Product Brief

タレス CN6100 ネットワーク暗号化装置

10 Gbps のスケーラブルで信頼性の高い通信データの暗号化

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

リアルタイムの低遅延とほぼゼロのオーバーヘッドという、ネットワークパフォーマンスのニーズを満たすことが実証された高速ネットワーク暗号化により、 移動中のデータを保護します。データセンター間やクラウド全体でネットワークを経由して送信されるデータに、妥協のないセキュリティを提供します。

タレスCN6100ネットワーク暗号化装置 (CN6100) は、小規模および大規模の企業、政府機関、サービスプロバイダーのクラウドに最適なソリューションです。CN6100は、ダークファイバー、メトロまたはワイドエリアイーサネットネットワーク(MANまたはWAN)を移動するすべの音声、ビデオ、およびデータ通信に対して、最大10Gbpsの安全なフルラインレートで透過的な暗号化を提供するように設計された、多用途で信頼性の高い暗号化装置です。で動作する高性能暗号化装置です。

パフォーマンス

CN6100は、パケットロスなしに全二重モードで最高速度で動作する高性能暗号化装置です。CN6100のカットスルーアーキテクチャは、フィールドプログラマブルゲートアレイ(FPGA)テクノロジを使用して、受信したデータフレームを処理します。これによりすべてのパケットサイズで一貫した低レイテンシ(遅延)が保証され、最適なパフォーマンスを実現し、スループットは、プロトコルのゼロモードで最大化されます。1Uユニットで、一般的な10　Gbps暗号化装置よりも30～60% 少ない消費電力で動作します。

CN6100 暗号化装置を選ぶ理由

信頼できるセキュリティ

- 真のエンドツーエンドの認証された暗号化
- 最先端の自動ゼロタッチ鍵管理
- FIPS 140-2 L3、Common Criteria、NATO、UC APL認定
- 35か国以上で、市場をリードする企業や政府機関に選ばれています

最大のネットワークパフォーマンス

- マイクロ秒の遅延(<6μS)
- ほぼゼロのオーバーヘッド
- 自己修復機能により最大限の稼働時間を実現

スケーラブルでシンプル

- ポイントツーポイント、ハブ&スポーク、フルメッシュ
- サードパーティの管理ツールからの完全に監査可能なアラームおよびイベントログ
- ホットスワップ可能なファンとサプライ品により現場でのサービスが可能

スケーラビリティ

CN6100は、主要ベンダーの業界標準ネットワーク機器と完全に相互運用可能です。「Bump in the Wire」設計と最大10Gbpsの可変速度ライセンスにより、CN6100は簡単にインストールでき、コスト効率に優れています。「全自動」のシンプルさと、アプリケーションとプロトコルの透過性が設計の基本原則としており、実装、操作、管理が簡単で、リソース要件が最小限に抑えられます。メンテナンス、機能強化、セキュリティアップデートのために、デバイスを簡単にフィールドアップグレードできます。タレスの高速ネットワーク暗号化装置ファミリ全体との完全な互換性により、エンドユーザーはあらゆるネットワーク環境で安全なデータ転送を実現できます。

認定されたセキュリティ

耐タンパ性を備えたCN6100は、Common　CriteriAおよびFIPS140-2レベル3要件の認定を取得済みで、標準ベースのエンドツーエンドの認証付き暗号化とクライアント側の鍵管理をサポートしています。高度なセキュリティ機能には、トラフィックフローセキュリティ、さまざまな楕円曲線のサポート(Safe　Curves、Brainpool、NIST)が含まれます。 VLANベースの暗号化は、ハブとスポーク環境で一意の鍵ペアを提供し、誤って構成されたトラフィックから保護します。 高保証環境の場合、暗号化機能はネストされた暗号化もサポートします。

最先端の鍵管理

CN6100は外部鍵管理サーバーに頼る必要はありません。堅牢なフォールトトレラントセキュリティアーキテクチャと改ざん防止シャーシを提供します。物理的および仮想的な職務の分離により、許可されたユーザーのみが鍵にアクセスできるようになります。暗号化鍵は、デバイスの耐タンパ性エンクロージャ内のハードウェアで安全に生成および保存され、鍵を物理的に抽出しようとする不正な試みがあった場合は、デバイスはゼロ化されます。

CN6100はハードウェアベースの乱数ジェネレータをサポートし、外部で生成されたエントロピーを使用して固有キーの生成と配布を行うことができます。将来に備えて、暗号化装置は量子鍵配布 (量子暗号化) と量子乱数生成をサポートしています。

次世代高速暗号化

クリプトアジリティ

タレスの高速ネットワーク暗号化装置は暗号化に柔軟に対応しており、幅広い楕円曲線やカスタム曲線をサポートするカスタマイズ可能な暗号化をサポートしています。アプライアンスでは、独自のエントロピー機能を導入することもできます。暗号化アジャイルプラットフォームは将来性があり、次世代またはカスタムアルゴリズムの応答性の高い展開を可能にします。量子の脅威に対応するため、タレスのネットワーク暗号化装置はすでに量子鍵配布(QKD)機能と量子乱数生成(QRNG)機能を活用して、将来を見据えたデータセキュリティを実現しています。

