PARTNER BRIEF

Providing Crucial Visibility into Encrypted Network Traffic

HIGHLIGHTS

- Visibility into encrypted traffic that could contain security threats
- Offloading the requirement to decrypt traffic from analytics tools
- Improving the performance and scale of analytics tools, resulting in significant cost reduction
- No disruption to production network traffic
- Combining the SSL decryption capability with other packet broker functionalities, such as packet data masking (for sensitive information), replication, load balancing, filtering, deduplication, and packet timestamping

Brocade and Symantec: Visibility in an Encrypted World

Business Challenge

Today's networks are highly complex entities, connecting millions, sometimes even billions, of devices across vast distances. This complexity has created security challenges, leading organizations to significantly increase their use of encryption technology. As a result, it is not unusual for 50 to 70 percent of data center traffic to be encrypted.

Although encryption improves security, it also creates new problems. Malicious traffic could be encrypted and escape detection, since network security devices cannot look inside the traffic. Moreover, most analytics tools used to analyze application traffic are not able to decrypt data, while those that can waste precious compute cycles doing so. This not only degrades performance, but also serves as an inefficient use of expensive tools. Organizations therefore need an effective way to gain visibility into encrypted traffic for analysis.

Solution: Brocade Envision Fabric and Symantec SSL Visibility Appliance

Rather than decrypting traffic in each analytics tool separately, Brocade and Symantec have devised a better approach: provide the decryption capabilities through the packet broker. Symantec's Encrypted Traffic Management (ETM) solution eliminates the encrypted traffic blind spot to combat the security threats hidden in encrypted traffic. It integrates with Brocade® Packet Broker, a device that sits between the traffic extraction point in the network (TAP or span/mirror port) and the analytics tools (for example: security devices, network performance management, application performance management, SIEM, forensics, IT management). Brocade Packet Broker can then manage encrypted traffic while maximizing the performance of all the analytics tools.

Figure 1 illustrates the Brocade Envision fabric network packet broker solution architecture. This architecture differentiates itself by combining the flexibility and scale of software functionality with the high performance of switching and routing hardware to provide maximum visibility at minimum cost.

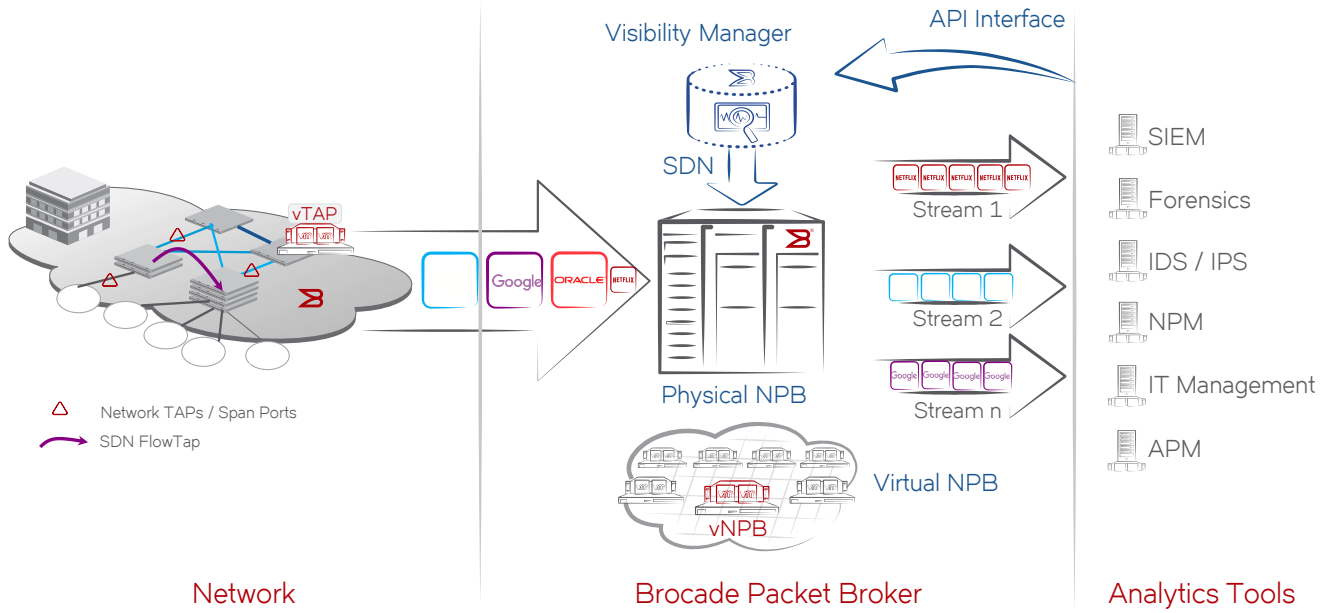

Figure 1: Brocade Envision fabric network packet broker solution architecture.

