Um dos dez maiores bancos do mundo utiliza HSM nShield da Entrust para fornecer serviços web confiáveis e seguros a seus clientes e parceiros

DESAFIO DO NEGÓCIO

Qualquer empresa voltada para o cliente com presença online verifica a identidade de seus usuários que usam seus serviços - e para os principais bancos do mundo isso não é exceção. Com o crescimento expansivo da internet e das transações online, dados confidenciais compartilhados online e na nuvem têm se tornado cada vez mais alvo de ataque.

Os serviços online utilizam mecanismos de login para conectar os navegadores dos usuários finais aos servidores web, e estas conexões são protegidas pela camada de soquetes de segurança (SSL), uma tecnologia que criptografa dados compartilhados na internet. O padrão SSL (a tecnologia por trás do símbolo do cadeado do navegador e mais propriamente conhecida como segurança da camada de transporte, ou TLS) é a forma de proteção básica para todas as comunicações pela internet.

> **« Diante do crescente tráfego de internet e dos muitos ataques de malware baseados em SSL, como o Heartbleed, este importante banco precisava aumentar e melhorar sua capacidade de inspecionar com segurança o tráfego SSL para garantir a inexistência de vírus escondidos ou outros malwares que pudessem infectar seus sistemas. »**

Banco líder mundial

Para fornecer serviços web confiáveis e seguros a seus usuários, as empresas devem cuidar da confidencialidade, integridade e disponibilidade dos dados processados pelo serviço. Diante do crescente tráfego de internet e dos muitos ataques de malware baseados em SSL, como o Heartbleed, este importante banco precisava aumentar e melhorar sua capacidade de inspecionar com segurança o tráfego SSL para garantir a inexistência de vírus escondidos ou outros malwares que pudessem infectar seus sistemas. Este projeto se concentrou especificamente na inspeção do tráfego gerado por parceiros, subsidiárias e funcionários do banco.

DESAFIO TÉCNICO

O aumento da quantidade de tráfego criptografado que circula nas redes atuais também pode fazer do SSL um vetor de ataques, já que o código contraventor pode se esconder e passar despercebido. A inspeção SSL é usada para filtrar elementos potencialmente perigosos escondidos dentro do conteúdo criptografado. Ela intercepta o tráfego do site, faz sua decodificação, inspeção e reencriptação para seu destino final.

Os módulos de segurança de hardware (HSM) oferecem uma camada adicional de segurança para o crescente número de chaves SSL usadas como resultado do processo de descriptografia e reencriptação. Descriptografar, inspecionar e reencriptar o tráfego para permitir que ele seja inspecionado e continue seu caminho para um servidor web (onde é novamente descriptografado) significa que as chaves necessárias para este processo são recuperadas com mais frequência. Geralmente, as chaves utilizadas não são as mesmas - o que leva à necessidade de uma proteção mais forte.

Os HSM fornecem um ponto comum de confiança, garantindo que todas as conexões críticas não só sejam protegidas, mas também

Banco líder mundial

possam ser confiáveis. De acordo com o arquiteto de segurança do banco, é possível inspecionar o fluxo de tráfego da internet sem um módulo de segurança de hardware (HSM), mas isso é muito perigoso.

É preciso proteger a tecnologia que descriptografa o tráfego da web, e isso significa proteger e proteger as chaves de descriptografia, que é o que os HSMs fazem.

