



Corporate  
Alliance



SOLUTIONS

## IBM and Cisco Deliver Identity-Based Networking Services

### IBM and Cisco: Next Generation e-business Solutions

#### Highlights:

- **Integrates the Tivoli Identity Manager with Cisco Identity-Based Networking Services (IBNS) to help ease customer identity management when enabling port-level user authentication**
- **Results in centralized identity management with the power to automate, audit, and enforce security access policies across all IT resources**
- **Delivers tightly provisioned identity-based access at the switch port level**
- **Enables customers to dynamically understand and control exactly who is accessing their network resources**

#### Threats to the Enterprise

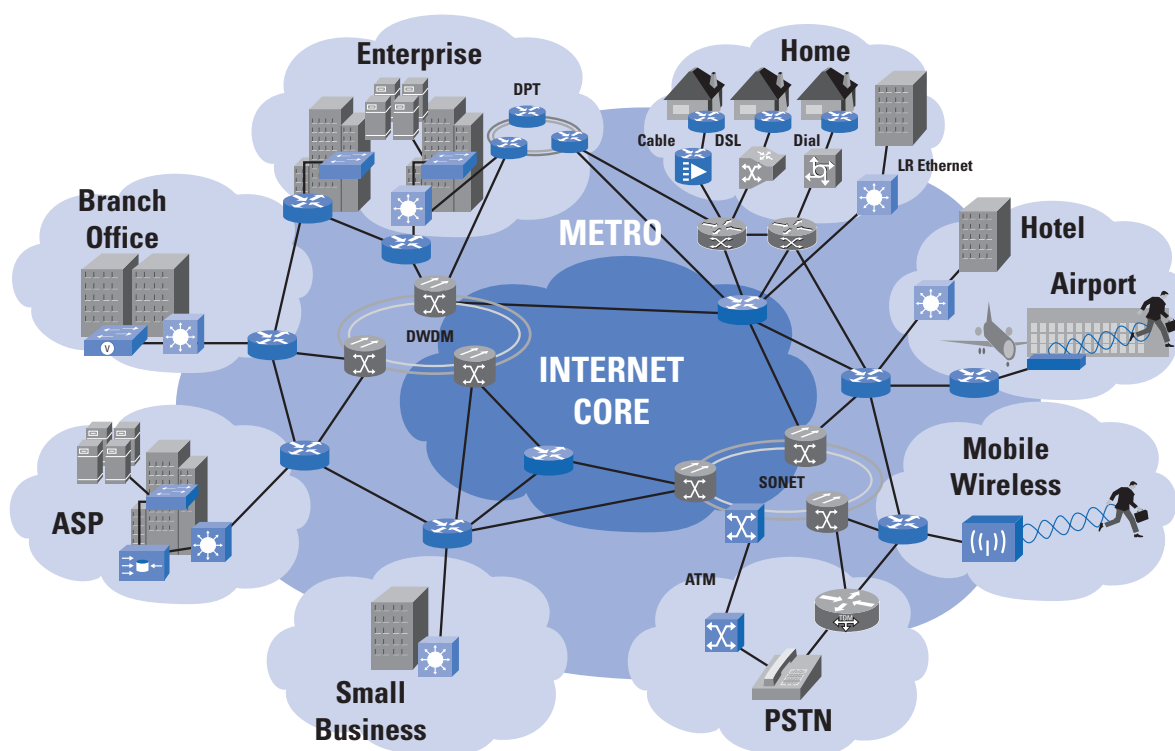
To address today's competitive e-business challenges, organizations are leveraging their IT infrastructures and extending the use of their IT investments in networks, systems, and applications to efficiently connect with customers, suppliers, and business partners. However, while many-to-many connectivity can drive 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 many enterprises. Businesses typically spend more to combat these evolving threats, yet their security capabilities often have not risen to meet the need.

IBM and Cisco Systems are helping enterprises address these security exposures in two key areas. The first is managing the identities of users who connect to the enterprise and the second is dealing with the "wellness" of a device connecting to the network. By knowing the identity of the individual connecting to the corporate network, an enterprise can better control the user's access. This solution brief will address techniques to help protect the enterprise from individuals who are not authorized to access resources over the network.

#### User Identities

In most enterprises today, the identity of the person connecting to the enterprise network is not known. The individual is given a TCP/IP address when connectivity (physical or wireless) is made, which allows access to any non-protected information in the enterprise whether this individual is authorized for that access or not. Given the state of the art today, the management of the credentials and ultimately the access to resources is limited to critical applications. The management of the users associated with these applications has been time consuming and difficult for most IT staffs and, therefore, the automated and centralized user rights management for an enterprise has not been done. This leaves the users who get connectivity access to the enterprise a wide range of latitude for unauthorized access (see Figure 1).

