

Cisco Products that Enable Federal Solutions

Cisco Network Access Guardian

Used for Access Control [link to article]

Cisco® Network Access Guardian is an all-in-one solution for user authentication, device security posture assessment, and automated remediation in federal government agencies. When an employee attempts to access the network using a Personal Identification Verification (PIV) card, Cisco Network Access Guardian:

- Identifies 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.
- Scans the device to determine if it complies with the agency's security posture. Agencies can configure Cisco Network Access Guardian to enforce their individual security policies by selecting from more than 25,000 preconfigured requirements or else defining their own. Citadel Hercules also includes DoD Security Technical Implementation Guide (STIG) policies for all Windows platforms.
- Automatically performs remediation if required, which might include repairing the infection, installing or removing software, or changing settings. No action from the employee or from the agency IT group is required.

Because it is an all-in-one solution, Cisco Network Access Guardian can be deployed more rapidly than separate solutions for user authorization and device security-posture checking, which must be integrated. For more information, visit www.cisco.com/go/fedsecurity.

Cisco Network Admission Control (NAC) Appliance

Used for Access Control [link to article]

Cisco NAC Appliance (formerly Cisco Clean Access) is an easily deployed Network Admission Control (NAC) product. The Cisco NAC product uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources. With Cisco NAC Appliance, network administrators can authenticate, authorize, evaluate, and remediate wired, wireless, and remote users and their machines prior to network access. It identifies whether networked devices such as laptops, IP phones, or game consoles are compliant with your network's security policies and repairs any vulnerabilities before permitting access to the network. If the device complies and the employee is authorized, network access is granted. If the device is noncompliant, the Cisco NAC Appliance quarantines the device and performs automatic remediation before granting access. For more information, visit www.cisco.com/go/nac.

Cisco Adaptive Security Appliance

Used for Secure Information Sharing [[link to article](#)]

The Cisco ASA 5500 Series Adaptive Security Appliance is a modular platform that provides the next generation of security and VPN services. It combines multiple security functions that federal agencies need for secure information sharing with their own employees and others in the community of interest. Providing security functions in one chassis reduces operational expense and simplifies government data centers. Available modules, called Cisco ASA Editions, include firewall, intrusion prevention, anti-x, and VPN. For more information, visit www.cisco.com/go/asa.

Cisco IPv6 Assessment Services

Used for IPv6 Transition [[link to article](#)]

Cisco offers a wide range of IPv6 implementation capabilities to address short-term requirements while also supporting a more gradual long-term approach incorporating best practices and knowledge derived from previous customer deployments. To design a migration roadmap best suited to your specific needs while mitigating transition, cost, security, and training concerns, Cisco provides assessment services that use a collection and reporting tool. The following items help us determine the most beneficial IPv6 deployment route for you:

- Report – A customized, color-coded survey that identifies your network's IPv6 capability status
- Score card – A confidential, high-level evaluation of the IPv6 capability of devices on the network, also color coded
- IPv6 capability assessment – A thorough analysis that compares your agency's network devices against the IPv6 business rules

After the report is compiled, Cisco creates a customized score card, assessment, and audit based on your IPv6 readiness, and then works with you to establish a migratory path aligned with your strategic business objectives. For more information, visit www.cisco.com/go/fedipv6.



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)