Product Brief

タレスCN4010 ネットワーク暗号化装置

コンパクト設計で高パフォーマンスな暗号化を実現

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

タレスCN4010ネットワーク暗号化装置（CN4010）は、価格と性能の新たな基準を打ち立てる、汎用性の高い費用対効果に優れた、ユーザー構成可能な使いやすいプラットフォームです。FIPSおよびコモンクライテリア認定を受けた、透過的で信頼性の高いフルラインレートでのネットワーク暗号化を提供します。CN4010は、高効率のイーサネット暗号化を保証する専用ハードウェア暗号化ソリューションとして、最先端の高性能、低電圧エレクトロニクスを活用し、すべての音声、ビデオ、データ通信をワイヤスピードで暗号化します。

CN4010は、費用対効果の高い最適な防衛グレードのセキュリティを提供します。デスクトップデバイスであるCN4010は、中小企業（SME）の商業部門や、中程度のネットワークニーズを持つ大企業向けの、エントリーレベルのHSEソリューションとして設計されています。また、広範囲に分散したコンピューティング環境や複数の支社拠点にも適しています。

CN4010暗号化装置が選ばれる理由

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、コモンクライテリア、NATO、UC APLに対応する設計
- 世界35カ国以上の市場をリードする民間企業や政府機関が採用

最大のネットワークパフォーマンス

- マイクロ秒の遅延（10 μS未満）
- 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

スケーラブルかつシンプル

- ポイントツーポイント、ハブアンドスポーク、フルメッシュ
- サードパーティの管理ツールから完全に監査可能なアラームおよびイベントログ

フォーマンス

CN4010は、高パフォーマンスな暗号化装置です。ポイントツーポイント、ハブアンドスポーク、メッシュ環境において、全二重モードでパケットロスなしに10/100/1000 Mbpsのフルラインレートで動作します。FPGA（フィールドプログラマブルゲートアレイ）技術を採用したCN4010のカットスルーアーキテクチャは、データフレームを受信と同時に処理することで、すべてのパケットサイズで一貫した低遅延を実現し、パフォーマンスを最適化します。信頼性の高いアプライアンスとして、CN4010には次のような利点もあります。

スケーラビリティ

CN4010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あり、「Bump in the Wire」設計と最大1 Gbpsの可変速度ライセンスを提供し、設置が簡単で費用対効果に優れています。「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を設計の基本原則としており、実装、運用、管理が容易で、必要なリソースを最小限に抑えられます。デバイスは、メンテナンス、機能拡張、セキュリティアップデートのために、簡単にフィールドアップグレードが可能です。CN4010は、ユニキャスト、マルチキャスト、ブロードキャストドメインにも対応しています。

認定されたセキュリティ

耐タンパ性を備えたCN4010は、コモンクライテリアおよびFIPS 140-2 Level 3の認定を取得済みで、標準ベースのエンドツーエンド認証付き暗号化、自動鍵管理をサポートし、強力なAES 256ビットアルゴリズムを利用しています。アプライアンスを将来にわたって保証するために、暗号化装置は量子鍵配布にも対応しており、デバイス間の安全な通信を保証します。

最先端の鍵管理

CN4010は、外部鍵サーバーに頼る必要がありません。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耐タンパ性を備えたシャーシを提供します。物理的および仮想的な職務分掌により、権限のある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において安全に生成および保管され、物理的に鍵を抜き取ろうとする不正が試みられた場合、デバイスはゼロ化されます。

CN4010はハードウェアベースの乱数発生器をサポートしており、外部生成されたエントロピーを固有鍵の生成と配布に使用できます。将来を見据えて、暗号化装置は量子鍵配布（量子暗号）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

タレスネットワーク暗号化装置は、クリプトアジリティ（暗号の俊敏性）を備えており、幅広い楕円曲線やカスタム曲線に対応したカスタマイズ可能な暗号化をサポートしています。また、独自のエントロピー機能の持ち込みも可能です。クリプトアジャイルなプラットフォームは将来を見据えた設計であり、次世代アルゴリズムやカスタムアルゴリズムを迅速に展開できます。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）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、トランスポート非依存モード（TIM; Transport Independent Mode）を提供する業界初の製品であり、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）、プロトコルにとらわれない移動中データの暗号化を実現します。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。

CN4010暗号化装置の概要

モデル	CN4010
プロトコルと接続性	
最大速度	1 Gbps
ジャンボフレームのサポート	
プロトコルおよびアプリケーション透過性	
ユニキャスト、マルチキャスト、ブロードキャストトラフィックの暗号化	
自動ネットワーク検出と接続確立	
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	
柔軟な暗号化ポリシーエンジン	
AES-GCM暗号化によるパケット単位の機密性および完全性*	
自動鍵管理	
暗号化とポリシー	
AES 128または256ビット鍵	128/256
オプションでサードパーティによる量子鍵配布（QKD）をサポート	
CFB、CTR、GCM暗号化モード*	
MACアドレスまたはVLAN IDに基づくポリシー	
ネットワーク停止時に自己修復可能な鍵管理	
認定取得	
コモンクライテリア、FIPS	
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での暗号化	
FPGAベースのカットスルーアーキテクチャ	
遅延（マイクロ秒/暗号化装置あたり）	< 10μS
管理	
フロントパネルLEDディスプレイ通知	
SMCおよびCM7を使用した一元的な構成と管理	
外部認証局（X.509v3）のサポート	
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）	
NTP（タイムサーバー）のサポート	
CRLおよびOCSP（証明書）サーバーのサポート	
保守性と相互運用性	
現場でのファームウェアのアップグレード	
外部プラグパック	

* ファームウェアのリリース待ち
すべての仕様は発行時点のものであり、予告なく変更される場合があります。

仕様

暗号化

- AES 128または256ビット鍵 X.509証明書
- 公開鍵基盤（PKI）に完全準拠

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）
- または暗号化されたインターフェース経由（インバンド）
- SNMPv3リモート管理
- SNMPv2cトラップ
- SNMPv1読み取り専用モニタリング
- IPv4およびIPv6対応
- 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

設置

- 寸法:（幅Wx高さHx奥行D）—（W:180 mm/7.1”、D:126 mm/5.0”、H:32 mm/1.3”）
- 重量: 0.5 kg /1.1 lbs

インターフェース

- RJ45インターフェース
- RJ-45シリアルコンソール
- デュアルUSBポート
- RJ45 LAN/AUXコネクタ

電力要件

- DC入力9-15V DC、消費電力6W
- ACプラグパック100-240V AC、47-63Hz

物理セキュリティ

- アクティブ／パッシブタンパ検出および鍵消去
- 改ざん防止マーキング
- アンチプロービングバリア

規制

- UL Listed、EMC（エミッションとイミュニティ）
- FCC 47 CFRパート15（米国）
- EN 60950-1 (CE)、EN 55022 (CE)、EN 61000-3-2 (CE)、EN 61000-3-3 (CE)
- EN 55024 (CE)、EN 61000-3-3 (CE)、EN 55024 (CE)
- ICES-003（カナダ）、AS/NZS CISPR 22 (C-Tick)

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。

© Thales - April 2024 • EHv1