



U.S. National Institutes of Standards and Technology

NIST 800-53 Mapping

Laconia Group conducted a cursory review of NIST 800-53 requirements and how Palo Alto Networks' products map to the government standards and requirements.

Palo Alto Networks Firewall products map quite closely to the NIST 800-53 standards. The PAN products appear to provide compliance with or facilitate a number of technical control areas within the NIST 800-53 standards and relevant publications that provide guidance to federal agencies. Specifically, Palo Alto Networks' firewall products address the functional control areas of Access Control (AC), Identification and Authentication (IA), and System and Communications Protection (SC). The sections below define the sub elements of those control areas where Palo Alto Networks firewall directly apply as well as interactively apply through other security mechanisms such as Active Directory (AD). This cursory review was conducted by: Mr. Jeffery Wheat, Chief Technology Officer of Laconia Group in Reston, Virginia.

Access Control:

- **AC-3 Access Enforcement**
- **AC-4 Information Flow Enforcement**
- **AC-17 Remote Access**
- **AC-20 Use of External Information Systems**

Identification and Authentication:

- **IA-2 User Identification and Authentication**
- **IA-3 Device Identification and Authentication**

System and Communications Protection:

- **SC-3 Security Function Isolation**
- **SC-7 Boundary Protection**
- **SC-14 Public Access Protections**
- **SC-18 Mobile Code**
- **SC-19 Voice Over IP (Through Application control)**
- **SC-20 Secure Name/Address Resolution Service (Authoritative Source) Through AD**
- **SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver) Through AD**
- **SC-22 Secure Name/Address Resolution Service (Resolution Service) Through AD**
- **SC-23 Session Authenticity**

INFORMATION SECURITY

Computer Security Division
 Information Technology Laboratory
 National Institute of Standards and Technology
 Gaithersburg, MD 20899-8930

August 2009 -- INCLUDES UPDATES AS OF 09-14-2009 (ERRATA PAGE XI)

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

This publication has been developed by NIST to further its statutory responsibilities under the ***Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347***. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is also provided in Circular A-130, Appendix III.