In this diagram, the enterprise network requires a visibility solution. Live data is streamed out of this network using one of the following methods:

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

From the network, the streaming data moves to the packet broker network. (Brocade Packet Brokers can be physical or virtual versions of the packet broker.) From the packet broker, the data then travels to the analytics tools. 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.

Based on this architecture, it is clear that the SSL decryption of network traffic is best performed at the packet broker layer. This is achieved by integrating the Symantec SSL Visibility Appliance with Brocade Packet Broker, as shown in Figure 2.

How It Works

Offline SSL Decryption Appliance

Offline deployment is an option when static keys are used, typically with RSA-only ciphers. The Symantec SSL Visibility Appliance is connected to Brocade Packet Broker at both ingress and egress ports. The traffic flows as follows:

1. A copy of network traffic is made, using either a TAP, SDN FlowTap, or span/mirror port on a switch.
2. This data comes to Brocade Packet Broker at its network (ingress) ports.
3. Brocade Packet Broker determines which traffic requires SSL decryption based on configuration, and sends that traffic to the Symantec SSL Visibility Appliance. Since the appliance receives only the traffic that requires decryption, it operates at its maximum performance capabilities and maintains privacy compliance.
4. The Symantec SSL Visibility Appliance sends the decrypted traffic to Brocade Packet Broker.
5. Brocade Packet Broker can then perform other required functions, such as packet data masking for sensitive data, data deduplication, packet timestamping, replication, filtering, and packet modifications, including header stripping, pattern matching, and more.
6. The data is now in the format most consumable by the analytics tool. Multiple analytics tools may be connected, and each may have its own separate requirements for the traffic sent to it. This traffic is then sent by Brocade Packet Broker to the respective tool from its tool (egress) ports.

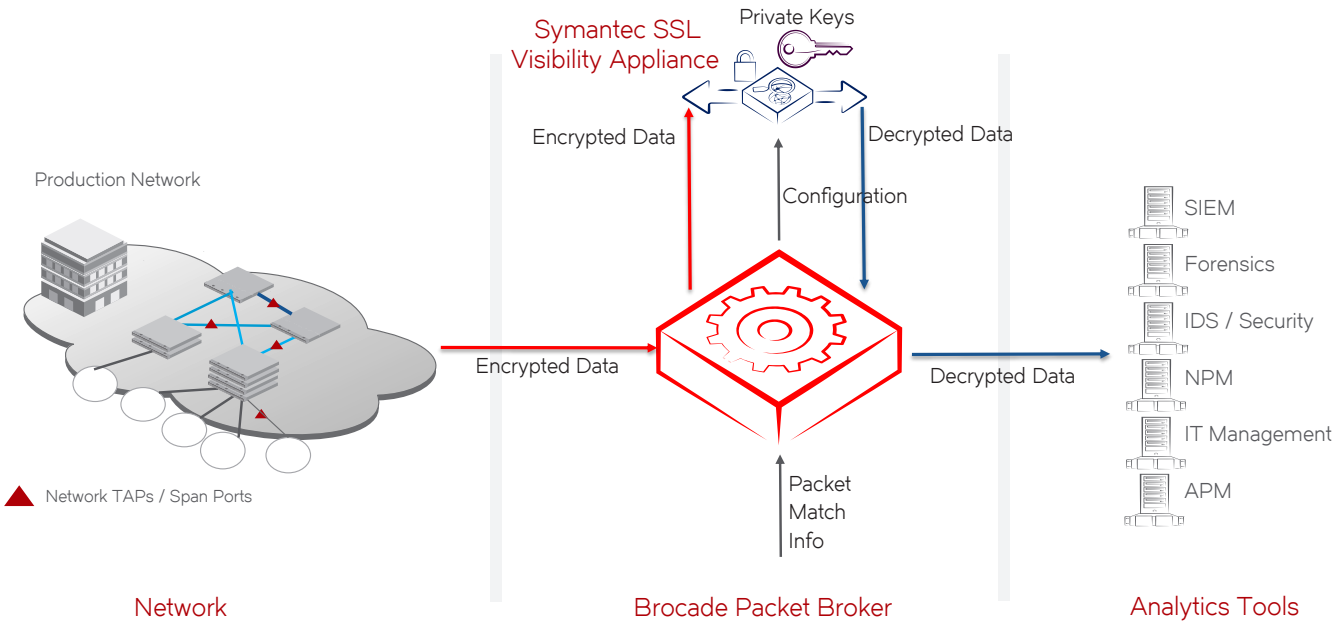

Figure 2: SSL decryption appliance deployed in offline mode.

Figure 2 shows these details of the traffic flow for the offline deployment model. This is the preferred model because it creates no disruption in the production network traffic.