**Figure 1: The Evolved Network Impacts Security**



This wide open access can result in users either maliciously or inadvertently causing security exposures to the enterprise. This problem has been greatly increased by the demands of the new computing and business models like on-demand, which drives companies to increase the number of users with access to the enterprise including business partners, temporary workers or, in some cases, competitors. Because of the basic structure of the identity infrastructures that have been built, enterprises are able to restrict access to certain applications. However, much of the data on the companies computing infrastructures may be available to everyone.

The ability for a diverse set of network users to access much of this information can create many problems. Access to sensitive information—whether it relates to business partners, competitors, or is simply beyond a role-based need to know—creates an exposure for many enterprises. Also, broad access to the enterprise can allow users who are not authorized or have a malicious intent to access the computing infrastructure. Unauthorized users can create havoc and be undetected by the enterprise.

## **Verifying Identities for Network Access**

### *Identity-Based Networking*

In today's mobile environment an individual who connects to the network may do so from many different locations. The network today does not know who the user is that is making requests for resources. A methodology for handling this exposure is available in Cisco's network access devices in conjunction with Cisco's Secure Access Control Server. When a request is made for access, the network challenges the individual to give valid credentials to take advantage of the network resources.

Cisco provides this capability by taking advantage of the industry standard 802.1x protocol. This protocol allows for the request of identity for network access. The capability is supported on most of the popular end point systems today. This is the same protocol commonly used with user authentication for wireless access. When a request is made to the network, a valid user identity needs to be established before the request can be satisfied.

it relates to **business partners, competitors,**  
or is simply beyond a role-based need to know—creates an

When an end point makes a network request, the network access device verifies the user prior to granting the request. The network access device will ask the end system for an identity. When the identity is supplied by the end system, the network access device will send this information to the Cisco Secure ACS for validation. If this is a valid user, the Cisco Secure ACS will tell the access point to grant the request. If not, the request will be denied.

Cisco Secure ACS is the policy definition point for network access. Therefore, Cisco Secure ACS contains all the valid users and the credentials that devices must present to get access to the network. When a network access device generates a user authentication request, the Cisco Secure ACS validates whether this user is valid and returns the appropriate response back to the access device.

