# Evolving demand requires federal networks to get smart

Gone are the days when networks were simply a way to transfer data from one place to another. While that is still the primary aim of networks in general, a host of other factors – security, cloud computing, mobility, explosive data growth and increased use of multimedia and collaboration tools — have rendered even those networks that are relatively modern virtually obsolete. In addition federal networks are facing increased stress from data center consolidation, which requires agencies to increase the efficiency, intelligence and cost-effectiveness of remaining networks.

Without infusing today's networks with more intelligence—greater visibility, analytics capabilities and improved security, to start—federal networks simply won't be able to keep pace. Instead, they will start experiencing more latency, bottlenecks, security problems, and space issues.

According to a recent study from the 1105 Public Sector Media Group, these pressures will significantly impact agency network complexity and capacity requirements. In fact, more than 30% of federal network managers say that their current network management solutions are inadequate and won't be able to support the types of demands their users will be demanding.

For most agencies, the solution is to transform their current network infrastructure into one that can handle these demands, creating, in essence, a more intelligent network. The intelligent network will not only be able to handle capacity, throughput and security issues, but full visibility into what's going on and ability to analyze network traffic and security issues for quick resolution.

The main elements of the next-generation intelligent network include:

**Visibility and efficiency enhancement:** As networks grow and change, existing tools may provide only limited visibility into network traffic. Tools in this category focus on enhancing the visibility and efficiency of traffic dispersed across physical and virtual networks.

**Continuous monitoring:** This technology transforms security control and risk determination into a dynamic process that provides near real-time security status. This is essential for fast response to security threats.

**Analytics:** Network intelligence tools examine IP data packets, metadata and other network metrics in real time to provide visibility into all network-based activity. With this information, network managers can make fast, impactful decisions.

**A centrally managed network infrastructure:** An intelligent network requires directly programmable network control, which allows administrators to adjust network-wide traffic flow on the fly. Increasing, enterprises are using software-defined networking (SDN) for this purpose.

## STATISTICALLY SIGNIFICANT:
## FEDERAL NETWORKS BY THE NUMBERS

**29.3**
The percentage by which network traffic is expected to increase throughout the federal government

**66**
The percentage of federal respondents who believe that Software Defined Networking (SDN) will be important in accommodating federal mandates

**79**
Federal network managers expect their agencies' total network load to increase by an average of 79% as a result of pursuing initiatives like big data, the cloud, mobility, security and data center consolidation

**95**
The White House's goal is for executive branch departments and agencies to achieve 95% implementation of priority cybersecurity capabilities by the end of FY14

**300**
The 2014 Federal IT Budget allocates more than $300 million for DHS to support continuous monitoring of federal networks

**5.77 MILLION**
The amount of money the federal government will spend on Big Data-related activities in 2018

**90**
The percentage of federal respondents who don't believe their agencies are fully prepared for a cyber attack

# Continuous monitoring: Bringing intelligence to cybersecurity

Protecting federal networks against threats continues to be top priority, and the best way to do so effectively is by continuously monitoring network traffic. It's so important, in fact, that continuous monitoring of federal information systems is a cross-agency priority area for improving federal cybersecurity.

Continuous monitoring is a critical component of an agency's cybersecurity strategy; not only does it identify vulnerabilities and abnormalities, but it can help agencies anticipate and mitigate future threats.

The technology works by collecting and analyzing network traffic security data continuously, ensuring that network managers are aware of impending threats and vulnerabilities in real time. With this type of advanced, persistent monitoring system, it's very effective at identifying security gaps quickly so they can be addressed immediately.

A comprehensive continuous monitoring strategy includes both processes and technology to provide a continuous feedback loop on both the effectiveness of security controls and potential risk. With this information, agencies can prioritize their actions based on the data at any given time.

The Department of Homeland Security recently teamed with the General Services Administration to offer agencies easy access to key continuous monitoring tools. The Continuous Diagnostics and Mitigation program was initially launched with products in four functional areas:

- Hardware inventory management
- Software inventory management
- Configuration setting management
- Vulnerability management

Eventually, CDM will cover 15 continuous monitoring capabilities.

## SMARTER NETWORKS WITH ANALYTICS

Today's networks are far from static. Everything from traffic flow to unanticipated demand can have a significant effect on network performance. The best way to keep pace with changing network demands is by using an analytics tool specifically designed for networks. These tools help network administrators identify and resolve issues before they become real problems.

Most network analytics tools use the dashboard approach, providing both standard reports and customized reports. Standard metrics include performance thresholds, packet loss, quality-of-service queue usage, interface errors and latency variations.

There are many valuable ways in which network administrators can use network analytics tools, including:

- Track key performance indicators (KPI)
- Analyze congestion periods
- Analyze peak period usage
- Evaluate routing efficiency
- Analyze network outages
- Analyze long-term data on network connections
- Analyze wireless use

With this information, network administrators can improve network performance and troubleshoot more effectively. For example, they can use the data to develop more effective policies for optimizing wide area network traffic, use wireless use data for capacity planning, fine-tune network access policies, avoid potential bottlenecks, develop optimized traffic routing plans, consolidate nodes, ensure better reliability and speed, reduce costs and improve overall traffic management.

