

Overview

DoD computer networks are frequent targets of attack and as such require proactive security measures to maintain the highest level of security. Maintaining a secure network has become increasingly difficult, considering the explosive amount of new vulnerabilities and the rapid growth of organized, concentrated attacks. The Defense Information Systems Agency (DISA) has developed a set of Security Technical Implementation Guides (STIG's) which, when applied, will decrease the vulnerability of DoD sensitive information. Each site network/communications infrastructure must provide secure, available, and reliable data for all customers.

The Network Infrastructure STIG is designed to supplement the security guidance provided by DoD-specific requirements and assist sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure network operations. The Network Infrastructure STIG Version 7 Release 1 contains 10 sections which provide the minimum requirements for:

- Enclave Perimeter
- Firewalls
- Routers
- Device Management
- Authentication, Authorization, and Accounting
- Passwords
- Network Intrusion Detection
- Switches and VLAN's
- Virtual Private Network
- IPv6 Transition Mechanisms

The Most Effective Solution for Complying with the DISA Network Infrastructure STIG

Manually performing periodic vulnerability assessments of network devices, is labor intensive, expensive and when considering the enormous scope and the diverse network of an enterprise, it is nearly impossible. Attempting to manually detect a single misconfigured vulnerable network device among thousands is a great example of the proverbial "needle in a haystack" and the key reason why many large enterprises have suffered from attacks. Refense VMS™ effectively solves this problem by easily and proactively identifying threats and vulnerabilities within a variety of network devices.

Refense VMS™ specifically assists in complying with DISA Network Infrastructure STIG by:

- Comparing the configuration of network devices against the security policies detailed in the STIG and isolating misconfigurations and known vulnerabilities
- Providing an efficient, automated solution to perform security audits of network devices and fully documenting the vulnerabilities and misconfigurations discovered
- Utilizing the highly customizable checks, enable network administrators to perform tailored auditing of environment specific or variable configurations such as peering routing or service filtering against BOGON lists
- Enabling the responsible officers with the unit to quickly disseminate security reports detailing the vulnerabilities identified within their organization, classified by the STIG Identifier (STIGID) and sorted by the vulnerability severity code for prioritized mitigation

Refense VMS™ Security Policy for DISA/DoD

Refense VMS™ supports the DISA Network Infrastructure STIG by delivering a security policy built upon the requirements and standards laid out in each section of the STIG. This security policy combined with customized checks meets 100% of the STIGID's relating to network device configuration. A tangible illustration of where Refense VMS™ directly meets the requirements of the STIG can be demonstrated using the Routers section of STIG where Refense VMS™ can identify misconfigurations against all 72 STIGID's. The DISA specific policy provided with Refense VMS™ is directly aligned with 9 of the 10 sections of the Network Infrastructure STIG and can be applied against many vendors' network devices.

About Refense VMS™

Refense VMS™ is a vulnerability and configuration management and compliance solution targeted at network devices.

Through the use of "checks", Refense VMS™ can identify misconfigurations against a security policy and isolate vulnerabilities that result from these misconfigurations, or from known security flaws within the vendor's operating system.

The Refense VMS™ appliance based vulnerability management solution includes:

- Proprietary security algorithms and an "Inside-Out" architecture
- Completely non-intrusive
- Lightning fast and accurate (<1% false positives)
- Strong in-depth visibility and reporting
- Service provider scalability (10,000 plus devices)
- Largest number of network device security checks
- Predefined security policies based on industry best practices and recommendations
- Scheduled scanning, supports online and offline scanning
- Instant ROI and low operational administration



About Refense

Refense Technologies, Inc. is a leading provider of vulnerability management solutions for network devices. The Company develops solutions that address security concerns within network devices, the foundation of an IT infrastructure.

With Refense VMS™, organizations can proactively identify and mitigate threats and vulnerabilities within wireless and wired networks.



Refense Technologies, Inc.
105 Brooks Ave
Raleigh NC 27607
Phone 1.800.432.6187
sales@refense.com
www.refense.com