

# Identity-Based Networks: Pathway to Cloud Computing

If your family members are the only ones using a storage locker, security is simple: only give out the lock combination to family members.

But let's say you want the economies of scale of a larger unit, and decide to share the costs with multiple families that each pay proportionately for the space they actually use. This creates new security challenges, such as making sure that only authorized users can come in, that they take only their own assets, and that you have a good record of who took what, and when.

And of course you'd prefer to authorize people as they drive up to the facility, not when they've gotten past the entrance and are already at the storage-unit door.

Like the above scenario to cloud computing, and you have a good idea of the types of security protections needed. Fortunately, these solutions are available today and already in use on agency networks.

## Keeping the Cloud Secure

Cloud computing refers to maintaining a common pool of computing resources, available on demand for whichever agency or department needs them at any given moment. "Agencies can confidently adopt cloud computing if they know they can access assets in the cloud whenever they want, and that no one else can," says Steven Craven, consulting systems engineer for the public sector, Cisco.

Agencies get this assurance when their networks can answer five questions:

- **Who are you?** The agency needs to know the identity of every person and device attempting to access the cloud. The person might be an agency employee, guest, contractor, or consultant. And the device might be a PC or laptop, IP phone, video surveillance camera, chemical sensor, or something else. The Information Awareness Office (IAO) requires use of 802.1X authentication.
- **Is your device healthy?** When a device attempts to connect to the agency network, it should be scanned to make sure it's infection-free and has the required antivirus software, operating system patches, and security settings. Government IT departments save time if the security solution can automatically perform remediation on noncompliant devices.
- **Where can you go?** Your identity determines which networks, applications, and resources you can access. A budget analyst, for example, needs access to agency financials while an IT staffer needs access to network management tools.
- **What service level do you receive?** People need different levels of service based on their role. For example, first responders and military personnel need assured service levels for voice, video, and data.
- **What are you doing?** Government needs a record of which users have accessed which resources, and from where. The same information is used for billing as well as incident investigation.

## Where You Authenticate Identity Makes a Difference

This five-questions approach is called role-based access control, and many agencies already use it. What's new is where it's performed, according to Tim Simon, federal marketing manager, Cisco. "Currently, most agencies authenticate the user on the host itself," he says. "The issue is that unauthorized users are already on the network before they're stopped, which increases the chances that intruders can steal private data or harm critical infrastructure."

Other disadvantages of authenticating users and devices on the host are that IT departments have to take the time to configure every application, and agency users need to sign in to each application separately, which is time-consuming and annoying.

## The Identity-Based Network

The Cisco Identity-Based Network moves up the point of authentication from the host to the network. When an employee, contractor, or guest attempts to sign on to the agency network, the network confirms that the person and the device are authorized, and then connects the user to the appropriate VLAN.

The IT department only needs to set up authentication once, not once for each application. And users only need to sign on once to access all network resources and applications, increasing their productivity.

Craven concludes, "An identity-enabled network provides better protection for an agency's assets. It also vastly simplifies deployment compared to host-based authentication." What's more, agencies can take advantage of the same technology when they move assets from the local network to the cloud.

To view a whitepaper on the Identity-Based Network, visit:

<http://fcw.com/Whitepapers/2009/11/Meeting-Govt-Security-Regulatory-Goals-through-NAC.aspx>

To sign up for a Security in the Cloud conference in January 2010, visit: [www.digitalgovernment.com/cisco](http://www.digitalgovernment.com/cisco)




**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).

 CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco-Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLXNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo 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. (0910R)

All contents are Copyright © 1992–2010 Cisco Systems, Inc. All rights reserved. This document is Cisco Public Information.