy-based systems helps organizations administer security in a consistent fashion across many systems and with many users. Furthermore, when enterprises establish a policy-based security solution, they can automate the execution of policies and facilitate rapid changes to those policies. Existing IT systems can support an enterprise's business priorities with greater agility and security, while also assisting in the compliance of auditing requirements.

Insufficient User Identity Information Can Pose a Security Threat

Today, many enterprises do not know the identity of each person connecting to their networks. When individuals establish physical or wireless connectivity, they are given TCP/IP addresses, which allow anyone—authorized or not—to access any nonprotected information in the enterprise. This wide-open access results in a security exposure of corporate assets to internal and external users. Innocently or maliciously, these users may compromise confidential information and may remain undetected by the enterprise.

This problem has been greatly increased by the demands of the new computing and business models. For example, the On Demand Business initiative from IBM helps companies leverage great levels of connectivity—including connectivity with partners, temporary workers and, in some cases, competitors—to drive efficiencies and new revenue-generating initiatives. As enterprises exchange sensitive information with partners and competitors, they have the responsibility of protecting that information—as well as additional internal information—from other users who have access to the network.

With their current identity infrastructures, enterprises can restrict access to certain applications but leave much of their data available to everyone. Because administering credentials and ultimately access to resources are handled by individual applications, user rights management has been time consuming, difficult for most IT staffs and limited to critical applications. Enterprises typically lack automated, centralized user rights management that could properly limit the unauthorized access of users who have attained a connection to the enterprise network.

Figure 1: Strategic Solution — Identity-Based Networking Services

Network perimeter indefinable

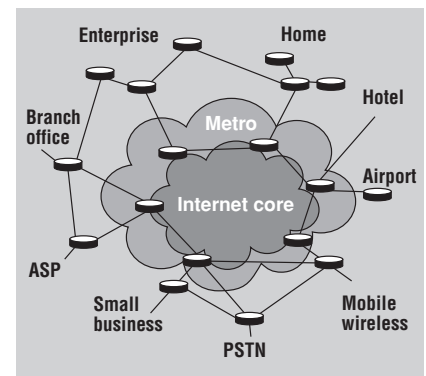
- Distributed Internet applications
- Ubiquitous access
- Expanded constituencies

Every network ingress point is a conduit to the network

- Identities
- Viruses, worms
- Hackers

New technologies introduce new risks

- Content and interactive applications
- VoIP, Wi-Fi, storage



Security Compliance for Devices Represents Another Challenge

Security Compliance for Devices Represents Another Challenge

Devices used to access the network—cell phones, PDAs, laptops, desktops, servers and more—all run different software and all contribute to the complexity of securing the enterprise. Many classes of these devices must be managed—from rogue devices—devices outside of the control of the enterprise—to well-understood servers. Several scenarios exist in which a device can become the weak link in the security model, including the following:

- When a rogue device that is not of a known quality accesses the network, it can masquerade as another user or identity with impunity.
- When a known device lacks the latest security updates, it may not function as a responsible device on the network.

By knowing the identity and the state of each device, an enterprise can control the relationship of the device to the network—restricting access based on the security exposures and policy violations of the device.

Rogue devices—devices outside of the control of the enterprise—can pose a substantial security risk. Legitimate fixed-function devices such as printers do not usually have the capability to inflict damage to the enterprise and would therefore typically be acceptable to the network. Other “smarter” devices, however, should be required to present their current state, then receive restricted access if they do not conform to the established security policy. Many of these devices may in fact be legitimate, such as those of vendors or visitors, but should be given only limited network access.

To help address new threats in today’s rapidly changing business environment, security updates are constantly being made available to both products and signatures. Devices that have been disconnected from the enterprise (such as those used while traveling) and individuals who do not heed the enterprise’s update requirements are ripe targets for malicious attacks. Consequently, the enterprise should proactively address these exposures—isolating these devices from the secure and production parts of the network until devices address the identified security exposures and policy violations.

The challenge of knowing the identity of a device beyond doubt becomes greater as devices become increasingly complex and roam outside the secure enterprise boundaries. To achieve an additional level of security, enterprises turn toward hardware-based technologies that provide more secure knowledge of device identities.

Implement a Policy-Based Approach to Manage Both User Identities and Devices

In the cases of both user identity management and device configuration management, the increasing variety and number of the types of data and resources the enterprise needs to manage can mean that a manual solution is no longer practical. Administrators do not have the time to initially apply or maintain on a consistent and cost-effective basis all of the combinations of rights for both users and devices.