トランスポート非依存モード

ネットワーク暗号化市場に変革をもたらすタレスのネットワーク暗号化装置は、ネットワークレイヤーに依存せず(レイヤー 2、レイヤー 3、レイヤー 4)、プロトコルとらわれない移動中データの暗号化を実現し、トランスポート独立モード(TIM) を初めて提供します。レイヤー3をサポートすることで、タレスのネットワーク暗号化装置は、重要なデータを保護するために、TCP/IPルーティングを使用してより多くの構成オプションをネットワークオペレーターに提供します。

CN6100 暗号化装置の概要

モデル	CN6100
プロトコル	イーサネット
プロトコルと接続性	
最大ポート速度	10 Gbps
最大シャーシスループット	10 Gbps
ジャンボフレームのサポート	あり
プロトコルとアプリケーションの透過性	あり
ユニキャストを暗号化します。マルチキャストおよびブロードキャストトラフィック	あり
自動ネットワーク検出と接続確立	あり
セキュリティ	
耐タンパ性と改ざん防止機能を備えたエンクロージャ、アンチプロービングバリア	あり
柔軟な暗号化ポリシーエンジン	あり
AES-GCM暗号化によるパケットごとの機密性と完全性	あり
自動鍵管理	あり
暗号化とポリシー	
AES 128 または 256 ビットキー	128/256
CTR、GCM 暗号化モード	あり
量子乱数ジェネレーター	あり
サードパーティ量子鍵配布(QKD)サポートオプション	あり
MACアドレスまたはVLAN IDに基づくポリシー	あり
ネットワーク障害発生時の自己修復鍵管理	あり
認定取得	
コモンクライテリア、FIPS	あり
パフォーマンス	
低オーバーヘッドの全二重ラインレート暗号化	あり
FPGAベースのカットスルーアーキテクチャ	あり
遅延(マイクロ秒／暗号化装置あたり)	<5@ 10 Gbps
管理	
フロントパネルLEDディスプレイ通知	あり
SMCおよびCM7を使用した一元的な構成と管理	あり
外部 (X.509v3) CA のサポート	あり
SNMPv3 を使用したリモート管理 (インバンドおよびアウトオブバンド)	あり
NTP(タイムサーバー)サポート	あり
CRL および OCSP (証明書) サーバーのサポート	あり
保守性と相互運用性	
現場でのファームウェアアップグレード	あり
二重冗長AC/DC電源	あり
プラグ可能な光XFP	XFP

仕様

物理セキュリティ

- アクティブ/パッシブタンパ検出とキー消去

暗号化

- AES 128 または 256 ビット キー X.509 証明書 (CFB、CTR、または GCM モード)
- ハードウェアベースの乱数ジェネレータ

デバイス管理

- 専用管理インターフェース(アウトオブバンド)
- 暗号化インターフェース(インバンド)
- SNMPv3 リモート管理
- IPv4およびIPv6対応
- Syslog サポート
- アラーム、イベント、監査ログ
- コマンドラインシリアルインターフェース
- TACAS+サポート
- RADIUS サポート

設置

- 寸法: 447mm, 43mm (1U), 328mm /17.6”, 1.7”, 12.9”
- 19インチラックマウント可能
- 重量: 8.5kg /18.7 lbs

電力要件

- AC入力: 100～240V AC、1.5A、60/50Hz
- DC入力: 40.5～60 VDC、2.0A
- 消費電力: 通常50W

規制

- UL 認定
- EMC（放射と耐性）
- FCC 47 CFR パート 15 (米国)
- EN 55024 (CE、60950-1 (CE)、61000-3-2 (CE)、61000-3-3 (CE)
- IEC 60950-1 第2版
- ICES-003（カナダ）

環境

- RoHS対応
- 最大動作温度: 50°C /122°F
- 動作温度40°C /104°Fで0～80%RH
- AS/NZS 60950-1、CISPR 22 (C-Tick)
- すべての仕様は公開時点で正確なものであり、予告なく変更される場合があります。

タレスについて

皆様がプライバシー保護を信頼して任せている相手は、そのデータを保護するためにタレスに頼っています。データセキュリティに関しては、組織が直面する決定的な局面は次々と増え続けています。その局面が暗号化戦略の策定、クラウドへの移行、コンプライアンス要件の順守のいずれであっても、デジタルトランスフォーメーションを保護するためにタレスに頼ることができます。

決断の瞬間のための確実なテクノロジー。

cpl.thalesgroup.com

お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com

すべてのオフィスの所在地と連絡先情報につきましては 、cpl.thalesgroup.com/ja/contact-usをご覧ください。