Uno de los diez bancos más importantes del mundo implementa los HSMs de Entrust para ofrecer servicios fiables y de confianza a sus clientes y colaboradores

RETO EMPRESARIAL

Cualquier empresa con una presencia en línea dirigida al cliente autentica a los usuarios a medida que utilizan los servicios, y los principales bancos del mundo no son una excepción. Con el crecimiento expansivo de Internet y las transacciones en línea, el intercambio de datos confidenciales en línea y en la nube se ha convertido rápidamente en el objetivo de los ataques.

Los servicios en línea utilizan mecanismos de inicio de sesión para conectar el navegador del usuario final a los servidores web y estas conexiones están protegidas por una capa de sockets seguros (SSL), una tecnología que cifra los datos en Internet. El estándar SSL (la tecnología tras el símbolo de candado en el navegador, llamada seguridad de la capa de transporte o TLS) es la forma de protección de todas las comunicaciones de Internet.

> **Ante el creciente tráfico en Internet y los abundantes ataques de software malicioso basados en SSL, como Heartbleed, este importante banco necesitaba aumentar y potenciar su capacidad para inspeccionar el tráfico SSL de forma segura para garantizar que no había virus ocultos u otro software malicioso que pudiera infectar sus sistemas.**

Banco líder a nivel mundial

Para ofrecer servicios web fiables y de confianza a los usuarios, las empresas deben asegurar la confidencialidad, la integridad y la disponibilidad de los datos que procesa el servicio. Ante el creciente tráfico en Internet y los abundantes ataques de software malicioso basados en SSL, como Heartbleed, este importante banco necesitaba aumentar y potenciar su capacidad para inspeccionar el tráfico SSL de forma segura para garantizar que no había virus ocultos u otro software malicioso que pudiera infectar sus sistemas. Este proyecto se centraba específicamente en inspeccionar el tráfico generado por los colaboradores, subsidiarios y empleados del banco.

RETO TÉCNICO

El aumento en la cantidad de tráfico cifrado que transita las redes en la actualidad puede convertir a la SSL en un vector para ataques, ya que el código malicioso puede esconderse y pasar desapercibido. La inspección de SSL se lleva a cabo para filtrar elementos potencialmente peligrosos que se esconden entre el contenido cifrado. Esto implica tener que interceptar el tráfico del sitio web, descifrarlo e inspeccionarlo, para luego volver a cifrarlo y enviarlo a su destino final.

Los módulos de seguridad de hardware (HSMs) ofrecen una capa de seguridad adicional para el creciente número de claves SSL que se están usando como resultado del proceso de descifrado y cifrado posterior. Descifrar, inspeccionar y volver a cifrar el tráfico para poder inspeccionarlo y que continúe con su camino hasta el servidor (donde se vuelve a descifrar) significa que las claves son necesarias para este proceso y que se recuperan con más frecuencia. Generalmente, todas las claves que se usan no son las mismas, por eso es necesaria una protección más sólida.

Los HSMs ofrecen una raíz de confianza, asegurando que todas las conexiones importantes no solo estén protegidas, sino que sean fiables. Según el arquitecto de seguridad del banco, es posible inspeccionar el flujo de tráfico de Internet sin un módulo de seguridad de hardware (HSM), pero también muy peligroso.

Banco líder a nivel mundial

Es muy importante proteger la tecnología que descifra el tráfico de los sitios web, lo que significa proteger y mantener seguras las claves de descifrado, que es lo que hacen los HSMs.