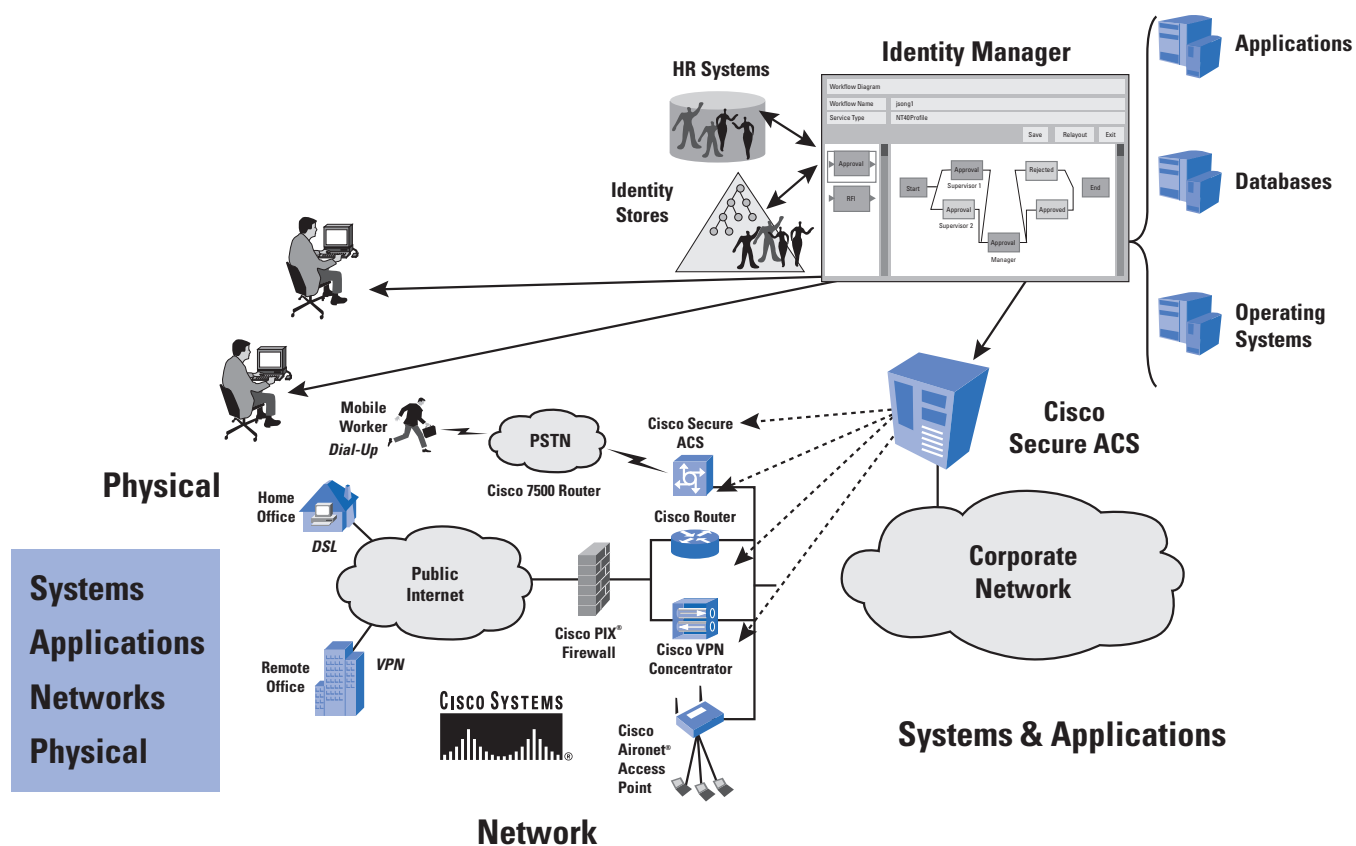
A layered approach to user access enforcement is a best practice for businesses to use. When looking at the architecture for an enterprise that wants to effectively manage access to resources, the enforcement of access needs to be multitiered. IBM and Cisco have provided a robust set of layered enforcement capabilities. Cisco Secure ACS and the network layer are the first line of defense to keep unknown users off a network. Subsequent layers of access control are provided by systems such as Tivoli Access Manager, which manages access to Web applications, end point intrusion prevention systems such as Cisco Security Agent, specific operating system access controls like the capabilities on z/OS provided with Resource Access Control Facility (RACF), and enforcement of the application specific access. This access control can provide additional granularity, such as specific rows in a data table, or may involve a relationship between the data and the requestor, as in the privacy situation.

### *Management of the User Population*

To implement and maintain the number of users required for a network level identity model, the enterprise should have a robust management solution. Maintaining the relationships required between the users who are allowed access to the enterprise, what rights they have in the enterprise, and maintaining the “enforcement” arms of the infrastructure creates a very large management problem. Tivoli Identity Manager and the integration that has been done with Cisco’s identity-based networking can help manage this environment. An enterprise can even extend this “logical access management” to include the physical world by integrating with a physical security vendor (badge readers, smart cards, digital video surveillance).

The process starts with an enterprise’s trusted source of users, like the human resources database. This database defines the individuals who have rights in the enterprise. There may be other “trusted” sources for partners, customers, and so forth, such as the enterprise’s relationship management system. All these systems carry some valuable information about the users, such as their department, responsibilities, title, and so forth. Tivoli Identity Manager provides an XML interface for these applications to import the changes for updating the enterprise’s enforcement engines. The information provided by these trusted sources is used to determine an individual’s access rights. This set of access rights matches the established enterprise policy for access to their resources. These policies can determine rights for building access, network access (including subnets that they are allowed to traverse), and applications and data they can access. These access domains change based on the attribute settings from the trusted sources (see Figure 2).

**Figure 2: Unified User Provisioning System, Application, Network, and Physical Access**



The key to making this process work is the automation capabilities of the identity solution. The automation of business processes related to changes in user identities is called lifecycle management. It is particularly important in a secure enterprise to remove user privileges when they are no longer needed. This is a key attribute to managing the security and risks of the enterprise. The responsiveness of the identity solution helps cut elapsed turn-on time, automates routine administrative tasks, and helps eliminate errors. Providing an interface to allow individuals to manage parts of their own access also can improve the overall system. Along with this, individuals who deal with the enterprise now view the enterprise as coordinated and are quick to address the changes that these individuals are entitled to. In the Identity-Based Networking Services case, managing the right level of access to network topologies is important. Also, dynamic business conditions drive constant access-based rights changes, which must be efficiently and effectively propagated throughout the enterprise.

When the rights of an individual are determined, Tivoli Identity Manager provisions the user to the appropriate enforcement points. These enforcement points may be badge readers, the network (through Cisco Secure ACS), Web applications (through Tivoli Access Manager), operating systems, or applications (by legacy mechanisms).

