ESG Lab Review

訳：株式会社テリロジー

Identity-Defined Networking from Tempered Networks

Date: July 2017 **Author:** Kerry Dolan and Tony Palmer, Senior Validation Analysts

はじめに

ESG ラボレポートは、Tempered Networks IDN（Identity-Defined Networking）ソリューションの実証テストレポートを紹介します。

ここでは、Tempered Networks の“**ID ファースト**”のアプローチで、ネットワーク環境とかロケーション（利用する場所）に関わらず、プライベートネットワーク、セグメント化、そしてどのようにセキュアな通信を構築するかといったところに重点を置いて実証テストを実施しました。

課題

ネットワークセキュリティの重要課題は、IP ベースのネットワークアドレスのしくみです。IP アドレスは基本的にインターネット通信の ICT 世界を進展させましたが、デバイスのロケーションを特定し、信頼性の高い自由な接続性のみを可能にするために設計されました。IP ベースのネットワークアドレスのしくみは ID（デバイスの識別子）でセッション認証をしたり、セキュリティを担保するために設計されたものではありません。その結果、企業の IT 部門は無制限のハッキングやサイバー攻撃に対して、ファイアウォール、VPN、ルーティングポリシー、ACL（Access Control List）、VLAN などの複雑なしくみを組み合わせてアクセスネットワークでのセキュリティを確保する必要がありました。ESG ラボの調査では、ネットワークとエンドポイントのサイバーセキュリティ対策が最優先だと報告しています（図 1 参照）。

ESG ラボでは、サイバーセキュリティの具体的な設備投資計画について調査を実施しました。「企業ユーザにとって次の 12-18 ヶ月間における最も重要な投資領域は次のうちどれだと思いますか？」というアンケート調査を行いました　（回答者：N = 418）。

