Web Traffic Tap on Cisco Web Security Appliance

Additional visibility, protection and flexibility for encrypted traffic analysis

Identifying and combating cyber threats is a growing challenge every day. With two thirds of web traffic being encrypted, malicious players can cloak their attacks within the Secure Sockets Layer (SSL) traffic while knowing that perimeter security solutions lack visibility into their activities. SSL is the de facto standard for web and other communications today. While encrypting web traffic protects end-users data from being viewed in transit, it also creates a blind spot for IT operations personnel. Several applications that operate in the domains of compliance and reporting, regulatory needs and lawful decryption cannot see anymore what they could earlier.

HTTPS protocol is the result of when HTTP is layered on top of SSL, thereby securing HTTP communication by providing secure authentication as well as session confidentiality. Enterprises and federal agencies will need an encrypted traffic management strategy that encompasses needs around data privacy and regulatory compliances. When you enable the Web Traffic Tap feature on Cisco® Web Security Appliance (WSA), it brings additional visibility into the HTTPS traffic. It also allows you to selectively identify traffic and tap it onto a dedicated interface. The customer can then run deep analysis on the tapped traffic using additional log analysis, forensic analysis and various passive security analysis tools.

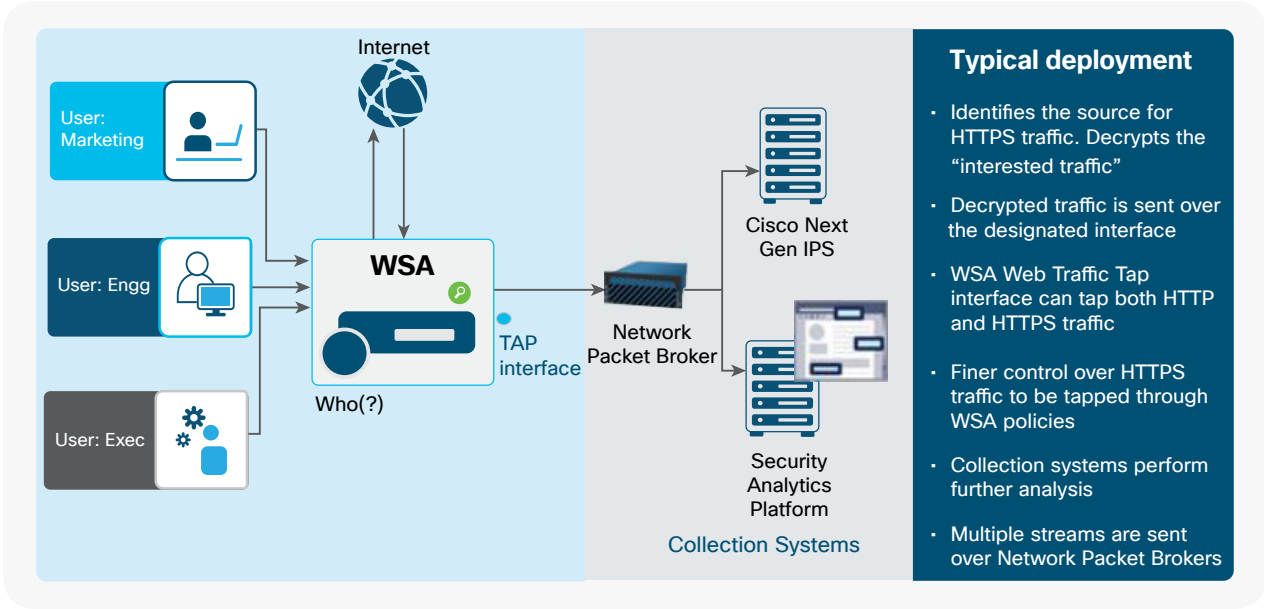
Benefits

- **Flexibility to deploy additional security devices** for Encrypted traffic without compromising end user experience.
- **No additional licensing cost for Web Traffic Tap:** Web Traffic Tap is included as part of the Cisco Web Security base bundle. Hence no additional licenses are required to deliver comprehensive SSL visibility for monitoring and analysis.
- **Selective traffic tapping helps preserve privacy:** Web Traffic Tap provides flexibility to configure tap policies as well as support for both HTTP and HTTPS traffic and finer controls through granular WSA policies by selective decisions through filtering. These policies can also be based on traffic destination of specific URL categories, client identities, and several other advanced options on WSA. Tap policies can also be time bound.
- **Deployment flexibility:** WSA is powered by a purpose-built operating system and can be centrally managed as part of an enterprise-wide solution deployment. From various capacities of hardware as well as virtual form factors, customers may use any of the combinations of physical or virtual appliances to design and calibrate their encrypted traffic management strategy.
- **Comprehensive reporting:** Web Traffic Tap provides easy reports on the percentage of traffic tapped out of the total traffic traversed and the WSA resources utilized by the tap feature. It also helps you manage WSA efficiently.

How web traffic tap can help

WSA supports SSL decryption based on configured decryption policies. To perform additional security analyses on web traffic, admin often rely on additional security devices that analyze the same traffic (as passive traffic). This solution often requires the customer to have an additional decryption device (SSL appliance) that can provide decrypted traffic to third-party security devices for analyses, forensics, and archiving. Web Traffic Tap is intended to assist customers replace the standalone, third-party decryption devices that currently enable them to have visibility. Such devices are usually placed before or after a WSA en route to the network's Internet gateway and cause decryption to happen twice, resulting in additional latency impacting end user experience. In addition, additional devices in the network add operational costs and maintenance overheads for the security administrators managing the network.

Figure 1. Typical WSA deployment using Web Traffic Tap



Next steps

Find out more about Cisco Web Security Appliance at www.cisco.com/go/wsa.

A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco web security will work for you.

Web Traffic Tap requires one of the WSA's interfaces to be the tap interface (output) and have that connected to the analysis/audit device. This can be achieved either by a direct connection or via a VLAN by means of a connected L2 switch. In case of more than one analysis/audit solution forming a collection system, the tap interface on WSA can be connected to a Network Packet Broker (NPB) device that enables efficient use of network tools and monitoring devices (Figure 1).

A separate set of Web Traffic Tap policies can be defined by WSA admin using the GUI. The parameters available by which the transactions can be filtered are similar to those available in WSA access policies. This makes tap policies extremely granular and very efficient.

Web Traffic Tap policies will be visible on the Security Management Appliance (SMA) similar to other access policies and can be added, modified, or viewed. Network settings, including enabling of the tap feature and choosing the tap interface, have to be done on individual WSAs.

Requirements

- Cisco Web Security Appliance (all supported models)
- *Collection system (configured system to receive the tapped data)
- Minimum AsyncOS® release: 11.5.1
- Enable HTTPS decryption feature on WSA
- Enable Web Traffic Tap feature on WSA

* **Note:**

- Collection system is required to be deployed in the network that can receive the tapped traffic for effective operation and to maximize value. Cisco has published whitepapers on solutions that can work together with WSA for the Web Traffic Tap feature

C45-741244-00 08/18