BROCADE

WHITE PAPER

# Brocade Network Visibility Enables Security and Analytics in Enterprise Networks

## TABLE OF CONTENTS


Background/Problem Statement ..... 2
Solution ..... 3
Generic Bro Use Case ..... 5
SSL/TLS Decryption Use Case ..... 5
Packet Data Masking Use Case ..... 6
Encryption between Remote Sites Use Case ..... 7
Conclusion ..... 7
Additional Resources ..... 8


Today's modern enterprises are distributed entities with very complex networks. These enterprises work with partners and contractors, and also have different organizations within, thus requiring several different access policies to various parts of their data center and campus networks. This creates a major problem: How do you balance the need for access with the need for security and IT policy enforcement?

Enterprise networks in every industry are being targeted by millions of hackers seeking access to private and confidential information. Facebook reported in 2011 that approximately 600,000 accounts were being compromised every day,[1] while Symantec found that over 200 million identities were exposed in 2014.[2] And it is not always rogue entities that are responsible. More than 59 percent of ex-employees admitted to stealing company data when leaving previous jobs.[3] Because of this surge in cyber crime, the global cyber security market is expected to skyrocket to $120.1B in 2017, from $63.7B in 2011.[4]

Such attacks are also becoming more sophisticated, organized, and frequent. At the same time, enterprises have a complex array of disparate systems with vastly different security requirements. Due to these factors, it can be extremely expensive to protect enterprise networks.

Proactively finding security issues in the networks and addressing them would significantly reduce the costs to organizations—both in terms of finances and reputations. Given the complexity of the networks, the solution must be scalable, crunch vast amounts of data, yet be relatively inexpensive and provide very fast turnaround times to mitigate threats in real time. This white paper looks at ways Brocade® Network Visibility products, together with common IPS/IDS security frameworks such as Bro, allow enterprise networks to be highly secure while keeping costs relatively low.

1 Todd Wasserman, "Facebook Says 600,000 Accounts Compromised Per Day," *Mashable*, http://mashable.com/2011/10/28/facebook-600000-accounts-compromised/#l._WsrdCsqJ, October 28, 2011.

2 Symantec, *Symantec Internet Security Threat Report: Top 10 Sectors Breached by Number of Identities Exposed*, https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf, April 2015.

3 GO-Gulf, "Cyber Crime Statistics and Trends," *GO-Gulf* (blog on Web site), http://www.go-gulf.com/blog/cyber-crime/, May 17, 2013.

4 Ibid.

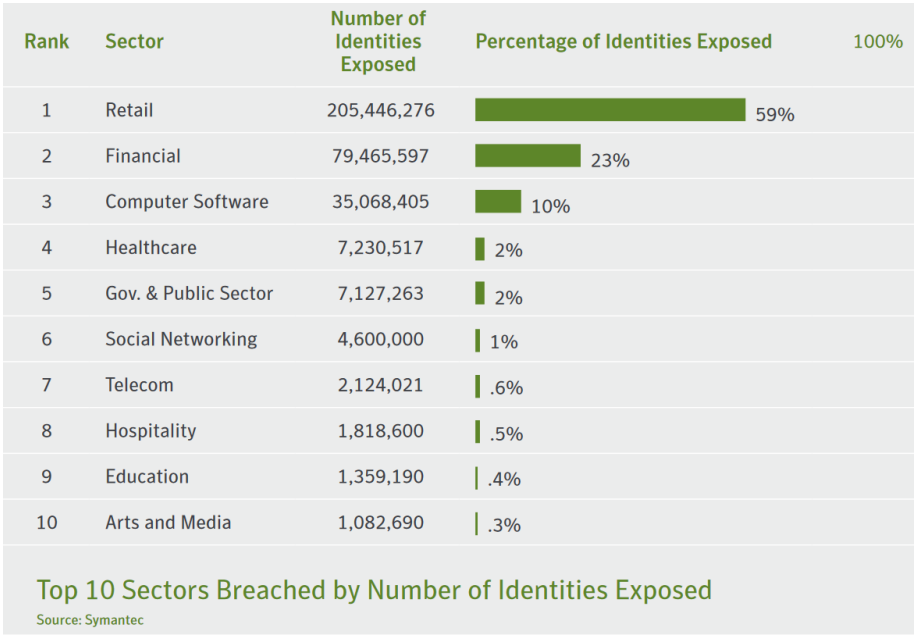


**Figure 1:** According to the *Symantec Internet Security Threat Report*, the top 10 sectors breached by number of identities exposed (based on data from 2014).

