Pico-UTM 100

小規模オフィス、スタジオ、家庭用に最適なインターネット フィルター

特徴

- 企業向けインターネットセキュリティ技術: ウイルス対策、侵入検知、インターネットセキュリティ、ファイアウォール
- 3分で設定完了、現有のネットワークトポロジーを維持可能
- 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Pico-UTM100を管理可能

機能

各状況に対応できる、企業向けインターネットセキュリティ技術

Pico-UTM100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。ウイルス対策、侵入検知、インターネットセキュリティ、ファイアウォールなどの企業のネットワークを守れる。

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

3分でブリッジモードを設定完了、Pico-UTM 100はWANポート1つとLANポート1つを配置、簡単に設定できる。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。

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、Pico-UTM 100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

Pico-UTM 100はCMS を導入し、ネットワーク管理者がリモートで複数のPico-UTM 100を監視、管理することができる。

* データベースを更新するにはライセンスまたはサブスクリプションが必要

パフォーマンス

セキュリティ機能	
スループット (無効化)	*833 Mbps*
スループット (有効化)	*700 Mbps*
同時セッション数	*30K*

試験用ソフトウェア: IXIA IxLoad HTTP Download 1MB.exe
附註: テスト結果はテスト環境およびデバイスによって異なる場合がある

外観・各部名称

仕様

商品名	Pico-UTM 100
ハードウェア	RAM : 256MB
	Flash : 512MB
インターフェース	Gigabit Ethernet WAN x 1 Port, Gigabit Ethernet LAN x 1 Port
電源	Universal Switching Power Adapter 100-240V AC IN, 12V DC
温度範囲	Operating Temperature : 0-40°C (32-104°F)
耐久性	MTBF (hrs) : 2,041,392
寸法	116 W x 25 H x 91 D (mm)
質量	135g

機能リスト

セキュリティ

企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（テスト版）
- 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の侵入検知
- 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

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サーバーとポートフォワーディング
- 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
- 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
- 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
- システムログのエクスポート

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Pico-UTMを設定できる
- Pico-UTM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

Pico-UTM 100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
https://www.pico-utm.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.