An organization needs the ability to establish a set of access rights policies that should be executed consistently. When changes to an individual user or device occur, the policies should rapidly be applied to grant and remove the appropriate access rights. When changes to policies occur, they should be applied to all of the affected users and devices.

Verify Identities That Seek Network Access

To create such a policy-based security infrastructure, an enterprise needs tools that can help its administrators create and modify business policies in a highly time-efficient fashion. Furthermore, the enterprise needs solutions that can automatically enforce and execute changes to its policies—helping save administrator time and driving accuracy.

The remaining sections of this paper help you understand how an enterprise can combine IBM and Cisco solutions to implement policy-based security solutions:

- First, learn how IBM and Cisco solutions enable an enterprise to implement identity-based networking and manage both user identities and access policies.
- Then explore how an enterprise can deploy IBM and Cisco solutions to check device security compliance, manage device security compliance policies and remedy nonsecure devices.
- Finally, review brief descriptions of key hardware and software components that an enterprise can use to establish an effective security solution today.

Verify Identities That Seek Network Access

A layered or multitiered approach can be a best practice for businesses that want to effectively manage user access to resources. IBM and Cisco provide a robust set of layered enforcement capabilities. The first line of defense is formed by Cisco Secure Access Control Server (Cisco Secure ACS) and the network layer, which help an enterprise keep unknown people from getting onto its network.

In today's mobile environment, an individual who connects to the network may do so from many different locations. By using Cisco's network access devices in conjunction with Cisco Secure ACS, an enterprise implements a methodology for addressing this challenge. When an access request is made, the network can challenge the individual to present valid credentials before allowing the user to take advantage of network resources.

By using Cisco solutions, an enterprise takes advantage of the industry-standard 802.1x protocol, which is designed for validating identities in response to requests for network access. Most popular end-point systems today support this capability. For example, 802.1x is the protocol most commonly used for user authentication in the case of wireless access.

When an end point makes a network request, the network access device asks the end system for an identity to verify the user before granting the request. After the end system supplies the identity, the network access device sends the identity information to Cisco Secure ACS for validation. If the user is valid, the Cisco Secure ACS instructs the network access device to grant the request; if not, the network access device denies the request.

Because Cisco Secure ACS contains all the valid users and credentials that devices must present to get network access, it serves as a place to define network access policies. The next two sections, "Manage the User Population" and "Leverage Automation to Manage Rapid Changes that Affect Access Rights," show you in greater detail how IBM and Cisco help an enterprise address the challenges of managing users by establishing and enforcing robust network access policies.

After the network layer, the other layers of access control give an enterprise more granular control over access to applications, operating systems and data:

- Use IBM Tivoli® Access Manager to manage access to Web applications.
- Leverage the robust capabilities of IBM z/OS®, provided with Remote Access Control Facility (RACF®), to establish specific access controls for operating systems.
- Enforce access that is specific to critical applications running on key operating systems. For example, to help an enterprise address privacy requirements, IBM solutions enable the enterprise to allow access only to specific rows within a data table, or to release data only when there is a relationship between the data and the requester.

Manage the User Population

Manage the User Population

Because a network's growing number of users is accompanied by an increasing variety of access rights and a more substantial enforcement infrastructure, implementing and maintaining a network-level identity model requires an enterprise to implement a robust management solution. By using IBM Tivoli Identity Manager—one of the leading identity management solutions—an enterprise can leverage its integration with Cisco Identity-Based Networking Services (IBNS) to automate deployment of a network-level identity environment.

The IBM solution is designed to help an enterprise integrate with physical security vendors (badge readers, smart cards, digital video surveillance and more). Management can be extended from managing access to logical entities such as applications and operating systems to managing access to the physical environment—and thereby helping create end-to-end security.

