One of the world's top ten banks deploys Entrust nShield HSMs to deliver trusted, reliable web services to its customers and partners

BUSINESS CHALLENGE

Any enterprise with a customer-facing online presence authenticates its users as they utilize services – and for the world's leading banks this is no exception. With the expansive growth of the internet and online transactions, sensitive data exchanged online and in the cloud has increasingly become a target for attack.

Online services use login mechanisms to connect end-user browsers to web servers, and these connections are protected by secure sockets layer (SSL), a technology that encrypts data on the internet. The SSL standard (the technology behind the padlock symbol in the browser and more properly referred to as transport layer security or TLS) is the de facto form of protection for all internet communications.

> **In the face of ever-growing internet traffic and prolific SSL-based malware attacks, such as Heartbleed, this leading bank needed to increase and enhance its ability to securely inspect SSL traffic to ensure there were no hidden viruses or other malware that could infect its systems.**

World Leading Bank

To deliver trusted and reliable web services to their users, enterprises must address the confidentiality, integrity, and availability of the data processed by the service. In the face of ever-growing internet traffic and prolific SSL-based malware attacks, such as Heartbleed, this leading bank needed to increase and enhance its ability to securely inspect SSL traffic to ensure there were no hidden viruses or other malware that could infect its systems. Specifically, this project focused on inspecting traffic generated from the bank's partners, subsidiaries, and employees.

TECHNICAL CHALLENGE

The increase in the amount of encrypted traffic traversing today's networks can also make SSL a vector for attacks, as malicious code can hide and go undetected. SSL inspection is used to filter out potentially dangerous elements hiding within encrypted content.

It involves intercepting website traffic, decrypting and inspecting it, and re-encrypting it for its final destination.

Hardware security modules (HSMs) offer an additional layer of security for the increasing number of SSL keys used as a result of the decryption and re-encryption process. Decrypting, inspecting, and re-encrypting traffic to enable it to be inspected and continue on its way to a web server (where it is again decrypted) means the keys necessary for this process are retrieved more frequently. Generally, all the keys used are not the same – which leads to the need for more robust protection.

HSMs provide a root of trust, ensuring all critical connections are not only protected, but can be trusted. According to the bank's security architect, it is possible to inspect internet traffic flow without a hardware security module (HSM), but very dangerous.

World Leading Bank

You need to protect the technology that decrypts the web traffic, and that means protecting and securing the decryption keys, which is what the HSMs do.

SOLUTION

The bank deployed Entrust nShield Connect HSMs to work in a twin "active-active" configuration in two data centers about 10 kilometers apart. The HSMs meet the security requirements of 45 proxy servers today and offer plenty of capacity for growth.

RESULTS

The Entrust nShield HSMs are expected to achieve at least five times the capacity of the legacy system. This will enable the organization to inspect internet traffic for possible hidden malicious code and ensure security as the system grows.

This world leading bank has worked with Entrust for more than 10 years and chose Entrust as its defacto HSM provider because of Entrust's deep experience with the technology and in addressing security issues. Entrust's professional services team were also deployed to install the HSMs and provide training to the bank's staff on their use.

World Leading Bank

Business need

- Deliver trusted and reliable web services to users

Technology need

- Monitor increasing amounts of internal internet traffic and protect monitoring technology
- Protect the organization's overarching IT infrastructure

Solution

- Entrust nShield Connect HSMs running "active-active" to manage and protect SSL keys

Result

- FIPS 140-2 Level 3 and Common Criteria EAL4+ certified security
- Five times the capacity of the legacy system
- Ability to easily scale up for future needs

ABOUT ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com