その結果を以下に示します。

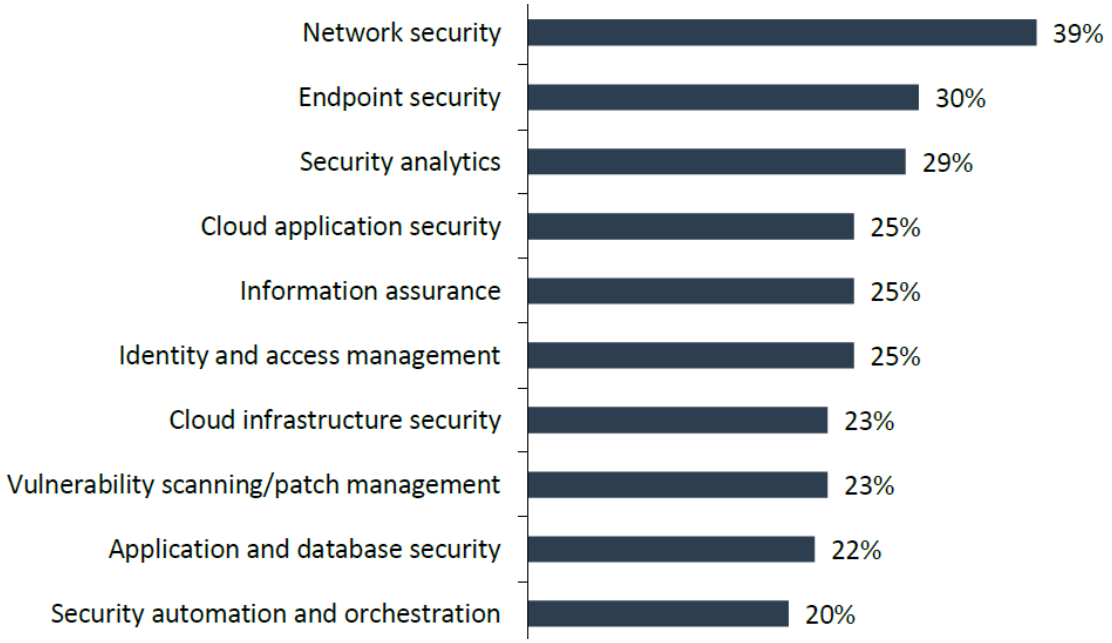


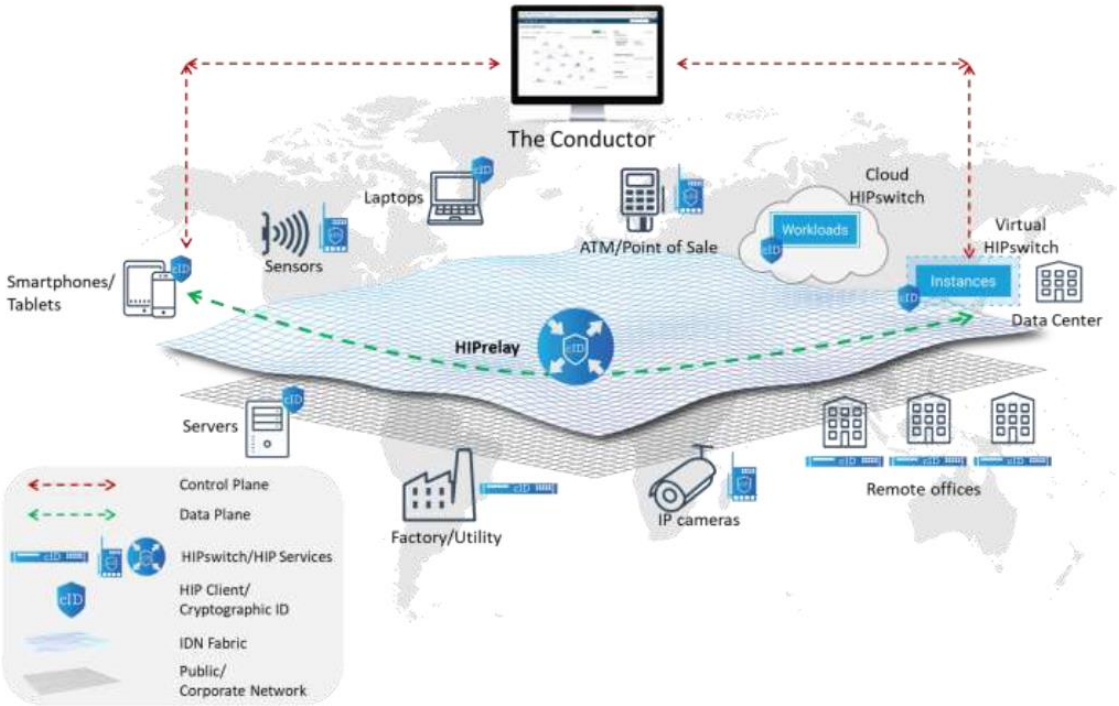
図 1. 2017 年トップ 10 のサイバーセキュリティ対策

ソリューション: Tempered Networks の Identity-Defined Networks

Tempered Networks は、サーバ、ラップトップ、携帯/スマホ、IP カメラ、ATM、各種 M2M センサーおよびその他 IoT デバイスを含むネットワーク接続デバイスのホスト ID を用いた認証可能なネットワークアーキテクチャを提供します。各エンドポイントデバイスは セキュリティを担保するために暗号化 ID で設定されています。これらデバイスがホワイトリストに登録され、相互のデバイス間で認証されると、これらデバイス同士で安全な暗号化通信トンネルが設定されます。これによってこれらデバイスは信頼され他から完全に隠蔽されるため、既存 IP ネットワークから偵察スキャンされることはありません。そして、ハッカーはこれら隠蔽されたデバイスを認識できないので、ハッキングされることはありません。

Tempered Networks ソリューションには、イーサネット、セルラー（LTE）、ワイヤレス（Wi-Fi）、高周波（Radio Frequency）、およびシリアルオーバーIP ネットワークが含まれ、運用中断なく展開できます。Tempered Networks は、更にインストールのし易さと管理の容易さによるコスト効率アップにも貢献しています。

図２．Tempered Networks IDN



Host Identity Protocol (HIP)

Tempered Networks ソリューションは、IETF（インターネット技術仕様標準化団体）によって 2015 年に承認された Host Identity Protocol（HIP）に準拠しています。HIP は、大手航空機製造メーカの生産現場で 10 年以上稼働しており、また数多くの一般企業、連邦政府機関および防衛関係でも採用されています。その後 HIP ベースの技術は Tempered Networks によって商品化されました。HIP は、デバイスの識別子（ID）とロケータを包含した従来の IP アドレスの役割を完全に分離させ、相互通信のデバイス認証に公開鍵識別子（PKI）ベースのホスト ID を用います。ミリタリーレベルの暗号化と PKI を採用しているため、DDoS 攻撃や中間者攻撃（Man-in-the-Middle）には堅牢となっています。