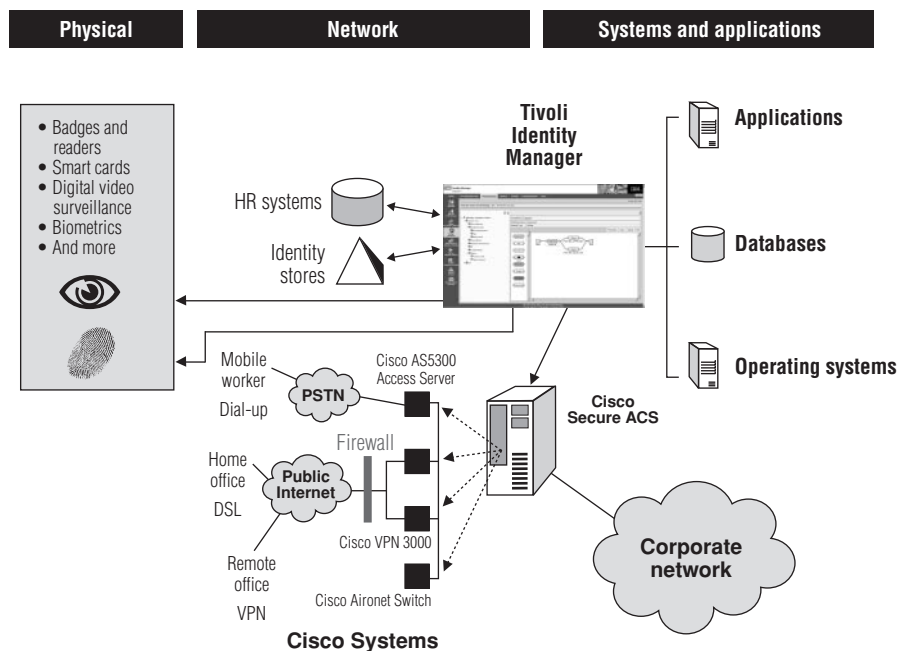
Identity management begins with an enterprise's trusted source of user information, such as a human resources database that defines the employees who have rights in the enterprise. Authoritative information about partners, customers and other groups may lie in other sources, such as a relationship management system. All of these systems carry some

valuable information about the users, including departments, responsibilities, titles and more. Tivoli Identity Manager provides an XML interface for sources of user information, which an enterprise can use to import changes and update enforcement engines.

An enterprise running Tivoli Identity Manager uses the information provided by these sources to determine each individual's access rights, in accordance with policies the enterprise establishes for resource access. Policies can determine rights for access to physical buildings, networks and subnets (which are particularly important in the case of IBNS), applications and data. After determining the rights of an individual, Tivoli Identity Manager provisions the user to the appropriate enforcement points, including:

- Badge readers.
- The network, using Cisco Secure ACS.
- Web applications, using IBM Tivoli Access Manager for e-business.
- Operating systems.
- Applications, using legacy mechanisms.

Figure 2: Overall Structure of a Security Solution



Leverage Automation to Manage Rapid Changes That Affect Access Rights

Leverage Automation to Manage Rapid Changes That Affect Access Rights

Rapidly changing business conditions drive constant access-based rights changes, which must be efficiently and effectively propagated throughout the enterprise. When an individual's attributes change at the source—or when access policies change—the domains that the individual can access should change dynamically. For example, removing or suspending user privileges when they are no longer needed is particularly important to limit unauthorized access to the network and applications.

Executing the appropriate business processes precisely when user identities change is called life-cycle management. A key to effective life-cycle management is automation. Because Tivoli Identity Manager is an automated identity management solution, it helps an enterprise minimize:

- The elapsed time it takes to turn rights on and off.
- The time administrators spend on routine tasks.
- Errors in provisioning access rights.

The automation capabilities of Tivoli Identity Manager enable an enterprise to be responsive to changes without sacrificing the appropriate controls for protecting assets. For example, the enterprise can automate the process of retrieving the manual approvals required for access. Tivoli Identity Manager helps the enterprise establish workflows for sending requests for approvals to “owners” of secure resources—and then to automatically execute those workflows in accordance with the enterprise's policies.

Additionally, Tivoli Identity Manager provides a reconciliation capability to help determine any mismatches between the user access policy and the actual access being granted at any time. By running this capability on a scheduled basis (for example, weekly), an enterprise can align its responsive changes to access rights with the business policies it sets.

