FORWARD NETWORKS

WHITE PAPER

Use a Digital Twin For Impeccable Cyber Command Readiness Inspections

What is a Cyber Command Readiness Inspection?

The Defense Information Systems Agency's (DISA) Cyber Command Readiness Inspections (CCRI) evaluate technical and operational compliance. With little notice, DISA can inspect any network that is connected to the Department of Defense Information Network. Inspections focus on:

- Validating DoD Standard compliance
- Identifying vulnerabilities on unclassified internet protocol routers (NIPRNET) and secret internet protocol routers (SIPRNET)
- Assessing situational awareness of cyber security posture
- Ensuring agencies' ability to protect against cyber threats

Inspectors will evaluate compliance using published guidelines, including:

- Security Requirements Guides (SRGs)
- Security Technical Information Guides (STIG)
- USCYBERCOM warnings and tactical directives/orders
- Communications Taskings Orders (CTO)

How is an inspection conducted?

There are four phases of the inspection: scope, inspect, document, and report.

SCOPE

During the scope phase, DISA will establish a clear line of effort before the onsite inspection by providing the organization with a list of equipment types and environments to be inspected.

INSPECT

In the inspect phase, inspectors manually review device configuration files for compliance. During these audits, inspectors check devices against their respected DISA STIGs and their severity level category (CAT) I, II, or III. CAT I is at the most significant risk and urgency, whereas CAT III is a recommendation that will improve IA posture but is not required for authorization to operate.

DOCUMENTATION

In the documentation phase, the assessment and authorization (A&A) inspectors review the previous three years of network documentation and incorporate any necessary updates (e.g. new mandates or regulations). During this phase, results from the inspection are uploaded to the DoD's Vulnerability Management System for tracking, inventory, and situational awareness purposes.

REPORTING

During the reporting phase, system and network administrators must patch their devices and virtual machines or create a Plan of Action & Milestones (POA&M) which details proposed work and the projected completion time-frame.

What happens in the Out-Brief?

On the last day of the CCRI, inspecting organization leadership and the communications directorate host an Out-Brief to discuss findings. The inspected networks must score at least 70 out of 100 points or face re-inspection. If the non-compliant result is not corrected within the time specified in the POA&M, the network is subject to disconnection from the Global Information Grid.

How can I be confident my network will pass CCRI?

Because the CCRI is conducted according to published processes and regulations, if you know your network's behavior, device configuration, and security posture, determining if you'll pass is simple. Collecting this information without the help of software is tedious and error prone.

The highly detailed, actionable data delivered by Forward Enterprise inoculates the team against failure by clarifying non-compliant issues and documenting remediation before the inspectors arrive. Preparing for a CCRI requires checking each device against the index of available STIGs and documenting it for remediation or POA&M. Additionally, the network configuration infrastructure will be checked against DISA CTOs, where hardware assets will be audited against DISA-approved product listings.

Because Forward Enterprise integrates with popular tools such as ServiceNow, Itential, and Ansible, remediating issues becomes much easier. The detailed information collected in Forward Enterprise can be shared within these applications; rather than troubleshooting, engineers are spending their time remediating issues.

Forward Networks provides state-driven, continuous validation and always current documentation to prevent surprises during the inspection process.

What's the most effective way to prepare for a CCRI?

When preparing a CCRI, most teams will spend months manually querying every device and route across all their networks to validate STIG findings, ensure routes to the internet are closed (or only permit mission-essential traffic through the firewalls), and verify specific hardware on the network. Results are then reported to higher headquarters. Traditionally, teams attempt to capture this data in spreadsheets, documents, and other applications as they labor to validate compliance.

AUTOMATE DATA COLLECTION WITH NQE

The Forward Enterprise Network Query Engine (NQE) automates much of this work by collecting configuration and state data on network devices (Forward Enterprise supports all major network hardware vendors). NQE then indexes this information into a searchable database.