主要なコンポーネント構成

Tempered Networks ソリューションは 2 つの主コンポーネントで構成されています：

- **Conductor**—物理環境または仮想アプライアンス（AWS クラウド上でも利用可能）対応の Conductor は、HIP サービスリソースをグローバルに接続し、保護するだけでなく HIP モードを必要に応じて ON/OFF する機能を備えたオーケストレーションエンジンです。Conductor を通過するデータトラフィックはありません。Conductor はセキュリティポリシーを設定し、HIP サービスリソースにエンフォースします。ネットワ

ーク上に配備された HIP サービスリソースは、自動的にコンダクタに登録されます。

- **HIP サービス**—IDN（Identity Defined Network）で保護されたデバイス間の安全な接続、クローク（隠蔽）、セグメンテーション、ID ベースルーティング、IP モビリティといった機能を実現します。
  - HIP サービスは、ラップトップやサーバ用の HIP ソフトウェアとして提供されます。また、物理アプライアンスの HIPswitch、VMware ESXi および Microsoft Hyper-V による仮想 HIPswitch も用意されています。HIP サービスをカスタムハードウェアに組み込むことも可能です。
  - HIPswitch を設置してエンドデバイスを接続すると、エンドデバイスは HIP 対応モードになり、マイクロセグメント化され、既存 IP ネットワークから完全にネットワーク分離されます。
  - HIP リレーは、HIPswitch モデル（HIPswitch400/v300）のアドオン製品です。
    - HIP リレーは、Tempered Networks の HIP エンドポイントソフトと連携して、ルーティングが難しい分散ホストまたはシステム間の通信を任意の場所から暗号通信で ID ベースルーティングを実現する暗号中継装置（ブリッジ）となります。
    - HIP リレーは、レイヤ 3 およびレイヤ 4 で対応する従来のルーティングプロトコルを使用しません。その代わりに、暗号化されたトラフィックを既存のインフラを通過させるために認証可能な暗号 ID ベースでルーティング接続します（ここでは終端したり、復号化したりしません）。
    - HIP リレーは、オンプレミスであろうとパブリッククラウドであろうと、HIP リレーをクラスターブリッジの中継としてインターネット上に分散させることも出来ます。

IDN は、SDN とか SD-WAN ソリューションとは異なり、既存ネットワークのインフラ環境を変更することなく、レイヤ 2 およびレイヤ 3 のネットワークをシームレスに統合します。

Tempered Networks ソリューションは、世界中に配置されたデバイスに対して、スケーラブルにオーバーレイネットワークを構築し、デバイスのセキュリティ保護を提供し、攻撃の危険性と脅威のリスクを即座に低減します。そして、きわめて簡単な導入操作と運用管理のし易さを実現し、セキュリティサービスの迅速なプロビジョニングを可能にします。

<ESG ラボ テスト結果>

ESG ラボは、スイッチ、ルータ、およびその他ネットワークデバイスを使用してテスト環境を構築しました。

標準イーサネットを介して、Windows OS のサーバ、ワークステーションおよび Mac リソースといった複数の異機種システムを接続したテスト環境を準備しました。物理環境、仮想環境、およびクラウドベースの HIP スイッチを使用しました。これらのテストでは、様々なリモートアクセスクライアント、オンプレミス、リモートサイトそしてクラウドベースのワークロードに関する IDN ファブリックパフォーマンス機能を実証するため、利用可能なすべての HIP サービスソフトを準備しました。

ID ベースのマイクロセグメント化によるハッカー阻止

ESG ラボでは、最初に ID ベースのターゲットサーバをマイクロセグメント化し、外部ハッカーの偵察スキャンをどのように阻止できるかをテストしました。図 3 に示すように、2 台の Windows サーバをオープンな共有ネットワークセグメントにインストールし、もう 1 台のサーバで Active Directory を動かしました。ESG ラボでは、1 台のサーバにリモートログインし、ネットワークデスカバリーとセキュリティ監査用の nMap（オープンソースユーティリティ）をインストールして、別のサーバに接続しました。nMap を用いて、Tempered Networks IDN プラットフォームの導入前と導入後で Windows サーバをチェック。このテストは、内部ネットワークに侵入したハッカーおよびその侵入痕跡を検出できないかどうかをシミュレーションするように設計されています。ハッカーは、内部ネットワークの無作為なスキャンを実行して、価値の高いターゲットサーバを識別することで、秘密の偵察スキャンを行います。

