CLOUD SECURITY AND SSL DECRYPTION OVERVIEW

04/17 WP-156-1

Table of Contents

INSPECTING NETWORK TRAFFIC IN THE CLOUD SERVICES ERA

THE PROBLEM WITH CLOUD AND WEB TRAFFIC INSPECTION TODAY

Growth of cloud services has ushered in a new computing architecture and, with it, a host of security challenges. Three such challenges include governing usage; protecting sensitive data and preventing its loss; and defending against threats that propagate in the cloud. Unlike traditional computing architectures in a corporate network - for which security solutions have been designed — cloud services enable security violations and threats to fly under the detection radar. This is partly because many cloud services are unknown to corporate IT and information security teams, but it is also because cloud traffic secured by the SSL (or the more generic TLS) encryption protocol often goes unmonitored by enterprises.

In traditional enterprise computing architectures, organizations may protect themselves from threats in SSL traffic by decrypting that traffic as it travels into and out of the network boundary. They do this using an inline hardware appliance whose job is to provide perimeter protection and govern network traffic. The limitation of inspecting traffic in this manner is that the appliance becomes a bottleneck. As cloud and web traffic increases and users demand high bandwidth with low latency, performing SSL decryption becomes an overhead to an already constrained system. For that reason, it is often the first thing to go.

Recognizing this, some organizations choose to dedicate an appliance solely to SSL inspection. While higher performance than enabling SSL decryption on a perimeter device already performing another function, this is still problematic because of the added cost, complexity, and overhead to system performance.

WHAT'S NEEDED: SSL DECRYPTION IN THE CLOUD, AT CLOUD SCALE

Rather than solve the problem of SSL decryption with more powerful processing at the network perimeter — which results in a game of keep-up as network traffic and user demands increase — why not take advantage of the cloud to perform this critical function? Cloud security solutions like Netskope provide this capability and do it in a manner that is optimized for today's cloud environments, whether users are accessing sanctioned or unsanctioned services.

NETSKOPE: SSL INSPECTION FOR THE WAY PEOPLE WORK TODAY

Netskope, the leader in cloud security, delivers SSL decryption, inspection, and inline policy enforcement not just *for* the cloud, but *in* the cloud. We deliver this at cloud scale, across all traffic, and in a way that's context aware, giving enterprises the granular visibility and control they need.

100% IN THE CLOUD AT CLOUD SCALE

Netskope unshackles you from having to choose between SSL decryption and network performance by delivering SSL inspection and policy enforcement 100 percent in the cloud at cloud scale. Unlike traditional security solutions that are limited by the compute, storage, and I/O available in a physical appliance, our cloud-scale platform is delivered from globally-distributed, secure data centers and has virtually infinite resources that can be applied to solve customer problems.

VISIBILITY AND CONTROL ACROSS ALL TRAFFIC

Whether you are deploying cloud security in forward or reverse proxy mode, and irrespective of whether your users are on premises, remote, on a mobile device, on a browser, or working from a desktop app, mobile app, or sync client, Netskope provides you the ability to decrypt SSL for traffic inspection and inline policy enforcement, with little to no impact to performance.

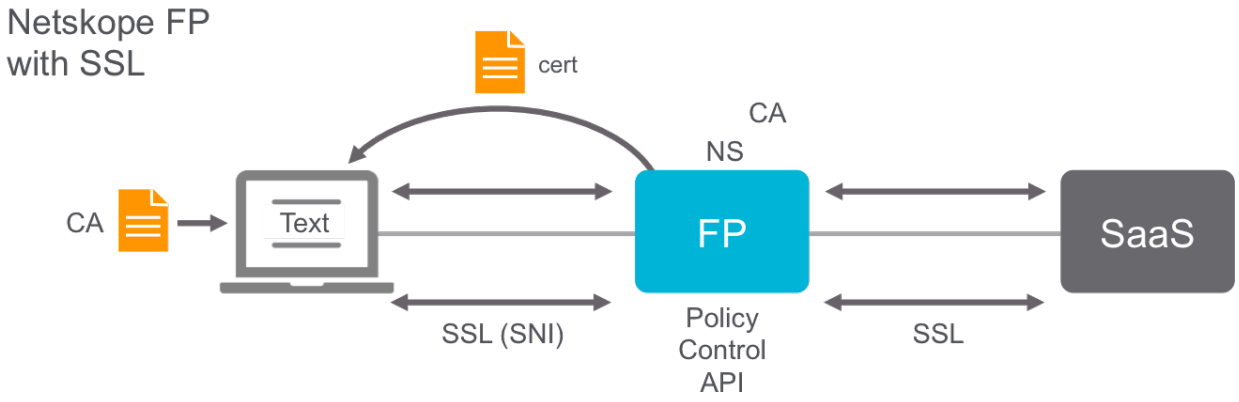
DEEP INSPECTION THAT'S CONTEXT AWARE

Once we decrypt SSL traffic, we provide you deep, contextual inspection. This means not only identifying the services your users are accessing and their byte movements, but decoding and normalizing API transactions that indicate precise activities, such as "upload," "download," "share," "edit," "delete," and dozens of others, as well providing rich metadata about users, devices, locations, and content. Put this all together and you get the fullest picture and most precise cloud policy enforcement in the industry.

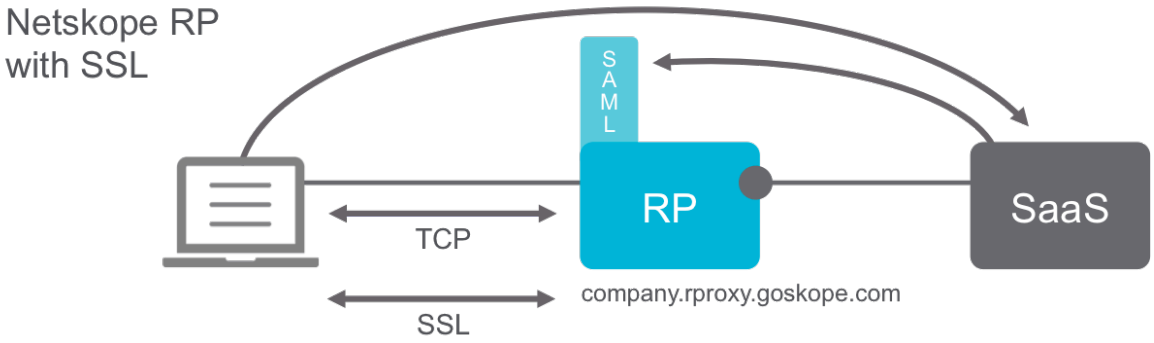
HOW NETSKOPE SSL DECRYPTION WORKS

In forward proxy mode, regardless of whether traffic steering occurs from the corporate network or the endpoint via a thin agent, the certificate used to trust the root Certificate Authority in the

Netskope forward proxy architecture is included and used in the SSL handshake. It is depicted here:



In reverse proxy mode, a certificate from a known Certificate Authority is issued to Netskope as part of the SAML redirect from the cloud service provider so that Netskope becomes part of an established trust chain. It is depicted here:



Netskope couples the above modes of inline traffic inspection and policy enforcement with non-SSL decryption cloud security deployment modes such as out-of-band API integration as well as perimeter log parsing and cloud service discovery and assessment.

By solving SSL decryption, inspection, and policy enforcement in the cloud at cloud scale, across all traffic, and with context awareness, Netskope gives you the deepest visibility and most granular control you need across your cloud services without having to make a performance or cost tradeoff.