SUNYAINFO

上元信安次世代ファイアウォール

SUNYAINFO NEXT GENERATION FIREWALL

デジタル時代のセキュリティを速やかに構築

ランサムウェアやゼロデイ攻撃、APT 攻撃などが次々と登場し、世界サイバーセキュリティ情勢は日々厳しくなります。各業界はデジタル化への転換を加速し、モバイル・インターネット、クラウドとネットワークの融合が常態化しています。従来の境界セキュリティ対策は、ネットワーク境界の曖昧化、ハッカー攻撃の産業化、攻撃対象領域の拡大化とともに、ますます力不足になっています。
上元信安次世代ファイアウォールは、ゼロトラスト・セキュリティモデル（Zero Trust Model）を元に、コアデジタルアセットとデータを防御することを旨とし、信頼の境界を再定義しています。上元信安次世代ファイアウォールは、豊富なアイデンティティ認証方式を融合し、応用・内容・アセットなどに基づく多次元精密管理を実現し、各種 DoS/DDoS 攻撃、ブルートフォース攻撃、弱いパスワード、脆弱性悪用、ウイルス、トロイ木馬などのネットワーク脅威を全面的に防御できます。
従業員がどこからアクセスしても、イントラネットリソースへのアクセスとセキュリティを確保することができます。企業、教育、金融などのユーザーにコスパが高く、効率的で一体化したセキュリティ防護体験を提供されます。

製品の特徴

アセット識別

トラフィックの自動学習と主動的スキャンの機能により、イントラネット上のアセットを検出し、アセットの所属部門や重要度などの属性よりユーザーの統合アセット管理を支援します。

ゼロトラスト管理

ローカル認証、Radius 認証、WeChat 認証、訪問者審査認証などさまざまなアイデンティティ管理方式をサポートし、インターネットにてリモートアクセスするユーザーもローカルユーザーも、そのアクセスに対してアイデンティティに基づくアセット権限管理を行うことができ、ライトゼロトラスト境界ソリューションを速やかに構築できます。

セキュリティ統合化

ユーザーとアプリケーションの統合セキュリティエンジン SAAE に基づき、パケットの単回解析され、侵入検知、ウイルス検知、Web セキュリティ分類及びコンテンツフィルタリングなどのセキュリティ機能を並行して実行され、全面的にネットワーク脅威を防御できます。

連携防御

脅威情報、サンドボックス、EDR などの連携防御ソリューションをサポートし、既知脅威と未知脅威を効果的に防御し、立体化なセキュリティ防御システムを構築されます。

暗号化トラフィック検出

暗号化トラフィックの解析、トラフィック内のアプリケーションの特定、従業員の HTTPS サイト訪問行動の監査、および暗号化トラフィック内の攻撃検知ができます。

IPv6 ネットワーク対応

IPv4/IPv6 ネットワークを対応し、完全な IPv4 over IPv6、NAT46、NAT64 などの移行技術を備え、かつ IPv6 ネットワークの侵入防御、ウイルス防御、URL フィルタリングなどのセキュリティ防御機能をサポートします。

セキュリティ可視化

ユーザー、場所、アセットに基づくセキュリティ分析（攻撃分類、リスク状況など）、攻撃チェーンとアセット攻撃段階の表示、脅威証拠の収集をサポートします。

スマート運用・保守

ポリシー分析機能（冗長ポリシー、非表示ポリシー、競合ポリシー、期限切れポリシーなどのワンクリック検出）をサポートし、ポリシーの最適化提案を提供することができます。SD-WAN コントローラー、ネットワーク管理プラットフォームとのドッキングをサポートし、集中的ステータス監視、ポリシーの知能作成・配布、一括メンテナンスなどのスマート運用・保守管理が実現できます。

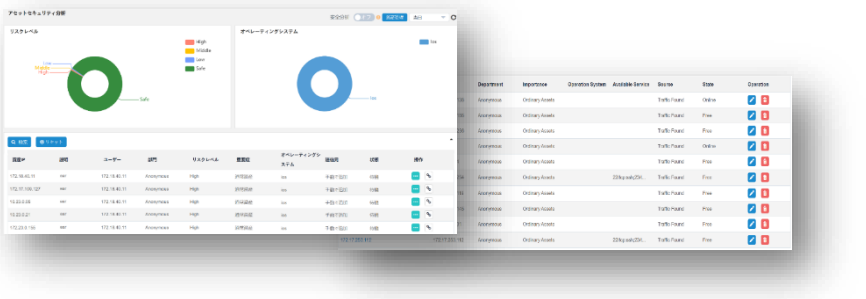
製品ハイライト

全方位防御システム

上元信安次世代ファイアウォールは、ユーザーが「事前、事中、事後」の全方位セキュリティ防御システムを構築することができ、従来の受動的応答から事前リスク監視、事中防御応答、事後証拠収集分析のクローズドループに転換し、ユーザーに全面的なセキュリティ防御が提供できます。