図 3．ESG ラボのテストベッド

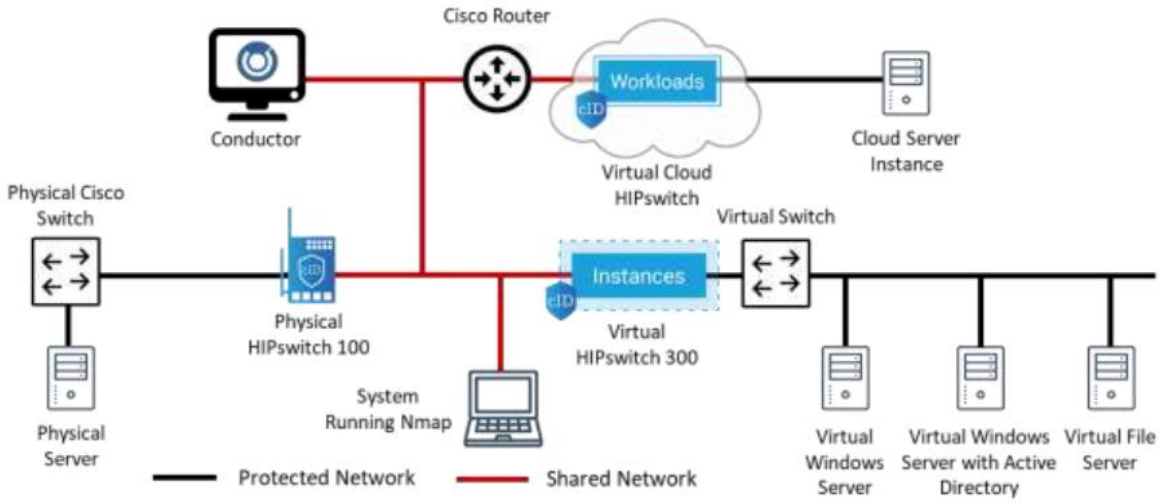


図 4 に示すように、ハッカーは Active Directory を実行する Windows サーバのポートすべてを 5 秒以下で偵察スキャンして認識しました。これによって、ハッカーが Active Directory 実行サーバを標的攻撃対象にして簡単に侵入出来たことがわかりました。

図 4．オープンの共有サブネット上の nMap 結果

```
$ nmap -Pn 10.11.1.120

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-05 10:03 PDT
Nmap scan report for 10.11.1.120
Host is up (0.011s latency).
Not shown: 982 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open http
88/tcp    open kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
443/tcp   open  https
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open ldapssl
3268/tcp open globalcatLDAP
3269/tcp open  globalcatLDAPssl
3389/tcp open  ms-wbt-server
49154/tcp open  unknown
49155/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.55 seconds
```

次に、ESG ラボでは、Active Directory をインストールした Windows サーバを信頼できる HIP 環境のマイクロセグメント領域に移動しました。nMap を再び実行しましたが、nMap はリスニングポートを検出できませんでした。マイクロセグメント化されたシステムは完璧に覆い隠され、ハッカーには見えなかったためです。

図 5 .サーバが Trusted Micro-segment に追加された後の nMap 結果

```
$ nmap -Pn 10.11.1.120

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-05 09:49 PDT
Nmap scan report for 10.11.1.120
Host is up.
All 1000 scanned ports on 10.11.1.120 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.78 seconds
```

ルーティング不可能なデバイス間の通信

次は、ルーティング不可能なデバイス間の通信による 2 つのシナリオを評価するテスト環

境です。図 6 に示すテスト環境は、IoT アプリケーションをエミュレートしたものです。ユーティリティ事業者（電力関係）が、各拠点の現場サイトに設置されたセンサーを利用可能な携帯電話サービスを利用してインターネット接続するというケースです。このテストケースでは、コーポレイト側での監視および分析作業のために、すべてのセンサーロケーションとの双方向通信が必要でした。そして、これらのセンサーロケーション間での通信も必要でした。

