Tera-UTM 12

産業向け向けネットワークセキュリティフィルター

- 産業向けネットワークセキュリティ＋産業用制御システム：アンチウィルス、不正侵入防止、マルウェアサイト防止、Anti-Region、ファイアウォール、ICSプロトコル検査
- 安定性が良い：Hardware bypassの機能でTera-UTM 12がメンテナンス、ダウンタイム、停電でもネットワークが中断されない
- 簡単に設定できる、直感的なインターフェイス
- 業界が認定されたウイルス データベースでネットワークを最新の脅威やウイルスから保護する
- CMS を導入し、リモートで複数のTera-UTM 12を管理可能

機能

各状況に対応できる、産業向けインターネットセキュリティ技術

Tera-UTM 12は特許取得済みのディープ パケット インスペクション(DPI)技術を使用し、全般的なセキュリティ機能を開発した。アンチウィルス、不正侵入防止、マルウェアサイト防止、Anti-Region、ファイアウォールなど。これらの機能は、ウイルスを駆除、悪意あるコンテンツ、攻撃をブロックできる。

産業用制御システム（ICS）に対する保護

Tera-UTM 12は、ICSプロトコルで転送されたパケットを検査することができる、Modbus、DNP3など。ユーザーがそれぞれの要件に応じてルールを定義できる。産業用制御システムのセキュリティを向上させる。

SSL / TLSトラフィックの検査機能を強化

Tera-UTM 12は、SSL/TLSトラフィックの復号化、検査、再暗号化を行い、HTTPSウェブサイトの閲覧を完全に保護することができる。また、ユーザーはURL、IPアドレス、ウェブサイトのホワイトリストを設定し接続が暗号化された状態に保つこともできる。

ネットワークを最新の脅威やウイルスから保護する

最新のウイルスと脅威の防止するため、Tera-UTM 12は業界が認定されたウイルス データベースを使用して、定期にシグネチャーを更新、より安全なネットワーク環境を提供する。

CMS を導入し、リモートで管理可能

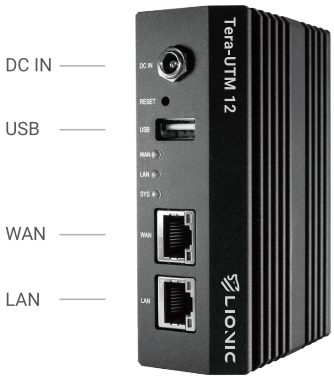
Tera-UTM 12はCMS を導入し、ネットワーク管理者がリモートで複数のTera-UTM 12を監視、管理することができる。

パフォーマンス

セキュリティ機能	
スループット(無効化)	*910 Mbps*
スループット(有効化)	*890 Mbps*
スループット(有効化+SSL/TLS スキャン)	*355 Mbps*
同時セッション数	*1000K*

無効化:すべての機能を無効化
有効化:アンチウィルス、不正侵入防止、マルウェアサイト防止

外観・各部名称



仕様

商品名	Tera-UTM 12
ハードウェア	Memory : 4G LPDDR4, 4000MT/s
	Flash : 8GB eMMC NAND Flash for O.S..
イーサネット	Chipset : 2 x AR8035-AL1A
	Speed : 2 x 10/100/1000 Mbps
	Support Hardware Bypass (Controlled By Cortex-M7)
インジケーターランプ	2 x Ethernet Active, 1 x Power Status (Green/Red 2color)
電源	7V~36V DC-in Lockbale
温度範囲　耐久性	Operation Temperature : 0-60°C
	Storage Temperature : -40~85°C 5%~95% Relative Humidity, non-condensing
寸法	108 W x 72 H x 38 D (mm)
認証	BSMI

機能リスト

セキュリティ

産業向けインターネットセキュリティ技術

- 一般的なプロトコルでのウイルス検出
  - FTP、HTTP、SAMBAなど
- ハイブリッド ウイルス スキャン
- ウイルスファイル破壊
- 実行ファイルのスキャン
- オフィスドキュメントのスキャン
- 圧縮ファイルのスキャン
- メールと添付ファイルのスキャン
- HTTPSでのSSL/TLSスキャン
- HTTPSでユーザー定義のホワイトリストをスキャン
- ランサムウェア検知機能の強化
- トロイの木馬検知機能の強化
- 1対多のウィルスシグネチャ
- クラウドウイルスデータベース
- サイバー攻撃ブロック
- 総当たり攻撃の検知
- ポートスキャンの検知
- DoS攻撃の検知
- プロトコル異常動作の検出
- SAMBAの不正侵入防止
- ボットネット攻撃検出
- 仮想パッチを即時更新
- 安全でないwebサイトにアクセスをブロック
- ドメイン名チェック
- URLチェック
- IPv4およびIPv6チェック
- 悪質・フィッシングサイトのクラウドデータベース
- セキュリティポリシーに応じたホワイトリスト設定
- TCP と UDP プロトコルの両方に対応ユーザー定義の ファイアウォール
- 許可/拒否するwebサイトリスト
- 検出した脅威の詳細情報リスト
- 脅威ログをエクスポート(CSV形式)
- 脅威ログをクラウドログサーバーにアップロード
- ICSプロトコルの異常検知
- ICSプロトコル用のユーザー定義ACL
- 脅威源分析、ジオブロッキング

ネットワーク

シームレス的に現有のネットワークトポロジーを維持可能

- ブリッジモード（初期値）で直観的にインストール可能
- ルーターモードのDHCPサーバーとポート転送
- モバイル端末保護用VPNサーバー
- Lionicクラウドサービスにアクセスするためのユーザー定義プロキシサーバー設定

監視＆コントロール

ネットワークを最新の脅威やウイルスから保護する

- 直観的なユーザーインターフェース
- DDNS でリモート アクセス
- リモート管理者へのアクセス権設定
- 暗号化された接続で安全なアクセスを実現
- VPNサーバーへのアクセスに2要素認証
- 検査済みトラフィックの概要
- 検出した脅威の統計情報
- システムリソースを監視
- システムユーザーのアクティビティ
- 再起動のスケジューリング
- ファームウェアとシグネチャの自動更新
- ユーザー定義によるシスログサーバーを設定、詳細なシステム状態を収集
- カスタマイズNTPサーバー設定
- 脅威検知通知メール
- ネットワーク診断ツール

- セキュリティ ポリシーとシステム設定のバックアップ/復元
- Lionic クラウド サービスのライセンス管理
- 日報／週報の自動生成
- システム負荷の自己診断
- ネットワークセキュリティのリスク評価
- ネットワーク診断ツール
- システムログのエクスポート
- ネットワークトラフィック分析

Central Management System 中央管理システム

CMS を導入しリモートでシステムを管理

- 動作状況のサマリーをビジュアル化
- ダッシュボードで防御の状態が見える
- リモートでTera-UTM 12を設定できる
- Tera-UTM 12のセキュリティポリシーを作成、応用する
- 脅威ログをエクスポート(CSV形式)
- シグネチャの更新
- リモートでファームウェアを更新
- 脅威検知通知メール
- システム ユーザーのアクティビティ履歴
- システムユーザの権限管理

Tera-UTM 12で
安全なネットワーク環境を実現しよう

LIONIC
Security Solution Provider

連絡窓口
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com

Lionic Corp.
https://www.lionic.com/
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.