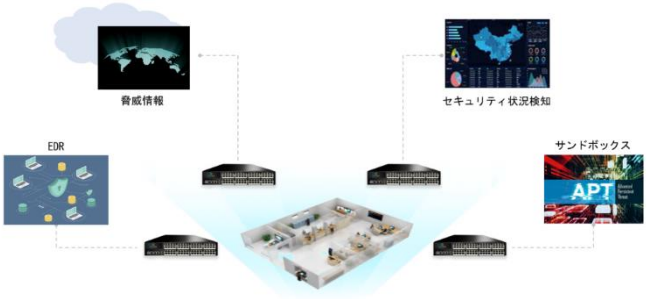
アセットリスク特定

上元信安次世代ファイアウォールは、主動的スキャンとホストトラフィック監視により、ネット中のアセット情報を識別します。アセットの視点から各種のセキュリティイベントに対して関連分析と統計を行うことによって、管理者がリスクホストを特定して、関連する脅威イベントに基づいて精確な防御を行います。



効率的な連携

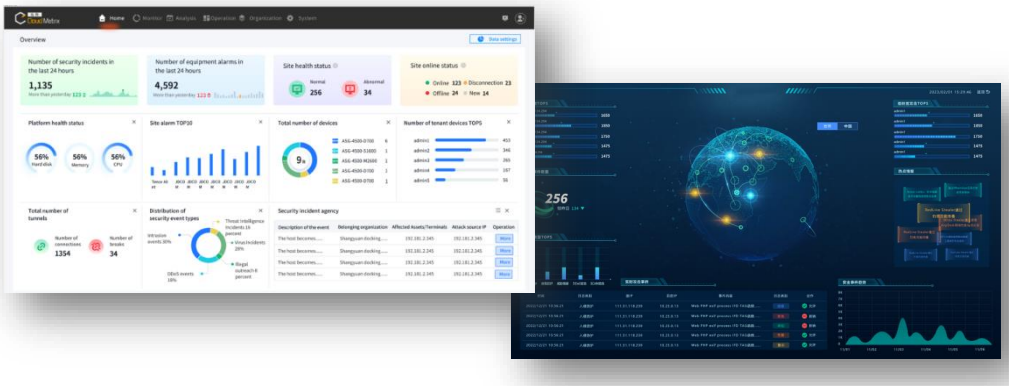
従来の次世代ファイアウォールは、「セキュリティライブラリ」に依存しており、受動的防御が多く、外部から高度な脅威を識別できず、すでにネットワークセキュリティの挑戦に応ずることができなくなります。上元信安の次世代ファイアウォールは、従来の次世代ファイアウォールと比べ、効率的な連携能力を備え、様々な外部セキュリティシステムと連携することで、ファイアウォールのセキュリティ防御能力を高める同時に、管理者による精密な運営・管理が実現できます。



スマート保守

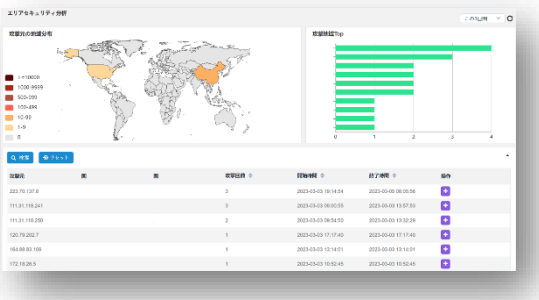
上元信安次世代ファイアウォールは、家庭用ルータークラスの簡単なオンライン設定能力（プラグアンドプレイ）を提供されす。ZTP ゼロタッチ構成により、ネットワーク管理者が自宅で支社デバイスの管理と保守を完了でき、保守期間を数日から数分間に短縮できます。

同時に、クラウドプラットフォームよりネットワークデバイス全体を統括設定・運用・保守を行い、地図などの可視化インタフェースとレポートに基づき、ネットワークとデバイスの状態をグラフ化で提示し、ネットワーク運用・保守担当者の操作体験と作業効率を高め、運用・保守の難易度を下げます。