Delegate Management, Self-Care and Regulatory Compliance

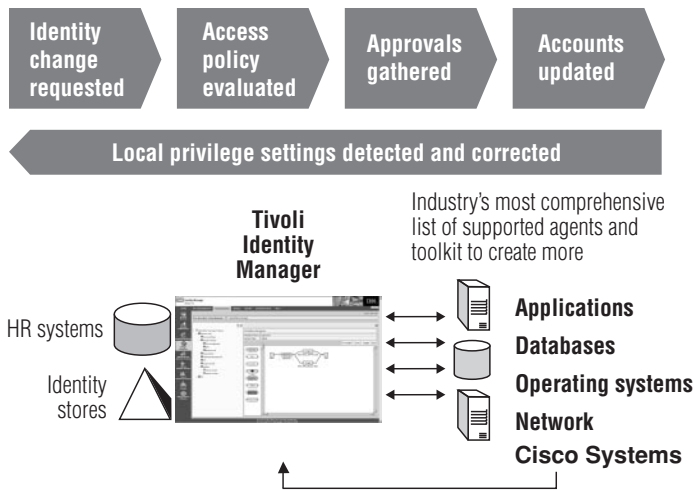
Because Tivoli Identity Manager helps automate the appropriate responses to changes in user identity information and in business policies, administrators can spend less time on these routine administrative tasks. The IBM solution also enables administrators to minimize time they spend:

- Managing security data and policies that should be controlled by others throughout the organization.
- Responding to password requests.
- Complying with auditing and regulatory requirements.

In many organizations, the network team is separate and maintains the controls over the network topology. Tivoli Identity Manager enables these organizations to delegate the management of the specifics of the IBNS structure to the network team. The solution enables an enterprise to retain centralized control while granting local autonomy, which can drive security and consistent policy on sensitive systems. Additionally, the network team can fine tune the network access policy through Tivoli Identity Manager because of their thorough understanding of the topology and characteristics of the network.

Establish Security Compliance Policies for Device Connectivity

Figure 3: Structure of an Identity Management Solution



Providing the capability for self-care is extremely important, especially in large environments where some users may not use their passwords frequently. Tivoli Identity Manager enables users who forget their passwords to provide some piece of personal data, a user ID and—possibly—a third authentication method to regain access. This capability helps an enterprise minimize the load on its help desk and free resources for more critical tasks. Furthermore, users who use the self-care capabilities view the enterprise as coordinated and quick to address the changes that affect their access rights.

Tivoli Identity Manager provides a wide number of audit capabilities and report tools that an enterprise can use to generate reports about the access rights of its network and application users. Accurate reports help the enterprise demonstrate compliance with both internal and external audits. In summary, when an enterprise implements a policy-based,

automated identity management infrastructure that draws on IBM and Cisco solutions, the enterprise helps:

- Minimize the costs associated with providing the high level of security that is now practical with an IBNS approach.
- Maximize the security of the network, operating systems and applications against both internal and external threats.
- Respond to the changing needs of the business.
- Provide the auditing required by regulatory and business process controls.

Establish Security Compliance Policies for Device Connectivity

As discussed at the outset of this paper, the other major category of security management relates to devices. For an enterprise to protect itself from devices that are corrupted or have not addressed the security vulnerabilities and policy violations that the enterprise identifies, the enterprise needs a way to understand the characteristics of a device. When an end point (any device) connects to the enterprise, the enterprise should be able to evaluate security compliance criteria such as:

- Operating system levels.
- Patch levels.
- Antivirus software levels.
- Behavior-based intrusion-prevention capabilities.
- Configuration settings that protect the device and the enterprise.

Establish Security Compliance Policies for Device Connectivity

To evaluate devices that make access requests, an enterprise first defines a policy for each class of devices—a policy consistent with the risks the enterprise is willing to take. Then the enterprise propagates the policy to devices throughout the enterprise, enabling the device to check itself for security compliance.

Finally, the network needs to enforce the security policy. Removing a device from the network is not sufficient; the enterprise should implement a closed-loop process to evaluate why a device has been isolated from the secure network and then apply the appropriate remedy. Only this complete process allows isolated devices to return to the secure environment and thereby enable users to again be productive.

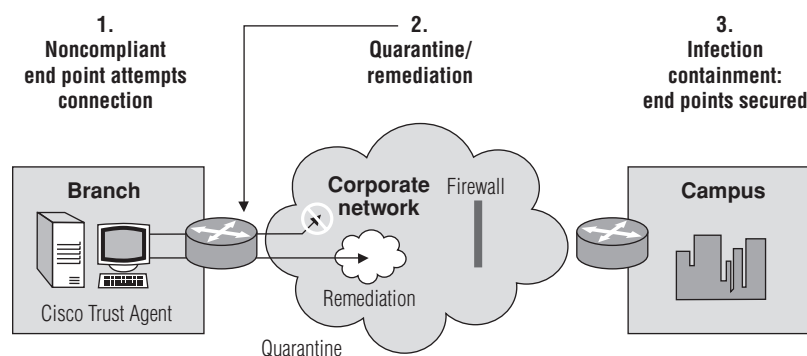
Cisco developed its Network Admission Control solution to help enterprises define and enforce security criteria that protect the enterprises from devices connecting to the network. The mechanisms Cisco has developed extend the EAP protocol at network layers two (EAP over 802.1x) and three (EAP over UDP) to transport the characteristics of a device and facilitate decisions about whether the device should be allowed onto the network. In turn, the network access devices interrogate devices about their current state and make decisions about whether to allow individual