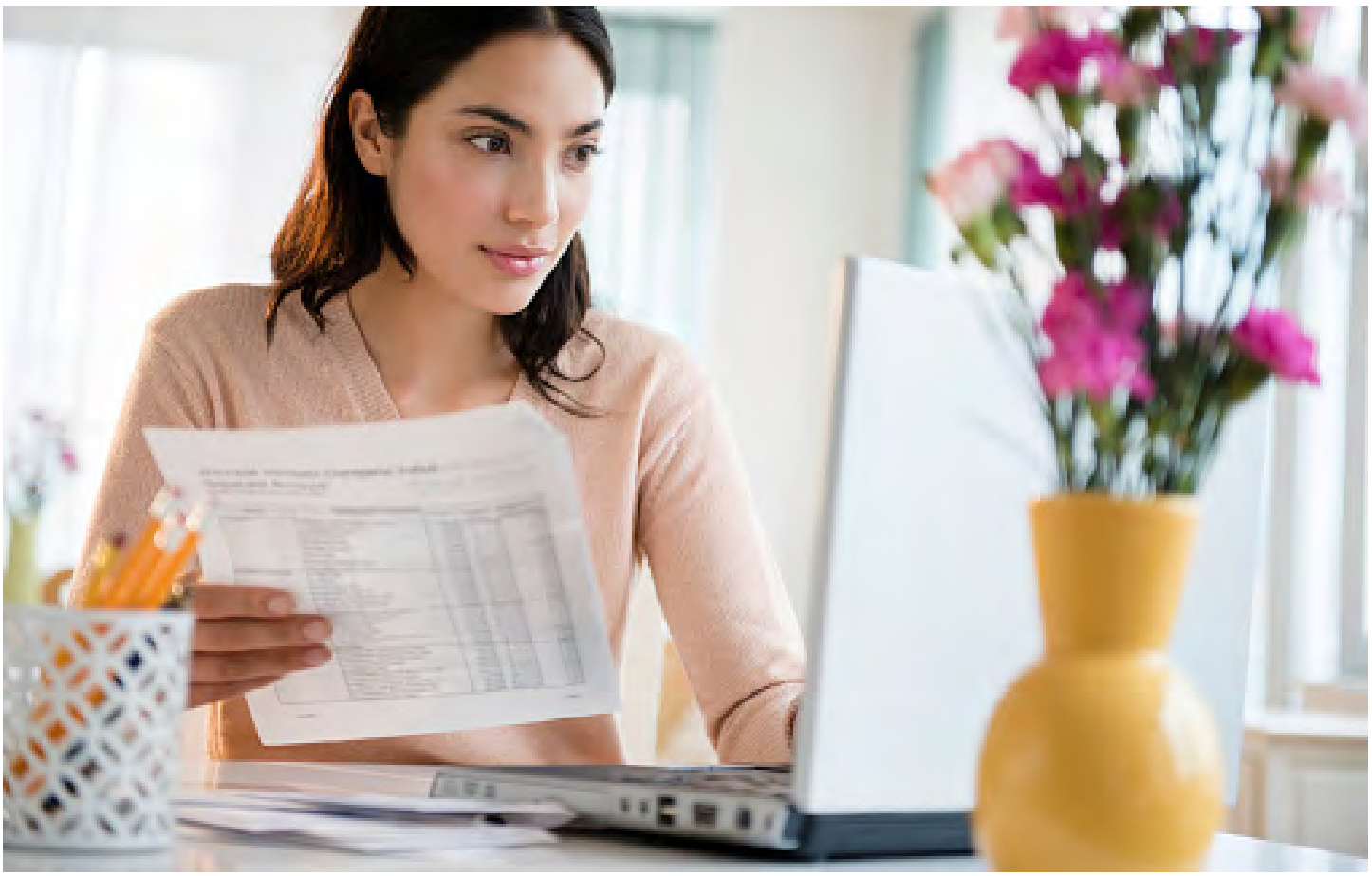
SOLUÇÃO

O banco implantou os HSM Connect nShield da Entrust para trabalhar em uma configuração dupla "ativa-ativa" em dois centros de dados a cerca de 10 quilômetros de distância. Os HS atendem hoje às exigências de segurança de 45 servidores proxy e oferecem muita capacidade de crescimento.

RESULTADOS

Espera-se que os HSM nShield da Entrust tenham pelo menos cinco vezes a capacidade do sistema legado. Isto permitirá que a organização inspecione o tráfego da internet para detectar possíveis códigos contraventores ocultos e garantir a segurança à medida que o sistema cresce.

Este banco líder mundial trabalha com a Entrust há mais de 10 anos e escolheu a empresa como sua fornecedora oficial de HSM devido à sua profunda experiência com a tecnologia e sua abordagem em questões de segurança. A equipe de serviços profissionais da Entrust também foi escolhida para instalar os HSM e fornecer treinamento aos funcionários do banco sobre seu uso.



Banco líder mundial

Necessidade do negócio

- Fornecer aos usuários serviços web confiáveis e seguros

Necessidades tecnológicas

- Monitorar quantidades crescentes de tráfego interno na internet e proteger a tecnologia de monitoramento
- Proteger toda a infraestrutura de TI da organização

Solução

- HSM Connect nShield da Entrust com configuração dupla "ativa-ativa" para gerenciar e proteger chaves SSL

Resultados

- Certificado de segurança FIPS 140-2 de nível 3 e Common Criteria EAL4+
- Cinco vezes a capacidade do sistema legado
- Capacidade de dimensionar facilmente para as necessidades futuras

SOBRE A ENTRUST

A Entrust mantém o mundo movendo-se com segurança, permitindo identidades, pagamentos e proteção de dados confiáveis. Hoje, mais do que nunca, as pessoas exigem experiências seguras e contínuas, quer estejam cruzando fronteiras, fazendo uma compra, acessando serviços de governo eletrônico ou entrando em redes corporativas. A Entrust oferece uma gama incomparável de soluções de segurança digital e emissão de credenciais no centro de todas essas interações. Com mais de 2.500 colegas, uma rede de parceiros globais e clientes em mais de 150 países, não é de admirar que as organizações mais confiáveis do mundo confiem em nós.

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com