BROCADE

WHITE PAPER

Maximizing Security and Visibility in Federal Networks

The Federal enterprise depends on information technology systems and computer networks for essential operations. These systems face large and diverse cyber threats that range from unsophisticated hackers to technically competent intruders using state-of-the-art intrusion techniques. Many malicious attacks are designed to steal information and disrupt, deny access to, degrade, or destroy critical information systems.

The Department of Homeland Security (DHS) works with each Federal civilian department and agency to promote the adoption of common policies and best practices that are risk-based and able to effectively respond to the pace of ever-changing threats. As systems are protected, alerts can be issued at machine speed when events are detected, helping to protect networks across the government information technology enterprise and the private sector. This enterprise approach will help transform the way Federal civilian agencies manage cyber networks. It will give them access to strategically sourced tools and services that can enhance the speed and cost-effectiveness of federal cybersecurity procurements, and allow consistent application of best practices.

This paper describes how Brocade® Network Visibility products, together with IPS/IDS security frameworks such as Bro, provide a real-time threat detection and mitigation solution for protecting Federal networks.

Background/Problem Statement

The Federal government has taken many steps aimed at addressing cyber threats to critical infrastructure, which includes systems and assets, whether physical or virtual, so vital to our nation that their incapacity or destruction would have a debilitating impact on national security, economic well-being, or public health or safety. Examples include banking and financial institutions, telecommunications networks, and energy production and transmission facilities, most of which are owned by the private sector. Despite the actions taken by several successive administrations and the executive branch agencies, the Federal government still faces significant challenges protecting its cyber-reliant critical infrastructures.

The Comprehensive National Cybersecurity Initiative (CNCI) consists of numerous mutually reinforcing initiatives intended to help secure the United States in cyberspace. They include:

- **Establish a front line of defense against today's immediate threats:** By creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal government.
- **Defend against the full spectrum of threats:** By enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- **Strengthen the future cybersecurity environment:** By expanding cyber education, coordinating and redirecting research and development efforts across the Federal government, and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

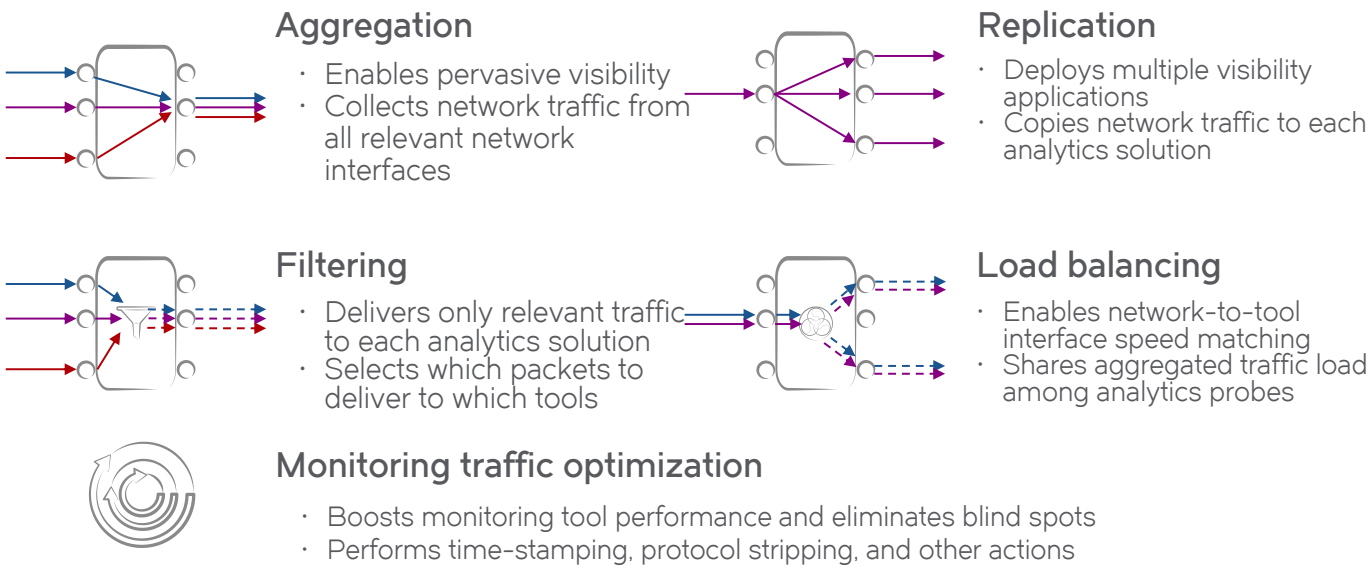

Figure 1: Key functionality provided by the packet broker.

In building the plans for the CNCI, cybersecurity specialists quickly realized that these goals could not be achieved without also strengthening certain key strategic foundational capabilities within the Federal government. Therefore, the CNCI includes funding within the Federal law enforcement, intelligence, and defense communities to enhance such key functions as criminal investigation; intelligence collection, processing, and analysis; and information assurance critical to enabling national cybersecurity efforts.