## Background/Problem Statement

Enterprise networks are incredibly diverse and complex, making them difficult to protect from intrusions and attacks. While the increasingly global nature of these networks is causing them to become even more complex, cyber criminals are displaying a higher level of collaboration, specialization, and sophistication in their attack capabilities.

In the meantime, critical infrastructure systems such as the power distribution grid, water distribution systems, oil and gas pipelines, and transportation systems are running on old, obsolete architectures that could be easily compromised. Many utilities and cash ATMs still run on Windows XP or derivative operating systems that Microsoft no longer supports.

Business leaders are also concerned about the very high financial costs associated with cyber crime. In 2013, 19 percent of U.S. entities reported financial losses ranging from $50,000 to $1 million, while 7 percent lost more than $1 million to cybercrime incidents.[5] In addition, these organizations face a huge risk of legal liability and costly lawsuits.

Following are recent examples of the quandaries that today's enterprises now face as a result of cyber crime:

- **March 2016:** Hackers used a phishing scam, and tricked a Snapchat employee into e-mailing them private personal information of 700 current and former employees. The employee thought the request was from Snapchat CEO Evan Spiegel. The identities of the attackers are unknown.[6]
- **March 2016:** Cybersecurity journalist Brian Krebs found data for sale in an underground cybercrime forum. It had come from a breach at Verizon Enterprise Solutions, a division of Verizon that provides IT services and data breach assistance to businesses and government agencies around the world. The personal information of about 1.5 million customers was stolen.[7]
- **February 2015:** Anthem Inc., an Indianapolis-based health insurance firm, had personal information of about 80 million customers stolen, including Social Security numbers, names, and addresses.[8] This was carried out as a phishing attack.[9]
- **2014 and 2011:** A hacking group called Guardians of Peace hacked the computer systems of Sony Pictures, shutting down most of the system. The group was able to take over the system and leak several unreleased films.[10] Personal information belonging to employees was also stolen. Prior to that, in 2011, hackers had infiltrated the PlayStation Network, and stole 77 million Sony records.[11]

These examples indicate that enterprise networks are targets for attacks, and the fallout can be very expensive. As Figure 1 from the *Symantec Internet Security Threat Report* shows, the attacks are mostly focused on the retail, financial, and computer software sectors, but

5 PwC (Pricewaterhouse Coopers), *U.S. Cybercrime: Rising Risks, Reduced Readiness, Key Findings from the 2014 U.S. State of Cybercrime Survey*, http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf, June 2014.

6 Judy Leary, "The Biggest Data Breaches in 2016, So Far," *IdentityForce* (Web site), https://www.identityforce.com/blog/2016-data-breaches, 2016.

7 Ibid.

8 Charles Riley, "Insurance Giant Anthem Hit by Massive Data Breach," *CNN*, http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html, February 6, 2016.

9 Virginia Commonwealth University, *VCUPhishingNet*, https://phishing.vcu.edu/2015/02/06/, February 6, 2016.

10 *Wikipedia*, https://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack.

11 *Wikipedia*, https://en.wikipedia.org/wiki/2011_PlayStation_Network_outage.

every single vertical has experienced the effects of cyber crime. When an attack is discovered, the affected organization has to hire forensic computer investigation services, fix the problem areas, fend off lawsuits, and pay for credit protection services, among other remediation measures.

Network security solutions such as Bro, Suricata, and Snort, which are widely used in the research and education community, are now gaining popularity among enterprises. Because these solutions are open source, they are not expensive. In addition, they are flexible and extensible, making them an attractive option for organizations that have development teams to customize and deploy them, or that require large-scale deployments (for which proprietary solutions may be prohibitively expensive). However, these solutions also have some drawbacks. They do not easily scale to support the vast amounts of data that need to be analyzed, and are unable to perform certain critical functions, such as SSL decryption, packet de-duplication, and packet data masking. Real-time threat mitigation is also difficult, since these tools are not aware of network topologies and do not know where to filter bad traffic.