## SDN BRINGS AGILITY TO THE NETWORK

**If you haven't yet heard the term software-defined networking (SDN), it's probably only a matter of time. Here's what you need to know:**

**What is SDN?** It is different way of designing, building and running networks that run in a data center—one that greatly increases network agility. It makes networks less expensive to build, faster, more efficient and easier to configure.

**How does it work?** In the SDN architecture, the control and data planes are separate and the network infrastructure is decoupled from network applications and features. An SDN environment also uses open application programming interfaces (APIs) to support all the services and applications running over the network.

**What does this mean for my network?** The SDN approach enables network administrators to shape traffic and deploy services in response to changing needs without interrupting individual switches or routers. It is scalable and provides automatic provisioning. Because it is programmable, it is easy to connect other components within a data center to improve traffic throughput and routing. It also improves Quality of Service and security while helping organizations quickly deploy new applications, services and infrastructure.

# A new approach to intelligent network monitoring

According to the General Accounting Office, the federal government had a record number of data breaches in 2012 (most recent data available).

The growth in cybersecurity incidents throughout government is certainly not due to a lack of effort, tools or desire; federal agencies and departments do their best to fully comply with all cybersecurity mandates and use a host of effective monitoring, analytics and performance management tools.

So if it's not the fault of the tools, the networks themselves or the people who run them, what's the problem? It's network visibility. Even the best tools are only as effective as the data they can see. In many cases, networks also may have just a handful of connection points to get the data to the tools. Not only does that limit the visibility to where the data was accessed, but it puts network managers in the unenviable spot of having to choose which tool will receive data at which time. The deluge of Big Data—much of it irrelevant to the mission of the tool—can limit visibility as well and can waste tool compute resources.

At the same time, federal networks are growing so big, so fast, with many sure to reach 10Gb, 40Gb or even 100Gb in the next few years. Because most network tools are processor-bound, they can't keep up with these higher speeds.

## GIGAMON VISIBILITY FABRIC™ IS A GAME-CHANGER

A Visibility Fabric is an intermediate layer of hardware and software that sits between the network infrastructure of switches and routers and an agency's network security monitoring tools. By running everything through a Visibility Fabric, each tool becomes much more efficient. The Visibility Fabric uses Flow Mapping™ technology to identify and direct traffic to one or more tools based on user-defined rules, all from a centralized fabric management console. Filtering, replication, and traffic intelligence applications like deduplication ensure that only the data required by each specific tool is sent to that tool. It works just as seamlessly with virtualized networks and cloud environments as it does with physical network environments.

## MONITORING CHALLENGES

Many agency networks face the challenge of too few mirror or SPAN ports through which to get data from a network, and difficulty provisioning mirror/SPAN ports fast enough. While a few ports works fine when only a few monitoring tools are involved, most agencies are using many tools to keep today's networks running. The Gigamon Visibility Fabric solves this problem by enabling agency networks to connect SPAN ports to a network port via a GigaVUE Traffic Visibility Node and then use the technology to replicate traffic to multiple tool ports. That gives more tools access to the same traffic.

The Department of Health and Human Services' Computer Security Incident Response Center (CSIRC) is just one of many agencies that has benefitted from Gigamon's Visibility Fabric. The CSIRC needed a way to connect the many network monitoring and analysis tools it was using to protect the network. At the same time, the solution had to be able to handle the traffic of multiple 10Gb networks and prepare for future network growth.

## MEETING CYBERSECURITY AND CONTINUOUS MONITORING MANDATES

To address the issue, the CSIRC implemented a Gigamon Visibility Fabric solution built on modular GigaVUE fabric nodes with patented Flow Mapping™. The resulting infrastructure means that traffic entering and exiting the inline security tools can be replicated, aggregated and filtered to out-of-band monitoring tools. As a result, network administrators now have full visibility into network traffic across geographically dispersed locations.

In addition to offering robust functionality, Gigamon is in process with FIPS 140-2. HHS is just one of dozens of agencies who are relying on Gigamon to enable the efficient implementation of security tools to meet the requirements of Continuous Diagnostics and Mitigation (CDM).

The Defense Information Systems Agency (DISA) is implementing a similar cyber initiative, selecting Gigamon to be a foundational component of its Joint Regional Security Stack (JRSS). Gigamon's Visibility Fabric is a strategic choice by DISA, as JRSS will be a critical element in the Department of Defense's Joint Information Environment (JIE) architecture.

With pervasive network visibility, agencies will be will be able to not only meet cybersecurity mandates, but avoid downtime, maximize investments, and ensure that their networks are ready for whatever future growth and challenges will bring. •