To complement these cybersecurity efforts, multiple tools used to perform various monitoring and security functions need to connect to monitored streams. These include tools for malware analysis, network packet capturing analysis, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) monitoring, and application monitoring. But there are challenges to effectively achieving such an ecosystem of tools. For example:

- Tool performance and interface speeds might be mismatched.
- The traffic being fed to the tool might contain no interesting information, degrading the tool's performance and increasing costs.
- Multiple tools require multiple copies of the data.
- Clustered tools require load balancing of the data.

These issues in turn prevent the tools from being connected directly to the monitored streams.

Pervasive Visibility with Brocade Packet Broker

Introducing a "packet broker" between the network and the analytics tools can solve these connectivity issues. The packet broker can be a hardware appliance or a software instance running in a Virtual Machine (VM). At a high level, the packet broker performs the following functions (detailed in Figure 1):

- Aggregation
- Replication
- Filtering
- Load balancing
- Monitoring traffic optimization

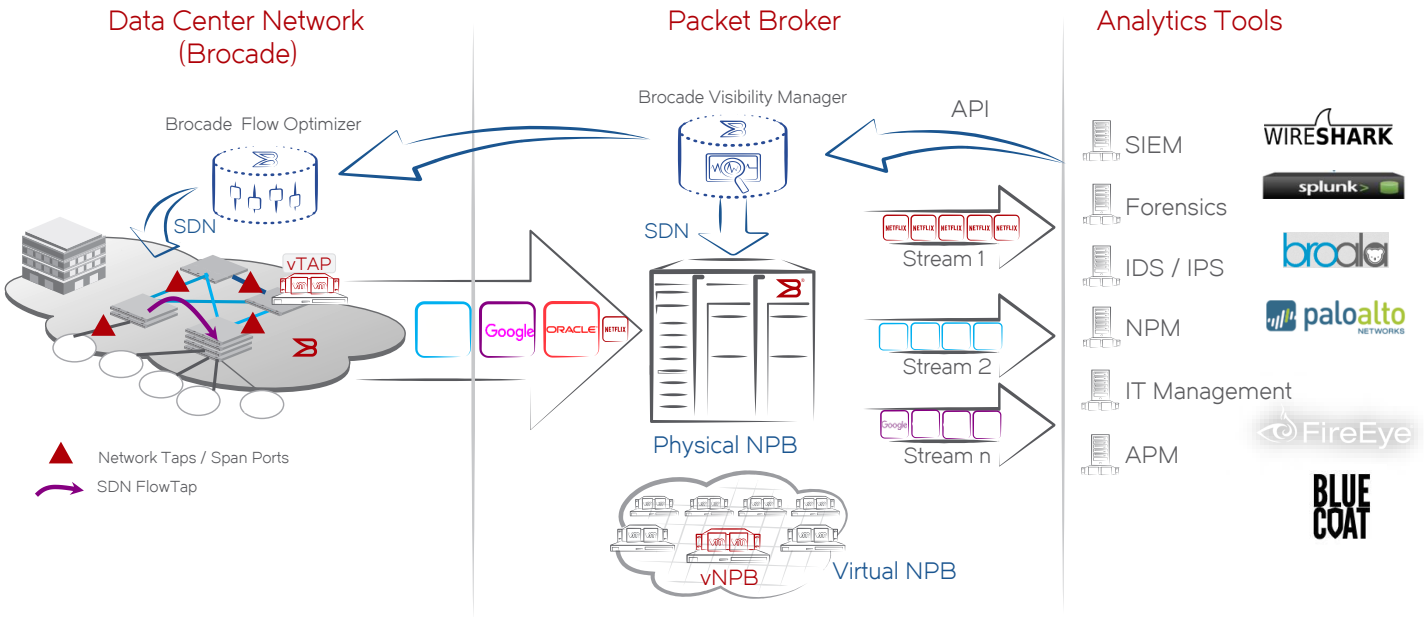

Figure 2: Brocade Packet Broker architecture.

Brocade, a leading vendor of data center networking products and solutions, also offers solutions for network visibility and analytics. These include physical as well as virtual packet brokers, and a management tool. Brocade Packet Broker is a scalable network visibility node for high-capacity network monitoring (see Figure 2). It enables pervasive visibility and delivers several key benefits, including:

- Dynamic flow creation, enabling real-time, on-demand traffic visibility
- Wire-speed traffic aggregation, regeneration, optimization, and load balancing to deliver maximum tool productivity
- Industry-leading 10 GbE, 40 GbE, and 100 GbE port density and backplane capacity, maximizing scale while minimizing space
- Scalable security monitoring and integration with Brocade Flow Optimizer for threat mitigation
- Optimized tool cost

Bro Use Case

The Bro Network Monitoring framework (www.bro.org) is a popular solution for network security. Bro analyzes network traffic in real time and performs many functions such as threat detection and mitigation, file extraction, and intrusion detection.