The Brocade Packet Broker solution, which includes hardware, software, and management components, solves all these issues in conjunction with the Bro network monitoring system. The rest of this document describes the solution in detail.

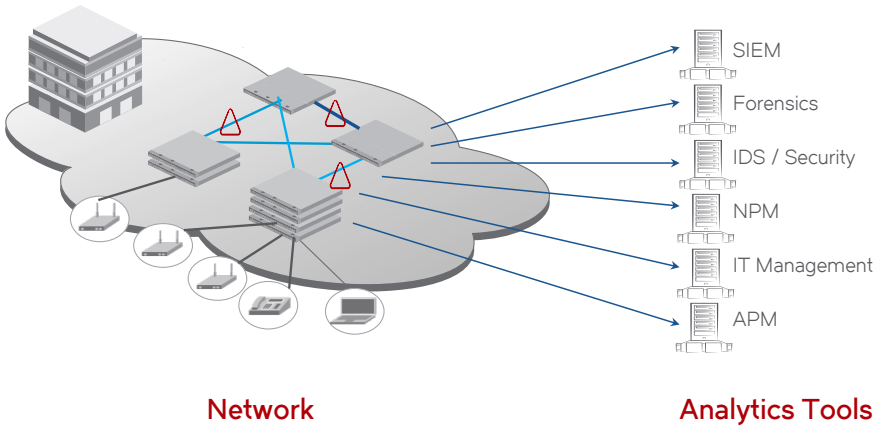


**Figure 2:** Connecting analytics tools directly to network TAPs.

## Solution

In order to obtain threat information in real time, most network security and analytics tools work off live data from the network. They can be fed this data directly, either from span ports or from optical TAPs (see Figure 2).

This approach, however, has several potential issues, including:

- Tool performance and interface speeds might have a mismatch.
- The traffic being fed to the tool might not contain any interesting information—degrading the tool's performance and increasing costs.
- Multiple tools require copies of the same data (replication).
- Clustered tools require load balancing of the data.

As a result, the pervasive visibility required for enterprises is often not possible. It is hindered by the complex network topologies and limitations related to feeding analytics tools directly. The existing solutions are therefore unable to scale. Hence, most organizations just monitor their perimeter WAN links and hope that they catch all the issues, when in fact they do not (see Figure 3).