Inline SSL Decryption Appliance

Inline deployment is required when dynamic keys are used for encrypted traffic, typically with Elliptic Curve ciphers. The Symantec SSL Visibility Appliance must be inline with the network traffic, so it can proxy the SSL connections to both the server and the client. The traffic flows as follows:

1. The Symantec SSL Visibility Appliance inspects all the production network traffic flowing through it, and decrypts specific flows based on configuration.
   a. A copy of this decrypted network traffic is sent via a connection to Brocade Packet Broker. The Symantec SSL Visibility Appliance behaves like an intelligent TAP with decryption capabilities.
   b. Network traffic that does not require decryption may also be sent to Brocade Packet Broker in this manner.
   c. There is no disruption to production network traffic because of the advanced high availability features of the Symantec SSL Visibility Appliance, which includes fail-to-wire capability.
2. This data comes to Brocade Packet Broker at its network (ingress) ports. All the data is unencrypted.
3. Brocade Packet Broker can then perform other required functions, such as packet data masking for sensitive data, data deduplication, packet timestamping, replication, filtering, and packet modifications, including header stripping, pattern matching, and more.
4. The data is now in the format most consumable by the analytics tool. Multiple analytics tools may be connected, and each may have its own separate requirements for the traffic sent to it. This traffic is then sent by Brocade Packet Broker to the respective tool from its tool (egress) ports.

This traffic flow for the inline deployment model is shown in Figure 3.

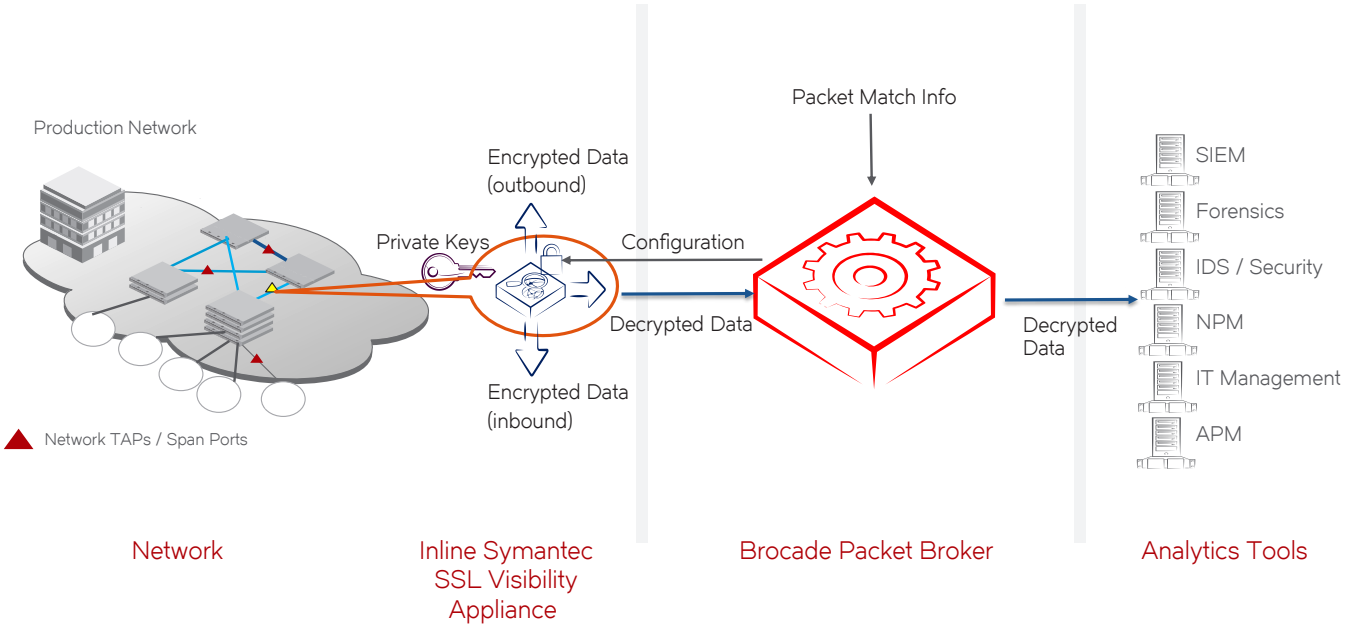

Figure 3: SSL decryption appliance deployed in inline mode.

Learn More

Brocade partners with companies of all sizes to deliver innovative solutions that help organizations maximize the value of their most critical information. To learn more, visit www.brocade.com.

About Brocade

Brocade networking solutions help organizations transition smoothly to a world where applications and information reside anywhere. Innovative Ethernet and storage networking solutions for data center, campus, and service provider networks help reduce complexity and cost while enabling virtualization and cloud computing to increase business agility. Learn more at www.brocade.com.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments, and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud, and infrastructure. Learn more at www.symantec.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