Brocade has partnered with Broala LLC (www.broala.com) to integrate the Bro network monitoring framework with the Brocade Packet Broker solution. Broala, a company formed by the creators of Bro, delivers an appliance that comes pre-installed with Bro and a large number of useful scripts. Broala also provides support for the appliance and expert-level customer support.

Brocade Packet Broker operates at the front end of the Bro node cluster, providing data stream aggregation, filtering, and load balancing functionalities (see Figure 3). Bro inspects the network traffic and generates a rich set of logs. In addition, Bro integrates with the Brocade Flow Optimizer over an open REST-based API interface. The Brocade Flow Optimizer is an intelligent, policy-based large-flow management application that gives insight into network traffic by providing visibility into large Layer 2 through Layer 4 traffic flows. The application improves visibility and control while offering new levels of network automation.

If Bro detects malicious traffic, it can send commands to the production network Brocade Flow Optimizer and block these flows, mitigating threats. Also, if Bro detects flows (from the packet broker) that it does not need to analyze,

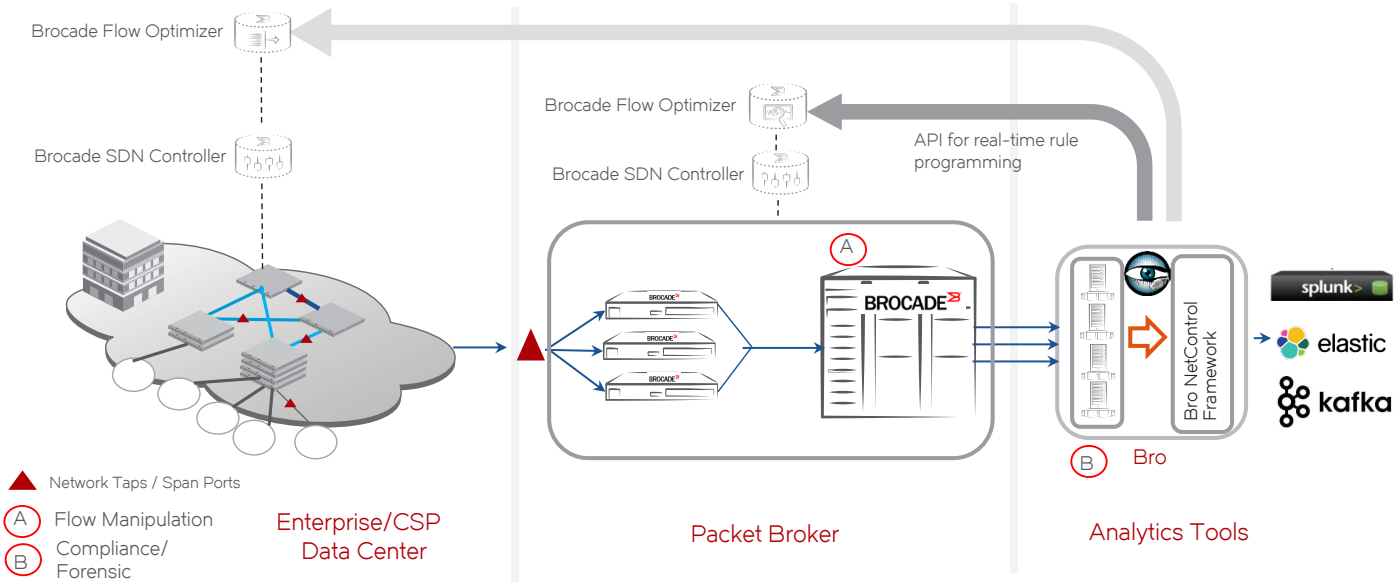

Figure 3: Generic Bro use case.

it can send shunting commands to the visibility network Brocade Flow Optimizer and shunt these flows. Shunting such elephant flows significantly reduces data processing by Bro and improves the performance of the Bro node cluster. It also reduces the amount of unnecessary log information going into visualization tools, resulting in significant cost savings.

The logs from Bro can be visualized in a variety of tools, including Splunk, Elastic Search, and Kafka.

Conclusion

Pervasive and sustained cyber-attacks could have a potentially devastating impact on Federal and non-Federal systems, disrupting the operations of governments, businesses, and the lives of private individuals. Network monitoring, threat analysis, and IPS/IDS security frameworks have to stay a step ahead to mitigate these threats. Packet brokers play a key role in providing a pervasive visibility infrastructure to accomplish these goals. Recent initiatives, such as Machine Learning, that aim to create threat signatures and mitigation plans require the ability to analyze the entire stream of data. Such frameworks can perform properly only in the presence of a packet broker.

For more information about Brocade solutions, visit www.brocade.com.

Corporate Headquarters
San Jose, CA USA
T: +1-408-333-8000
info@brocade.com

European Headquarters
Geneva, Switzerland
T: +41-22-799-56-40
emea-info@brocade.com

Asia Pacific Headquarters
Singapore
T: +65-6538-4700
apac-info@brocade.com