Tivoli Identity Manager provides the capabilities to control these access rights. Although an enterprise wants to be responsive, it needs the appropriate controls in place to protect assets. These controls include the ability to automate the process of retrieving the required sign-offs for access. A business needs the following to provide proper access to critical resources: (1) the workflows associated with sending requests to owners of the secure resources for their approval and (2) the mechanisms to provide the level of control. Also, accounts that are no longer in policy need to be removed or suspended to ensure unauthorized access to the network

and applications does not occur. Tivoli Identity Manager provides a reconciliation capability to determine any mismatches between the policy for user access and the actual access at any time. Most customers would run this on some scheduled basis such as weekly.

The ability to delegate the management of the IBNS structure to the network team is a key component in many organizations where the network team is separate and maintains the controls over the network topology. The ability to delegate retains centralized control and local autonomy, which can ensure security and consistent policy on sensitive systems. In addition, the network team continues to best understand the topology and characteristics important in the network.

In large environments where the access may not occur on a regular basis, providing the capability for self care is extremely important. The ability for a user who has forgotten a password to use something familiar to get access is important. Providing the individual's mother's maiden name or some other piece of data along with the user ID and possibly a third authentication method provides a way for users to gain access again. This capability can reduce help-desk load and free resources for more critical tasks.

Providing generalized access to the network in many cases violates the rules and regulations being put in place by governments to protect the personal information. These rules and regulations in most cases are process related and look at the methods used to grant access. To prove compliance or to ensure the controls a business needs, audits are performed. The infrastructure put in place must provide the accurate reporting capabilities to satisfy the needs of internal and external audits. Tivoli Identity Manager provides a wide number of audit capabilities and access to report tools, which can be used to generate reports associated with the access rights of users in the network and for applications.

In summary, the management infrastructure needs to lower costs associated with providing the high level of security that is now practical with an IBNS approach. These security measures protect the enterprise from unauthorized access. These same tools must be responsive to the changing needs of the business while also providing the auditing required by regulatory and business process controls.

## **Solution Components:**

### *Cisco Products*

Cisco Catalyst® switches, including Catalyst 6500, 4500, 3550, and 2950 switches

Cisco Secure Access Control Server

Cisco Aironet® Access Points

### *IBM Products*

IBM Tivoli Identity Manager

*Solution can also include:*

IBM Tivoli Access Manager for e-business

IBM Tivoli Directory Integrator

IBM Tivoli Directory Server

IBM WebSphere® Portal

IBM WebSphere

IBM @server

## **Engage World-Class Service**

To ensure a smooth implementation, IBM Global Services can work with customers to define security policy and access control requirements, design and plan the solution based on defined compliance and remediation policy, install and test the integrated identity solution, including business and systems consulting, design, project management, procurement, and cabling.

One of the world's leading services providers, IBM Global Services brings the IT, networking, security and identity management skills needed to implement a successful user management process project. These capabilities have been honed through years of consulting for and deploying user installation solutions of all sizes. IBM Global Services has developed technical and process skills with the technology associated with user life cycle management. This experience can be applied to user management projects to speed execution and manage project risk.

From consulting, planning, and design through integration and testing, IBM Global Services can offer end-to-end services solutions for identity-based networking management. IBM Global Services business and technology consultants, with extensive industry experience and proven track record, understand the key role that the user plays in business.

For more information on how IBM and Cisco team together to provide identity-based networking management, see:

[www.cisco.com/go/ibm](http://www.cisco.com/go/ibm)  
[www.cisco.com/en/US/products/sw/conntsw/index.html](http://www.cisco.com/en/US/products/sw/conntsw/index.html)  
[www.ibm.com/security/cisco](http://www.ibm.com/security/cisco)  
[www.ibm.com/websphere](http://www.ibm.com/websphere)  
[www.ibm.com/tivoli](http://www.ibm.com/tivoli)  
[www.ibm.com/security](http://www.ibm.com/security)  
[www.ibm.com/software](http://www.ibm.com/software)



Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
[www.cisco.com/go/ibm](http://www.cisco.com/go/ibm)



IBM Global Services  
Route 100  
Somers, NY 10589  
[www.ibm.com/security/cisco](http://www.ibm.com/security/cisco)

Copyright © 2004 IBM Corporation. All rights reserved.

IBM, the IBM logo, the e-business logo, the eServer logo, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems, 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.

Aironet, Catalyst, Cisco, Cisco Systems, the Cisco Systems logo, and PIX are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document 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.