セキュリティ可視化

上元信安次世代ファイアウォールは、地理的・アセット的視点からサイバーセキュリティ分析を行い、攻撃検知とデータディープ検知に基づき、多角度から可視化分析・提示を行い、様々な形式のグラフ展示よりネットワーク状況をわかりやすく、ネットワークセキュリティを「見極め」され、より精確なセキュリティ対策と防護強化を行うことができます。

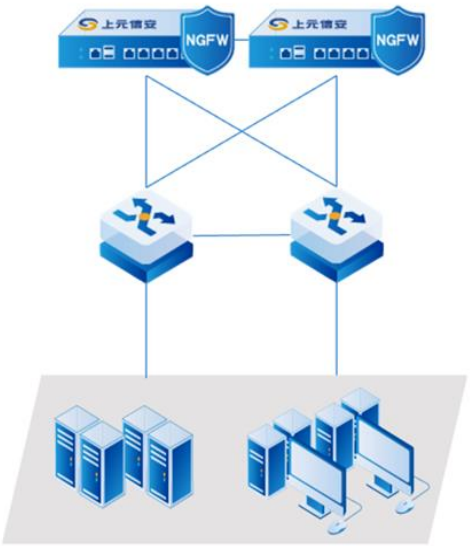


地域セキュリティ分析

攻撃チェーン解析

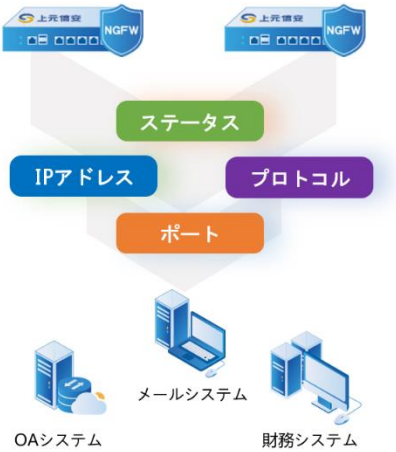
使用シーン

境界セキュリティ防御シーン



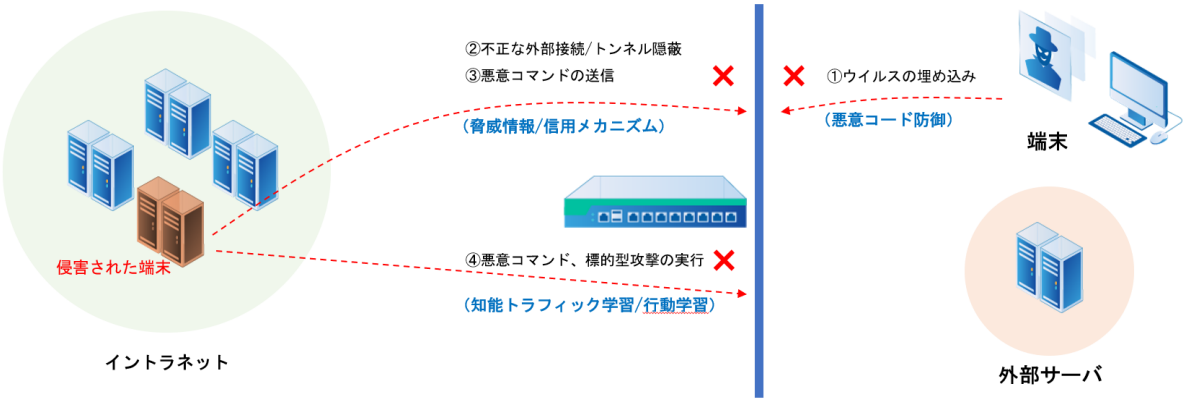
- **アクセス制御**：多ユニット精密化の管理隔離で、リスク拡散を防止されます。また、スマートポリシー分析エンジンを提供することより、管理者のポリシー管理に最適化案を提出され、保守効率を高めることができます。
- **アセット管理**：イントラネットアセット状況の自動識別、アセット属性及び重要度の自動定義により、セキュリティポリシーの迅速引用、セキュリティリスクの迅速特定を容易にします。
- **セキュリティ防御**：DDoS、侵入防御(IPS)、アンチウイルス、URL フィルタリングなどのセキュリティ機能を提供し、イントラネットセキュリティを効果的に防御できます。
- **クラウド端末連携**：脅威情報、サンドボックス、EDR などの連携防御ソリューションを提供し、既知脅威と未知脅威を効果的に防御でき、立体化セキュリティ防御システムを構築できます。
- **セキュリティ可視化**：多角度から可視化データ分析を行い、さまざまな形式のグラフ展示により、ネット状況を見やすくされ、サイバーセキュリティを「見極める」ことができます。