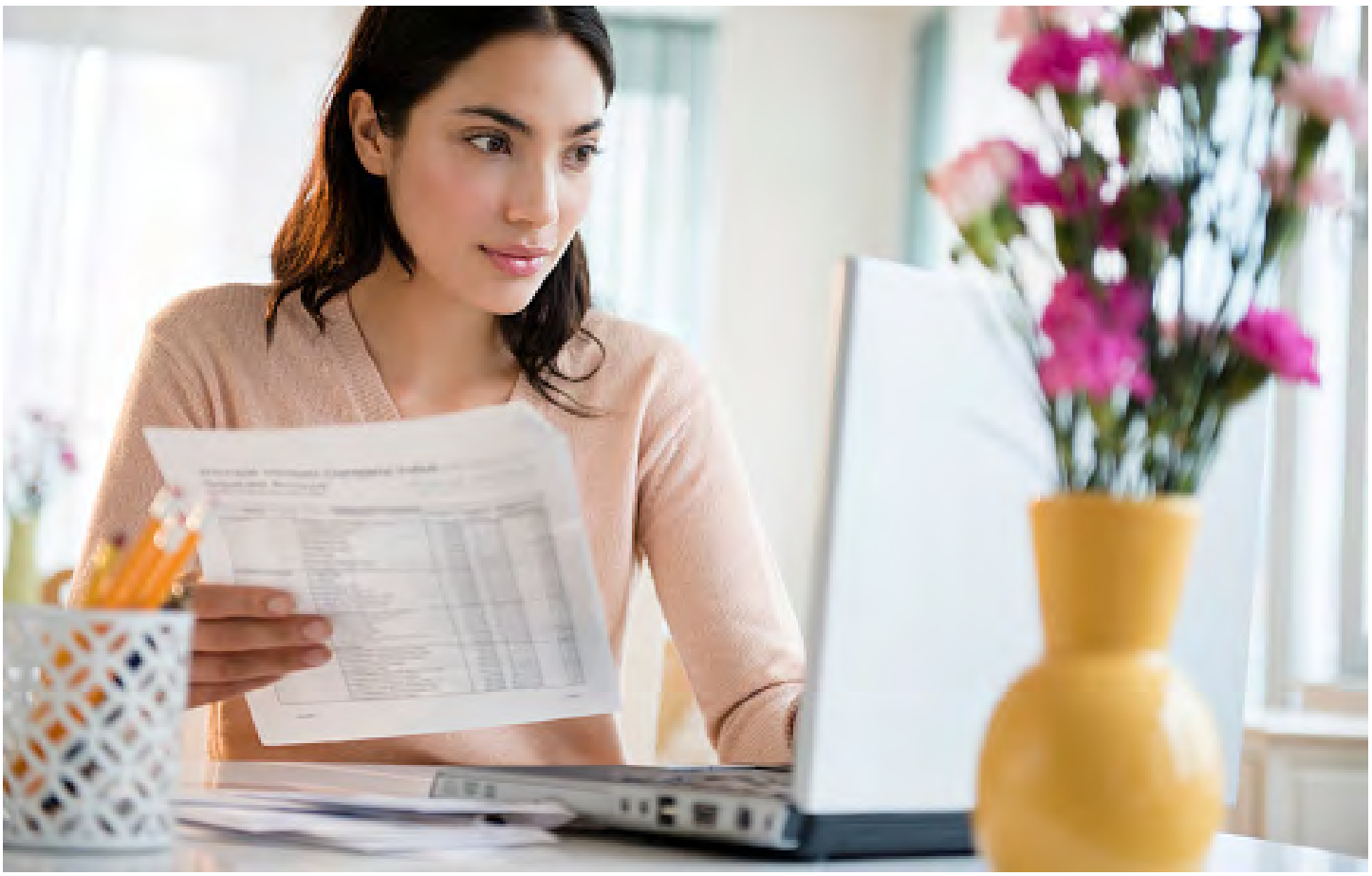
SOLUCIÓN

El banco implementó HSMs nShield Connect de Entrust para trabajar en una configuración gemela "activo-activo" en dos centros de datos situados a unos 10 kilómetros de distancia. Los HSMs cumplen con los requisitos de seguridad de 45 servidores proxy y ofrecen una gran capacidad de crecimiento.

RESULTADOS

Se espera que los HSMs nShield de Entrust consigan al menos cinco veces la capacidad del sistema anterior. Lo que permitirá a la empresa inspeccionar el tráfico de Internet en busca de posibles códigos maliciosos ocultos y garantizar la seguridad al mismo tiempo que crece el sistema.

Este banco líder mundial ha trabajado con Entrust durante más de 10 años y eligió a Entrust como su proveedor de HSMs de facto debido a la profunda experiencia de Entrust con la tecnología y el tratamiento de problemas de seguridad. El equipo de servicios profesionales de Entrust también se desplegó para instalar los HSMs y proporcionar formación al personal del banco sobre su uso.



Banco líder a nivel mundial

Necesidades del negocio

- Ofrecer servicios web fiables y de confianza a los usuarios

Necesidades tecnológicas

- Monitorizar las cantidades crecientes de tráfico de Internet interno y proteger la tecnología de monitorización
- Proteger la infraestructura informática general de la empresa

Solución

- HSMs nShield Connect de Entrust ejecutando una configuración "activo-activo" para gestionar y proteger las claves SSL

Resultado

- Certificación FIPS 140-2 Nivel 3 y seguridad con certificación Common Criteria EAL4+
- Cinco veces más capacidad que el sistema anterior
- Capacidad para ampliar fácilmente en caso de necesidades futuras

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com