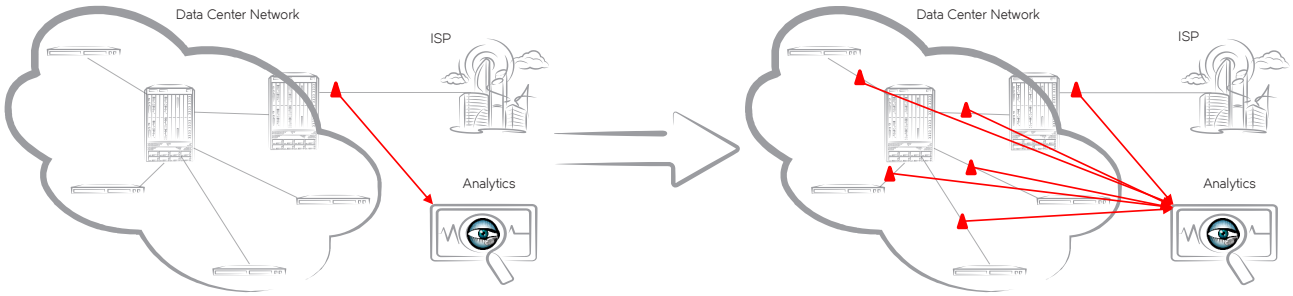


**Figure 3:** Pervasive visibility in the network.

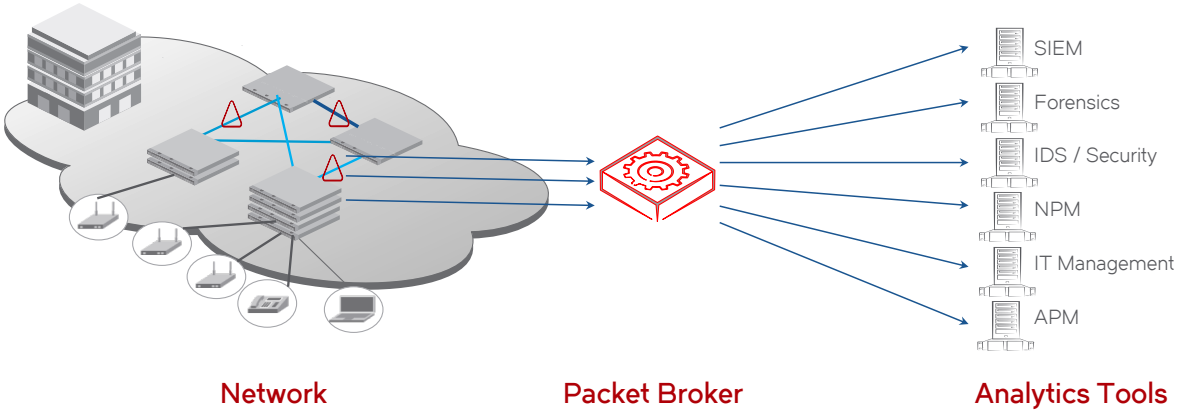


**Figure 4:** Brocade Packet Broker connected to network TAPs and analytics tools.

These challenges can be easily solved with the introduction of a "packet broker" between the network and the analytics tools, as shown in Figure 4.

The packet broker can be a hardware appliance, or a software instance running in a VM. At a high level, it performs the following functions:

- **Aggregation:** Supports pervasive visibility, which requires that a large number of network interfaces be TAP'd, by aggregating all this traffic to feed the tools.
- **Mirroring:** Copies the network traffic to each analytics tool.
- **Filtering:** Delivers only the relevant traffic to each analytics tool.
- **Load balancing:** Shares aggregated traffic load among instances of an analytics tool.
- **Interface speed matching:** Enables hardware buffering to connect network and tool interfaces running at mismatched speeds.

Brocade, a leading vendor of 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. Figure 5 shows the Brocade Packet Broker architecture. On the left side is an enterprise network that requires a visibility solution. Live data is streamed out of this network via one of the following methods:

- Optical TAPs
- Span/mirror ports
- SDN FlowTap (only specified flows TAP'd)

From the network, this streaming data comes to the packet broker network in the middle. Brocade Packet Brokers can be any combination of physical and virtual versions of the packet broker. From the packet broker, the data then travels to the analytics tools (types and examples are shown in Figure 5).

The packet broker network is managed by a software visibility manager. A single visibility manager can manage multiple packet brokers, even across disparate locations. The visibility manager exposes a REST API that the analytics tools can use to control the data flow toward them. For real-time threat mitigation, filters may also be applied on the production network via the Brocade Flow Optimizer tool. These use the Brocade SDN Controller to manage the flows on the respective networks.