devices onto the network. Additionally, the process leverages the Cisco Secure ACS to define the access rights. (More information about how to optimally define and manage access rights can be found in the following section, “Manage Device Compliance Policies Effectively.”)

Enterprises that want to limit most of their network access to secure devices can require each end-point device to install Cisco Trust Agent (CTA) software—and provide only limited access to nonresponsive devices. CTA is freely available and enables customers and partners to provide an interface for network access devices. Cisco Security Agent—as well as several antivirus vendors—incorporates and utilizes CTA to provide information to the network about the characteristics of the end-point device. When the device connects to the network access device, or when the network access device polls the end-point device, CTA communicates with both the compliance plug-ins at the end point and the network access device.

The network access devices are responsible for requesting information from the end-point devices and for sending that information to Cisco Secure ACS. In turn, Cisco Secure ACS compares the information against the defined security policy and, if appropriate, returns the correct Virtual Local Area Network (VLAN) for the end-point device to the access point.

Figure 4: Steps in the Isolation/Remediation Process



Manage Device Compliance Policies Effectively

If the end-point device does not comply with security policy, the network access device isolates the device in a private “quarantine” network and then returns to CTA information about why the device was isolated and how to remedy it. The network access device then polls the end-point device on the private network until the device is remedied. Finally, the network access device allows the remedied end-point device to access the enterprise’s production network.

Cisco has shipped several network access devices with these isolate-and-remedy capabilities and plans to make these capabilities pervasive across the wide variety of Cisco network access devices. The section “Isolate and Remedy Devices That Do Not Comply with Security Policies” explains how IBM solutions work with these Cisco capabilities to help an enterprise both enforce security and restore productivity.

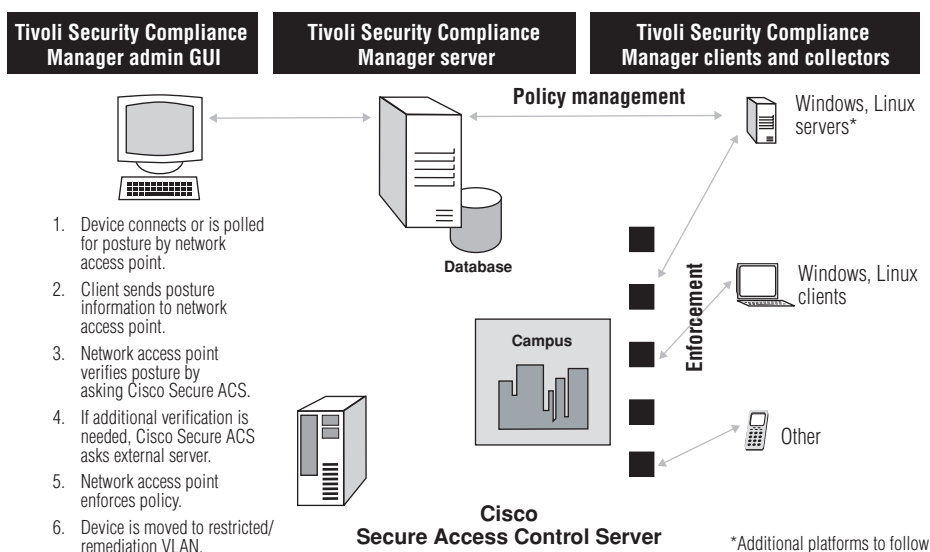
Manage Device Compliance Policies Effectively

Setting and maintaining the security access policies for devices that connect to an enterprise’s network are keys to effectively protecting the computing infrastructure from malicious and inadvertent damage. Cisco Secure ACS provides a user interface that an enterprise can use to define the policy it wishes to enforce. But because Cisco Secure ACS is a key, performance-sensitive component of the network infrastructure, enterprises should not overload the Cisco Secure ACS with sophisticated policy matching.