Using this information, engineers can run customized checks to detect noncompliance or document compliance. In most cases,these checks run in under an hour (compared to weeks when undertaken manually) and provide engineers with a detailed account of the network's topology, behavior, and configuration.
(See Figure 1)

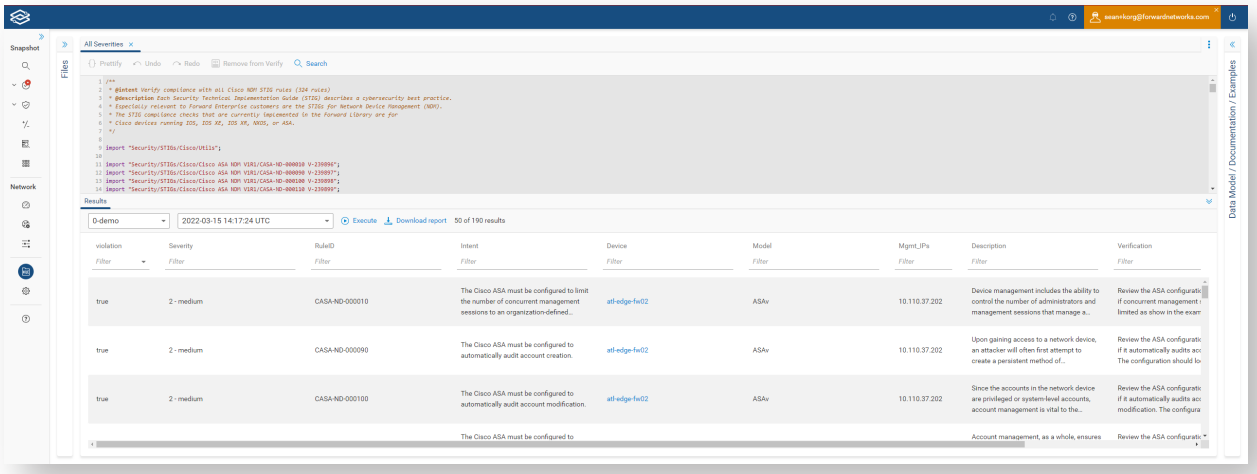

Figure 1: Sample NQE Compliance Verification Report

NQE enables a “fire and forget policy” whereby engineers can write and set NQE checks to run during snapshot processing and receive a timely, actionable alert if noncompliance is detected. Forward Enterprise documents who created NQE checks, when they were enabled, and when the last time they were updated and by whom.

Often there is an overlap between queries. NQE can export information from one query to another, eliminating repetitive work and reducing the potential for human error. To reduce the need to manually transfer data, NQE supports use of external databases (e.g. Github/lab Nautobot) within the platform.

NQE delivers a detailed view of network behavior in an intuitive table format and supports exporting the data as a CSV file to facilitate sharing information with teams that do not have access to the platform.

Additionally, technicians can view reports via Forward Networks’ comprehensive application programming interface (API).

How do I ensure network changes won’t negatively impact CCRI results?

Accuracy in documentation is imperative for passing a CCRI. However, networks are continuously changing, especially during the inspection. Documenting precisely when changes are made and by whom is virtually impossible without continuous monitoring. Forward Enterprise collections become snapshots that detail network configuration over time, including when changes were made and by whom.

Operators can perform network collections at their discretion, including on-schedule, on-demand, or event-based. All three methods can be configured with an API, while scheduled and on-demand collections can also be set up with the user interface. Event-based collections are triggered by workflows from other platforms and applications calling Forward Networks API to start a collection.