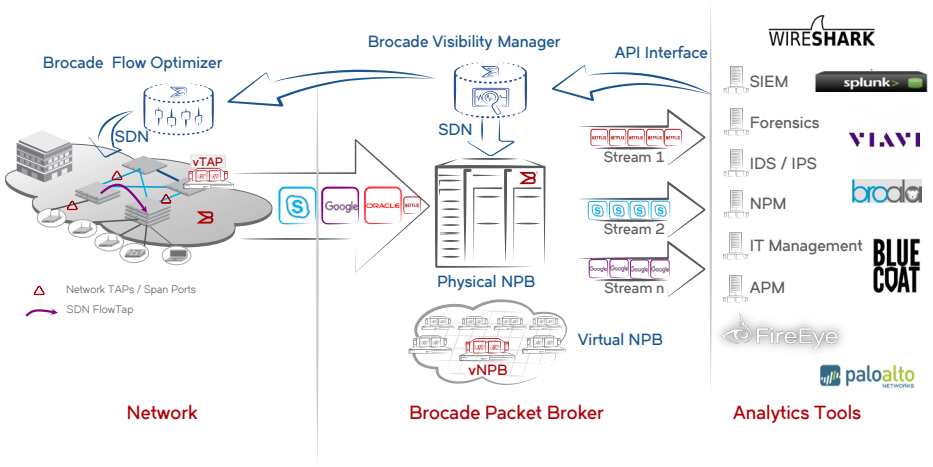


**Figure 5:** Brocade Packet Broker architecture.

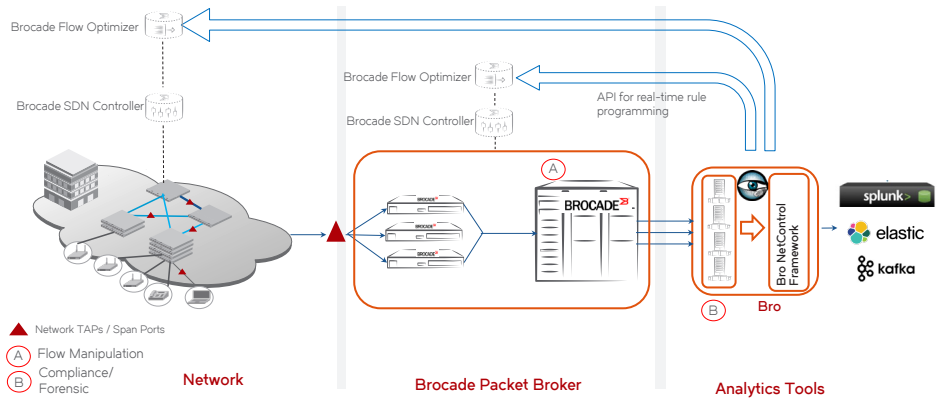


**Figure 6:** Generic Bro use case.

## Generic Bro Use Case

To protect against attacks while keeping costs within budget, enterprises that require huge scale and have in-house expertise often utilize open source solutions. The community aspects of these solutions make them robust and flexible. One of the more popular solutions for network security is the Bro Network Monitoring platform (www.bro.org). Bro analyzes network traffic in real time and performs a variety of functions, including threat detection and mitigation, file extraction, and rich logging of network metadata.

Brocade is working closely with Broala (www.broala.com), a company formed by the creators of Bro, to integrate the Bro network monitoring platform with the Brocade Packet Broker solution. Broala offers turnkey appliances that provide comprehensive network visibility based on Bro. Broala also provides commercial support for the appliance and customer-deployed Bro installations.

Figure 6 shows the details of the integration between the Brocade Packet Broker solutions and Bro/Broala. Bro monitors and analyzes network traffic coming from the Brocade Packet Broker. If it detects traffic violating the site's cybersecurity policy, it can send commands to the Brocade Flow Optimizer to block these flows. If it detects flows coming from the packet broker that it determines are not important to analyze, it can send commands to the Brocade Flow Optimizer in the non-production visibility network to shunt these flows. Shunting involves dropping the flows at the Brocade Packet Broker. This significantly reduces the data going to Bro, which can greatly improve its performance.

The logs from Bro can be visualized and analyzed using a variety of tools, such as Splunk, Elastic Search, and Kafka.

## SSL/TLS Decryption Use Case

To improve security, more and more traffic in the campus and the data center is now encrypted. From virtually nothing just a few years ago, it is not uncommon to see 50 to 70 percent of data center traffic encrypted today. While encryption improves security, it also creates new problems: Malicious traffic could be encrypted, and the DPI detection mechanisms would be rendered ineffective because they would not be able to look inside this traffic.

Organizations therefore need a solution that can provide visibility into the encrypted traffic. This is typically achieved by providing the private keys and certificates to a decryption device. If done in the firewall, the traffic in the data center or campus is vulnerable. Hence, end-to-end encryption is common nowadays. This means that it is necessary to decrypt TAP'd data for the purpose of visibility and monitoring.

In the aforementioned packet broker use cases, the packet broker is always deployed in an offline mode. That way network traffic is not disrupted, and network performance is not affected by the packet broker. The same reasons apply in the use case for decrypting encrypted traffic. This is possible for traffic encrypted with only the RSA cipher suite. In this case, traffic is TAP'd just as in the previous use cases and sent to the packet broker, which then sends encrypted traffic

