



## DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549  
FORT MEADE, MARYLAND 20755-0549

MEMORANDUM FOR DISTRIBUTION

25 November 2015

SUBJECT: Palo Alto Networks Security Technical Implementation Guide (STIG) Version 1

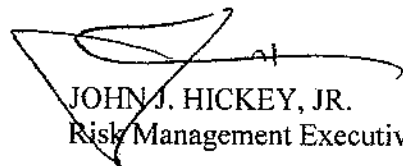
Reference: DoD Instruction 8500.01

DoD Instruction 8500.01 tasks DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders” and DoD Component heads “ensure that all DoD IT under their purview complies with applicable STIGs, security configuration guides, and SRGs.”

This STIG considered all the applicable technical NIST SP 800-53 Rev 4 requirements as defined in the Network Device Management, Application Layer Gateway, and Intrusion Detection and Prevention System SRGs. It provides the technical security policies, requirements, and implementation details for applying security concepts to the Palo Alto Networks platform (physical and virtual machine).

In accordance with DoD Instruction 8500.01, the Palo Alto Networks STIG Version 1 is released for immediate use. The document is available on <http://iase.disa.mil>.

Point of contact for this action is DISA STIG Support Desk, email: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil).

  
JOHN J. HICKEY, JR.  
Risk Management Executive

UNCLASSIFIED