In response, enterprises can use IBM Tivoli Security Compliance Manager as the policy definition and management component for Cisco Network Admission Control. Tivoli Security Compliance Manager can be leveraged to limit the resource constraints on Cisco Secure ACS and enable sophisticated policy definition and checking. Tivoli Security Compliance Manager enables an enterprise to:

- Define a policy for a particular class of devices using a flexible GUI.
- Manage the collector components of the policy. Collectors are Java™ routines that run on the end-point system to determine the presence and absence of specifically defined compliance criteria. Each compliance criterion requires a routine that understands how to check for that particular exposure in the corresponding end-point operating environment. Tivoli Security Compliance Manager allows an enterprise to associate a set of available collectors with a policy.
- Deliver the policy—along with the collectors associated with the policy—to the required end points.
- Perform the compliance check when requested by the network.
- Report on the compliance status of end points in the enterprise. Tivoli Security Compliance Manager provides a rich set of reporting capabilities for audit purposes.

Figure 5: Tivoli Security Compliance Manager Architecture and Process Steps



Isolate and Remedy Devices That Do Not Comply with Security Policies

Cisco Secure ACS needs to keep track of the policy that each device must adhere to. Tivoli Security Compliance Manager helps an enterprise simplify this requirement—and minimize the workload on Cisco Secure ACS—by enabling Cisco Secure ACS to know only the number of the policy that each class of devices must comply with, rather than the detailed descriptions of every check in that policy. Tivoli Security Compliance Manager abstracts detailed check information for Cisco Secure ACS. As compliance criteria change over time, the enterprise updates the local version of the compliance policy to keep devices protected for the enterprise.

When a device connects to the enterprise—and on a regular basis if it remains continuously connected—Cisco network access devices can challenge the device to provide the current policy that it has successfully met. Devices running the Tivoli Security Compliance Manager client can respond to the network with the current policy status of the end point. (As with CTA, enterprises can require that devices run the Tivoli Security Compliance Manager client and offer limited access to those that do not respond to Tivoli Security Compliance Manager requests.)

The Tivoli Security Compliance Manager server is designed to provide sophisticated capabilities to track and manage the compliance of end points. Not all the characteristics of an end point necessarily need to be part of the network admission process. An enterprise can monitor and track the compliance of additional security measures without using them for access enforcement. This monitoring capability may be useful for reporting, auditing and preparing to add compliance criteria to the enforcement layer.

In summary, enterprises use Tivoli Security Compliance Manager to centrally control the compliance of end points with policy the enterprise defines, enforce policy before and during device connections to the network, and audit and report on the current state.

Isolate and Remedy Devices That Do Not Comply with Security Policies

When an end point does not comply with the enterprise's policy or respond to its challenges, Cisco network access devices (in conjunction with Cisco Secure ACS) move the end point to an isolated part of the network. The isolated end point might be misconfigured or lack some required software update or security product. Alternatively, the enterprise may place additional requirements on users to maintain a certain level of security, such as password strength or power-on passwords.

Whatever the reason for the isolation—and whether isolation restricts all access or only limits access to certain parts of the network—isolation can impact a user's productivity. Adequately returning an end point to the secure network and thereby restoring user productivity require that the solution enable the enterprise to correct these problems. IBM solutions work closely with Cisco solutions to remedy isolated devices.

