JUNIPER NETWORKS SECURITY TECHNICAL IMPLEMENTATION GUIDES COMPLIANCE SERVICE DATASHEET

Service Overview

The Security Technical Implementation Guides (STIG) Compliance Service enables organizations to adapt rapidly, gaining the agility, resiliency, and security needed to support their missions. By ensuring compliance of network infrastructure, the service protects critical platforms with simplicity and efficiency.

Service Description

Today, US government agencies manually audit their networks against Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) device by device. To improve efficiency, Juniper has developed a service that validates the network configuration against current STIG files and flags out-of-compliance devices so they can be remediated. This service greatly reduces the effort and likelihood of human error when updating critical infrastructure for compliance.

According to DISA, STIGs "are the configuration standards for DOD [information assurance, or IA] and IA-enabled devices/systems…The STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack." STIG requirements are comprehensive and include mobile devices, operating systems, cloud networks, and applications. Requirements cover all areas of device or software configuration to achieve secure integration while also focusing on the security of the systems to prevent breaches or cybersecurity incidents.

Compliance-based operations require a repeatable and efficient process that provides on-demand access, flexible expansion, and reliable, accurate evaluation of systems to identify vulnerabilities. IT teams often face limited resources as they focus on the manual adherence to the application of policies and guidelines that are constantly changing, while also having to understand the impacts to an unlimited product set. Organizations need a solution focused on removing the manual and time-consuming work of a task that can miss potential vulnerabilities in the network and decrease the security posture for the organization.

Juniper Networks® Security Technical Implementation Guides Compliance Service relies on a Juniper platform to transform the traditional ways of compliance scanning and remediation. The result is an automated approach that gives organizations an agile, secure, and expandable capability to bring operational efficiency to the required standards set forth by DISA and the Department of Defense (DOD).

The service also enables organizations to adapt rapidly, providing the agility, resiliency, and security needed to protect critical infrastructure with unprecedented simplicity and operational efficiency. With this awareness, network operators can quickly evaluate network compliance as new threats arise, even during rapidly changing network conditions.

Architecture and Key Service Components

All STIG code resides within a customer's private repository. Juniper® Professional Services provides for the maintenance of STIG library, bug fixes, new STIG updates from DISA, ATOM text editor support (if used), and open-source tooling updates.

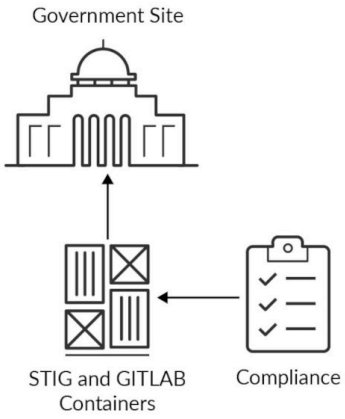

Figure 1: U.S. Government STIG primary site

Features and Benefits

With the Juniper Networks Security Technical Implementation Guides Compliance Service, organizations can take advantage of the re-usability and extensibility of an advanced network compliance and auditing tool versus manually auditing.

Automated On-Demand Auditing

The Juniper Networks STIG compliance platform transforms the traditional ways of scanning and remediation. Using an automated approach that gives organizations an agile, secure, and expandable capability, it brings operational efficiency to the required standards set forth by DISA and DOD agencies and contractors. It reduces per device audit time from hours to minutes, enabling network operators to quickly evaluate network posture as new threats arise during rapidly changing network conditions.

DISA STIG Security Risks Identification

Organizations can audit rapidly, providing the agility, resiliency, and security needed to protect critical infrastructure with unprecedented simplicity and operational efficiency.

Service Specifications

Deliverable	Description	Features and Benefits
Solution Workshop	Conduct an interactive solution workshop to review the requirements, functionality, and specifications the solution must meet.	Adapt best-practice design to customer environment leveraging the experience Juniper consultants have acquired working with hundreds of successful enterprises.
Solution Deployment	Deploy the solution in the customer's environment.	Utilize process-driven approach to ensure efficiency and accuracy; ensure that the platform is correctly installed and functioning.
Knowledge Transfer Workshop	Conduct a knowledge transfer workshop to review features, functionality, and extensibility of the solution. Anticipated activities include troubleshooting and maintenance of the solution.	Accelerate infrastructure availability and employee readiness for improved operational efficiencies.
Ongoing Annual Support	Access the customers STIG and GITLAB docker containers for break-fix work, software patches, and STIG updates.	Remain current on STIG data and assured that the platform performs at optimal level.

Ordering Information

Juniper has extensive experience working with federal agencies and supporting their specialized network and security requirements. Juniper offers IC/DOD-certified solutions for missions that demand unfailing network performance.

Learn more about ordering and Juniper solutions for Federal.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240 1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700

Juniper Networks | Driven by Experience™