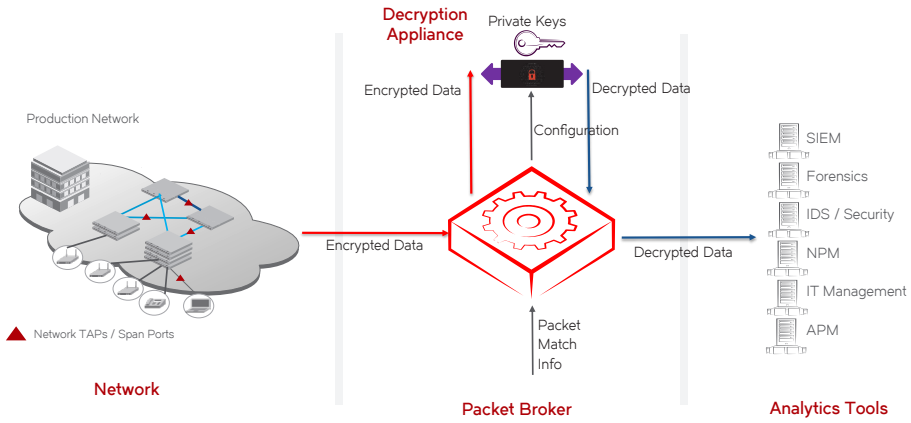


**Figure 7:** SSL/TLS decryption with an offline decryption appliance.

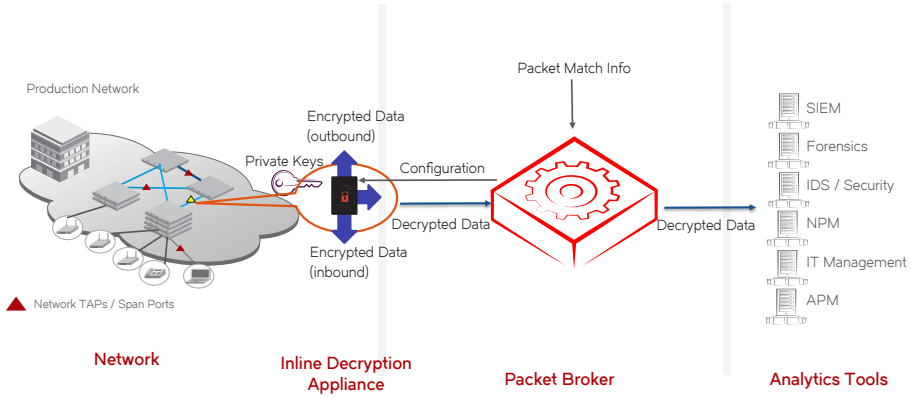


**Figure 8:** SSL/TLS decryption with an inline decryption appliance.

to the decryption appliance. Next, the appliance decrypts the traffic and sends it back to the packet broker. At that point, the traffic is treated just like all other unencrypted traffic. This topology is shown in Figure 7.

However, these RSA ciphers are no longer regarded as having the best security. New, more secure ciphers, such as the Elliptic Curve Diffie-Hellman variants with re-signing, are gaining popularity. They cannot be decrypted in the offline mode described above. To gain visibility into traffic encrypted with these ciphers, it is necessary to install an appliance inline in the network traffic path. This appliance acts as an SSL/TLS proxy to both ends of the encryption pipe. It decrypts the traffic crossing it and sends it to the packet broker. It is necessary to ensure that the connectivity between the decryption appliance and the packet broker is secure. This is shown in Figure 8.

Brocade is partnering with Blue Coat (now part of Symantec) to provide the decryption solutions described above. The Blue Coat appliance may be deployed in either of the topologies shown, and used to gain visibility into encrypted data.

## Packet Data Masking Use Case

Data on the network often contains sensitive information, such as personal account numbers, personal IDs, and Social Security numbers. Sometimes this information is inadvertently present in the traffic data. While poor practices are occasionally to blame, SSL/TLS decryption is usually the culprit since it often exposes information that was encrypted for privacy reasons.

This information needs to be kept away from analytics tools because it can fall into the wrong hands, and its presence makes the network less secure. To safeguard against this, Brocade Packet Broker has a feature in the Brocade Session Director software that allows users to mask sensitive data. The data can be replaced either with a default random pattern or something specified by the user that mimics the original pattern, but the value is meaningless. Thus, the analytics tool can still identify the data by the pattern (so it can recognize a Social Security number for example), but the value of that pattern is of no use to anyone.