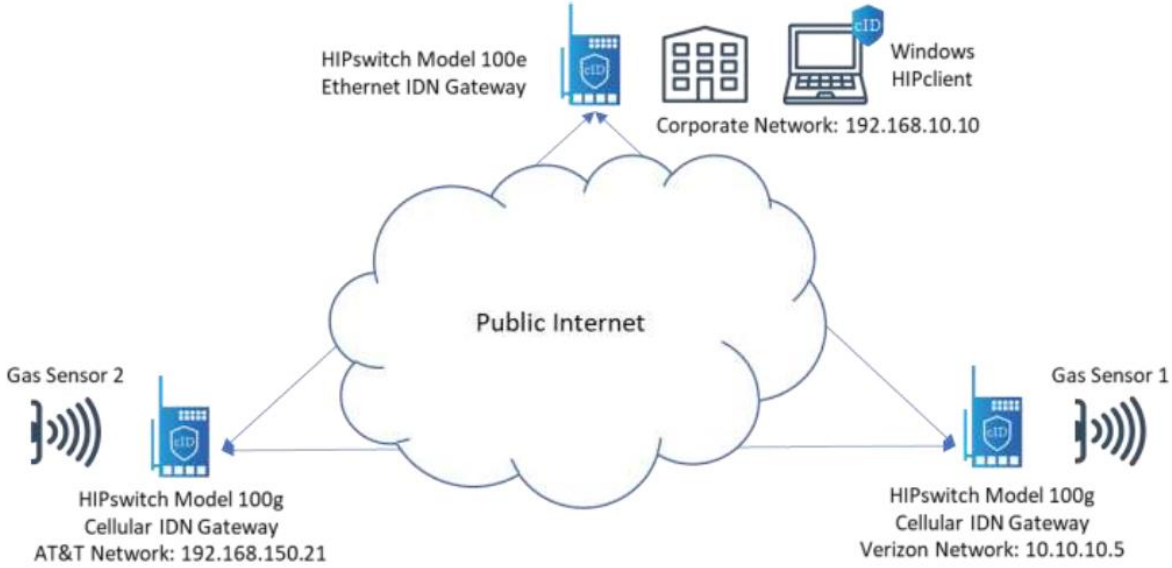


図６．２つの異なるセルラーネットワーク間のルーティング

HIPswitch モデル 100g セルラー用 IDN ゲートウェイを使用して、ESG ラボはセンサーとコーポレイトネットワークの Windows システムとの間の信頼関係を短時間で作成しました。すべてのデバイスは、既存の IP ネットワークを再構成することなく、双方向に通信することが出来ました。