アセットセキュリティ管理シーン



- **アセット検知**：イントラネットアセット状況の自動識別、アセット属性及び重要度の自動定義により、セキュリティポリシーの迅速引用、セキュリティリスクの迅速特定を容易にされます。
- **リスクスキャン**:イントラネットアセットのオープンポート、弱いパスワードなどのセキュリティリスクを識別し、ユーザーによる効果的なセキュリティリスク監視と予知されます。
- **攻撃プロファイリング**：アセットを視点とし、攻撃と防御の論理に従って、攻撃者をスキャン、侵入、暴露、漏洩などの角度に分け、攻撃チェーンを構成することで、アセットの侵入経路と侵入程度を明確に把握し、セキュリティイベントのレビューと遡源分析を容易に行います。
- **セキュリティ可視化**：多角度から可視化データ分析を行い、さまざまな形式のグラフ展示により、ネット状況を明確にし、サイバーセキュリティを「見極める」ことができます。
- **アセットプロファイリング**：アセットの視点から、各アセットのリスクレベルと防護状況などのセキュリティ情報を表示できます。攻撃イベントに基づきアセットの被撃傾向、攻撃の種類と比率などの状況を分析・統計されます。

ランサム・マイニング防御シーン



- **アクセス制御**：多ユニット精密化の管理隔離で、リスク拡散を避けます。また、スマートポリシー分析エンジンを提供し、管理者のポリシー管理に最適化案を提出され、保守効率を高めることができます。
- **ポートスキャン**:イントラネットサーバ、業務システムなどのポート開放状況を識別し、135、139、445などのリスクポートを速やかに検知し、マルウェアによる拡散と侵入を防御するために、事前監視とブロックできます。
- **セキュリティ防御**：侵入防御、アンチウイルス対策、悪意 URL フィルタリング、脅威情報検出などの機能を提供され、ゾンビ、トロイ木馬、ウイルス、悪意コードの侵入などのセキュリティリスクを効果的に遮断されます。
- **外部接続の検出**：サーバによる主動的な外部接続行動を検出することで、外部接続行動を早期に発見され、リアルタイムでブロックすることができます。
- **セキュリティ可視化**：多角度から可視化データ分析を行い、さまざまな形式のグラフ展示により、ネット状況を明確にし、サイバーセキュリティを「見極める」ことができます。

機能特徴

ネットワーク

対応可能：物理インタフェース、ブリッジインタフェース、VLAN、トンネルインタフェース、
ループバックインタフェース、統合インタフェース
静的ルーティング、動的ルーティング（RIP、OSPF、BGP）、ポリシールーティング、
ISP ルーティング、アプリケーションルーティング
送信元 NAT、宛先 NAT、静的 NAT、透過 NAT、ALG
透過配置、ルーティング配置、バイパス配置、ハイブリッド配置、仮想回線の 5 種類の運用モード
インタフェース静的 IP、DHCP クライアント、PPPoE クライアント設定
DHCP サーバ、DHCP リレー
DNS サーバ、DNS プロキシ

IPv6

対応可能：IPv4/IPv6 デュアル・スタック、NAT66 の、アドレス変換
NAT64 と NAT46 のクロスプロトコル変換
IPv6 ルーティング、IPv6 トンネリング技術

IPv6 侵入防御、ウイルス対策、URL、アプリケーション識別、DDOS 対策
IPv6 トラフィック管理と監査、セッション管理、ブラックリスト、弱いパスワードスキャン、および
ポートスキャン
IPv6 ユーザーの識別と認証、IP アドレスおよび MAC のバインド

VPN

対応可能：IPsec VPN と SSL VPN
キーの事前共有、証明書認証、IPsec VPN マルチインスタンス、SSL VPN プロトコル
暗号化と認証、SSL VPN ユーザーバインド、VPN 多要素認証
Windows 32/64 の VPN クライアント、Android、IOS
ポータルページのポート、タイトル、ロゴ、およびアナウンス内容カスタマイズ

アプリケーション

対応可能：アプリケーション識別、アプリケーション行動識別、デスクトップ、Web、モバイルアプリ識別
アプリケーション、アプリケーションシグネチャーDB の定期的更新、アプリケーション行動監査、
HTTPS 監査、URL 監査のカスタマイズ、Web ページキーワード、ファイル種類、WEB アクセス制御