Figure 9 shows the packet broker topology for data masking. The user can configure Brocade Packet Broker with rules that match the traffic that may need data masking. This traffic is sent by Brocade Packet Broker to Brocade Session Director, which masks the relevant data.

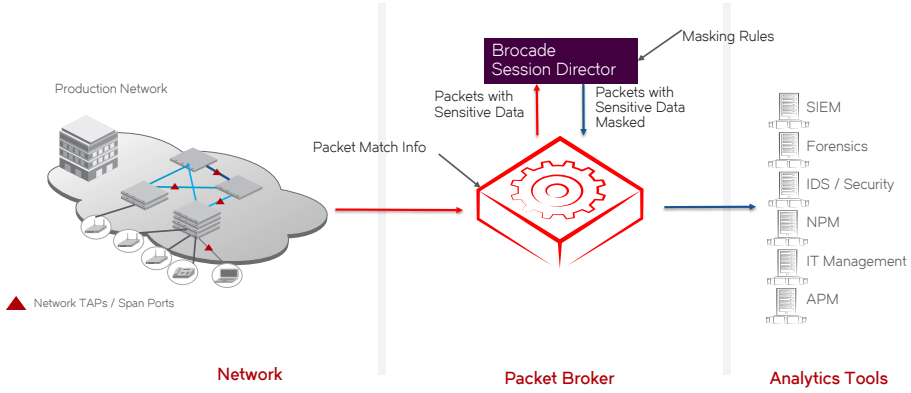


**Figure 9:** Packet data masking topology.

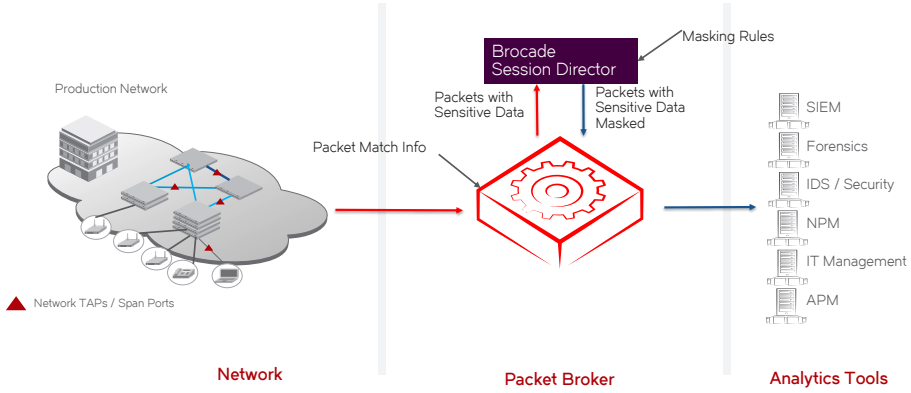


**Figure 10:** Encryption between remote sites use case.

## Encryption between Remote Sites Use Case

Most modern enterprises have geographically distributed locations, each of which may run its own independent network that is connected to an organization-wide backbone or regional network.

When network visibility data is collected at one site, not all of it is analyzed at the same site. Part of the data may be sent to a central monitoring and analysis cluster. This data is typically very sensitive; therefore, it needs to be encrypted before it is sent over the public networks, so that it is protected from malicious entities. Brocade Packet Broker has these encryption capabilities in hardware, allowing for secure transport of this sensitive data across public networks (see Figure 10).

## Conclusion

Today's modern enterprises are increasingly global or distributed, and have networks that require a high degree of performance, yet need to be protected from an exponentially increasing barrage of cyberattacks. Various tools are available to help enterprises monitor and secure their networks, but they do not easily scale to support the high levels of traffic and users seen today.

Brocade Packet Broker uniquely addresses this urgent problem by enabling enterprises to optimize the use and cost of their existing security and visibility analytics tools.

## Additional Resources

1. Brocade Network Visibility and Analytics page: http://www.brocade.com/en/possibilities/solutions/network-visibility-and-analytics.html
2. *Symantec Internet Security Threat Report*: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf
3. *U.S. Cybercrime Report* from PricewaterhouseCoopers: http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf
4. *California Data Breach Report*: https://oag.ca.gov/breachreport2016

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



BROCADE