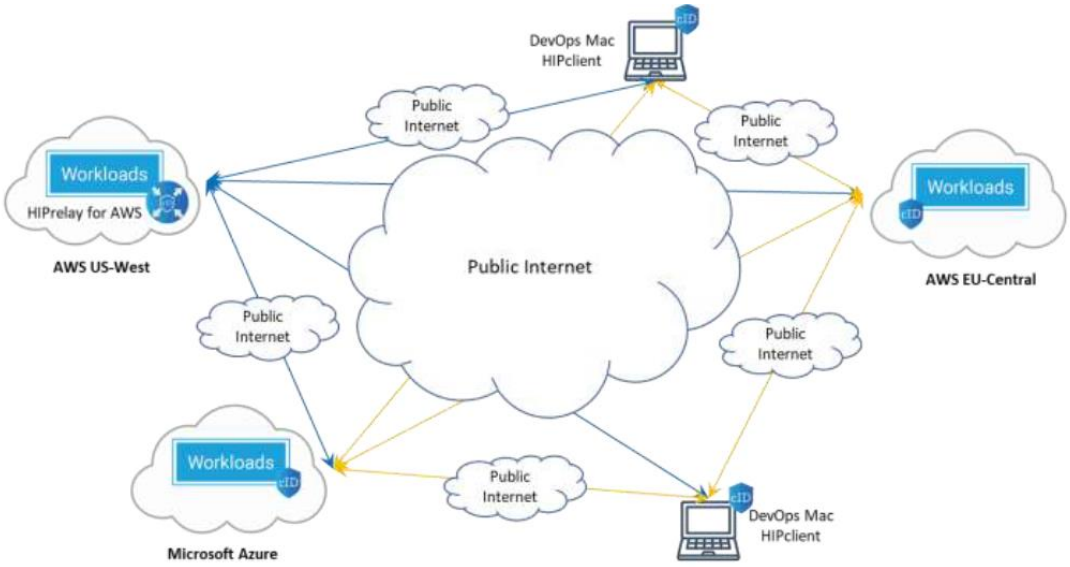


図 7． DevOps のマルチクラウドピアリング

図 7 に示すように、Tempered Networks の HIP リレーと HIPswitch によって ESG ラボでマルチリージョンとマルチクラウドのペアリング構成を構築出来ました。DevOps のリソースは、Amazon 欧州中央部と米国西部の間、および Amazon 米国西部と Microsoft Azure の間で共有されました。

何故これが重要なのか？

今日のあらゆる組織においてセキュリティ対策は最優先事項です。ニュースを見ても、多くの脅威が台頭していることは周知の事実です。しかし、様々なネットワークを利用するビジネスでは、複雑なセキュリティ環境やプロセス工程によって脆弱性の悪化を引き起こします。最近のビジネスでは、多くの場所で色々なデバイスをネットワーク接続する必要があるために、セキュリティ対策は必須です。そのため、これらデバイスの接続を安全にすることは最も重要なのです。

Tempered Networks ソリューションは、暗号ホスト ID を使用して、従来の IP ネットワークを超えたセキュリティを強化します。 ESG ラボでは、他のネットワークトラフィックから隔離された安全で暗号化された通信チャネルを迅速かつ簡単に構築できる Tempered Networks の能力を検証しました。ESG ラボは、ルーティング不可能なデバイス間の安全な通信と、さまざまなクラウドとプロバイダとの間でのセキュアなピアリングも確認しました。

カストマーインタビュー（某大手航空会社）

ESG ラボは、世界中に 500 以上の拠点を持ち、年間売上数百億ドルを誇る米国大手航空会社のコーポレイトインフラの最高責任者兼アーキテクトの某氏を単独インタビューしました。同社は、米国および欧州連合（EU）のプライバシー保護法、サーベンス・オクスリー法（企業改革法）、PCI-DSS、医療保険における HIPAA 法など、135 カ国のコンプライアンスを遵守しています。

同社は、Tempered Network ソリューション環境を 1 日で構築しました。彼らは DNS 未使用でミッションクリティカルなアプリケーションを数多く使っており、これらアプリケーションは単一の宛先 IP アドレスで書かれていました。その結果、これらアプリケーションのトラブルによってマルチロケーションユーザに深刻な可用性の問題で波及的影響を起こしています。具体的に、アクセス先のアプリケーションサーバで何かトラブルが起き、オフラインになった場合、IT 管理者がデータセンターで同一の IP アドレスと同一のセキュリティ認証による新しいサーバを立ち上げるまではすべてのアクセスリソースとの通信は不能になります。彼らは数か所にバックアップのデータセンターを利用していますが、もしメインのデータセンターのリソース全体がトラブルでオフラインになってしまった場合、同じメインのアプリケーションサーバと同じ IP アドレスを設定した新しいサーバを別サイトのバックアップデータセンター内に準備する必要があるだけでなく、グローバルで展開している MPLS ネットワークのルーティング設定の変更も必要となり、場合によっては 1 時間以上のダウン状態が続く可能性がありました。迅速な可用性要件を満たせないばかりか、アプリケーションサーバのソフトウェアをアップグレードすることも非常に困難な状態でした。Tempered Networks ソリューションの導入によって、これらの問題課題を解決しました。同社コーポレイトインフラ担当の某氏は、“Tempered Networks 製品は、ネットワークチームが Tempered Networks の製品を使用することでインフラ環境を変更する必要なくビジネスニーズに応じてアプリケーションが稼働している場所を容易に動かすことが出来、別の物理サーバにトラフィックフローを移行できるので、アプリケーションのアップグレード、および可用性に対処できます”とコメントしています。重要なアプリケーションサーバには、サーバ認証用の保護機能が組み込まれていますが、クライアント認証用の保護機能は含まれていないため、スプーフィングに対して脆弱となっていました。

ネットワークとアクセス制御にデバイス暗号の ID を使用する Tempered Networks ソリューションでは、IDN ファブリック内で必要な場所にその HIP サービス製品を配置することによって既存のクライアントセキュリティが不要になりました。