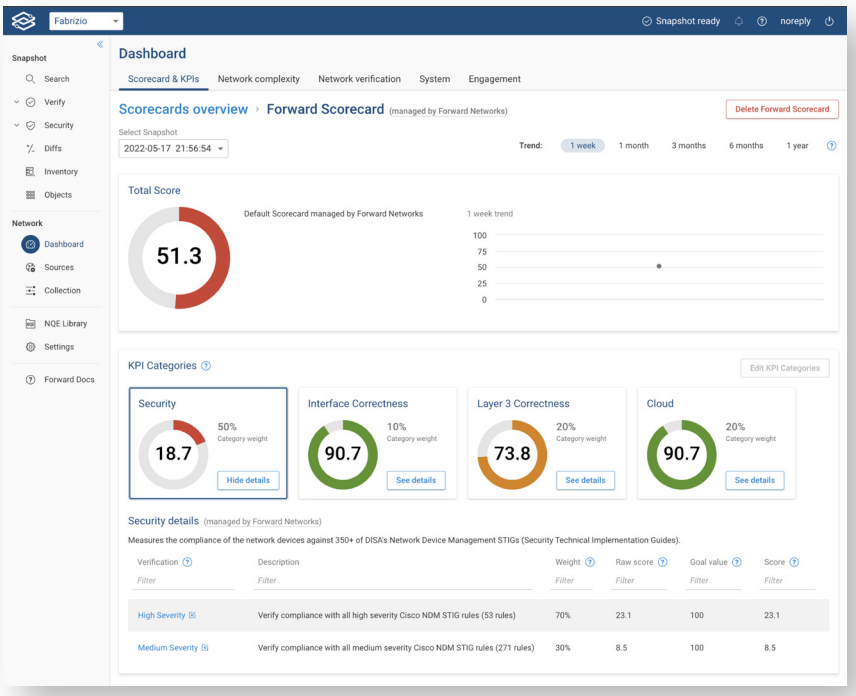

Figure 2: Sample Scorecard and KPI Dashboard

If the network is not behaving as intended, the Behavior Diffs function compares snapshots over time and highlights changes in the desired date range.

The Scorecard and KPI dashboard can track CCRI metrics with graphs and detailed reports to ensure objectives are met. See Figure 2.

Documentation

During your team's inspection and documentation phase, members must produce documentation that details changes or responses to inspectors' questions on a particular device, STIG, or CTO. Forward Networks can handle documentation in one of two ways, on or off-platform.

Off-platform, you can utilize many Forward Networks APIs to store needed information in Git style repositories for version control. Integrations enable the data to be stored in ServiceNow, where the data can be stored, parsed, and shared with engineers who may not have access.

For on-platform documentation, NQE documents network behavior over time and enables operators to include intent and description for each check. This shared single source of truth assures that other network operators and engineers know the reasoning behind the results and behaviors of the network.

Additionally, inspectors will require a Visio diagram of your network. When created manually, a Visio diagram of network topology requires months of work and is out of date as soon as it's complete. Using Forward Networks, operators can export a Visio VSDX layout immediately. Depending on the requirements, this diagram can reflect the current topology or provide a historical reference using any previously collected snapshot.

What's the simplest way to store and share CCRI inspection data?

Information collected before, during, and after the CCRI will need to be shared and stored as part of the process and as discovered issues are remediated. To simplify this process, Forward Networks is developing an XCCDF format (based on XML format) output that can be directly utilized in applications similar to DISA's EMASS program, sharing findings with others that use DISA's STIG viewer application.

In today's quick changes and standardization world, more teams are utilizing automation orchestrators such as Itential, TerraForm, Ansible, and Norinir to assist with remediation, utilizing Forward Networks NQEs to gather host devices into inventories that these orchestrators can use to target machines for remediation.

How do I get started?

To learn how Forward Networks is helping other agencies succeed in their missions, please visit www.forwardnetworks.com/federal.

Because each agency network is unique, so is the path to successfully completing and passing a CCRI. For a customized look at how Forward Networks can help your agency confidently enter and pass a CCRI, please contact us for a personal demo.

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed and secured. Forward's advanced software delivers a "digital twin" of the network, enabling network operators to verify compliance, predict network behavior, and simplify network management. The platform supports devices from all major networking vendors and cloud operators, including AWS, Azure, and Google Cloud Platform.