Isolate and Remedy Devices That Do Not Comply with Security Policies

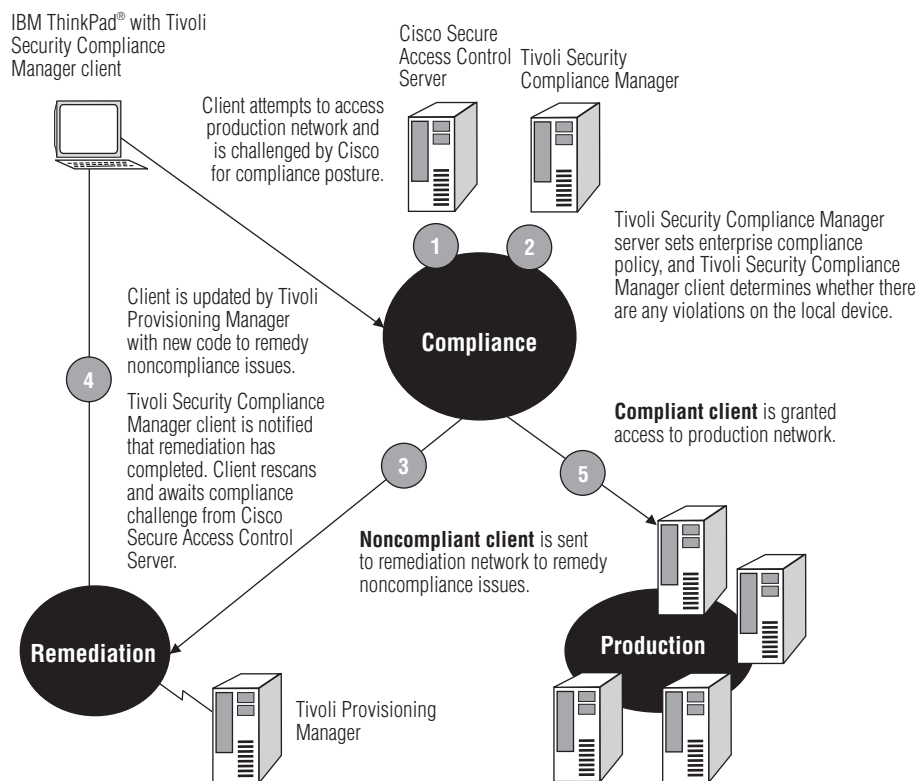
When the network isolates a device, it returns to the Tivoli Security Compliance Manager client a token that represents the reason the network denied the end point access to the production network: either the end point has the wrong level of policy or which compliance check the end point failed. Additionally, the token includes a string that represents the location the end point can get fixed. The Tivoli Security Compliance Manager client then triggers the subsystem that remedies the location where the error resides.

IBM Tivoli Provisioning Manager provides a solution that enterprises can use to remedy end points. Leveraging the solution's rich workflow environment and wide range of end points, enterprises centrally manage the software and configuration for end points.

Tivoli Provisioning Manager accepts the token from Tivoli Security Compliance Manager and runs a set of processes to trigger the remedy. These processes interrogate the token to understand what needs to be changed on the end point, and trigger the automated or interactive processes to make the required corrections. Tivoli Provisioning Manager includes the following remediation scenarios:

- Software levels (typically operating system levels and fix packs)
- Patch levels
- Virus and firewall update
- Last virus scan
- Password strength and history
- Policy level

Figure 6: Steps in the Compliance-and-Remediation Process



Achieve a Highly Secure Enterprise Computing Infrastructure with IBM and Cisco Products

For the included remediation capabilities, an enterprise prepares Tivoli Provisioning Manager with the specific updates that it requires of end points in the network. When an end point is isolated, Tivoli Provisioning Manager utilizes a specific remediation service to correct the error specified in the token, whether by installing software updates or by correcting configuration issues.

The most basic method Tivoli Provisioning Manager uses to make the required changes is over a Secure Shell session. In the future, more sophisticated device management capabilities will be provided for updating the target system.

Once errors are corrected, the network again interrogates the end point. At this point the compliance check should succeed and the device is readmitted to the secure production network.

Tivoli Provisioning Manager provides the framework and full set of software management capabilities for end points that enterprises can leverage to extend and automate their remediation and software management processes. The product allows an enterprise to add remediation processes as the need arises.

In the Microsoft® Windows® environment, IBM Rescue and Recovery with Antidote Delivery Manager provides a similar ability for end points to retrieve updates to become compliant with policy. When Tivoli Security Compliance Manager moves a noncompliant Windows end point to a quarantine network, the IBM Rescue and Recovery client can be configured to check a repository for required updates.

In environments where Tivoli software is not present, Antidote Delivery Manager will address situations where the latest Antidote Delivery Manager log entry does not match the requirements for the enterprise. Antidote Delivery Manager will be architected to utilize Cisco Network Admission Control to remove the end point from the network.

Achieve a Highly Secure Enterprise Computing Infrastructure with IBM and Cisco Products

The keys to protecting an enterprise's computing infrastructure are knowing who has access to the enterprise's resources and the security state of the devices used for connection. Restricting access to the network and other resources can best be achieved with a broad, automated identity management capability and a layered approach to enforcement. Superior management of the compliance of end points that connect to the enterprise includes remedying those end points when they do not comply with the enterprise's security policy.

