THALES

Módulo de Segurança de Hardware

Thales nShield Connect

PRINCIPAIS BENEFÍCIOS

OPERACIONAIS

> Fornece uma flexibilidade operacional incomparável, disponibilidade e escalabilidade elevadas em ambientes virtuais e em nuvem que alavancam a arquitetura exclusiva do Security World

> Reduz o custo total para conformidade regulamentar (por exemplo, PCI DSS), bem como tarefas de gerenciamento de chave para o dia a dia, incluindo o backup e o gerenciamento remoto

> Assegura com enorme garantia a continuidade dos negócios, com registro HSM simplificado, eficiente provisionamento de chave recursos de hardware completamente resilientes, incluindo duas fontes de alimentação hot swap e ventoinhas redundantes substituíveis em campo

SEGURANÇA

> Oferece proteção certificada para operações e chaves criptográficas protegidas por hardware inviolável para melhoramento significativo da segurança em aplicações críticas

> Estabelece uma separação forte de funções e controles duplos através de políticas administrativas sólidas, incluindo uma autenticação multifator baseada na função e uma autorização flexível baseada em quórum

> Permite a execução segura de um código de aplicativo crítico para a segurança dentro dos limites de segurança do hardware

O nShield Connect é o principal módulo de segurança de hardware (HSM) da família Thales de soluções de proteção de dados de alta segurança. A plataforma de certificação independente realiza o gerenciamento de chaves e operações criptográficas, como criptografia e assinatura digital em nome de uma ampla variedade de aplicativos comerciais e de negócios criados pelo cliente e sistemas de segurança crítica, incluindo infraestruturas de chave pública (PKIs), sistemas de gerenciamento de identidade, banco de dados, aplicações web, implantações de extensão para sistemas de nome de domínio (DNSSEC) e assinatura de códigos.

O nShield Connect é o meio mais eficaz de estabelecer os níveis adequados de controle físico e lógico para sistemas baseados em servidor onde os recursos de segurança são considerados inadequados. Em virtude de requerimentos de conformidade em desenvolvimento e padrões gerais de consciência profissional, o uso de HSMs nShield fornece uma medida tangível de segurança dentro de Data Centers tradicionais, ambientes virtuais e para serviços baseados na nuvem. Todos os HSMs da Thales nShield se caracterizam pela arquitetura de gerenciamento de chave líder do mercado, o Security World, que permite a automatização de pesadas tarefas administrativas propensas a risco, garante a recuperação de chave e elimina pontos únicos de falha e processos dispendiosos e intensivos de backup manual.

Microsoft GOLD CERTIFIED Partner ISV

ORACLE CERTIFIED PARTNER

T SERVICES

www.tservices.com.br

> Thales nShield Connect

Especificações Técnicas*

Capacidades Funcionais

- Chave segura onboard e storage/processamento de aplicativos
- Descarregamento/aceleração criptográfica
- Controle de acesso multinível autenticado
- Separação forte de funções (administrador e operador)
- A opção nToken fornece uma autenticação de cliente incomparável
- Disposição de chave segura, replicação, backup e recuperação
- Storage ilimitado de chaves protegidas
- Agrupamento, balanceamento de carga e autenticação de multifator "k de n"
- Separação lógica/criptográfica ilimitada de chaves de aplicativos

Sistemas Operacionais Suportados

- Físicos: Windows, Linux, Solaris, IBM AIX, HP-UX
- Virtuais: suporta diversos fornecedores de software VM, incluindo VMware, Hyper-V e AIX LPARs

Interfaces de Programa Aplicativo (IPAs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI e CNG
- nCore (interface Thales de baixo nível para desenvolvedores)

Escalabilidade, Compatibilidade e Atualizações

- Até 100 clientes
- Compatível com Thales nShield Solo (PCI/PCIe), nShield Edge e netHSM
- Software atualizável

Conectividade do Host

- Duas portas Ethernet Gigabit (serviço para dois segmentos de rede)

Criptografia

- Algoritmos assimétricos de chave pública: RSA (1024, 2048, 4096, 8192), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
- Algoritmos simétricos: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, 3DES
- Hash/resumo de mensagem: SHA-1, SHA-2 (224, 256, 384, 512 bits)
- Implementação total de Suite B com Criptografia de Curva Elíptica (CCE) totalmente licenciada, incluindo Brainpool e curvas personalizadas

Segurança e Conformidade Ambiental

- UL, CE, FCC
- RoHS, WEEE
- FIPS 140-2 nível 2 e nível 3, NIST SP 800-131A
- Critérios Comuns EAL4+

Alta Disponibilidade

- Storage de estado sólido completo
- Alimentação dupla de hot swap
- Componentes de campo substituíveis (alimentação e ventoinhas)
- 47.000 hrs de MTBF (método de contagem de 2 peças para notificação Mil-Std 217F)

Gerenciamento e Monitoramento

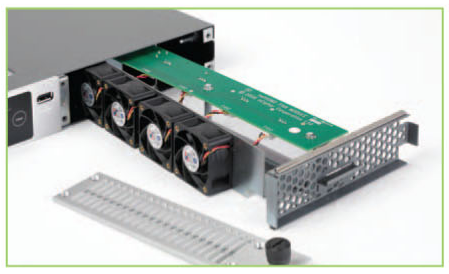
- Controle de acesso remoto multi-usuário/sem operador
- Suporte de diagnósticos syslog
- Monitoramento do desempenho do Windows
- Interface de linha de comando (CLI)/interface gráfica do usuário (GUI)
- Monitoramento compatível com SNMPv3

Características Físicas

- Montagem em rack 1U de 19 pol. padrão com um leitor integrado de cartões inteligentes
- Dimensões: 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8 pol.)
- Peso: 11,5 kg (25,4 lbs)
- Tensão de entrada: 100-240v CA com alternância automática 50-60Hz (nominal) / chave liga-desliga e tomada IEC 320
- Consumo de energia: até 1,2A em 110v CA 60Hz ou 0,6A em 220v CA 50Hz
- Dissipação de calor: 327,6 a 362,0 BTU/hr (carga total)
- Temperatura: operação de 5 a 40°C (41 a 104°F), armazenamento entre -20 a 70°C (-4 a 158°F)
- Umidade: operação de 10 a 90% (relativa, sem condensação em 35%), armazenamento entre 0 a 85% (relativa, sem condensação em 35%)

Continuidade de Negócios

Uma memória em estado sólido completa projetada para a continuidade de negócios, o nShield Connect também inclui uma alimentação dupla hot swap e uma bandeja de ventoinha substituível em campo que permite o reparo no local. Para aumentar ainda mais a disponibilidade, diversos HSMs podem ser combinados para o balanceamento de carga e failover. O suporte a SNMP permite o monitoramento remoto de alimentações, temperatura, velocidade das ventoinhas e outros parâmetros.



O nShield Connect inclui uma alimentação dupla de hot swap, bandejas substituíveis em campo e trilhos de deslizamento opcionais para a montagem em rack.

Modelos Disponíveis e Desempenho

O nShield Connect está disponível em três versões diferentes:

Modelos	500	1500	6000
Assinatura (tps) em 1024bit RSA	500	1500	6000
Assinatura (tps) em 2048bit RSA	150	500	3000
Assinatura (tps) em 4096bit RSA	65	165	500
Licenças de cliente inclusas	3	3	3
Nº máx. de clientes	10	20	100
Painel frontal	Preto	Preto	Prata

* O desempenho pode variar conforme o sistema operacional, aplicativo, topologia de rede e outros fatores.

Américas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Ásia-Pacífico: Unit 4101, 41/F, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europa, Oriente Médio e África: Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com