

Access Control: First Step in Information Sharing Within Communities of Interest

Today's dynamic operational environments rely on close collaboration among communities of interest – with goals as diverse as peacekeeping, humanitarian response, and commerce. Until recently, security constraints forced each partner to build and maintain their own infrastructure. When partners needed to share information, they typically had to approach someone they knew personally. “In the early days of information sharing, trust was based on personal relationships,” says Howard Schmidt, President and CEO of R&H Security Consulting, LLC, and former Special Adviser for Cyberspace Security. “You worked with someone, gave them a little information with the understanding they would protect it, and then they shared their information with you.”

The establishment of government Information Sharing and Analysis Centers (ISACs) underscored the need for a more institutionalized process for information sharing – one that could survive longer than personal relationships. “Government needs automated systems that ensure that information gets to the right person, at the right time, on any device,” says Schmidt.

Access Control: The First Step

“Of the four requirements for secure information sharing among agencies – access control, content protection, data protection, and watchdog services – access control is often the first that agencies implement,” says Chris Shenefiel, federal government industry solutions manager for Cisco. Federal agencies have made progress in network access control by implementing Personal Identification Verification (PIV) cards that comply with FIPS 201.

By authorizing users, PIV cards only address one half of the access-control challenge, however. The other half is verifying the security posture of the device used for access. “Communities of interest need a way to ensure that employees can only access the network if they are using a device that is infection free, installed with required software or patches, and otherwise complies with the agency security policy,” says Tim Simon, Cisco Federal security marketing manager.

The Big Three for Access Control: Identify, Scan, and Remediate

To provide effective access control in a community of interest, the solution needs to:

- *Identify* the user and the user's role. Federal contractors, for example, might be given access to a separate VLAN that does not provide access to servers containing sensitive information.
- *Scan* the user's device – PC, laptop, or personal digital assistant – to determine if it complies with the agency's security policy. Policies can stipulate the presence of required software, absence of unauthorized software, misconfiguration, software defects, and user account issues such as null passwords.
- *Perform automatic remediation* if required, which might include repairing the infection, installing or removing software, or changing settings. “To scale for the needs of communities of interest, it's important that remediation not require any action from either the employee or the agency IT group,” says Simon.

Cisco Network Access Guardian

In response to the needs of growing numbers of government communities of interest and HSPD-12 requirements, the Cisco U.S. Federal Center of Excellence has developed an all-in-one solution for user authentication, device security posture assessment, and automated remediation. Cisco Network Access Guardian is a tested solution for Common Access Card (CAC) environments that provides additional network security. For more information on Cisco Network Access Guardian, visit <http://www.cisco.com/go/fedsecurity>.



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, Inc.
 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.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0701R)