侵入検知防御

対応可能：侵入検知技術、IP 断片再構築、TCP ストリーム再構築などの攻撃識別
内から外へ、外から内への侵入防御ポリシー
イベントシグネチャーDB 5000+（手動、自動、定期アップデート）
IPS カスタマイズ・ルール、プロトコル分析、SQL インジェクション検出、
バッファリングオーバーフロー、セキュリティ脆弱性対策
ポートセキュリティスキャン、ワーム防御対策、ネットワークデータベース攻撃、GGI 攻撃、
IPS アラート

ウイルス防御

ウイルス検知技術、200 万以上のウイルスライブラリ、定期的なサービス更新、カスタマイズウイルス署名
ファイル形式のスキャンと悪意 Web サイトの監視、ウイルスホワイトリストの設定

行動管理

対応可能：Web サイトアクセス管理、URL の分類、キーワード、ファイル転送行動から WEB アクセスを管理
されます。
メール送受信にセキュア管理を行い、アカウント、内容、添付ファイルなどの角度から検査・分析を行い、
重要情報の流出や外部リスクの侵入を防止することができます。
オンラインリアルタイム更新の URL DB、URL 種類のカスタマイズ、千万単位の URL シグネチャーDB を提供
されます。

スマート通信制御

対応可能：4 レベルの内蔵アプリケーションの通信制御、総帯域幅管理
優先度チャネル設定、通信制御ポリシー、オンデマンド帯域幅、アプリケーション速度制限、
通信制御ホワイトリスト

追加セキュリティ機能

対応可能：ポートスキャン、弱いパスワードスキャン、サーバ外部接続管理、
ブルートフォース攻撃防御

ユーザー管理

ユーザーの自動識別、多種類認証方法
静的バインド、ローカル認証、WEB 認証、Portal 認証
他の認証方法：SMS 認証、訪問者 QR コード認証、ハイブリッド認証、
AD ドメインシングルサインオン、認証不要
ユーザー監視、ユーザー通信量制限、ユーザーのブルートフォース攻撃防御

連携

対応可能：クラウド脅威情報、20 種類以上の脅威分類
最近のホットセキュリティイベントの検索、脅威検知
第三者 EDR との連携へのユーザーアクセス
EDR 連動ポリシーの設定とファイアウォールへの EDR アセットの同期
ホストサンドボックスとクラウドサンドボックスの連動、不審なファイルやホストの行動分析
IDS デバイス連携、侵入セキュリティイベント遮断

高可用性

主主と主備モードのサポート、予備機管理、インタフェース連携
標準の VRRP、HA 切り替え、HA 同期、HA 監視

システム保守

対応可能：https/http、SSH、telent、console 管理
三権分立、管理者の一意性確認、ページのタイムアウト設定、オンライン管理者の人数設定、
パスワード有効期限の設定
デュアルシステムバックアップ、統括管理プラットフォームとの連携による遠隔保守管理、
設定バックアップ
冗長ポリシー、競合ポリシー、期限切れポリシー、空白ポリシーなどを検出するポリシー分析
WEB グラフィックの診断ツール、ping/trace/token ツール、パケットキャプチャツール、
システム情報アラート

ログと監視

対応可能：ログのローカル保存と外部送信、ログ検索、エクスポート、および消去
システムログ、アプリケーション制御ログ、監査ログ、セキュリティログ、侵入ログ、ウイルスログ、
脅威情報ログ
ログエクスポート、ログ設定、ヘルス統計、セキュリティレポートの生成およびエクスポート

型番仕様

ASG-4500-D700 デスクトップ型

千ギガビット電気ポート x5

コンボポート x1

CON ポート x1

USB ポート x1

項目	ASG-4500-D700
スループット	2Gbps
グッドプット	1.4Gbps
最大同時接続数	300,000
1 秒あたりの新規接続数	10,000
IPSec トンネル数	400
IPSec スループット	280Mbps
電源仕様	外付 AC、18W
電源	110～240V
外形寸法（W×D×H、mm）	240mm ×182mm ×28mm
重さ	1.24KG
動作環境温度	0-40℃
動作環境湿度	5-85%（結露なし）

北京上元信安技術有限公司
Beijing Sunyainfo Technology Co.,Ltd.
電話番号： +86 010-6298-1164
+86 400-067-0050
住所：北京市海淀区上地金隅嘉華ビル E 館
Web サイト： www.sunyainfo.com