同社プロジェクトチームは、物理 HIP スイッチ、仮想 HIP スイッチおよびアプリケーション用の HIP サーバソフトとクライアント用の HIP クライアントを組み合わせて、100 以上のグローバル拠点の空港と 3 つのデータセンターで展開する予定です。これによって世界中で運行中のエアバス機内設置の HIP スイッチを介して空港の地上ネットワークとセキュアな通信をしたり、運行フライト情報を安全に 3 つのグローバルなデータセンターで中断なく情報管理できるようになります。
さらに、セルラーから Wi-Fi ネットワークへの移動が可能で、アプリケーション接続を切断することなくアクセス制御を行える Tempered Networks の HIP クライアントを 60,000 以上の従業員モバイル端末に使用する予定です。

＜ここでの重要なポイント＞

大規模なグローバル企業にとって、機敏性（アジリティ）は不可欠であり、ダウンタイムは高額な損害になる可能性があります。同社組織にとって、Tempered Networks ソリューションは、ネットワークトポロジを変更することなく、ネットワークの根本的な課題を解決しています。セキュリティを強化するだけでなく、ビジネスの混乱を最小限に抑え、アプリケーションのモビリティを強化し、アプリケーションの可用性を向上させ、運用管理を大幅に削減します。特に重要なサーバシステムは、システムをダウンさせることなく、リアルタイムのニーズに応じて他環境に迅速にバックアップルーティングすることが必要です。
Tempered Networks ソリューションは組織が必要とする安全なデータ環境を構築出来るよう支援しています。これは、特にビジネスニーズの変化に伴い、ネットワークの変更が困難な場合に有益となります。“Tempered Networks ソリューションが我々に与えるもう一つのすばらしいことは、ビジネス部門だけで Tempered の仕組みルールを決定できるということです。そして、素晴らしいのは、ビジネスポリシーの変更によってネットワークインフラを変更せずに行えることです”とチーフアーキテクトはコメントしています。

より大きな真実とは

企業組織は今、ビジネス市場で競争するために、グローバルな展開に向けて柔軟でダイナミックな接続性を求めています。殆どのデータセンターは、オンプレミスとクラウドベースのサービスやモバイルデバイスを混在させてハイブリッドクラウドを利用する傾向にあり、IP カメラやマシンセンサー等の IoT デバイスとの接続も多くで行っていますす。残念

ながら、クラウドと IoT の接続は、特に水道、電力などの重要な社会インフラでは制御システムがオンラインになるため、リスクが増大します。サイバー犯罪者が金融上の利益を得るために個人情報にアクセスするだけなく、国家レベルの脅威にも脅かされるといったリスクもあります。
企業組織では今、ネットワークとセキュリティの複雑な構成で使用しています。これによって単純な人為的な設定ミスや IP アドレスの変更によってセキュリティパラダイムを崩壊し、脆弱な環境を増大させます。そしてこれらの課題対策に多額の管理コストを必要としています。企業組織は、競合に勝ち抜くために柔軟で機敏な環境を構築するために懸命に対応していますが、セキュリティが担保されなければ、何の対策にもなりません。
Tempered Networks の IDN は、ネットワークアーキテクチャを従来の IP アドレスに基づいた接続性とポリシー設定から暗号化 ID に基づくセキュアなアーキテクチャに変更します。

ESG ラボは、Tempered Networks の IDN を用いて、数ステップのクリック操作でセグメント化してデバイスを隠したり、第三者のアクセスからこれらセグメント化されたデバイスをネットワーク分割できることを検証しました。どの IP リソースも、ネットワーク、サブネット、クラウド間を容易に移動でき、セキュアなリモート接続、DR /フェールオーバー、セキュアなデバイス間通信を実現できました。インストールと設定は非常にシンプルで素早く操作。Conductor は、スケーラブルなオーケストレーションの役割を提供できることも確認しました。

ESG ラボは、Tempered Networks の IDN ソリューションに非常に感銘を受けました。ロードマップには、それを改善する機能がいくつかあります。特に、Windows デバイスだけでなく、Linux と iOS のエンドポイントの追加は良いビジネス拡大につながるでしょう。IDN は、ネットワーキングをより簡単にし、コストを削減しながらセキュリティを向上させたいユーザには大きな価値があります。