SWG: Trust, Management, & Privacy

The SmartEdge Advantage

bitglass

Challenges with Secure Web Gateways in the Cloud

Deploying cloud based secure web gateways presents three significant challenges.

Specifically, in a conventional cloud-based SWG, the organization must store a private key and associated certificate on a third-party cloud server, with the associated loss of trust. Secondly, the organization has to manage client certificates on each endpoint. Finally, traffic is decrypted and inspected in the cloud on third-party servers, resulting in a loss of privacy and security for end users and sovereignty for the organization.

The Bitglass SmartEdge architecture addresses all three challenges. Details can be found below.

1. **Trusting keys on SWG**
2. **Managing certificates**
3. **Privacy & data sovereignty**

#1 Trusting Keys on Secure Web Gateway

When an organization deploys a conventional SWG, it places a private key & corresponding public key certificate on the SWG. If the SWG is an on-premises appliance, the risks are controlled. When the SWG is a third-party server in the cloud, the risks are substantial. For this reason, organizations such as financial institutions and government entities find it challenging to deploy conventional SWGs in the cloud.

Bitglass SmartEdge SWG with patent-pending Trapdoor Proxy technology uses self-managed keys and certificates on the server. There is no need to place institutional keys and certificates in the cloud, mitigating risk.

#2 Managing Certificates on Endpoints

Conventional SWGs require the active management of certificates on endpoints. Certificates need to be installed, rotated, and managed as they expire. This constitutes substantial administrative overhead for IT administrators.

In the case of Bitglass' SmartEdge SWG with patent-pending Trapdoor Proxy technology, each SmartEdge agent carries a fully functional crypto engine. Keys and certificates are self-generated periodically on the endpoint agent. Even if a device is stolen or compromised, the keys on the device cannot be used to spoof any other device, by virtue of Trapdoor technology. As a result, there is no administrative overhead required to manage certificates on the endpoints.

#3 Privacy & Data Sovereignty

In a conventional SWG, encrypted traffic is decrypted and inspected on third-party servers in the cloud. To minimize latency, these servers are distributed across the globe. When a user travels, their traffic may be decrypted and inspected in foreign jurisdictions without regard to data sovereignty.

With the Bitglass SmartEdge SWG, traffic is decrypted and inspected directly on the endpoint. Data centers for the management of the SmartEdge agents may be located only in chosen jurisdictions to ensure data sovereignty, and without compromising latency and user experience.

Summary

Bitglass' SmartEdge SWG with patent-pending Trapdoor Proxy technology uniquely addresses key challenges with the deployment of cloud SWG; preserving trust, privacy, and data sovereignty, all while minimizing management overhead.