The following integrated IBM and Cisco products help enterprises implement the identity and device management to mitigate weaknesses in their organizations' internal controls, and optimize compliance with the requirements of government regulations and audits.

User Access and Identity Management Components

- Cisco Secure ACS—Provides a centralized identity networking solution and simplified user-management experience across all Cisco devices and security-management applications. Enforces assigned policies by allowing network administrators to control who can log into the network and the privileges of each user. Records security audit or account billing information. Extends access security by combining authentication, user and administrator access, and policy control from a centralized identity networking framework. Helps maximize flexibility and mobility, security and user productivity.

Achieve a Highly Secure Enterprise Computing Infrastructure with IBM and Cisco Products

- Tivoli Access Manager for e-business—Implements a policy-based access control solution for On Demand Business and enterprise applications that is in the leader quadrant of Gartner’s Magic Quadrant. Helps manage growth and complexity, control escalating management costs and address difficulties of implementing security policies across a wide range of Web and application resources. Integrates with On Demand Business applications out-of-the-box to deliver a secure, unified and personalized experience. Leverages authentication and authorization APIs—and integrates with application platforms such as J2EE™—to secure access to business-critical applications and data spread across the extended enterprise.
 - Tivoli Identity Manager and IBM Directory Server—Tivoli Identity Manager provides a secure, automated and policy-based user management solution across both legacy and On Demand Business environments. Integrates intuitive, Web-based administrative and self-service interfaces with existing business processes to simplify and automate the management of users and provisioning of resource entitlements. Tivoli Identity Manager can automate user life-cycle management and use identity data for auditing, reporting and more. It can take advantage of the robust scalability and reliability of the IBM Directory Server.
- Device Compliance and Remediation Components**
- Tivoli Security Compliance Manager—Deploys a security policy compliance product for small, medium and large businesses. Implements an early warning system that identifies security vulnerabilities and security policy violations. Defines consistent security policies, and monitors compliance of these defined security policies. Bases security policies on both internal security requirements and industry-standard security policies.
 - Cisco Trust Agent—Installs client software on hosts that must have their policy state validated before the network permits access. Leverages the Cisco Network Admission Control model to allow only compliant systems access to network resources and thereby limit potential security risks from rogue or nonupdated systems. Enables Cisco Network Admission Control to determine if Cisco Security Agent and antivirus software are installed and current, as well as the current operating system and patch level. You can obtain Cisco Trust Agent at no charge—either from Cisco as a standalone application or bundled with Cisco Security Agent—or from Cisco Network Admission Control participants (with Trend Micro’s OfficeScan, for example).
 - IBM ThinkVantage™ technologies—Provides better user and device authentication, and reduces the device exposure to tampering with IBM laptops and desktops, which help lead the industry in providing “smart” devices that include a hardware-rooted trust capability.
 - Tivoli Provisioning Manager—Automates the manual provisioning and deployment process using best-practice workflows. Leverages prebuilt workflows to control and configure major vendors’ products. Customized workflows can be created to automatically execute the data center’s best practices and procedures in a consistent, error-free manner. For example, using automation workflows to provision and deploy a server (from bare metal to full production) with the single push of a button.
 - IBM Rescue and Recovery with Antidote Delivery Manager—Uses a unique capability to remedy clients even when the primary operating system has been disabled by a virus, worm or other software issue. Reacts to Windows events quickly, efficiently and with confidence by providing an ongoing ability to deliver payloads. Disables connectivity in Windows to prevent the spread of harmful software. Creates a secure repository for updates. Leverages IBM Rescue and Recovery backup facilities to facilitate recovery from catastrophic worms and viruses.

For More Information

For More Information

To learn more about IBM security solutions and integrated solutions from IBM, contact your IBM sales representative or visit ibm.com/security

More information about Tivoli security management solutions can be found at ibm.com/tivoli

For more information about IBM and Cisco security solutions visit ibm.com/security/cisco



Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
www.cisco.com/go/ibm



International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
ibm.com/security/cisco

© 2004 All rights reserved.

IBM, the IBM logo, RACF, ThinkPad, ThinkVantage, Tivoli and z/OS are trademarks of International Business Machines Corporation in the United States, other countries or both.

Cisco, Cisco Systems and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates or for an unlimited period of time. IBM reserves the right to alter product offerings, prices and specifications at any time, without notice.

Each IBM and Cisco customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. Neither IBM nor Cisco provides legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.